

---

# ASSURITY CERTIFICATION AUTHORITY CERTIFICATE POLICY

---

## Contents

1. INTRODUCTION.....	8
1.1 Overview .....	8
1.2 Document Name and Identification.....	8
1.3 PKI Participants .....	8
1.3.1 Certification Authorities .....	8
1.3.2 Registration Authorities .....	8
1.3.3 Subscribers .....	8
1.3.4 Relying Parties .....	8
1.3.5 Other Participants.....	8
1.4 Certificate Usage.....	8
1.4.1 Appropriate Certificate Uses .....	8
1.4.2 Prohibited Certificate Uses.....	9
1.5 Policy Administration.....	9
1.5.1 Organization Administering the Document .....	9
1.5.2 Point of Contact.....	9
1.5.3 Person Determining CPS Suitability for the Certificate Policy .....	9
1.5.4 CP Approval Procedures.....	9
1.6 Definitions and Acronyms .....	9
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES.....	11
2.1 Repositories .....	11
2.2 Publication of Certification Information .....	11
2.3 Time or Frequency of Publication .....	11
2.4 Access Controls on Repository.....	11
3. IDENTIFICATION AND AUTHENTICATION .....	12
3.1 Naming .....	12
3.1.1 Types of Names .....	12
3.1.2 Need for Names to Be Meaningful.....	12
3.1.3 Anonymity or Pseudonymity of Subscribers .....	12
3.1.4 Rules for Interpreting Various Name Forms .....	12
3.1.5 Uniqueness of Names.....	12
3.1.6 Recognition, Authentication, and Role of Trademarks.....	12
3.2 Initial Identity Validation .....	12
3.3 Identification and Authentication for Re-Key Requests .....	12
3.4 Identification and Authentication for Revocation Request .....	12
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....	13
4.1 Certificate Application .....	13

4.2	Certificate Application Processing .....	13
4.3	Certificate Issuance.....	13
4.4	Certificate Acceptance .....	13
4.5	Key Pair and Certificate Usage .....	13
4.5.1	Subscriber Private Key and Certificate usage .....	13
4.5.2	Relying Party Usage of Subscriber's Public Key and Certificate .....	13
4.6	Certificate Renewal .....	13
4.7	Certificate Re-Key .....	14
4.8	Certificate Modification .....	14
4.9	Certificate Revocation and Suspension .....	14
4.10	Certificate Status Services .....	14
4.11	End of Subscription .....	14
4.12	Key Escrow and Recovery .....	14
5.	MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS .....	15
5.1	Physical Security Controls .....	15
5.1.1	Site Location and Construction .....	15
5.1.2	Physical Access .....	15
5.1.3	Power and Air Conditioning.....	15
5.1.4	Water Exposures .....	15
5.1.5	Fire Prevention and Protection.....	15
5.1.6	Media Storage .....	15
5.1.7	Waste Disposal .....	15
5.1.8	Off-site Backup.....	15
5.2	Procedural Controls .....	15
5.2.1	Trusted Roles .....	15
5.2.2	Number of Persons Required Per Task .....	16
5.2.3	Identification and Authentication for Each Role .....	16
5.2.4	Roles Requiring Separation of Duties .....	16
5.3	Personnel Security Controls.....	16
5.3.1	Qualifications, Experience, and Clearance Requirements .....	16
5.3.2	Background Check Procedures .....	16
5.3.3	Training Requirements .....	16
5.3.4	Retraining Frequency and Requirements .....	16
5.3.5	Job Rotation Frequency and Sequence.....	16
5.3.6	Sanctions for Unauthorized Actions .....	16
5.3.7	Independent Contractor Requirements .....	16
5.3.8	Documentation Supplied to Personnel.....	17

