ASSURITY CERTIFICATION AUTHORITY CERTIFICATE POLICY

Contents

History Log

Version	Date	Description
1.0	14 APR 2020	First release
2.0	15 JUL 2021	Version 2.0 release Editorial changes made generally, including the following substantive edits in the following sections: (a) Including the meaning of 'Not applicable' and clarifying the sections where the topics do not apply to CAs; and (b) Updated Section 1.6 definition of 'Applicant'.
2.1	27 OCT 2022	Version 2.1 release Editorial changes made generally to include subsections required by RFC 3647 on PKI Certificate Policy and Certificate Practices Framework i.e.: (a) 3.2.1 – 3.2.6 (b) 3.3.1 and 3.3.2 (c) 4.1.1 and 4.1.2 (d) 4.2.1 – 4.2.3 (e) 4.3.1 and 4.3.2 (f) 4.4.1 – 4.4.3 (g) 4.6.1 – 4.6.6 (h) 4.7.1 – 4.7.7 (i) 4.8.1 – 4.8.7 (j) 4.9.1 – 4.9.16 (k) 4.10.1 – 4.10.3 (l) 4.12.1 and 4.12.2 (m) 9.1.1 – 9.1.5 (n) 9.2.1 – 9.2.3 (o) 9.3.1 – 9.3.3 (p) 9.4.1 – 9.4.7 (q) 9.6.1 – 9.6.5 (r) 9.10.1 – 9.10.3 (s) 9.12.1 – 9.12.3 (t) 9.16.1 - 9.16.5 (u) 9.17

1. INTRODUCTION

1.1 Overview

This Certificate Policy ("**CP**") defines the procedural and operational requirements that CAs need to adhere to when issuing and managing Certificates. Pursuant to the IETF's Certificate Policy and Certification Practices Framework, RFC 3647, this CP is divided into nine parts that cover the security controls and practices and procedures for issuing and managing Certificates.

While this CP is structured in accordance with the RFC 3647, the sections state "Not applicable" where the topic does not apply to CAs.

This CP forms the basis on which future CPs may be issued by the CA. This CP may be amended or further CPs may be issued by the CA to indicate a Certificate's applicability to a particular community or class of applications with common security requirements.

1.2 Document Name and Identification

This document is the Certification Authority CP, version 2.1, effective date: 27 October 2022.

1.3 PKI Participants

1.3.1 Certification Authorities

A CA's Public Key Infrastructure ("**PKI**") operations includes receiving Certificate Requests, issuing, suspending, reinstating, revoking and renewing Certificates; and, maintaining, issuing, and publishing CRLs and OCSP responses. CA typically comprises of the Root CA and Issuer CA. A CA should form a policy authority to have oversight on the adherence and compliance to the requirements of this CP.

1.3.2 Registration Authorities

Refer to the definition of Registration Authority in Section 1.6.

1.3.3 Subscribers

Refer to the definition of Subscriber in Section 1.6.

1.3.4 Relying Parties

Refer to the definition of Relying Party in Section 1.6.

1.3.5 Other Participants

Not applicable.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The "key usage" and "extended key usage" fields in a Certificate define the purpose of the Certificate. Each Relying Party must evaluate the application and associated risks before deciding on whether to use or rely on a Certificate issued under this CP in accordance to the sensitivity and requirements of their information.

1.4.2 Prohibited Certificate Uses

CA shall state the use cases for which the usage of Certificates issued by the CA is disallowed.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The CA's PKIPA maintains this CP.

1.5.2 Point of Contact

Assurity Trusted Solutions Pte Ltd,
mTower,
460 Alexandra Road, #28-04,
Singapore 119963.
Attention: NCA Operations

Requests can also be made via email to nca.ops@assurity.sg

1.5.3 Person Determining CPS Suitability for the Certificate Policy

The CA's PKIPA shall approve the CPS of the CA as having met the requirements of this CP.

1.5.4 CP Approval Procedures

The CA's PKIPA shall review and approve amendments to the CP.

1.6 Definitions and Acronyms

Activation Data: Data values, other than keys or smartcard, that are required to access cryptographic modules (for example, a PIN, a passphrase, or a manually-held key smartcard).

Applicant: A Person that applies for a Certificate but has not been issued with that Certificate.

Authentication (or its derivatives or variants such as "Authenticate", "Authenticated"): The process of establishing an identity based on a trusted credential.

Certificate: A digitally-signed record that binds a Public Key and an identity in the format specified by ITU-T Recommendation X.509.

Certification Authority (CA): An entity/organization that is trusted by one or more users and is responsible for the creation, issuance, revocation, and management of Certificates.

Certification Practice Statement or CPS: A statement of the practices that the CA employs in the management of Certificates life cycle.

