THE CERTIFICATION PRACTICE STATEMENT

for

SINGPASS ACCOUNT (INDIVIDUAL) CERTIFICATES

of

GOVERNMENT TECHNOLOGY AGENCY

as

CERTIFICATION AUTHORITY

History Log

Version	Date	Description
1.0	20 August 2024	First release
2.0	20 January 2025	Version 2.0 release Added new type of Certificate issued by the CA (i.e. the Signing Certificate). Changes made to the following sections to describe the issuance of Signing Certificates: (a) Added Section 1.4.1(b) to reflect that a Subscriber may be issued a Signing Certificate. (b) Updated Section 3.2.3 to include processes for Authentication of Individual Identity for the issuance of a Signing Certificate. (c) Updated Section 7.1 to add the Certificate Profile and Certificate Extensions for Signing Certificates.
2.1	30 June 2025	Version 2.1 release Removed references to the use of ATS Authentication Certificates issued by Assurity Trusted Solutions Pte. Ltd.

Contents

1 INTRODUCTION

1.1 Overview

This Certification Practice Statement ("**CPS**") describes the certification policies, procedures and practices that apply to Certificates within the class of Certificates referred to as Singpass Account (Individual) Certificates.

This CPS is structured in accordance with the Internet Engineering Task Force 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 "Not applicable" 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 from the CA's 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 Certification Practice Statement for Singpass Account (Individual) Certificates, Version 2.1, effective date 30 June 2025, OID 1.2.702.0.1009.100.1.

1.3 PKI Participants

1.3.1 Certification Authorities

The Certification Authority is Government Technology Agency (UEN: T16GB0002G), a body corporate established under the Government Technology Agency Act 2016 and having its office at 10 Pasir Panjang Road, #10-01 Mapletree Business City, Singapore 117438 (the "**Certification Authority**" or "**CA**").

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 issues Certificates to the Issuer CA, and the Issuer CA issues Certificates to the Subscribers.

Issuance of Certificates to Issuer CA by Root CA: The Root CA [Singapore National Root CA – B1] issues Certificates to the following Issuer CAs:

(a) Issuer CA [Singapore NDI Intermediate CA 1 – B1]; and
(b) Issuer CA [Singapore NDI Intermediate CA 1 – B2].

Issuance of Certificates to Subscribers by Issuer CA: The Issuer CA [Singapore NDI Intermediate CA 1 – B1] and Issuer CA [Singapore NDI Intermediate CA 1 – B2] issues Certificates to Subscribers in accordance with this CPS. In this CPS, the term "Certificate" refers to such directly aforementioned Certificate, excluding Certificates issued to Issuer CAs or unless the context indicates otherwise.

The CA's PKIPA 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 (excluding the Government Technology Agency of Singapore, to the extent that it is performing its role as a CA). The RA will be performing its RA role using Singpass.

1.3.3 Subscribers

Applicant applies to the Issuer CA through the RA for the issuance of a Certificate. Upon a successful Certificate application, the Applicant becomes a Subscriber. The subject of a Certificate is the party so named in that Certificate.

At present, the Issuer CA only issues Certificates to natural persons who are Specified Individuals.

1.3.4 Relying Parties

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

1.3.5 Other Participants

Not applicable.

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.

1.4.1 Appropriate Certificate Uses

A Subscriber may only be issued the following Certificates by the Issuer CA pursuant to this CPS:

(a) the Authentication Certificate: a Certificate used by the Subscriber to Authenticate the Subscriber's identity to gain access to protected resources, e.g. logging into an electronic service; and

(b) the Signing Certificate: a Certificate used by the Subscriber to facilitate the electronic signing of documents and transactions.

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

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

Requests can also be made via our website at https://www.singpass.gov.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 natural person who is a Specified Individual that (a) applies for a Certificate but has not been issued with that Certificate; or (b) applies for a new Certificate before the expiry of the Certificate that has been previously issued.

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 this CPS.

Certificate Policy or 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 or CSR: A message conforming to PKCS #10 specification, in which an Applicant submits a request to a CA, 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.

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 2010 as appointed pursuant to Section 27 of the Electronic Transactions Act 2010.

Intermediate (or Issuer) CA: A CA that exists in the middle of a trust chain between the Root CA and the Subscribers' 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 recognised standards organization for a specific object or object class.

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 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.