5.4	Audit Logging Procedures .....	17
5.4.1	Types of Events Recorded .....	17
5.4.2	Frequency of Log Processing .....	17
5.4.3	Retention Period for Audit Log .....	17
5.4.4	Protection of Audit Log .....	17
5.4.5	Audit Log Backup Procedures.....	17
5.4.6	Audit Collection System .....	17
5.4.7	Notification of Event-Causing Subject.....	17
5.4.8	Vulnerability Assessments .....	17
5.5	Records Archival .....	17
5.5.1	Types of Records Archived .....	17
5.5.2	Retention Period for Archive .....	17
5.5.3	Protection of Archive .....	18
5.5.4	Archive Backup Procedures.....	18
5.5.5	Requirements for Time-stamping of Records .....	18
5.5.6	Archive Collection System .....	18
5.5.7	Procedures to Obtain and Verify Archive Information.....	18
5.6	Key Changeover .....	18
5.7	Compromise and Disaster Recovery .....	18
5.7.1	Incident and Compromise Handling Procedures .....	18
5.7.2	Computing Resources, Software, and/or Data are Corrupted .....	18
5.7.3	Entity Private Key Compromise Procedures .....	18
5.7.4	Business Continuity Capabilities After a Disaster .....	18
5.8	CA Termination .....	18
6.	TECHNICAL SECURITY CONTROLS .....	19
6.1	Key Pair Generation and Installation .....	19
6.1.1	Key Pair Generation .....	19
6.1.2	Private Key Delivery to Subscriber.....	19
6.1.3	Public Key Delivery to Certificate Issuer .....	19
6.1.4	CA Public Key Delivery to Relying Parties .....	19
6.1.5	Key Sizes .....	19
6.1.6	Public Key Parameters Generation and Quality Checking .....	19
6.1.7	Key Usage Purposes .....	19
6.2	Private Key Protection and Cryptographic Module Engineering Controls .....	19
6.2.1	Cryptographic Module Standards and Controls .....	19
6.2.2	Private Key (N Out of M) Multi-Person Control .....	20
6.2.3	Private Key Escrow .....	20

6.2.4	Private Key Backup .....	20
6.2.5	Private Key Archival .....	20
6.2.6	Private Key Transfer Into or From a Cryptographic Module .....	20
6.2.7	Private Key Storage on Cryptographic Module .....	20
6.2.8	Method of Activating Private Key .....	20
6.2.9	Method of Deactivating Private Key .....	20
6.2.10	Method of Destroying Private Key .....	20
6.2.11	Cryptographic Module Rating .....	20
6.3	Other Aspects of Key Pair Management .....	20
6.3.1	Public Key Archival .....	20
6.3.2	Certificate Operational Periods and Key Pair Usage Periods .....	20
6.4	Activation Data .....	20
6.4.1	Activation Data Generation and Installation .....	20
6.4.2	Activation Data Protection .....	21
6.4.3	Other Aspects of Activation Data .....	21
6.5	Computer Security Controls .....	21
6.5.1	Specific Computer Security Technical Requirements .....	21
6.5.2	Computer Security Rating .....	21
6.6	Life Cycle Technical Controls .....	21
6.6.1	System Development Controls .....	21
6.6.2	Security Management Controls .....	21
6.6.3	Life Cycle Security Controls .....	21
6.7	Network Security Controls .....	21
6.8	Time-Stamping .....	22
7.	CERTIFICATE, CRL, AND OCSP PROFILES .....	23
7.1	Certificate Profile .....	23
7.1.1	Version Number(s) .....	23
7.1.2	Certificate Extensions .....	23
7.1.3	Algorithm Object Identifiers .....	23
7.1.4	Name Forms .....	23
7.1.5	Name Constraints .....	23
7.1.6	Certificate Policy Object Identifier .....	23
7.1.7	Usage of Policy Constraints Extension .....	23
7.1.8	Policy Qualifiers Syntax and Semantics .....	23
7.1.9	Processing Semantics for the Critical Certificate Policies Extension .....	23
7.2	CRL Profile .....	23
7.2.1	Version Number(s) .....	24

7.2.2	CRL and CRL Entry Extensions .....	24
7.3	OCSP Profile .....	24
7.3.1	Version Number(s) .....	24
7.3.2	OCSP Extensions.....	24
8.	COMPLIANCE AUDIT AND OTHER ASSESSMENTS .....	25
8.1	Types of Assessment.....	25
8.2	Frequency or Circumstances of Assessment .....	25
8.3	Identity/Qualifications of Assessor .....	25
8.4	Assessor's Relationship to Assessed Entity .....	25
8.5	Topics Covered by Assessment.....	25
8.6	Actions Taken as a Result of Deficiency.....	25
8.7	Communication of Results .....	25
9.	OTHER BUSINESS AND LEGAL MATTERS.....	26
9.1	Fees .....	26
9.2	Financial Responsibility.....	26
9.3	Confidentiality of Business Information.....	26
9.4	Privacy of Personal Information .....	26
9.5	Intellectual Property Rights .....	26
9.6	Representations and Warranties.....	27
9.7	Disclaimers of Warranties .....	27
9.8	Limitations of Liability .....	27
9.9	Indemnities .....	27
9.10	Term and Termination.....	27
9.11	Individual Notices and Communications with Participants.....	27
9.12	Amendments .....	27
9.13	Dispute Resolution Provisions .....	27
9.14	Governing Law .....	27
9.15	Compliance with Applicable Law.....	27
9.16	Miscellaneous Provisions.....	28

## History Log

Version	Date	Description
1.0	14 APR 2020	First release

# 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 for authentication and document signing. Authentication Certificates allow a Subscriber to prove the Subscriber’s identity to gain access to protected resources e.g. logging into an electronic service. Document signing Certificates allow Subscribers to add an electronic, digital signature to a document that not only proves the ownership of the document, but also protects the integrity of the document. 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.