Certificate Signing Request or CSR: A message conforming to PKCS #10 specification, in which an Applicant submits a request to a Certification Authority, via the RA, in order to apply for a Certificate.

Certificate Revocation List or CRL: A list of Certificates that have been revoked by the CA before their expiration date and shall no longer be trusted.

Certificate Request: A request from an Applicant requesting that the Issuer CA issue a Certificate to the Applicant, which request is validly authorised by the Applicant.

FIPS: United States NIST Federal Information Processing Standards for use in computer systems.

Intermediate (or Issuer) CA: A CA that exists in the middle of a trust chain between the Root CA and the Subscriber Certificates.

Key Pair: A Private Key and its associated Public Key.

OCSP: Online Certificate Status Protocol to report the real-time revocation status of Certificates.

Object Identifier: A unique alphanumeric or numeric identifier registered with an internationally recognized standards organization for a specific object or object class.

Person: A natural person or body incorporate or unincorporated (including a partnership, society) and its successors and assigns.

PKIPA: The CA's PKI Policy Authority which oversees the CA's operations, comprising of senior management of the CA.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and it is used to create digital signatures and/or to decrypt data that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that is made public to verify a digital signature or to encrypt messages. The Public Key is usually provided via a Certificate.

Registration Authority (RA): An entity that is responsible for the enrollment function such as validating the identity of Applicants, the approval or rejection of Certificate applications, initiating Certificate revocations or suspensions under certain circumstances, processing Subscriber requests to revoke or suspend their Certificates, and approving or rejecting requests by Subscribers to renew or re-key their Certificates.

Relying Party: A Person that acts in reliance on a Certificate issued by the CA.

Relying Party Agreement: The agreement or terms of services between each Relying Party and the CA (if any) with respect to any services related to the Certificate's use, including the use of the CA's repository.

Root CA: In a hierarchical PKI, the CA whose Public Key serves as the most trusted datum (i.e. the beginning of a trust path) for a security domain.

Subscriber: A Person that has been issued a Certificate, and is authorised to use, the Private Key that corresponds to the Public Key listed in the Certificate.

Subscriber Agreement: The agreement or terms of services between each Subscriber and the CA for the Certificate issued.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

CA shall publish all publicly trusted Root CA and Issuer CA Certificates, CRL, CP, CPS, Relying Party Agreements and Subscriber Agreements in online repositories.

2.2 Publication of Certification Information

CA shall not publish the Subscribers' Certificates publicly on its repository. Only the CA's Root and Issuer CA Certificates are publicly available on the repository.

2.3 Time or Frequency of Publication

Root CA and Issuer CA Certificates are published in the repository as soon as possible after issuance. CRLs for Subscriber Certificates are issued at least once every hour and are valid for 7 days. New CRLs for Subscriber Certificates may be published prior to the expiration of the current CRL and would supersede such current CRL. CRLs for Issuer CA Certificates are issued at least once every 12 months (under normal operations i.e. upon expiry of the current CRL for Issuer CA Certificates) or 24 hours (if Issuer CA's Certificate is revoked).

New or updated versions of this CPS, CP, Subscriber Agreement(s) or Relying Party Agreement(s) are published after the CA's policy authority's approval. At least one copy of the previous version will remain available online after publication of the latest version. Archived copies of all CPSs under which the CA has ever issued a Certificate are kept in accordance with the CA's retention policy.

2.4 Access Controls on Repository

Artefacts in the CA's repository shall be publicly available.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

Issuer CA shall issue Subscriber Certificates with a non-null subject Distinguished Name ("**DN**"). All Certificates' subject DN shall consist of Common Name ("**CN**"), Organisation, Organisation Unit and Country. Detailed attributes of the Subscriber Certificates are in the Certificate profile.

3.1.2 Need for Names to Be Meaningful

Issuer CA shall use DNs that identify both the subject and issuer of the Certificate. CN of the subject DN shall consist of sufficient information to identify the Subscribers e.g. name and national identification number.

3.1.3 Anonymity or Pseudonymity of Subscribers

Issuer CA shall not issue Certificates for Internationalised Domain Names or Punycode version; and, anonymous or pseudonymous Certificates. Internationalised Domain Names are web addresses written in languages that contain characters not supported by the English alphabet.

3.1.4 Rules for Interpreting Various Name Forms

DNs in Certificates shall adhere to X.500 naming standards.

3.1.5 Uniqueness of Names

Issuer CA shall enforce uniqueness of each subject name in a Subscriber Certificate in the CN attribute of the subject DN.

3.1.6 Recognition, Authentication, and Role of Trademarks

Subscribers may not request Certificates with any content that infringes the intellectual property rights of another entity. This CP does not require that an Applicant's right to use a trademark be verified. However, Issuer CA may reject any applications or require revocation of any Certificate that is part of a dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Issuer CA shall define the method to prove possession of the private key.

