ASSURITY CERTIFICATION AUTHORITY CERTIFICATION PRACTICE STATEMENT

History Log

Version	Date	Description
1.0	14 APR 2020	First release

Contents

1 INTRODUCTION

1.1 Overview

This Certification Practice Statement ("**CPS**") describes the certification policies, procedures and practices applicable to the authentication and document signing Certificates issued by the Government of Singapore's appointed National Certification Authority ("**NCA**"), Assurity Trusted Solutions Pte. Ltd. (the "**Certification Authority**", "**CA**"). 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 facilitate the Subscribers to make electronic signatures.

The CA is a wholly-owned subsidiary of the Government Technology Agency of Singapore, with registered office at PSA Building, 460 Alexandra Road, #28-04, Singapore 119963 and company registration number 201013383H.

This CPS is structured in accordance with the Internet Engineering Task Force (IETF) RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework dated November 2003 with regard to content, layout and format. While section titles are included in this CPS in accordance with the structure of RFC 3647, the sections state "No Stipulations" where the topic does not apply to services of the CA. Additional information may be presented in subsections of the standard structure where necessary.

This CPS identifies the roles, responsibilities and practices of all entities involved in the lifecycle, use, reliance upon and management of the CA's Certificates.

This CPS can be downloaded on the CA's repository at https://www.nca.gov.sg/repository ("**Repository**"). This CPS may be updated from time to time and reviewed annually. The laws of the Republic of Singapore shall govern the enforceability, construction, interpretation and validity of this CPS. No part of this CPS may be reproduced without prior written permission of the CA.

1.2 Document Name and Identification

This document is the Assurity Certification Authority CPS, version 1.0, effective date: 14-04-2020].

1.3 PKI Participants

1.3.1 Certification Authorities

The CA issues and manages the lifecycle of Certificates in accordance with this CPS. The CA comprises of the Root CA and Issuer CA.

The Root CA [Singapore National Root CA – G1] issues the Issuer CA [Singapore NDI Intermediate CA 1 – G1] Certificate and the Issuer CA issues Subscribers' Certificates in accordance with this CPS.

The CA's PKI Policy Authority ("**PKIPA**") which comprises of senior management of the CA oversees the CA's operations. The PKIPA is responsible for the approval of this CPS and overseeing the adherence of the CA's Certificate practices to this CPS.

1.3.2 Registration Authorities

At present, the RA is the Government of Singapore (together with its representative, the Government Technology Agency of Singapore). The RA collects and verifies the identity of a prospective Subscriber of the CA's services and captures other information that will be included in the prospective Subscriber's Certificates. The RA will be performing its RA role using its electronic identification service - SingPass services.

1.3.3 Subscribers

Applicant applies to the Issuer CA, through the RA and the electronic identification service of such RA, for the issuance of a Certificate. Upon a successful Certificate application, the Applicant becomes a Subscriber of the CA's services. The subject of a Certificate is the party so named in that Certificate. At present, the Issuer CA issues Certificates to natural persons only.

1.3.4 Relying Parties

Relying Parties are entities that act in reliance on a Certificate issued by the Issuer CA.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

A Subscriber's Certificate issued by the Issuer CA is formatted data that cryptographically binds an identified Subscriber with a Public Key. A Subscriber's Certificate allows a Person taking part in an electronic transaction to prove its identity to other participants in such transaction.

1.4.1 Appropriate Certificate Uses

Subscribers' Certificates issued by the Issuer CA pursuant to this CPS may be used for document signing and to Authenticate the identity of Subscribers based on the Subscribers' Certificate. The "key usage" and "extended key usage" fields found within the Subscriber's Certificate defines the appropriate use of the Subscriber's Certificate. Prior to using or relying on the Subscriber's Certificate, among other things, each Relying Party should determine for

itself that the use of such Certificate is reasonable and appropriate under the given circumstances.

1.4.2 Prohibited Certificate Uses

Subscribers' Certificates issued by the Issuer CA shall be used and relied upon in accordance with applicable law.

The CA's Certificates are not designed, intended, or authorised for use in critical infrastructure systems such as the operation of nuclear facilities, aircraft navigation or communication systems, or weapon control systems, or otherwise where failure or reliance on the CA's services could lead directly to death, personal injury, or severe environmental damage.

1.5 Policy Administration

1.5.1 Organization Administering The Document

The CA's PKIPA maintains this CPS.

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

1.5.3 Person Determining CPS Suitability for the Policy

The CA's PKIPA determines the suitability and applicability of this CPS for its CP(s).

1.5.4 CPS Approval Procedures

The PKIPA reviews and approves this CPS from time to time. Amendments may be made by either updating or revising the CPS or by publishing an addendum. The approved CPS is published on the CA's Repository.

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.

Baseline Requirements: The CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly - Trusted Certificates ("**Baseline Requirements**") and the Guidelines for Extended Validation Certificates ("**EV Guidelines**") both of which are published at http://www.cabforum.org, which may be amended from time to time.

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

Certificate Policy (CP): A listed set of rules that indicates the applicability of a Certificate to a particular community or PKI implementation with common security requirements.

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.

Compromise (or its derivative or variant, "Compromised"): Suspected, loss, loss of control or use of a Private Key associated with a Certificate where the integrity cannot be confirmed.

Controller: The Controller for the purposes of the Electronic Transactions Act (Cap. 88) as appointed pursuant to Section 27 of the Electronic Transactions Act (Cap. 88).

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

Hardware Security Module (HSM): A physical computing device that safeguards and manages digital keys for strong Authentication and crypto processing.

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

Key Generation Script: A documented plan of procedures for the generation of a CA Key Pair.

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 recognised 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 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

The CA publishes its Root CA Certificate, Issuer CA Certificate, CPS, CP, Relying Party Agreement(s), and Subscriber Agreement(s) on the Repository, which is publicly available.

CRL and OCSP responses are published at URLs http://www.nca.gov.sg/SNRCA-G1.crl, http://www.nca.gov.sg/SNICA-G1.crl and http://ocsp.nca.gov.sg respectively, as specified in the Certificate's CRL Distribution Points or Authority Information Access field. CRL will be publicly available but OCSP responses will only be available to recipients authorised by the CA.

The CA operates its PKI that ensures that its Root CA Certificate, Issuer CA Certificate, CRLs and OCSP responder are available online on the Repository and the above URLs 24 hours a day, 7 days a week, with minimal interruption.

2.2 Publication of Certificate Information

The Issuer CA does not publish Subscribers' Certificates publicly on the Repository. A Subscriber's Certificate can only be obtained from such Subscriber. Only the CA's Root CA 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 on the Repository as soon as possible after issuance. CRLs for Subscribers' Certificates are issued at least once every hour and are valid for 7 days. New CRLs for Subscribers' 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 PKIPA'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 Repositories

Information published on the CA's repositories are public information, internationally available and unrestricted. The CA has implemented appropriate security controls to prevent unauthorised write access to its repositories.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

At present, the Issuer CA only issues individual identity Certificates to the general public. The CA may issue server and OCSP response signing Certificates for use in its internal operations.

The Issuer CA issues Certificates with a non-null subject Distinguished Name ("**DN**"). All Certificates' DN consists of Fully Qualified Domain Name ("**FQDN**") or Common Name ("**CN**"), Organisation, Organisation Unit and Country. Refer to Section 7 CERTIFICATE, CRL, AND OCSP PROFILES for detailed attributes of the Certificate.

3.1.2 Need for Names to Be Meaningful

The Issuer CA uses DNs that identify both the subject and issuer of the Certificate. FQDN or CN of a Subscriber's Certificate's subject consists of the subject's National Identity Number ("**NID**") and name. The NID is the National Registration Identity Card Number ("**NRIC**"), Foreign Identification Number ("**FIN**") or passport number of each individual.

3.1.3 Anonymity or Pseudonymity of Subscribers

The CA does not issue Certificates for Internationalised Domain Names ("**IDN**") or Punycode version; and does not issue 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 adhere to X.500 naming standards.

