GOVTECH SINGPASS
CERTIFICATE POLICY

Contents

1. INTRODUCTION 7

1.1 Overview 7

1.2 Document Name and Identification 7

1.3 PKI Participants 7

1.3.1 Certification Authorities 7

1.3.2 Registration Authorities 7

1.3.3 Subscribers 7

1.3.4 Relying Parties 7

1.3.5 Other Participants 7

1.4 Certificate Usage 7

1.4.1 Appropriate Certificate Uses 7

1.4.2 Prohibited Certificate Uses 8

1.5 Policy Administration 8

1.5.1 Organization Administering the Document 8

1.5.2 Point of Contact 8

1.5.3 Person Determining CPS Suitability for the Certificate Policy 8

1.5.4 CP Approval Procedures 8

1.6 Definitions and Acronyms 8

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 10

2.1 Repositories 10

2.2 Publication of Certification Information 10

2.3 Time or Frequency of Publication 10

2.4 Access Controls on Repository 10

3. IDENTIFICATION AND AUTHENTICATION 11

3.1 Naming 11

3.1.1 Types of Names 11

3.1.2 Need for Names to Be Meaningful 11

3.1.3 Anonymity or Pseudonymity of Subscribers 11

3.1.4 Rules for Interpreting Various Name Forms 11

3.1.5 Uniqueness of Names 11

3.1.6 Recognition, Authentication, and Role of Trademarks 11

3.2 Initial Identity Validation 11

3.3 Identification and Authentication for Re-Key Requests 11

3.4 Identification and Authentication for Revocation Request 11

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 12

4.1 Certificate Application 12

4.2 Certificate Application Processing 12

4.3 Certificate Issuance 12

4.4 Certificate Acceptance 12

4.5 Key Pair and Certificate Usage 12
4.5.1 Subscriber Private Key and Certificate usage 12
4.5.2 Relying Party Usage of Subscriber’s Public Key and Certificate 12
4.6 Certificate Renewal 12
4.7 Certificate Re-Key 12
4.8 Certificate Modification 13
4.9 Certificate Revocation and Suspension 13
4.10 Certificate Status Services 13
4.11 End of Subscription 13
4.12 Key Escrow and Recovery 13
5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS 14
5.1 Physical Security Controls 14
5.2 Procedural Controls 14
5.3 Personnel Controls 14
5.4 Audit Logging Procedures 14
5.4.1 Types of Events Recorded 14
5.4.2 Frequency of Log Processing 14
5.4.3 Retention Period for Audit Log 14
5.4.4 Protection of Audit Log 14
5.4.5 Audit Log Backup Procedures 14
5.4.6 Audit Collection System 15
5.4.7 Notification of Event-Causing Subject 15
5.4.8 Vulnerability Assessments 15
5.5 Records Archival 15
5.5.1 Types of Records Archived 15
5.5.2 Retention Period for Archive 15
5.5.3 Protection of Archive 15
5.5.4 Archive Backup Procedures 15
5.5.5 Requirements for Time-stamping of Records 15
5.5.6 Archive Collection System 15
5.5.7 Procedures to Obtain and Verify Archive Information 15
5.6 Key Changeover 15
5.7 Compromise and Disaster Recovery 15
5.7.1 Incident and Compromise Handling Procedures 15
5.8 CA Termination 16
6. TECHNICAL SECURITY CONTROLS 17
6.1 Key Pair Generation and Installation 17
6.1.1 Key Pair Generation 17
6.1.2 Private Key Delivery to Subscriber 17
6.1.3 Public Key Delivery to Certificate Issuer 17

6.1.4 CA Public Key Delivery to Relying Parties 17
6.1.5 Key Sizes 17
6.1.6 Public Key Parameters Generation and Quality Checking 17
6.1.7 Key Usage Purposes 17
6.2 Private Key Protection and Cryptographic Module Engineering Controls 17
6.2.1 Cryptographic Module Standards and Controls 17
6.3 Other Aspects of Key Pair Management 17
6.3.1 Public Key Archival 17
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 17
6.4 Activation Data 17
6.5 Computer Security Controls 18
6.5.1 Specific Computer Security Technical Requirements 18
6.6 Life Cycle Technical Controls 18
6.7 Network Security Controls 18
6.8 Time-Stamping 18
7. CERTIFICATE, CRL, AND OCSP PROFILES 19
7.1 Certificate Profile 19
7.1.1 Version Number(s) 19
7.1.2 Certificate Extensions 19
7.1.3 Algorithm Object Identifiers 19
7.1.4 Name Forms 19
7.1.5 Name Constraints 19
7.1.6 Certificate Policy Object Identifier 19
7.1.7 Usage of Policy Constraints Extension 19
7.1.8 Policy Qualifiers Syntax and Semantics 19
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 19
7.2 CRL Profile 19
7.3 OCSP Profile 19
8. COMPLIANCE AUDITS AND OTHER ASSESSMENTS 20
8.1 Types of Assessment 20
8.2 Frequency or Circumstances of Assessment 20
8.3 Identity/Qualifications of Assessor 20
8.4 Assessor’s Relationship to Assessed Entity 20
8.5 Topics Covered by Assessment 20
8.6 Actions Taken as a Result of Deficiency 20
8.7 Communication of Results 20
9. OTHER BUSINESS AND LEGAL MATTERS 21
9.1 Fees 21
9.2 Confidentiality of Business Information 21
9.3 Privacy of Personal Information 21