3.2.2 Authentication of Organization Identity

Issuer CA shall define methods used to verify the identity of an Applicant and the Applicant's organization prior to issuing organization Certificates.

3.2.3 Authentication of Individual Identity

Issuer CA shall define methods used to verify the identity of an Applicant prior to issuing Certificates.

3.2.4 Non-Verified Subscriber Information

Not applicable.

3.2.5 Validation of Authority

Issuer CA shall define the authority that verifies an Applicant's specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a certificate.

3.2.6 Criteria for Interoperation

Issuer CA shall define the criteria for interoperability such as cross-certification or unilateral certification.

3.3 Identification and Authentication for Re-Key Requests

Re-keying a Certificate consists of creating a new Certificate with a different Public Key (and serial number) while retaining the remaining contents of the old Certificate that describe the subject. Issuer CA does not support re-key requests i.e., to replace an old Certificate (e.g., upon expiry) - issuance of a new Certificate is required instead.

3.3.1 Identification and Authentication for Routine Re-key

Not applicable.

3.3.2 Identification and Authentication for Re-key after Revocation

Not applicable.

3.4 Identification and Authentication for Revocation Request

Refer to Section 4.9 on Certificate revocation.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

At present, only the Applicant can request for a Certificate.

4.1.2 Enrollment Process and Responsibilities

Applicants shall submit sufficient information to allow the Issuer CA or RA to successfully perform the required verification. Issuer CA shall protect communications and securely store information presented by the Applicant.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Issuer CA or RA shall perform identification and authentication functions.

4.2.2 Approval or Rejection of Certificate Applications

Issuer CA or RA shall reject any Certificate application that cannot be verified and may also reject a Certificate application if the Issuer CA believes that issuing the Certificate could damage the CA's reputation or business.

4.2.3 Time to Process Certificate Applications

Certificate applications processing time greatly depends on the processing complexity and network latency between the Applicant, the RA and the Issuer CA. As such, the Issuer CA only makes reasonable efforts to process Certificate applications immediately upon the receipt of the Certificate applications.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

The Issuer CA or RA shall verify the format and information of the CSR from the Applicant. Upon successfully validating the CSR, the Issuer CA issues the Certificate and returns the Certificate to Subscriber. If a RA is involved, the RA shall deliver the Certificate to the Subscriber.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Upon successful receipt of the Certificate, the Subscriber shall be notified of the completion of the Certificate issuance process.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Issuer CA shall define the methods that constitute Certificate Acceptance by the Applicant.

4.4.2 Publication of the Certificate by the CA

The Issuer CA shall not publish the Subscribers' Certificates publicly on the Repository. Only the CA's Root CA Certificate and Issuer CA Certificate are published publicly on its Repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Issuer CA may notify any other entities about Certificates that it issues.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate usage

Subscribers are obligated to protect their Private Keys from unauthorised use or disclosure. Where a Certificate is expired or revoked, Subscribers must not use such Certificates. Certificates shall only be used in accordance to their intended purpose as specified in the key usage extension in the Certificates.

4.5.2 Relying Party Usage of Subscriber's Public Key and Certificate

A Relying Party shall use its discretion when relying on a Certificate and shall consider the totality of the circumstances and risk of loss prior to relying on a Certificate. Such circumstances may include business impact or risk of loss. The Relying Party shall make a risk assessment before deciding to use the Certificate.

4.6 Certificate Renewal

There shall be no extension of the Subscriber's Certificate. Each renewal request shall be considered as a new Certificate Request.

4.6.1 Circumstances for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.7 Certificate Re-Key

Issuer CA does not provide Certificate re-key services or accommodate Certificate re-key requests. Revocation of the current Certificate and issuance of a new Certificate, with a new Key Pair, are required.

4.7.1 Circumstance for Certificate Rekey

Not applicable.

4.7.2 Who May Request Certification of a New Public Key

Not applicable.

4.7.3 Processing Certificate Re-Keying Requests

Not applicable.

4.7.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Not applicable.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Not applicable.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.8 Certificate Modification

Issuer CA does not provide Certificate modification services. Revocation of the current Certificate and issuance of a new Certificate, with modified Certificate attributes, are required.

4.8.1 Circumstances for Certificate Modification

Not applicable.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Certificate revocation is a process whereby the lifecycle of a Certificate has ended prematurely. The serial number of a Certificate is blacklisted by adding the serial number to a CRL. The Issuer CA will publish the updated CRL online to its public repository as specified in the Certificate's CRL Distribution Points. The Issuer CA may remove the serial numbers from the CRL when revoked Certificates expire to promote efficient CRL file size management.