3.1.5 Uniqueness of Names

The Issuer CA enforces the uniqueness of each subject name in a Subscriber's Certificate by entering the subject's NID and name in the CN attribute of the subject field.

In the event of any dispute concerning name claim issues, the name claim dispute resolution process, as may be prescribed by the Issuer CA from time to time, shall apply. The Issuer CA shall be the final arbiter of all such claims in relation to Subscriber names in all Certificates, and shall have the sole and absolute discretion to accept or reject any name.

3.1.6 Recognition, Authentication, and Role of Trademarks

The Issuer CA does not determine the validity of an Applicant's right to use any copyright materials, "Doing Business As" (DBA)/trademark and does not resolve disputes of such natures. The trademarks, service marks, proprietary words or symbols of the rightful owner shall not be used without the express prior written consent of the rightful owner. The Issuer CA may reject any application or require revocation of any Certificate that is a part of such disputes.

3.2 Initial Identity Validation

The Issuer CA uses the RA and the electronic identification service of such RA to validate the identity of an Applicant. The RA shall ascertain the identity of an Applicant in the manner as set out in Section 3.2.3. CSRs received by RA will be forwarded to the Issuer CA. However, in the event that the Applicant's identity cannot be accurately identified or if there are any issues or concerns that such RA has with the Applicant's identity or with the validation thereof, such RA may in its sole discretion refuse to forward the CSR to the Issuer CA.

3.2.1 Method to Prove Possession of Private Key

The Applicant uses the SingPass Mobile application ("**SPM**") to request for a Certificate. The RA will perform identity validation using SPM. Upon successful Authentication (refer to Section 3.2.3), a personalized generated Key Pair is installed on the Applicant's SPM. The Applicant generates a CSR, in PKCS#10 format, and submits the CSR to the Issuer CA through the RA. This is to establish that the Applicant possesses the Private Key which corresponds to the Public Key in the CSR.

3.2.2 Authentication of Organization Identity

At present, the Issuer CA does not issue Certificates to organizations.

3.2.3 Authentication of Individual Identity

An Applicant must have a valid[1] SingPass account ("**SingPass 1FA**") prior to requesting for a Certificate. SingPass 1FA refers to the SingPass account username and password.

RA Authenticates an Applicant's identity, via the SPM, using the following methods:

(a) SingPass 2FA – For an Applicant who has SingPass 2FA, i.e. SMS-OTP and/or hardware token, the SPM shall Authenticate the Applicant's identity using SingPass 1FA and 2FA; and

(b) SingPass activation pin mailer – An Applicant who does not have SingPass 2FA cannot request for a Certificate instantaneously using the SPM. Instead, the SPM will direct the

[1] A valid SingPass account is one which is not terminated, not suspended and not dormant.

Applicant to enrol or register for an activation pin mailer, to be sent to the Applicant's residential address. Upon receiving the activation pin mailer, the Applicant can then complete the Certificate Request using the SPM.

3.2.4 Non-Verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

The authority of an individual Applicant requesting for an individual Certificate is verified under Section 3.2.3. At present, an Applicant cannot request for a Certificate on behalf of an organization.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-Key Requests

Issuer CA does not support re-key requests. Issuance of a new Certificate is required.

3.4 Identification and Authentication for Revocation Request

Revocation requests are submitted by Subscribers or their authorised agents via a designated channel to revoke a particular Certificate.

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

Applicant who decides to apply for a Certificate with the Issuer CA will be required to submit a CSR through RA. The RA's system sends the CSR to the Issuer CA's system via a secured network connection between the RA and Issuer CA systems. Applicants are solely responsible for submitting a complete and accurate CSR for each Certificate. The enrollment processes include:

1. Subscriber is required to accept and agree to the Subscriber Agreement (as may be amended from time to time) on SPM;
2. Subscriber generates Subscriber Key Pair on SPM;
3. RA delivers a CSR (including the Subscriber's Public Key) to the Issuer CA; and
4. Issuer CA returns a Certificate to the Subscriber via RA.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

RA is responsible for validating the identity of the Applicant. Refer to Section 3.2 Initial Identity Validation.

4.2.2 Approval or Rejection of Certificate Applications

Applicants are required to check the accuracy of the data before submitting the Certificate application. RA, on behalf of the Issuer CA, shall reject any Certificate application that cannot be verified. The Issuer CA may also reject a Certificate application if the Issuer CA believes that issuing the Certificate could damage the CA's reputation or business.

If the Certificate application is accepted and successfully validated in accordance with this CPS, RA, on behalf of the Issuer CA, will approve the Certificate application and issue the Certificate. RA and the Issuer CA are not obligated to reveal the reasons for Certificate applications that are rejected. However, no restrictions are imposed on rejected Applicants to re-apply for a new Certificate.

4.2.3 Time to Process Certificate Applications

Under normal operating circumstances, RA issues, on behalf of the Issuer CA, a Certificate upon processing the CSR within a reasonable time. Issuance waiting time is greatly dependent on processing complexity and network latency between the Applicant, RA and the Issuer CA. As such, the Issuer CA only makes reasonable efforts to issue the Certificates immediately upon the receipt and processing of the CSR.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

RA verifies the format of and information contained in the CSR from the Applicant prior to forwarding the CSR to the Issuer CA. Upon receipt and processing of the CSR, the Issuer CA issues a Certificate and returns the signed Certificate to the RA.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The RA will deliver the Certificate to the Subscriber's SPM in a secure manner within a reasonable time. The Certificate is automatically installed on the Subscriber's device on which SPM is installed. Upon installation of the Certificate, SPM will display a message indicating the successful installation.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The Subscriber is deemed to have accepted the Certificate upon installation of the Certificate on the Subscriber's SPM.

4.4.2 Publication of the Certificate by the CA

The Issuer CA does 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

The Issuer CA does not 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

The Subscriber's responsibilities relating to the use of the Subscriber's Private Key and Certificates are set out in the Subscriber Agreement.

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

A Relying Party's responsibilities relating to the reliance on a Subscriber's Public Key and Certificates are set out in the Relying Party Agreement.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

There shall be no extension of the Subscriber's Certificate. Each renewal request will be treated as a new Certificate Request (and not as an extension of an earlier-issued Certificate).

4.6.2 Who May Request Renewal

A Subscriber self-enrolls for a new Certificate through the RA.

4.6.3 Processing Certificate Renewal Requests

Subscriber will undergo the initial registration process for a new Certificate through the RA. During such process, the CA re-validates information of the Subscriber and updates any new information changes.

4.6.4 Notification of New Certificate Issuance to Subscriber

Refer to 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Refer to 4.4.1 Conduct Constituting Certificate Acceptance.

4.6.6 Publication of the Renewal Certificate by the CA

Refer to 4.4.2 Publication of the Certificate by the CA.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The Issuer CA does not notify any other entities about Certificates that it issues.

4.7 Certificate Re-Key

The Issuer CA does not provide Certificate re-key services. 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

No stipulation.

4.7.2 Who May Request Certification of a New Public Key

No stipulation.

4.7.3 Processing Certificate Re-Keying Requests

No stipulation.

4.7.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

No stipulation.

4.7.6 Publication of the Re-Keyed Certificate by the CA

No stipulation.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

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, is required.

4.8.1 Circumstances for Certificate Modification

No stipulation.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

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 or Authority Information Access field.

The Issuer CA may remove the serial numbers from the CRL when revoked Certificates expire to promote efficient CRL file size management. Prior to performing a revocation, the Issuer CA will verify the authenticity of the revocation request. The 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:

1. the Subscriber or its authorised agent submits an Authenticated revocation request to the Issuer CA, via the RA;
2. the Root or Issuer CA's Private Keys or system is compromised in a manner materially affecting the Certificate's reliability;
3. 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;
4. the Subscriber did not request for and did not grant any authorisation for the initial Certificate Request;
5. there is a breach of a material obligation under the CPS or the relevant Subscriber Agreement by the Subscriber;
6. the Subscriber is deceased;
7. 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;
8. the Certificate is not issued in accordance with the CPS or applicable industry standards;

9. when the Issuer CA or RA becomes aware of a change in the information contained in the Certificate;
10. the Issuer CA receives a lawful and binding order from a government or regulatory body to revoke the Certificate or otherwise where it is required by law;
11. 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;
12. any information in the Certificate is inaccurate or misleading;
13. the continued use of the Certificate is harmful and undermines the Issuer CA's trust infrastructure;
14. the Certificate can no longer guarantee that a signature verification key can be assigned to a specific Person;
15. the Subscriber is no longer entitled to hold the Certificate; and
16. the Certificate is no longer needed.