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 1.0, effective date: 14-04-2020.

## 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

No stipulation.

## 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 PKI Policy Authority, which comprises of the CA's senior management, maintains this CP.

#### **1.5.2 Point of Contact**

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

Requests can also be made via email to [nca.ops@assurity.sg](mailto:nca.ops@assurity.sg)

#### **1.5.3 Person Determining CPS Suitability for the Certificate Policy**

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

#### **1.5.4 CP Approval Procedures**

The CA's policy authority 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 a 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 (CPS): A statement of the practices that the CA employs in the management of Certificates life cycle.

Certificate Signing Request (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 (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.

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 (“**IDN**”) or Punycode version; and, anonymous or pseudonymous Certificates. IDN 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**

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

### **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.

### **3.4 Identification and Authentication for Revocation Request**

Refer to Section 4.9 on Certificate revocation.

## **4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS**

### **4.1 Certificate Application**

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

### **4.2 Certificate Application Processing**

Issuer CA shall define Certificate application procedures, and the Issuer CA's and/or external service provider's responsibilities in these procedures. For example, the Issuer CA may make use of services provided by a RA to perform identity validation and accept Certificate applications on behalf of the Issuer CA.

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

### **4.4 Certificate Acceptance**

Issuer CA shall define actions that lead to an acceptance of the Certificate issued to the Subscriber.

### **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. Subscriber shall undergo the same procedures for issuance of a new Certificate in Section 4.2.

## **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.

## **4.8 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.

## **4.9 Certificate Revocation and Suspension**

Issuer CA shall define the circumstances where a Subscriber Certificate may be suspended and circumstances under which a Subscriber Certificate must be revoked. Issuer CA shall define the Subscriber Certificate suspension and revocation procedures, including who can make such request (such as the individual that made the Certificate application, or an entity with the requisite legal jurisdiction and authority), and methods or processes to suspend or revoke a Subscriber Certificate. Issuer CA shall avail the status of suspended or revoked Subscriber Certificates using the CRL and OCSP service (refer to Section 4.10).

## **4.10 Certificate Status Services**

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

## **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.

## **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 relevant education and certification qualifications, work experience and security clearance commensurate 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**

No stipulation.

## **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**

No stipulation.

### **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**

No stipulation.

### **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**

No stipulation.

### **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**

No stipulation.

### **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**

No stipulation.

#### **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**

No stipulation.

#### **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**

No stipulation.

### **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**

No stipulation.



## **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. If fees are imposed, CA shall specify provisions for fees charged, such as:

- (a) Certificate issuance of renewal fees;
- (b) Certificate access fees;
- (c) Revocation or status information access fees;
- (d) Fees for other services such as providing access to CP, CPS and relevant agreements; and
- (e) Refund policy.

### 9.2 Financial Responsibility

CA shall define resources available to the CA to support its CA services, remain solvent and protect against liabilities arising from its CA services, such as:

- (a) Insurance coverage;
- (b) Minimum level of assets necessary to operate its CA services; and
- (c) Warranty coverage.

### 9.3 Confidentiality of Business Information

CA shall define the method and procedures for handling confidential business information that it might collect or generate in offering its CA services, such as:

- (a) Scope or definition of confidential information;
- (b) Information that is not considered to be confidential; and
- (c) 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, such as:

- (a) Develop an applicable privacy plan that applies to the CA’s participants;
- (b) Define what is PII and what is not;
- (c) Responsibilities of personnel handling PII to protect it from compromise and unauthorised disclosure;
- (d) Consent for collection of PII; and
- (e) Disclosure of PII pursuant to judicial, administrative process in a private or governmental proceeding, or in any legal proceeding.

### 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**

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

## **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**

CA shall define the time period in which a CP or a CPS remains in force and the circumstances under which the document, portions of the document, or its applicability can be terminated.

## **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**

CA shall define the procedures for amending the CP and CPS. Change procedures may include a notification mechanism to provide notice of proposed amendments to affected parties and circumstances that would require a change in CP OID or CPS 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

No stipulation.