The Issuer CA will also publish the revocation status via the OCSP service as specified in the Certificate's Authority Information Access field.

The Subscriber may request for the revocation of Certificates through the Issuer CA or RA.

The Issuer CA may revoke any Certificate in its sole discretion if it has knowledge or has reasonable suspicion (where applicable) that any of the following, non-exhaustive, circumstances has occurred:

(a) the Root or Issuer CA's Private Keys or system is compromised in a manner materially affecting the Certificate's reliability;

(b) the Subscriber's Private Key is Compromised in a manner materially affecting the Subscriber's Certificate's reliability or it is changed, lost, stolen or made public;

(c) the Subscriber did not request for the initial Certificate Request;

(d) there is a breach of a material obligation under the CPS or the relevant Subscriber Agreement by the Subscriber;

(e) the Subscriber is deceased;

(f) the Subscriber's, RA's or the Issuer CA's obligations under the CPS are delayed or prevented by circumstances beyond that party's reasonable control, including computer or communication failure, or in situations where information is compromised materially;

(g) the Certificate is not issued in accordance with the CPS or applicable industry standards;

(h) when the Issuer CA or RA becomes aware of a change in the information contained in the Certificate;

(i) to meet or comply with any order or request of any court, government body, regulatory authority or law enforcement agency to revoke the Certificate;

(j) where revocation of the Certificate is required for compliance with any applicable laws or regulations;

(k) the Issuer CA operations are envisaged to cease for any reason and there has been no arrangement for another CA to provide revocation support for the Certificates;

(l) any information in the Certificate is inaccurate or misleading;

(m) the continued use of the Certificate is harmful and undermines the Issuer CA's trust infrastructure; and

(n) the Certificate can no longer reliably validate that a private key can be assigned to a specific Subscriber.

The Issuer CA is under no obligation to disclose the reason for revocation of any Certificate.

4.9.2 Who Can Request Revocation

The Subscriber may request for revocation of Certificates. Revocation can also be initiated at the discretion of the Issuer CA.

4.9.3 Procedure for Revocation Request

Issuer CA shall define the methods for receiving requests for Certificate revocation.

4.9.4 Revocation Request Grace Period

Issuer CA may define a grace period for Certificate revocation requests.

4.9.5 Time within Which CA Must Process the Revocation Request

The Issuer CA shall revoke the Certificates upon receipt of an Authenticated revocation request from the Subscriber in accordance with the process stated in Section 4.9.3.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties shall ensure that the Certificate remains valid and has not been revoked or suspended by accessing the Certificate status services defined in Section 4.10.

4.9.7 CRL Issuance Frequency

Refer to Section 2.3 Time or Frequency of Publication.

4.9.8 Maximum Latency for CRLs

CRLs are posted automatically to the online repository as specified in the Certificate's CRL Distribution Points or Authority Information Access field within a reasonable time after generation, usually within minutes of generation, subject to the processing times and network latency of the CA's systems.

4.9.9 On-Line Revocation/Status Checking Availability

Refer to Section 4.10.2 on the availability of Certificate status services.

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.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Regarding Key Compromise

The CA will use commercially reasonable methods to notify Subscribers if their Private Key may have been or is suspected to be Compromised. This includes cases where new vulnerabilities have been reported or cryptographic algorithm is deemed not secure.

If the CA's Private Key is or is suspected to be Compromised, the CA shall take commercially reasonable steps to remedy the breach, which may include suspension or revocation of existing Certificates, generation of replacement Certificates, and notification of Subscribers and Relying Parties.

4.9.13 Circumstances for Suspension

Certificate suspension may be used when the Issuer CA wants to disable a Subscriber's Certificate. Unlike Certificate revocation which disables a Certificate permanently, Certificate suspension can be lifted by the Issuer CA to reactivate the Certificate.

4.9.14 Who Can Request Suspension

Issuer CA shall define who can submit a request for Certificate suspension.

4.9.15 Procedure for Suspension Request

Issuer CA shall define the methods to receive Certificate suspension request.

4.9.16 Limits on Suspension Period

Issuer CA shall define the duration of the Certificate suspension period and circumstances that will reactivate a suspended Certificate.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Issuer CA shall provide Certificate status services using OCSP and CRL.

4.10.2 Service Availability

Issuer CA shall define the availability of the Certificate status services.

4.10.3 Optional Features

Issuer CA may define optional Certificate status features.

4.11 End of Subscription

A Subscriber's subscription to the CA's services ends when the Subscriber Agreement is terminated in accordance with its termination terms.