9.4 Intellectual Property Rights 21
9.5 Representations and Warranties 21
9.6 Disclaimers of Warranties 21
9.7 Limitations of Liability 21
9.8 Indemnities 21
9.9 Term and Termination 21
9.10 Individual Notices and Communications with Participants 21
9.11 Amendments 22
9.12 Dispute Resolution Provisions 22
9.13 Governing Law 22
9.14 Compliance with Applicable Law 22
9.15 Miscellaneous Provisions 22

History Log

Version	Date	Description
1.0	20 AUG 2024	First release
1.1	04 NOV 2024	Updated section 5.1 on physical security controls, section 5.3 on personnel controls, section 5.7 on compromise and disaster recovery, section 6.5 on computer security controls, and section 6.7 on network security controls

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, including the Singpass Account (Individual) Certificate and the Singpass Foreign Account (Individual) 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 a CA. This CP may be amended or further CPs may be issued by a 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 1.1, effective date: 4 Nov 2024.

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 to and compliance with 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

CA shall specify other PKI participants (if any) in the relevant CPS(es).

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 with 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

CA's PKIPA maintains this CP.

1.5.2 Point of Contact

Government Technology Agency
Mapletree Business City
10 Pasir Panjang Road #10-01, Singapore 117438
Attention: NCA Operations, Singpass

Requests may also be made via our website at https://www.singpass.gov.sg/.

1.5.3 Person Determining CPS Suitability for the Certificate Policy

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

1.5.4 CP Approval Procedures

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, issued by the CA in accordance with the applicable CPS. "**Certificate**" includes the Singpass Account (Individual) Certificate and the Singpass Foreign Account (Individual) Certificate.

Certification Authority or 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. "**CPS**" includes the documents entitled "Certification Practice Statement for Singpass Account (Individual) Certificates" (Policy OID: 1.2.702.0.1009.100.1) and "Certification Practice Statement for Singpass Foreign Account (Individual) Certificates" (Policy OID: 1.2.702.0.1009.100.2), each as may be revised from time to time.

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.

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.

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 or 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. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate legal entity, but can be part of the CA.

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 applicable agreement or terms of services between each Subscriber and the CA for the Certificate issued. "**Subscriber Agreement**" includes the documents entitled "Subscriber Agreement for Singpass Account (Individual) Certificates" and "Subscriber Agreement for Singpass Foreign Account (Individual) Certificates", each as may be revised from time to time.

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 24 hours. CRLs for Issuer CA Certificates are issued at least once every 12 months (under normal operations) or 24 hours (if Issuer CA’s Certificate is revoked).

New or updated versions of the CPS(es), this CP, Subscriber Agreement(s) or Relying Party Agreement(s) are published after the CA’s policy authority’s approval. Archived copies of all CPs 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 issues Certificates with a non-null subject Distinguished Name (“**DN**”).

3.1.2 Need for Names to Be Meaningful

Issuer CA uses DNs that identify both the subject and issuer of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

Issuer CA shall not issue Certificates for Internationalised Domain Names or Punycode version, or 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 DN for all Subscribers.

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

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 with 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 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 as described 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/or OCSP service (refer to Section 4.10).

4.10 Certificate Status Services

Issuer CA shall provide Certificate status services using OCSP and/or 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

Physical Access Control. Access to data center facilities is controlled and limited to personnel with approved, purpose-specific permissions. Access requests specify both intent and duration, adhering to a "least privilege" approach. Once authorized, individuals can enter specific areas required for their tasks, and access is promptly revoked once their need expires.

Monitoring and Intrusion Detection. Security is maintained through video surveillance and intrusion detection systems. Access points, especially to restricted areas, are monitored with alerts triggered for unauthorized or unusual activity. Multi-factor authentication is required at entrances, and security teams continuously monitor any incidents.

Equipment and Environmental Safeguards. All critical systems, including power, climate control, and fire suppression, are set up with redundancy and are continuously monitored. Backup power, climate management, and fire safety measures protect infrastructure from environmental hazards. Regular preventive maintenance ensures that all essential systems operate reliably and that risks of disruptions are minimized.