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 or an authorised agent of the Subscriber may request for revocation of a Certificate. Revocation can also be initiated at the discretion of the Issuer CA.

4.9.3 Procedure for Revocation Request

The Issuer CA may revoke a Certificate that it issued upon receiving an Authenticated revocation request from the Subscriber, or its authorised agent, made via the RA.

Upon successful revocation, the Issuer CA will issue an updated CRL and shall make reasonable attempts to notify the requestor through the RA. The date and time of all transactions in relation to the revocation of Certificates shall be logged.

4.9.4 Revocation Request Grace Period

No stipulation.

4.9.5 Time within Which CA Must Process the Revocation Request

The Issuer CA shall revoke the Certificate immediately upon receipt of an Authenticated revocation request from the Subscriber, which is submitted from the Subscriber's PKI device, or after receiving directions from the CA's PKIPA on material breaches or after validating the revocation request in accordance with the process stated in Section 4.9.3.

4.9.6 Revocation Checking Requirement for Relying Parties

The Issuer CA operates a CRL file and OCSP responder for checking the validity of Certificates. Relying Parties shall ensure that the Certificate remains valid and has not been revoked or suspended by accessing the CRL or OCSP.

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

The Issuer CA makes Certificate status information available online via the OCSP service to recipients authorised by the CA. OCSP responses are provided within a commercially reasonable time after the request is received, subject to transmission latencies over the Internet.

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

No stipulation.

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 can be used when a Subscriber or the Issuer CA wants to temporarily disable usage of Subscriber's Certificate. Suspension can be used in situations, such as investigations, temporary loss of the Subscriber's device on which SPM is installed or when a Subscriber leaves the country for an extended period of time. Unlike Certificate revocation which disables a Certificate permanently, Certificate suspension status can be lifted and such Certificate can thereafter be used till the expiry date of that Certificate.

4.9.14 Who Can Request Suspension

Refer to 4.9.15 Procedure for Suspension Request.

4.9.15 Procedure for Suspension Request

The Issuer CA may suspend a Certificate upon receiving an Authenticated suspension request from:

1. the Subscriber, via the RA;
2. an authorised agent of the Subscriber, via the RA; or
3. a Person acting on behalf of the Subscriber (if the Subscriber is not available), via the RA.

The Issuer CA may suspend a Certificate if the CA has reasonable grounds to believe that the Certificate is unreliable.

The Issuer CA may consider revoking a Certificate if revocation is justified in the light of all the evidence available to it.

The Issuer CA may reinstate any Certificate in accordance with its reinstatement procedure, as may be prescribed by the Issuer CA from time to time.

Upon successful suspension and reinstatement of Certificates, the Issuer CA issues an updated CRL and shall make reasonable attempts to notify the Subscriber through the RA. The date and time of all transactions in relation to the suspension of Certificates shall be logged.

4.9.16 Limits on Suspension Period

Certificate suspension may last as long as the validity period of Certificate.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The CA operates two forms of Certificate status services i.e. the OCSP and CRL. URLs of the OCSP and CRL are specified in the Certificate's CRL Distribution Points or Authority Information Access field. The CA may choose to use content delivery network, cloud-based services to improve its service availability.

4.10.2 Service Availability

The CA's Certificate status services are available 24 hours a day, 7 days a week, with minimal interruption.

4.10.3 Optional Features

No stipulation.

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

The CA does not escrow the CA's Private Keys nor provide services to escrow Subscribers' Private Keys. The Subscriber shall not escrow his Private Keys.

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

5.1 Physical Security Controls

5.1.1 Site Location and Construction

The CA hosts its systems on a pair of Government Data Centres ("**GDC**") in separate locations. GDCs are equipped with logical and multiple layers of physical controls designed to deter intruders. Visitors undergo security clearance before accessing the data centres. Accessibility is limited only to trusted personnel. The CA operates its operations under strict GDC security policies designed to detect, deter, and prevent unauthorised access.

5.1.2 Physical Access

GDC security personnel are on duty 24 hours per day, 365 days per year. Access to secure areas of the buildings requires the use of two-factor authentication control mechanisms (i.e. an access card with pin and/or biometric controls). The visitors, company, time, and purpose of each visit are recorded on physical logs. Multiple layers of doors and barriers need to be cleared to reach the CA's systems. The exterior and internal passageways of the buildings and racks are under constant video surveillance.

Activation Data, cryptographic modules, or removable hardware used to administer the CA are locked up in safes on-site and off-site.

5.1.3 Power and Air Conditioning

GDC uses multiple load-balanced heating, ventilation, and air conditioning ("**HVAC**") systems for heating, cooling, and air ventilation. All power supplies have a primary and secondary power source. Uninterrupted power supplies ("**UPS**") and diesel generators provide backup power in the event of power failure.

5.1.4 Water Exposures

The cages and racks housing the CA's systems are located on raised flooring, and the data centres are equipped with monitoring equipment to detect excess moisture.

5.1.5 Fire Prevention and Protection

GDC is equipped with fire detection, alarm and suppression mechanisms.

5.1.6 Media Storage

The CA uses the backup service provided by GDC which provides the required security controls that protects backup media from unauthorised access.

5.1.7 Waste Disposal

The CA adheres to the Government's Policy on ICT Security for media sanitization to handle disposal of data. The media sanitization policy specifies the appropriate action to take e.g. overwrite, cryptographic erase or degauss, depending on the sensitivity of the data and the type of storage media used.

5.1.8 Off-Site Backup

The CA maintains regular backup copies of any information necessary to recover from a system failure. Backups are stored securely in off-site locations. Backup copies of CA's Private Keys and Activation Data are stored off-site in locations that are accessible only by trusted personnel.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted roles are assigned such that the functional roles of each individuals are distributed and no single individual can circumvent the security of the CA's systems. Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. Trusted roles include but are not limited to the following:

1. Key custodian: Authorised to hold the CA's Activation Data that is necessary for HSM operations;
2. Security Officer: Responsible for administering the security policies and implementing security procedures and controls in day-to-day operations;
3. System Administrator: Authorised to install, configure and maintain the day-to-day operations of the CA's systems for the issuance, revocation or suspension of Certificates;
4. System Operator: Responsible for monitoring the uptime and alerts, and maintenance of the CA's systems on a day-to-day basis;
5. Developer: Responsible for the development of software to support the day-to-day business functions of the CA; and
6. Auditor: Authorised to view audit logs of the CA's systems.

5.2.2 Number of Persons Required Per Task

The CA implements an "n out of m" rule on the number of individuals required to perform tasks such as CA system initialization, CA Key Pair generation, key backup and import operations.

5.2.3 Identification and Authentication for Each Role

The CA's personnel shall have personal accounts and are required to use 2-factor authentication to access the systems to perform their trusted roles.

5.2.4 Roles Requiring Separation of Duties

The CA implements Role Based Access Control ("**RBAC**") policies that enforce separation of duties such as restricting individuals from assuming multiple roles, and preventing any individual from having more system access than required to perform their roles or subverting the checks and balances system.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The CA's PKIPA is responsible and accountable for the CA's compliance with this CPS and day-to-day PKI operations. Before appointing any individual to any trusted role, background checks will be conducted and the candidate will be required to undergo security clearance prior to being employed. The CA's PKIPA shall ensure that all personnel assigned to trusted roles have the experience, information security awareness, right qualifications, and trustworthiness required to perform their duties under this CPS.

5.3.2 Background Check Procedures

The CA's hiring processes verify candidate employees' identities using official identification documents such as national identity cards or passports. Background checks include identity documents, country of residence, family, employment history, education, character references, bankruptcy status and criminal history. All employees in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the CA's operations.