4.12 Key Escrow and Recovery

CA does not escrow the CA's Private Keys nor provide services to escrow Subscribers' Private Keys. The Subscriber's Private Key shall always be kept in the Subscriber's custody and private key escrow is prohibited.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

5.1 Physical Security Controls

CA shall define the physical security controls of the facility that hosts the CA systems, including the following:

5.1.1 Site Location and Construction

CA shall conduct its operations from a secure data center equipped with logical and physical controls that makes the CA's equipment and records inaccessible to non-trusted personnel.

5.1.2 Physical Access

CA shall implement physical access protection mechanisms such as guards, access logs, door/rack/cage locks and intrusion sensors, and shall provide robust protection against unauthorised access to CA equipment and records.

5.1.3 Power and Air Conditioning

Hosting facility shall be equipped with backup power supply system and sufficient environmental controls to protect the CA systems.

5.1.4 Water Exposures

Hosting facility shall be equipped with protection mechanisms against water exposure.

5.1.5 Fire Prevention and Protection

Hosting facility shall be equipped with fire detection, alarm and suppression mechanisms.

5.1.6 Media Storage

CA shall backup and store its system and records in a backup location that is separate from its primary operations facility, protected from fire and water damage.

5.1.7 Waste Disposal

CA shall ensure that obsolete data on media are securely erased before disposal.

5.1.8 Off-site Backup

CA shall take periodic system backups sufficient to recover from system failure and shall store the backups at an off-site location.

5.2 Procedural Controls

5.2.1 Trusted Roles

CA shall segregate the functions and duties performed by persons in trusted roles such that no one person can circumvent the security of the CA systems. CA shall list and define these trusted roles.

5.2.2 Number of Persons Required Per Task

Trusted roles consist of vetted and approved employees, contractors, or consultants that require access to or control over the CA's operations. Trusted role positions are subject to a clearly defined set of

responsibilities that maintain strict “separation of duties”; for example, no single person is able to perform either a validation or a fulfillment task without a secondary review by another “trusted” team member. The personnel considered for trusted role positions must successfully pass the screening and training requirements of Section 5.3.3. Trusted role positions may include, but are not limited to, system administrators, operators, engineers, and certain executives who are designated to oversee CA operations. CA shall specify the number of persons (e.g. n out of m rule), acting in a trusted role, to perform tasks such as accessing CA’s Private Keys, generating a CA Key Pair, or creating a backup of a CA Private Key.

5.2.3 Identification and Authentication for Each Role

CA shall specify the identification and Authentication requirements for each trusted role.

5.2.4 Roles Requiring Separation of Duties

CA shall ensure that individual personnel does not assume multiple trusted roles to achieve separation of duties.

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

CA shall ensure that personnel have the experience and expertise with their assigned trusted roles.

5.3.2 Background Check Procedures

CA’s hiring procedures shall include background checks to ensure that candidate employees are suitable for the trusted roles.

5.3.3 Training Requirements

CA shall provide adequate training to the CA’s personnel to upkeep their skillset needed to perform their assigned trusted roles.

5.3.4 Retraining Frequency and Requirements

Refer to 5.3.3.

5.3.5 Job Rotation Frequency and Sequence

Not applicable.

5.3.6 Sanctions for Unauthorized Actions

CA shall impose strict administrative or disciplinary actions on personnel found to have carried out actions not authorised under this CP, or the CPS or other required procedures.

5.3.7 Independent Contractor Requirements

CA shall impose strict governance (e.g. security policies and clearance) on the contractors hired to develop or maintain the CA systems.

5.3.8 Documentation Supplied to Personnel

CA shall provide its personnel with adequate materials and knowledge base to perform their assigned trusted roles.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

CA shall list the types of audit events recorded e.g. Certificate lifecycle management and security events.

5.4.2 Frequency of Log Processing

CA shall define the frequency with which the logs are processed.

5.4.3 Retention Period for Audit Log

CA shall define the offline and online retention period for audit logs.

5.4.4 Protection of Audit Log

CA shall implement protection mechanism such as access control i.e. who can access the audit logs and data integrity checks against unauthorised modification and deletion.

5.4.5 Audit Log Backup Procedures

CA shall backup audit logs on a daily basis.

5.4.6 Audit Collection System

CA shall specify whether an internal and/or external system is used for log collection.

5.4.7 Notification of Event-Causing Subject

Not applicable.

5.4.8 Vulnerability Assessments

CA shall conduct regular vulnerability assessment to review the audit logs to identify potential attempts to breach the security of the system and security weaknesses in the system.

5.5 Records Archival

5.5.1 Types of Records Archived

The CA shall maintain archived backups of application and system data. Archived information may include, but are not limited to, the following:

(a) Audit data, as specified in Section 5.4
(b) Data related to Certificate Requests, verifications, issuances, and revocations;
(c) CA policies, procedures, entity agreements, compliance records;
(d) Cryptographic device and key life cycle information; and
(e) Systems management and change control activities.