5.2 Procedural Controls

CA puts in place systems and processes to ensure that no one person can circumvent the security of the CA systems or modify the CA system without detection.

5.3 Personnel Controls

All CA personnel have sufficient experience and expertise to carry out their assigned roles. CA personnel are legally required to protect the security of information relating to CA operations, including applicable information security requirements under the Government Technology Agency Act 2016, Public Sector (Governance) Act 2018 and Official Secrets Act 1935.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

CA maintains audit logs for system related matters. Logs will contain the date and time of events, and details of each event.

5.4.2 Frequency of Log Processing

Logs are automatically processed and stored by the CA’s system.

5.4.3 Retention Period for Audit Log

CA retains its logs for a minimum of one year.

5.4.4 Protection of Audit Log

CA implements access controls to prevent unauthorized personnel from accessing the audit logs.

5.4.5 Audit Log Backup Procedures

CA conducts backup of its audit logs.

5.4.6 Audit Collection System

CA maintains a system to collect and store audit logs.

5.4.7 Notification of Event-Causing Subject

Not applicable.

5.4.8 Vulnerability Assessments

CA conducts vulnerability assessments at such period as may be determined by the CA.

5.5 Records Archival

5.5.1 Types of Records Archived

CA maintains archived backups of application and system data. This may include, but are not limited to, audit data and certificates issued.

5.5.2 Retention Period for Archive

Archived records are generally kept for 7 years.

5.5.3 Protection of Archive

CA has security controls in place to protect archived records against unauthorised access, modifications and deletion.

5.5.4 Archive Backup Procedures

CA has a system in place to archive backups.

5.5.5 Requirements for Time-stamping of Records

Refer to Section 6.8.

5.5.6 Archive Collection System

Not applicable.

5.5.7 Procedures to Obtain and Verify Archive Information

CA has procedures in place to retrieve archive 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 has procedures to handle incidents and restore services in case of a compromise or disaster.

The CA has an incident response plan which documents the steps to be taken in event of system compromise and/or system failure, to restore service for users. The incident response plan includes procedures for investigating and escalating the incident for an appropriate response. The incident response plan is reviewed regularly, and training is conducted to familiarize CA personnel with the incident response plan. In the event of an incident, the CA may notify participants which include the RA, Subscribers, and Relying Parties where necessary.

5.8 CA Termination

CA shall define the procedures for termination and termination notification of the 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 140-2 level 3 validated cryptographic module.

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

The asymmetric key pairs used are at least 256-bit ECDSA.

6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable.

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.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Refer to Section 6.1.1.

6.3 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

Not applicable.

6.5 Computer Security Controls

CA implements computer security controls to prevent unauthorized access to the CA’s computer systems. CA reviews its security risks on a regular basis; this may include reviews and updates to the Government Instruction Manual and its guidelines. Updates to security policy and practices are communicated to personnel directly involved in the CA operations, which can be in the form of email, circulars, website updates or training.

6.5.1 Specific Computer Security Technical Requirements

The CA implements 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) enforce access control via an access control matrix, which is reviewed regularly and logged;

(e) log all security events;

(f) monitor for malicious activity and anomalous behavior, including unauthorized access to the system; and

(g) periodically assess the security of the CA’s system through security review and penetration testing.

6.6 Life Cycle Technical Controls

CA conducts scan(s) for vulnerabilities and conducts security review and penetration testing, at an interval as may be determined by the CA.

6.7 Network Security Controls

CA has network security controls in place to prevent unauthorized access to the CA’s system. This includes proper network configuration to allow access only from authorized services or components and using firewalls to prevent unauthorized traffic to CA systems.

6.8 Time-Stamping

CA includes a timestamp on its 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.

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

Not applicable.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

7.2 CRL Profile

Issuer CA shall publish CRLs that conform to RFC 5280.

7.3 OCSP Profile

OCSP messages generated by the CA shall conform to RFC 5019 and/or RFC 6960.

8. COMPLIANCE AUDITS AND OTHER ASSESSMENTS

8.1 Types of Assessment

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

8.2 Frequency or Circumstances of Assessment

CA shall define the frequency of the compliance audits and/or assessments.

8.3 Identity/Qualifications of Assessor

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

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 audits and assessments.

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.

9.2 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.

9.3 Privacy of Personal Information

CA shall define the method and procedures to protect personally identifiable information it might collect in offering its CA services.

9.4 Intellectual Property Rights

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

9.5 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.

9.6 Disclaimers of Warranties

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

9.7 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.

9.8 Indemnities

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

9.9 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.

9.10 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.

9.11 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).

9.12 Dispute Resolution Provisions

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

9.13 Governing Law

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

9.14 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 CA’s refusal to render its services.

9.15 Miscellaneous Provisions

Not applicable.