5.3.3 Training Requirements

The CA provides training from time to time to all personnel involved in the CA's operations. The training relates to the individual's job functions such as:

1. Basic Public Key Infrastructure ("**PKI**") knowledge;
2. Information security awareness such as common threats and risks, phishing, social engineering tactics;
3. Authentication and vetting policies and procedures (including CA's CP/CPS);
4. Product knowledge, operations and administration on the CA systems;
5. Applicable industry and government guidelines; and
6. Business Continuity Plans and Disaster Recovery procedures.

The CA maintains records of the personnel who have attended the trainings and the level of training attained. The CA may send its personnel for certification courses or examinations. New employees undergo on-the-job training and mentoring by senior members of the team. An external subject matter expert may be engaged from time to time to conduct refresher training.

5.3.4 Retraining Frequency and Requirements

Personnel may undergo retraining to maintain skill levels that are consistent with industry-relevant standards and to ensure smooth running of the CA's operations. Changes on the CA's operations are documented such that these changes are recorded and its personnel are trained, if necessary, to upkeep with these changes.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The CA's employees who fail to comply with this CPS, CP or CA-related operational procedures will be subjected to appropriate disciplinary actions. Depending on the severity of the breaches, employees may be re-assigned to other roles or terminated from their duties.

5.3.7 Independent Contractor Requirements

Independent contractors are required to adhere to the IT security policies, security clearances, non-disclosure agreements, and rules of engagement, when engaged as a contractor under the CA's contractual terms. Any breaches of such terms will result in the termination of the working agreements and damages to be claimed from the contractor.

5.3.8 Documentation Supplied to Personnel

Personnel in trusted roles are provided with the work instructions and training necessary to perform their duties. Documents supplied shall include the CP, CPS, CA/Browser Forum Baseline Requirements, technical and operational documentation needed to maintain the day-to-day operations of the CA. Personnel are also given access to information on internal systems on a need-to-know basis, educated on security awareness and documentation, identity-vetting policies and procedures and any other information.

5.4 Audit Logging Procedures

The CA's system events are logged (refer to Section 5.4.1 Types of Events Recorded). All logs are sent to a central log server. Audit logs are maintained to reconstruct a particular action or set of actions, to trace the actions of an application or individual user, and to hold a specific individual accountable for his/her actions.

5.4.1 Types of Events Recorded

The CA enables automatic logging, whenever possible, for the following significant events:

1. CA Private Key lifecycle management events, including:
    a) Key generation, backup, storage, recovery, archival and destruction;
    b) Cryptographic device lifecycle management events; and

c) Multiple failed logins.

2. CA and Subscriber's Certificate lifecycle management events, including:
   a) Certificate issuance, renewal, suspensions and revocation;
   b) All verification activities required by this CPS;
   c) Acceptance and rejection of CSR;
   d) Changes to Certificate profiles;
   e) Issuance of Certificates; and
   f) Generation of CRLs.

3. Security events, including:
   a) Successful and unsuccessful system access attempts;
   b) Actions or operations performed on the systems;
   c) Security profile changes;
   d) System crashes, hardware failures, and other anomalies;
   e) Assess to CRLs and OCSP responses;
   f) Firewall, web application firewall, proxies and router logs; and
   g) Entries to and exits from the CA facility.

Where events cannot be automatically recorded, the CA implements manual procedures using hardcopy logs, to satisfy the logging requirements. For each request, the CA records the relevant (a) date and time, (b) type of event, (c) success or failure, (d) user or system that caused the event or initiated the action, and (e) purpose of changes. All event records are available to auditors as proof of the CA's practices.

5.4.2 Frequency of Log Processing

Audit logs are examined periodically for malicious activities and operational events, and where possible, the CA's system operators are alerted automatically. Additional attention is given to important operations or events such as critical patching or critical vulnerabilities discovered. The CA reviews its audit logs to ensure that it has not been tampered with, and to review for anomalous, suspicious or unusual activity in response to alerts generated within the CA systems. Any anomalies or irregularities discovered are investigated and remediated if applicable. The CA documents any actions taken as a result of these reviews.

5.4.3 Retention Period for Audit Log

Audit logs for all Certificate transactions, activities and events shall be kept up to 7 years.

5.4.4 Protection of Audit Log

The CA implements a trusted role (i.e. the Auditor role, see Section 5.2.1) that restricts access to audit logs. The audit logs are digitally signed to protect the integrity of audit logs against unauthorised modification or deletion.

5.4.5 Audit Log Backup Procedures

The CA uses GDC's backup service to perform daily backup of audit logs.

5.4.6 Audit Collection System

The CA manages its own central logging system that collects audit logs from the CA systems that the CA owns (e.g. web servers, API gateway, application servers, databases and load balancers). Logs related to the hosting environment, in particular the network devices (e.g. switches, routers and firewalls) are collected and processed by GDC.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

The CA performs regular vulnerability scans in its systems and implements relevant patches or mitigating controls to address discovered vulnerabilities. An independent third party security provider conducts an annual assessment to maintain the security posture of the CA system.

5.5 Records Archival

5.5.1 Types of Records Archived

The CA complies with all record retention policies mandated by Singapore law and the Controller's accreditation requirements. The CA includes sufficient detail in all archived records to show that a Certificate was issued in accordance with this CPS.

5.5.2 Retention Period for Archive

Audit logs for all Certificate transactions, activities and events are kept up to 7 years.

5.5.3 Protection of Archive

Archived records are signed to ensure integrity before being placed into long term storage. Controls are in place to prevent unauthorised modification, substitution, or destruction of data. Archives are not released except required by law. Archived records are stored at a secure off-site location.

5.5.4 Archive Backup Procedures

Backups are performed on a daily basis at a secure location using scheduled jobs. An offline backup is taken at the end of any key generation ceremony.

5.5.5 Requirements for Time-Stamping of Records

The CA's systems are all synchronized to a trusted time source (non-cryptographic method). Refer to Section 6.8. All logs consist of data indicating the time at which the event occurred.

5.5.6 Archive Collection System (Internal or External)

The CA uses an internal archive collection system.

5.5.7 Procedures to Obtain and Verify Archive Information

Upon receiving a formal request by a Subscriber, authorised agent, or a party involved in a dispute over a transaction involving the CA, the CA may conduct its own internal investigation and may retrieve the information from the archives. Access and use of archived data are restricted in accordance with the CA's internal security policies and procedures.

5.6 Key Changeover

Key changeover procedures enable the smooth transition from the expiring Issuer CA Certificates to the new Issuer CA Certificates. Prior to the expiry of the Issuer CA Private Key, the Issuer CA ceases to use the expiring Issuer CA Private Key to sign Issuer CA Certificates (well in advance of expiration). The expiring Issuer CA Private Key is only used to sign CRLs and OCSP responder Certificates and kept until all the Subscribers' Certificates signed using the expiring Issuer CA Private Key have expired. A new Issuer CA signing Key Pair is commissioned and all subsequent Subscribers' Certificate issuance and CRLs for Subscribers' Certificates are signed with the new Issuer CA's Private Key. Both the expiring and the new Key Pairs of the Issuer CA may be concurrently active. This key changeover process helps minimize any adverse effects from CA Certificate expiration.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The CA handles incidents and compromise in accordance to its internal incident management policies. If a disaster causes disruption to the CA's operations, the CA has backup facilities in place to reinstate operations as quickly as possible, using backup copies of data, hardware, software and CA's Private Keys. The CA reviews and test its incident management procedures according to regulatory requirements. If there are any incidents such as:

1. Compromise of key;
2. penetration of CA system and network;
3. unavailability of infrastructure; and/or
4. fraudulent registration and generation of Certificates, Certificate suspension and revocation information,

the CA will promptly report to the relevant authority and investigate such incidents immediately.

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

The CA's operations are designed and setup in high availability mode. The CA maintains regular backup of system data and CA's Private Keys. If a disaster causes disruption to the CA's operation, day-to-day operations shall be re-established as quickly as possible using backup copies of data, hardware, software and CA's Private Keys at a secure facility.