5.5.2 Retention Period for Archive

CA shall define the time period under which the archived records are kept.

5.5.3 Protection of Archive

CA shall define the security controls to protect archived records against unauthorised access, modifications and deletion.

5.5.4 Archive Backup Procedures

CA shall define its data backup procedures.

5.5.5 Requirements for Time-stamping of Records

Refer to Section 6.8.

5.5.6 Archive Collection System

CA shall specify whether an internal and/or external system is/are used for records archival.

5.5.7 Procedures to Obtain and Verify Archive Information

CA shall define the procedures used to retrieve archived records and may include procedures to verify the accuracy of archived information.

5.6 Key Changeover

CA shall define the procedures to transit from expiring CA Certificates to new CA Certificates.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

CA shall have formal incident response, disaster recovery, and business continuity plans that contain documented procedures to notify participants that include RA, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. Business continuity and security management plans do not have to be publicly disclosed, but the CA shall make them available to auditors upon request and annually test, review, and update the procedures.

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

CA shall specify the recovery procedures used, in the event that the CA system, including its servers, network devices and data, is corrupted.

5.7.3 Entity Private Key Compromise Procedures

CA shall specify the recovery procedures used, in the event that the CA's Private Keys are compromised.

5.7.4 Business Continuity Capabilities After a Disaster

CA shall have a business continuity plan to ensure business continuity following a disaster.

5.8 CA Termination

CA shall define the procedures for termination and termination notification of a CA.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA shall generate the CA's Key Pairs on a FIPS 140 level 3 validated cryptographic module, involving multiple individuals acting in trusted roles. When generating the CA's Key Pairs, the CA shall create auditable evidence to show that the CA has enforced role separation and followed its CA key generation process. An independent auditor shall witness the CA key generation ceremony.

6.1.2 Private Key Delivery to Subscriber

Subscriber's Private Key shall be generated at the Subscriber's custody. The Issuer CA does not generate or deliver Private Keys to the Subscribers or provide other Subscriber key management services.

6.1.3 Public Key Delivery to Certificate Issuer

Subscriber's Public Key shall always be delivered to the Issuer CA in a secure fashion and in a manner which binds the Subscriber's verified identity to the Public Key.

6.1.4 CA Public Key Delivery to Relying Parties

CA shall avail the CA's public Certificates, including its Root CA and Issuer CA Certificates, on a publicly accessible repository.

6.1.5 Key Sizes

CA shall use the following key size, signature algorithm and hash algorithm for signing the respective Certificates:

(a) Root CA: 521-bit ECDSA key with Secure Hash Algorithm 2 (SHA-384)
(b) Issuer CA: 384-bit ECDSA key with Secure Hash Algorithm 2 (SHA-384)
(c) Subscriber: 256-bit ECDSA key with Secure Hash Algorithm 2 (SHA-256)

6.1.6 Public Key Parameters Generation and Quality Checking

CA shall generate the CA's Public Key parameters using secure random number generators built into the cryptographic modules that are FIPS validated.

6.1.7 Key Usage Purposes

Issuer CA shall specify the intended purposes of the Subscriber's Certificates issued by the Issuer CA in the key usage extension fields and technically limit their functionality in X.509 compliant software.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Refer to Section 6.1.1.

6.2.2 Private Key (N Out of M) Multi-Person Control

CA shall ensure that multiple trusted personnel are required to act in order to access and use the CA's Private Keys, including any CA Private Key backups.

6.2.3 Private Key Escrow

Refer to Section 4.12.

6.2.4 Private Key Backup

CA shall backup all CA Private Keys on FIPS 140 level 3 validated cryptographic modules.

6.2.5 Private Key Archival

The CA does not archive its CA Private Keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

CA shall only allow transfer of CA Private Keys for backup purpose only.

6.2.7 Private Key Storage on Cryptographic Module

CA shall store all CA Private Keys on a FIPS 140 level 3 validated cryptographic module.

6.2.8 Method of Activating Private Key

CA shall develop key ceremony scripts to activate its Private Keys.

6.2.9 Method of Deactivating Private Key

CA shall develop methods to deactivate its Private Keys.

6.2.10 Method of Destroying Private Key

CA shall develop methods to destroy its Private Keys.

6.2.11 Cryptographic Module Rating

Refer to Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

CA shall archive its Public Keys.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Issuer CA shall state the validity periods of Certificates issued to Subscribers.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

CA shall specify procedures to generate Activation Data.

6.4.2 Activation Data Protection

CA shall define procedures to protect Activation Data against unauthorised use.

6.4.3 Other Aspects of Activation Data

Not applicable.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

CA shall implement security controls that:

(a) Authenticate the identity of users, using multi-factor authentication, before permitting access to the system or applications;
(b) enforce minimum password length and complexity;
(c) manage the privileges of users and limit users to their assigned roles;
(d) protect all communication channels;
(e) log all security events;
(f) harden the system configuration based on industry standard;
(g) periodically scan for vulnerabilities; and
(h) periodically assess the security posture of the CA's system through security review and penetration testing.

6.5.2 Computer Security Rating

Not applicable.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

CA shall ensure that the CA's systems and applications are secure by design.

6.6.2 Security Management Controls

CA shall implement tools and procedures to ensure that the CA system adheres to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.

6.6.3 Life Cycle Security Controls

Not applicable.

6.7 Network Security Controls

CA shall implement appropriate network security controls, including turning off any unused network ports and services, only using network software that is necessary for the proper functioning of the CA systems and using network perimeter devices to ensure only authorised traffic to the CA systems.

6.8 Time-Stamping

CA shall ensure that the accuracy of clocks used for time-stamping of data, logs and archived records.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

Issuer CA shall list all attributes of the Subscriber Certificates issued by the Issuer CA.

7.1.1 Version Number(s)

Issuer CA shall issue X.509 version 3 Subscriber Certificates.

7.1.2 Certificate Extensions

Issuer CA shall list all extensions of the Subscriber Certificates issued by the CA.

7.1.3 Algorithm Object Identifiers

Issuer CA shall list all algorithms used to sign the Subscriber Certificates issued by the Issuer CA.

7.1.4 Name Forms

Issuer CA shall use Distinguished Names (DN) that are composed of standard attribute types, such as those identified in RFC 5280. Issuer CA shall include a unique serial number in each Certificate. The content of the Subscriber's Certificate Issuer DN must match the Subject DN of the Issuer CA to support name chaining. The Common Name (CN) attribute must be present and the contents should be an identifier for the Subscriber's Certificate such that the Subscriber's Certificate name is unique across all Subscriber Certificates issued by the CA.

7.1.5 Name Constraints

Not applicable.

7.1.6 Certificate Policy Object Identifier

The Issuer CA asserts that the Certificate, identified by its Object Identifier, is managed in accordance with the policies that are identified herein.

7.1.7 Usage of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

The Issuer CA shall list the Certification Practice Statement that applies to the Subscriber Certificates issued by the Issuer CA in the Certificate Policies extension.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

7.2 CRL Profile

Issuer CA shall list all attributes of the CRL published by the Issuer CA.

7.2.1 Version Number(s)

Issuer CA shall publish CRLs that conform to RFC 5280.

7.2.2 CRL and CRL Entry Extensions

Issuer CA shall list all extensions of the CRL published by the Issuer CA.

7.3 OCSP Profile

7.3.1 Version Number(s)

OCSP responders shall conform to RFC 5019 and RFC 6960.

7.3.2 OCSP Extensions

Not applicable.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Types of Assessment

CA shall list the types of compliance audit or assessments that the CA conducts.

8.2 Frequency or Circumstances of Assessment

CA shall define the frequency of the compliance audit and/or assessment.

8.3 Identity/Qualifications of Assessor

CA shall ensure that the auditors engaged have the necessary skillset to conduct the compliance audit and/or assessment.

8.4 Assessor’s Relationship to Assessed Entity

CA shall ensure that there is no conflict of interests with the auditor engaged for the compliance audit and assessment.

8.5 Topics Covered by Assessment

The assessment must conform to industry standards that cover the CA's practices and evaluate the integrity of its PKI operations.

8.6 Actions Taken as a Result of Deficiency

CA shall define procedures to remediate any deficiencies found during the compliance audit and assessment.

8.7 Communication of Results

CA shall define the authorised third-party entities entitled to see the results of the compliance audit and assessment.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

CA may impose fees for its services.

9.1.1 Certificate Issuance and Renewal Fees

If fees are imposed, CA shall specify provisions for Certificate issuance and renewal fees charged.

9.1.2 Certificate Access Fees

If fees are imposed, CA shall specify provisions for Certificate access fees charged.

9.1.3 Revocation or Status Information Access Fees

If fees are imposed, CA shall specify provisions for Certificate revocation or status information access fees charged.

9.1.4 Fees for Other Services

If fees are imposed, CA shall specify provisions for fees charged for other services such as providing access to CP, CPS and relevant agreements.

9.1.5 Refund Policy

If fees are imposed, CA shall specify its refund policy.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

CA shall define insurance coverage to support its CA services, remain solvent and protect against liabilities arising from its CA services.

9.2.2 Other Assets

CA shall define the minimum level of assets necessary to operate its CA services, remain solvent and protect against liabilities arising from its CA services.