5.7.3 Entity Private Key Compromise Procedures

Upon the discovery of a Compromise of the CA's Private Key, the CA's PKIPA will immediately convene an emergency incident response team to assess the situation, the materiality and scope of the incident, and take appropriate action, which will minimally include the following:

1. collecting all information related to the incident;
2. notifying the Controller of the breach;
3. reasonably notifying existing Subscribers and Relying Parties;
4. revoking the Issuer CA Certificate and issuing the final CRL immediately;
5. as quickly as possible, issuing a new Issuer CA Certificate and start operations from the new Issuer CA;
6. preparing an incident report analysing the cause of the incident and documenting the lessons learned; and
7. incorporating lessons learned into the implementation of long-term solutions and the Incident Response Plan.

The CA will cease its operations until compromise has been remediated and security of the CA systems have been reinstated. If a disaster physically damages all of the CA's equipment and destroys all copies of the CA's keys, data and backups, the CA will provide notice to all interested parties that the CA is aware of at the earliest possible time.

5.7.4 Business Continuity Capabilities after a Disaster

To plan for and recover from disasters, the CA has developed a business continuity plan ("**BCP**"). The CA reviews and updates the BCP and supporting documents according to regulatory requirements. The CA's operations are designed and set up in high availability mode and backup systems are located at a separate, diverse location in the event of a disaster.

5.8 CA Termination

Before terminating its CA activities, the CA will:

1. Provide notice and information about the cessation of CA operations by sending emails to its customers, Subscribers, and Relying Parties; and
2. Transfer all responsibilities to a qualified entity capable to continue operations.

If no qualified successor entity exists, the CA will:

(a) Stop all issuance of Certificates in adherence to this CPS;
(b) Revoke all Certificates on a date as specified in the notice and publish the final CRL;
(c) Ensure records are archived properly for a period of time deemed fit by the CA;
(d) Destroy CA's Private Keys; and
(e) Make other necessary arrangements that are in accordance with this CPS.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The CA's Key Pairs are generated by multiple trusted individuals using a HSM device, following a scripted key generation ceremony. The HSM device is certified to be FIPS 140-2 Level 3 and EAL 4+ compliant. Access to the HSM device requires the use of Activation Data.

The key generation ceremony is performed by the CA's personnel acting in different trusted roles with RA. There is auditable evidence during the key generation process to prove that the CPS was followed and segregation of roles was enforced during the key generation process.

An independent auditor will witness and validate that each CA key is generated in accordance with this CPS. The whole process is witnessed by an independent auditor. After the CA's keys are generated, the auditor issues an attestation letter that the CA has:

1. Documented its key generation procedures;
2. Included appropriate detailed procedures and controls in its Key Generation Script; and
3. Performed all of the procedures as required by the Key Generation Script.

6.1.2 Private Key Delivery to Subscriber

Subscriber's Private Key is automatically generated on the Subscriber's device on which SPM is installed during self-enrolment. 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

The Subscriber self-enrolls, generates its Key Pair and submits the CSR containing the Subscriber's Public Key to the Issuer CA via the RA as part of the Certificate enrollment process. The Subscriber's information is Authenticated by the RA. Only those requests that passed the RA's validation will be forwarded to the Issuer CA for processing and Certificate issuance.

6.1.4 CA Public Key Delivery to Relying Parties

The Root CA and Issuer CA Certificates can be obtained from the CA's Repository.

6.1.5 Key Sizes

The CA validates the keys, signature algorithms, and hash algorithms for signing Certificates, CRLs and OCSP from time to time. Choice of algorithm and key size will align with the Baseline Requirements or SSL industry standards. The CA uses the following keys, signature algorithm and hash algorithm for signing the respective Certificates:

1. Root CA: 521-bit ECDSA key with Secure Hash Algorithm 2 (SHA-384)
2. Issuer CA: 384-bit ECDSA key with Secure Hash Algorithm 2 (SHA-384)
3. Subscriber: 256-bit ECDSA key with Secure Hash Algorithm 2 (SHA-256)

6.1.6 Public Key Parameters Generation and Quality Checking

The CA guarantees the quality of the CA's Public Key parameters using pseudo-random number generation provided by FIPS 140-2 Level 3 HSM.

6.1.7 Key Usage Purposes

Certificates issued by the Issuer CA include relevant "key usage extension fields" that specify the intended use of the Certificate and technically limit their functionality in X.509 compliant software. Currently, the Issuer CA issues Subscribers with two Certificates, one for document signing and one for authentication.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The CA's cryptographic modules comply with the FIPS 140-2 Level 3 standards for the generation of the CA's Public Key parameters and protection of CA's Private Keys.

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

The CA implements "n out of m" procedures to ensure that multiple personnel in trusted roles are required to access the CA's Private Keys.

6.2.3 Private Key Escrow

The CA does not escrow its CA Private Keys and does not provide Private Key escrow services for Subscribers.

6.2.4 Private Key Backup

The CA's Key Pairs are generated and backed up by multiple trusted individuals using at least FIPS 140-2 Level 3 certified cryptographic module during the key generation ceremony. Private Keys are always stored in an encrypted form and never exist in plaintext form.

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 keys are generated by and in a cryptographic module which comply with FIPS 140-2 Level 3 standards. Private Keys are exported from the cryptographic module only for backup purposes. The CA's Private Keys are always stored in an encrypted manner and never exist in plaintext form. Activation Data used to activate the backups are stored securely and require at "n out of m" trusted personnel to access.

6.2.7 Private Key Storage on Cryptographic Module

The CA's Private Keys are generated and protected using cryptographic module which comply with FIPS 140-2 Level 3 standards.

6.2.8 Method of Activating Private Key

The CA's Private Keys are activated following instructions and documentations of the cryptographic module manufacturer during a key ceremony. The whole process follows a script and is witnessed by independent third party auditors.

6.2.9 Method of Deactivating Private Key

The CA's Private Keys are deactivated via logout procedures when not in use or when maintained in an off-line state. The CA never leaves its HSM device in an unlocked or unattended state.

6.2.10 Method of Destroying Private Key

When the CA's Private Keys have reached the end of their lifespan, Private Keys are removed from the cryptographic module. The CA initializes the HSM device and associated backup tokens according to the specifications of the hardware manufacturer. If the initialization procedure fails, the CA will physically remove and destroy any hardware storage or key material to destroy all capability to extract any Private Key.

Subscribers are solely responsible for the protection of their Private Keys. Subscribers shall destroy their Private Keys by uninstalling SPM when the corresponding Certificate is revoked or expired or if the Private Key is no longer needed.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The CA archives its Public Keys in accordance with Section 5.5 of this CPS.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Root CA and Issuer CA Certificates have validity period of 20 years and 10 years, respectively. Certificates issued to Subscribers shall have a validity period of 2 years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The CA activates the cryptographic module containing CA's Private Keys according to the specifications of the HSM manufacturer that is FIPS 140-2 Level 3 certified during a key ceremony.

6.4.2 Activation Data Protection

Activation Data is protected from disclosure using a combination of cryptographic, physical and logical access control mechanisms. Multiple personnel in trusted roles (refer to Section 5.2.2) are required to access the CA Private Keys or HSM containing the CA Private Keys.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The CA implements the following security controls:

1. access to systems and applications, including the remote workstations, requires 2-factor authentication;
2. minimum password length and complexity are enforced;
3. RBAC is implemented to manage the privileges of users and limit users to their assigned roles;
4. communication channels between system components are secured using mutual Transport Layer Security;
5. central logging for all events and security logs are sent to the Government's Cyberwatch Centre for security monitoring;
6. system configuration is hardened based on guidelines published by the Centre for Internet Security or product principals; and
7. conduct of periodic vulnerabilities assessment and penetration testing and security review to assess the security posture of the CA's system.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The CA selected a vendor to implement and support the CA systems by a tendering process. The evaluation of the vendors was based on their ability to execute, local support, reputation and strong financial backing. Cybersecurity professionals reviewed the CA system to ensure that it was secure by design. The CA system was also subjected to internal and external security testing, including Red Teaming exercise, to remediate any development or design flaws.