9.2.3 Insurance or Warranty Coverage for End-Entities

CA shall define warranty coverage to support its CA services, remain solvent and protect against liabilities arising from its CA services.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

CA shall define the scope or definition of confidential information.

9.3.2 Information Not Within Scope of Confidential Information

CA shall define information that is not within the scope of confidential information.

9.3.3 Responsibility to Protect Confidentiality Information

CA shall define responsibilities of personnel handling confidential information to protect it from compromise and unauthorised disclosure.

9.4 Privacy of Personal Information

CA shall define the method and procedures to protect Personally Identifiable Information ("**PII**") it might collect in offering its CA services.

9.4.1 Privacy Plan

CA shall develop an applicable privacy plan that applies to the CA's participants.

9.4.2 Information Treated as Private

CA shall define what is PII.

9.4.3 Information Not Deemed Private

CA shall define what is not PII.

9.4.4 Responsibility to Protect Private Information

CA shall define responsibilities of personnel handling PII to protect it from compromise and unauthorized disclosure.

9.4.5 Notice and Consent to Use Private Information

CA shall obtain consent for collection of PII.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

CA shall define methods and procedures for disclosure of PII pursuant to judicial, administrative process in a private or governmental proceeding, or in any legal proceeding.

9.4.7 Other Information Disclosure Circumstances

CA shall define other information disclosure circumstances (if any).

9.5 Intellectual Property Rights

CA shall declare its ownership of intellectual property rights for artefacts generated from the CA services.

9.6 Representations and Warranties

9.6.1 CA Representation and Warranties

CA shall state the representations and warranties for Subscribers and Relying Parties in the Subscriber Agreement and Relying Party Agreement respectively.

9.6.2 RA Representation and Warranties

CA shall set out the RA's representation and warranties when participating in the issuance and management of Certificates.

9.6.3 Subscriber Representation and Warranties

Representations and warranties required to be provided by the Subscriber are as set out in the Subscriber Agreement.

9.6.4 Relying Party Representations and Warranties

Representations and warranties required to be provided by the Relying Party are as set out in the Relying Party Agreement or CPS.

9.6.5 Representations and Warranties of Other Participants

The CPS shall state the representations and warranties for other participants (if any).

9.7 Disclaimers of Warranties

CA shall set out the terms that expressly disclaim representations and warranties for its CA services.

9.8 Limitations of Liability

CA shall set out limitations of liability terms for its CA services and a recommended reliance limit. CA may define the recommended reliance limit in the Subscriber Agreement and Relying Party Agreement.

9.9 Indemnities

CA shall set out the terms that indemnify for CA losses in the Subscriber Agreement and Relying Party Agreement.

9.10 Term and Termination

9.10.1 Term

CA shall define the time period in which a CP or a CPS remains in force.

9.10.2 Termination

CA shall define the circumstances under which the CP or CPS, portions of the CP or CPS, or its applicability can be terminated.

9.10.3 Effect of Termination and Survival

CA shall define this in the CP or CPS.

9.11 Individual Notices and Communications with Participants

CA may establish communication methods in which the CA and other PKI participants can communicate on a one-to-one basis in order for such communications to be legally effective.

9.12 Amendments

9.12.1 Procedure for Amendment

CA shall define the procedures for amending the CP and CPS.

9.12.2 Notification Mechanism and Period

The procedures for amending the CP and CPS may include a notification mechanism to provide notice of proposed amendments to affected parties.

9.12.3 Circumstances Under Which OID Must Be Changed

CA shall define the circumstances that would require a change in CP or CPS OID or pointer (URL).

9.13 Dispute Resolution Provisions

CA shall define the procedures utilised to resolve disputes arising out of the CP, CPS, or agreements.

9.14 Governing Law

This CP shall be governed by and interpreted in accordance with the laws of the Republic of Singapore.

9.15 Compliance with Applicable Law

Subscribers and Relying Parties of the CA's services shall comply with all applicable laws and regulations. Any failure may result in the CA's refusal to render its services.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

For each Subscriber and Relying Party, this shall be as set out in the Subscriber Agreement and Relying Party Agreement, respectively.

9.16.2 Assignment

For each Subscriber and Relying Party, this shall be as set out in the Subscriber Agreement and Relying Party Agreement, respectively.

9.16.3 Severability

For each Subscriber and Relying Party, this shall be as set out in the Subscriber Agreement and Relying Party Agreement, respectively.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

For each Subscriber and Relying Party, this shall be as set out in the Subscriber Agreement and Relying Party Agreement, respectively.

9.16.5 Force Majeure

For each Subscriber and Relying Party, this shall be as set out in the Subscriber Agreement and Relying Party Agreement, respectively.

9.17 Other Provisions

Not Applicable