6.6.2 Security Management Controls

The CA maintains both technical and procedural mechanisms to manage changes to its system. End-point protection software, installed on all CA systems, protect the system against unauthorised traffic, malware, virus and unauthorised modification. Software updates or patches undergo a rigorous patch management process where these updates/patches are downloaded only from authorised sources into controlled environments, scanned for malware, and compared against the hash, to validate the integrity of the sources before installation.

All change requests need to be approved by the CA's management before implementation.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

The CA's systems are hosted within the secured data centres. Network security controls such as firewalls and perimeter control devices are provided by the data centres and configured to only allow authorised access to the CA's systems. The CA hardens its operating systems to ensure that only required services are configured to run the CA functions. All unused services, ports and software are disabled and blocked.

6.8 Time-Stamping

The CA uses the GDC Network Time Protocol to synchronize all systems to a common system clock such that there is a consistent time-stamping of the CA's data, logs and archived records.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

AUTHENTICATION CERTIFICATE		
Attribute	**Value**	**Description**
Version	3	Certificate format version.
Serial Number	<128bit value>	Certificate unique serial number (auto-generated).
Signature Algorithm	sha256ECDSA	Cryptographic algorithm used by CA to sign the Certificate.
Signature Hash Algorithm	sha256	Algorithm used to generate the hash
Valid from	<start validity date and time>	Date and time of Certificate issuance.
Valid to	<end validity date and time>	Date and time of Certificate expiration.
Issuer DN		
Common Name (CN)	Singapore NDI Intermediate CA 1 - G1	Issuer CA name.
Organization (O)	Assurity Trusted Solutions Pte Ltd	Issuer organization name.
Country	SG	Issuer country.
Subject DN		
Serial Number	<UUID>	Subject unique serial number.
Given Name	<Given name>	Subject given name.
Surname	<Surname>	Subject surname.
Common Name (CN)	<NRIC / FIN / Passport No.> <Name>	Name = Surname + Given name
Organization (O)	National Digital Identity	
Organization Unit (OU)	SingPass Mobile Authentication	
Country	SG	Subject country.
Subject Public Key	ECDSA 256 bit subject public key	Subject public key.
Signature	<computed signature value>	Certificate computed signature value by issuer.

DOCUMENT SIGNING CERTIFICATE		
Attribute	**Value**	**Description**
Version	3	Certificate format version.
Serial Number	<128bit value>	Certificate unique serial number (auto-generated).
Signature Algorithm	SHA256ECDSA	Cryptographic algorithm used by CA to sign the Certificate.
Signature Hash Algorithm	sha256	Algorithm used to generate the hash
Valid from	<start validity date and time>	Date and time of Certificate issuance.
Valid to	<end validity date and time>	Date and time of Certificate expiration.
Issuer DN		
Common Name (CN)	Singapore NDI Intermediate CA 1 - G1	Issuer CA name.
Organization (O)	Assurity Trusted Solutions Pte Ltd	Issuer organization name.
Country	SG	Issuer country.
Subject DN		
Serial Number	<UUID>	Subject unique serial number.
Given Name	<Given name>	Subject given name.
Surname	<Surname>	Subject surname.
Common Name (CN)	<NRIC / FIN / Passport No.> <Name>	Name = Surname + Given name
Organization (O)	National Digital Identity	
Organization Unit (OU)	SingPass Mobile Digital Signature	
Country	SG	Subject country.
Subject Public Key	ECDSA 256-bit subject public key	Subject public key.
Signature	<computed signature value>	Certificate computed signature value by issuer.

7.1.1 Version Number(s)

All Certificates issued from the CA are X.509 version 3 Certificates.

7.1.2 Certificate Extensions

AUTHENTICATION CERTIFICATE		
Attribute	**Value**	**Description**
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	Certificate type and constraint. This is a critical extension.
Key Usage	Digital Signature Key Encipherment	Certificate key usage/purpose. This is a critical extension.
Extended Key Usage	Client Authentication	Certificate additional key usage/purpose.
Authority Key Identifier	<Issuer Certificate hash value>	
Subject Key Identifier	<Subject Certificate hash value>	
Certificate Policies	CPS=https://www.nca.gov.sg/repository	
Certificate Policy OID	1.2.702.0.1008.1.1	
CRL Distribution Points	URL=http://www.nca.gov.sg/SNICA-G1.crl	
Authority Information Access		
OCSP	URL=http://ocsp.nca.gov.sg	
CA Issuer	URL=http://www.nca.gov.sg/SNICA-G1.cer	

DOCUMENT SIGNING CERTIFICATE		
Attribute	**Value**	**Description**
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	Certificate type and constraint.
Key Usage	Digital Signature Non-Repudiation	Certificate key usage/purpose.
Authority Key Identifier	<Issuer Certificate hash value>	
Subject Key Identifier	<Subject Certificate hash value>	
Certificate Policies	CPS=https://www.nca.gov.sg/repository	
Certificate Policy OID	1.2.702.0.1008.1.10	
CRL Distribution Points	URL=http://www.nca.gov.sg/SNICA-G1.crl	
Authority Information Access		
OCSP	URL=http://ocsp.nca.gov.sg	
CA Issuer	URL=http://www.nca.gov.sg/SNICA-G1.cer	

7.1.3 Algorithm Object Identifiers

Certificates are signed using the following algorithms:

Algorithm	Object Identifier
ECDSAWithSHA256	{iso(1) member-body(2) sg (702) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 2 }

7.1.4 Name Forms

Refer to Section 7.1 Certificate Profile above.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

Certificate	OID
Authentication	1.2.702.0.1008.1.1
Document Signing	1.2.702.0.1008.1.10

7.1.7 Usage Of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

Policy Qualifier extension is used to state the policies (e.g. CP and CPS) under which the Certificate was issued.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

Attribute	Value	Description
Version	2	Certificate format version
Issuer	CN = Singapore NDI Intermediate CA 1 - G1 O = Assurity Trusted Solutions Pte Ltd C = SG	Entity that has signed and issued the CRL
Effective date	CRL issue date	Issuance cate of the CRL
Next update	CRL issue date + 7 days	When the CRL will be next updated
Signature algorithm	sha384ECDSA	Algorithm used to sign the CRL
Signature hash algorithm	sha384	Algorithm used to generate the CRL hash
Revoked Certificates		
Serial number	<revoked Certificate serial number>	Serial number identifying the revoked Certificate
Revocation date	<date and time Certificate revoked>	Date and time of Certificate revocation
CRL reason code	<reason code>	See RFC5280

7.2.1 Version Number(s)

The CA issues version 2 CRLs that conform to RFC 5280.

7.2.2 CRL and CRL Entry Extensions

Attribute	Value	Description
CRL Extension		
Authority Key Identifier	<Issuer Certificate hash value>	
CRL Number	<Running number>	A monotonically increasing sequence number

7.3 OCSP Profile

Attribute	Value	Description
Version	3	Certificate format version.
Serial Number	<128bit value>	Certificate unique serial number (auto-generated).
Signature Algorithm	sha384ECDSA	Cryptographic algorithm used by CA to sign the Certificate.
Signature hash algorithm	sha384	Algorithm used to generate the hash
Valid from	<start validity date and time>	Date and time of the Certificate issuance.
Valid to	<end validity date and time>	Date and time of the Certificate expiration.
Issuer DN		
Common Name (CN)	Root CA OCSP Singapore National Root CA – G1 Issuer CA OCSP Singapore NDI Intermediate CA 1 - G1	CA that issued the OCSP certificate
Organization (O)	Assurity Trusted Solutions Pte Ltd	Issuer organization name.
Country	SG	Issuer country.
Subject DN		
Common Name (CN)	Root CA OCSP Singapore National Root CA OCSP Responder 1 – G1 Issuer CA OCSP Singapore NDI Intermediate CA OCSP Responder 1 - G1	OCSP certificate common name
Organization (O)	Assurity Trusted Solutions Pte Ltd	
Country	SG	Subject country.
Subject Public Key	ECDSA 384 bit	Subject public key.
Signature	<computed signature value>	Certificate computed signature value by issuer.

7.3.1 Version Number(s)

The CA's OCSP responders conform to version 3 of RFC 6960.

7.3.2 OCSP Extensions

Attribute	Value	Description
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	Certificate type and constraint.
Key Usage	Digital Signature	Certificate key usage/purpose.
Extended Key Usage	OCSP Signing	Certificate additional key usage/purpose.
Authority Key Identifier	<Issuer Certificate hash value>	
Subject Key Identifier	<Subject Certificate hash value>	
Certificate Policies	CPS=https://www.nca.gov.sg/repository	
Certificate Policy OID	Root CA OCSP 1.2.702.0.1008.1.101 Issuer CA OCSP 1.2.702.0.1008.1.101	
OCSP No Revocation Check	<Must be present>	

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Types of Assessment

The practices in this CPS are designed to meet or exceed:

1. CA accreditation requirements of the Info-communications Media Development Authority ("**IMDA**"), issued by the Controller;
2. applicable laws e.g. applicable provisions of the Electronic Transactions Act (Cap. 88) and Electronic Transactions (Certification Authorities) Regulations 2010 (S650/2010); and
3. industry standards such as CA/Browser Forum – Baseline Requirements for the Issuance and Management of Publicly – Trusted Certificates.

8.2 Frequency or Circumstances of Assessment

The audit, conducted by an independent third party auditor, to assess the CA's compliance with IMDA's CA accreditation requirements is conducted every 2 years.

8.3 Identity/Qualifications of Assessor

Auditors must be from a reputable and competent firm that possesses the necessary qualification and experience to conduct an assessment in accordance to the Compliance Audit Checklist for CA accreditation set forth by the Controller.

8.4 Assessor's Relationship to Assessed Entity

The CA uses an independent and qualified external third party auditing firm that does not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against the CA.

8.5 Topics Covered by Assessment

The audit conforms to the Compliance Audit Checklist for CA accreditation set forth by the Controller and covers the CA's business practices disclosure and the adherence of the CA's operations to this CPS.

8.6 Actions Taken as a Result Of Deficiency

If an audit reports any material non-compliance with applicable laws, this CPS, or any other contractual obligations related to the CA, then

1. the auditor will document the findings;
2. the auditor will promptly notify the CA; and
3. the CA will develop a remediation plan to comply with this CPS. The CA's PKIPA may review the findings, accept the findings as non-material or submit a plan to comply with this CPS, which may require additional actions if necessary, to rectify any significant issues raised.

8.7 Communication of Results

The results of each audit are reported to the CA's PKIPA only. The CA shall furnish a copy to any third-party entities which are mandated by law, regulation, or agreement to receive a copy of the audit results.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

The CA currently does not impose any fees on Subscribers and Relying Parties for its services. However, the CA reserves its right to impose such fees in the future.

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

The CA maintains insurance coverage for its potential liabilities arising from its CA services.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

The CA's warranty coverage for end-entities is specified in its Subscriber Agreement and Relying Party Agreement.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following non-exhaustive types of information are confidential to the CA:

1. CA's Private Keys;
2. Activation Data used to access Private Keys;
3. personal information of Subscribers (not including such information as may be publicly available on the Subscriber's Certificate);
4. internal documentation relating to the CA's operations;
5. security practices used to protect the confidentiality, integrity, or availability of information;
6. audit logs and archived records, including Certificate application records and documentation submitted in support of Certificate applications whether successful or rejected; and
7. transaction records, financial audit records, and external or internal audit trail records and any audit reports.

The following, non-exhaustive types of information are confidential to the RA:

1. personal information of Subscribers (not including such information as may be publicly available on the Subscriber's Certificate);
2. internal documentation on the RA's operations;
3. security practices used to protect the confidentiality, integrity, or availability of information;
4. audit logs and archived records, including Certificate application records and documentation submitted in support of Certificate applications whether successful or rejected; and
5. transaction records, financial audit records, and external or internal audit trail records and any audit reports.

9.3.2 Information Not Within the Scope of Confidential Information

All information published on the CA's Repository is public information.

9.3.3 Responsibility to Protect Confidential Information

The CA's employees, agents, and contractors are contractually obligated and responsible for protecting confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The CA will collect, use and disclose personal data in accordance with its obligations under the Singapore Personal Data Protection Act 2012 (Act 26 of 2012) ("**PDPA**"). Please refer to the CA's Privacy Statement available at http://www.assurity.sg/privacy.html (as may be amended from time to time) for more details.

9.4.2 Information Treated as Private

In this CPS, "*personal data*" has the same meaning as "*personal data*" as defined in the Singapore Personal Data Protection Act 2012 (Act 26 of 2012).

9.4.3 Information Not Deemed Private

Please refer to Section 9.4.1 Privacy Plan above.

9.4.4 Responsibility to Protect Private Information

Please refer to Section 9.4.1 Privacy Plan above.

9.4.5 Notice and Consent to Use Private Information

Please refer to Section 9.4.1 Privacy Plan above.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Please refer to Section 9.4.1 Privacy Plan above.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

The CA owns all intellectual property rights, without limitation, to the following:

1. this CPS and CP;
2. Certificates;
3. revocation information;
4. the CA's logos, trademarks and service marks;
5. the Root CA and Issuer CA Key Pairs; and
6. the Root CA and Issuer CA Certificates.

The CA does not allow derivative works of its Certificates or products without prior agreement. The CA retains all intellectual property rights in the Certificates, including the Key Pairs.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The CA's representations and warranties are limited to those as expressly set out in the relevant agreement entered into between the CA and such Subscriber or Relying Party.

9.6.2 RA Representations and Warranties

The CA shall require RAs operating on their behalf to represent that they have followed this CPS and the relevant CP when participating in the issuance and management of Certificates.

9.6.3 Subscriber Representations 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.

Without prejudice to the above, each Relying Party warrants that it will:

1. only use or rely on a Certificate for uses that are consistent with the key usage extension fields stated in the Certificate;
2. not use or rely on a Certificate:
    a. unless it has:
        i. determined for itself that its use or reliance on such Certificate is reasonable and appropriate under the given circumstances, including considering:
            1. the nature and economic value of the transaction and the level of risk in light of the attributes of such Certificate and the level of assurance of identity and authentication of the Subscriber provided by such Certificate as described in the CP and/or CPS;
            2. the potential loss or damage that would be caused by an erroneous reliance or identification or a loss of confidentiality or privacy of information, or unenforceability of the transaction;
            3. its previous course of dealing with the Subscriber (if any); and
            4. any other indicia of reliability or unreliability pertaining to the Subscriber or the application, communication, or transaction;
        ii. checked such Certificate (including referencing the CRL and OCSP responses) to determine if such Certificate is valid and is not expired, revoked or suspended; and
        iii. acted in good faith and reasonably having regard to the circumstances when using or relying on such Certificate;
    b. for hazardous or unlawful (including tortious) activities; and
    c. in relation to the access or operation of critical infrastructure systems such as but not limited to the operation of nuclear facilities, aircraft control, navigation, or communication systems, weapon control systems or any other system requiring fail-safe operation where reliance on a Certificate could lead to death, personal injury, or severe environmental damage;
3. not:

a. remove, circumvent, impair, bypass, disable or otherwise interfere with security-related features of the Certificate and Repository, including but not limited to any features that prevent or restrict access or use of any particular functionalities or features of it;
b. use, transmit or upload (as the case may be), any device, software, exploits, routine, or malware, including but not limited to any viruses, Trojan horses, worms, time bombs, robots, data-mining or data scraping tools or cancel bots that may introduce security vulnerabilities, damage or interfere with the proper operation of the Certificate or Repository or that may intercept or expropriate any content or personal data from the Certificate, Repository, or any related services, software, data or other materials provided by the CA; and
c. use the Certificate or Repository or any related services, software, data or other materials provided by the CA in any manner that could damage, disrupt, disable, overburden, or impair its operation or use.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

EXCEPT AS PROVIDED IN SECTION 9.6.1 ABOVE, THE CA EXPRESSLY DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, IN RELATION TO THIS CPS, ANY CERTIFICATES OR THE INFORMATION PROVIDED WITH RESPECT TO THE CERTIFICATES OR THE REPOSITORY, THE KEY PAIRS, THE PARTICIPATION OF ANY SUBSCRIBER, RELYING PARTY OR ANY OTHER PKI PARTICIPANT OR ANY RELATED SERVICES, SOFTWARE, DATA OR OTHER MATERIALS PROVIDED BY THE CA, AND HEREBY DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES OF ANY KIND TO YOU OR ANY THIRD PARTY, WHETHER ARISING FROM USAGE OR CUSTOM OR TRADE OR BY OPERATION OF LAW OR OTHERWISE, INCLUDING BUT NOT LIMITED TO ANY REPRESENTATIONS OR WARRANTIES AS TO THE ACCURACY, COMPLETENESS, CORRECTNESS, CURRENCY, TIMELINESS, RELIABILITY, AVAILABILITY, INTEROPERABILITY, SECURITY, NON-INFRINGEMENT, TITLE, MERCHANTABILITY, SATISFACTORY QUALITY OR FITNESS FOR ANY PARTICULAR PURPOSE OF THIS CPS, ANY CERTIFICATES OR THE INFORMATION PROVIDED WITH RESPECT TO CERTIFICATES OR THE REPOSITORY, THE KEY PAIRS, THE PARTICIPATION OF ANY SUBSCRIBER, RELYING PARTY OR ANY OTHER PKI PARTICIPANT OR ANY RELATED SERVICES, SOFTWARE, DATA OR OTHER MATERIALS PROVIDED BY THE CA.

EXCEPT AS PROVIDED IN SECTION 9.6.1 ABOVE, THE CA FURTHER DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, TO ANY APPLICANT, SUBSCRIBER OR ANY RELYING PARTY:

1. THAT ANY CRYPTOGRAPHIC TECHNIQUES OR METHODS USED IN CONDUCTING ANY ACT, TRANSACTION, OR PROCESS INVOLVING OR UTILIZING A CERTIFICATE IS RELIABLE;
2. AS TO THE "NON-REPUDIATION" OF ANY CERTIFICATE, KEY PAIR, OR MESSAGE OR THE "NON-REPUDIATION" BY A SUBSCRIBER AND/OR RELYING PARTY OF ANY TRANSACTION ENTERED INTO BY THE SUBSCRIBER AND/OR RELYING PARTY INVOLVING THE USE OF OR RELIANCE UPON A CERTIFICATE (BECAUSE NON-REPUDIATION IS DETERMINED, AMONG OTHER THINGS, BY LAW); AND
3. THE STANDARDS OR PERFORMANCE OF ANY EQUIPMENT, SYSTEM OR SOFTWARE USED IN CONNECTION WITH THE CERTIFICATES, REPOSITORY, THE KEY PAIRS OR ANY RELATED HARDWARE OR SOFTWARE, WHICH ARE NOT UNDER EXCLUSIVE OWNERSHIP OR CONTROL OF OR WHICH ARE LICENSED TO THE CA, INCLUDING BUT NOT LIMITED TO ANY ELECTRONIC TERMINAL, SERVER OR SYSTEM, OR TELECOMMUNICATION OR OTHER COMMUNICATIONS NETWORK OR SYSTEM.

9.8 Limitations of Liability

9.8.1 Applicable to All Certificates

The limitations of liability of the CA in respect of each Subscriber and Relying Party shall be as set out in the Subscriber Agreement and Relying Party Agreement, respectively.

9.8.2 Recommended Reliance Limit

The CA's reliance limit shall mean its maximum liability for any and all claims, suits, demands, actions or other legal proceedings as specified under the Subscriber Agreement and Relying Party Agreement, as the case may be (under the clause titled "*Limitation of Liability*" (or such equivalent heading), as may be amended from time to time).

The CA's liability for any use of or reliance on any Certificate is strictly to be limited to (a) Subscribers who have agreed to be bound by the Subscriber Agreement; (b) and Relying Parties who have agreed to be bound by the Relying Party Agreement. In all other cases, the CA shall not be liable for any damage or loss of any kind, whether foreseeable or not, whatsoever and howsoever caused (whether in contract, tort (including negligence), breach of a statutory duty or in any other way), even if the CA has been advised of the possibility of such damages.

9.9 Indemnities

Indemnities required of each Subscriber and Relying Party shall be as set out in the Subscriber Agreement and Relying Party Agreement, respectively.

9.10 Term and Termination

9.10.1 Term

This CPS and any amendments thereto are effective when published to the CA's online Repository and remain in effect until replaced with a newer version.

9.10.2 Termination

This CPS and any amendments thereto remain in effect until replaced by a newer version.

9.10.3 Effect of Termination and Survival

This CPS and any amendments thereto remain in effect until replaced by a newer version, upon which such newer version shall apply in full force and effect in respect of all Subscribers, Applicants, Relying Parties and other participants (including with regards all Certificates issued pursuant to such earlier version of the CPS).

9.11 Individual Notices and Communications with Participants

The CA will use commercially reasonable methods to communicate with Subscribers, Applicants, Relying Parties and other participants through the RA.

9.12 Amendments

9.12.1 Procedure for Amendment

The CA's PKIPA determines revisions to this CPS from time to time as standards or business requirements changes. The CPS is reviewed at least annually. An updated version of this CPS will be uploaded to the online Repository upon the CA's PKIPA's approval.

9.12.2 Notification Mechanism and Period

Notification of amendments to this CPS are made by posting an updated version of the CPS to the online Repository from time to time.

9.12.3 Circumstances Under Which OID Must Be Changed

No stipulation.

9.13 Dispute Resolution Provisions

Any dispute, difference, or claim between any participants arising out of or in connection with this CPS (including any question regarding its existence, validity, or termination) shall be resolved by reference to arbitration, with the CA having the option of electing to refer the dispute to the Courts of the Republic of Singapore.

Where the CA is a defendant or respondent, the CA shall be given notice by the complainant before the commencement of any legal action against the CA to enable the CA to elect to have the dispute submitted to arbitration. The CA may, at its sole discretion, elect to have any dispute referred to a court by written notice to the participant(s) involved and shall make the election within thirty (30) days of receipt of the complainant's written notice. The complainant's written notice shall:

1. state the specific dispute, difference, or claim to be resolved and the nature of such dispute, difference, or claim; and
2. include a request that the CA makes an election whether the dispute, difference, or claim as stated shall be resolved by reference to arbitration or by court proceedings.

Should the CA fail to make the election to have the dispute referred to a court within thirty (30) days of the receipt of the written notice, the dispute, difference or claim shall be resolved by arbitration. The CA may elect to refer to arbitration all or any part of the dispute or difference as stated by the complainant in its written notice.

Where the dispute is referred to arbitration, it shall be administered by the Singapore International Arbitration Centre ("**SIAC**") in Singapore in accordance with the Arbitration Rules of the SIAC ("**SIAC Rules**") for the time being in force, which rules are deemed to be incorporated by reference in this Clause. Further:

1. the seat of the arbitration shall be Singapore;
2. the tribunal shall consist of one (1) arbitrator to be agreed upon in accordance with the SIAC Rules, save that if no agreement is reached within thirty (30) days after receipt by one party of such a proposal from the other, the arbitrator shall be appointed by the Chairman of the SIAC;
3. the language of the arbitration shall be English; and
4. all information, pleadings, documents, evidence and all matters relating to the arbitration shall be confidential.

Any reference to arbitration under this Section shall be a submission to arbitration within the meaning of the Arbitration Act (Cap. 10) for the time being in force. The application of Part II of the International Arbitration Act (Cap. 143A), and the Model Law referred thereto, to this Agreement is hereby expressly excluded.

9.14 Governing Law

This CPS 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 accept and agree to use Certificates in compliance with all applicable laws and regulations. The CA may refuse to issue or may revoke Certificates if it is in the reasonable opinion, such issuance or the use of such Certificates would violate applicable laws and regulations.

9.16 Miscellaneous Provisions

No stipulation.