PKI: Public Key Infrastructure.

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. 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: Any person or entity (including any company or association or body of persons, corporate or unincorporated) 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 Repository.

Repository: The CA's repository which is accessible at https://repository.nca.gov.sg/.

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.

Singpass: The electronic identification, authentication, or authorisation service of the Government of Singapore known as "*Singpass*" through such devices, websites, channels or platform, as may be designated by the Government of Singapore and Government Technology Agency of Singapore from time to time, provided upon the Singpass Terms of Use.

Singpass Account: The account which the Applicant has for the purposes of Singpass.

Singpass app: The mobile application designed to, amongst other things, be used as an authentication form factor, known as "*Singpass*", from the following approved online stores: (a) the official Apple App Store accessible at https://www.apple.com/sg/ios/app-store or such other successor site; (b) the official Google Play accessible at https://play.google.com or such other successor site; (c) the official HUAWEI AppGallery accessible at https://appgallery.huawei.com; and (d) such other websites as may be specified by the Government of Singapore and/or Government Technology Agency of Singapore from time to time.

Singpass Face Verification: The biometrics identification, authentication and authorisation service of the Government of Singapore and Government Technology Agency of Singapore that utilises facial recognition technology, as further described under Annex 1 of the Singpass Terms of Use.

Singpass Terms of Use: The terms of use of Singpass which is accessible at https://www.singpass.gov.sg/home/ui/terms-of-use or such other successor site.

Singpass Password: The valid password that the Applicant uses in conjunction with the Singpass Username to access Singpass or other password-protected or secure areas of Singpass.

Singpass Username: The unique login identification name or code which identifies the Applicant for purposes of Singpass.

Singpass Website: The website of Singpass which is accessible at www.singpass.gov.sg or such other successor site.

Specified Individual: This is a natural person who is a Singapore citizen or resident with a Singapore National Identity Number ("**NID**"). The NID is the National Registration Identity Card Number ("**NRIC**") or Foreign Identification Number ("**FIN**").

Subscriber: A natural person who is a Specified Individual 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 as specified in the Subscribers' Certificates. 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 (in the case of the Root CA Certificate and Issuer CA Certificate) and the URLs specified in the Subscriber's Certificates (in the case of the CRL and OSCP responses) 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 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, CP, Subscriber Agreement(s) or Relying Party Agreement(s) are published after the CA's policy authority's approval. 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 Repository are public information, internationally available and unrestricted. The CA has implemented appropriate security controls to prevent unauthorised write access to its Repository.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

The Issuer CA issues Certificates with a non-null subject Distinguished Name ("**DN**").

3.1.2 Need for Names to Be Meaningful

The Issuer CA uses DNs that identify both the subject and issuer of the Certificate. Refer to Section 7 for detailed attributes of Certificate's DN.

3.1.3 Anonymity or Pseudonymity of Subscribers

The CA does not issue Certificates for Internationalised Domain Names or Punycode version; and does not issue 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 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 using a combination of subject DN attributes. Refer to Section 7 for subject DN attributes.

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 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 must use the Singpass app to make a Certificate Request. After the RA successfully performs the Authentication of Individual Identity under Section 3.2.3, a personalized generated Key Pair is installed on the Applicant's Singpass app. 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.

At present, an Applicant is not permitted to act through one or more agents to make a Certificate Request.

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

Prior to an Applicant making a Certificate Request, the Applicant must have:

(a) a valid Singpass Account[1]; and

(b) the Singpass app installed on the Applicant's device.

Authentication Certificate

For a Certificate Request for an Authentication Certificate, RA authenticates an Applicant's identity using any process which the RA may determine from time to time, which may include but is not limited to any one of the following processes, whether through the Singpass app or otherwise:

(a) requiring the Applicant to login to the Applicant's Singpass Account using the Singpass Username and Singpass Password and using any one of the following second-factor authentication methods:

    (i) sending a SMS One-Time Password to the Applicant's mobile number that is registered under the Applicant's Singpass Account, and requiring that such SMS One-Time-Password be correctly inputted in the Applicant's Singpass app within the stipulated timeframe;

    (ii) sending a further activation PIN mailer to the Applicant's Registered Address, and requiring that such PIN contained in the PIN mailer be correctly inputted in the Applicant's Singpass app within the stipulated timeframe; or

    (iii) Singpass Face Verification, by comparing the unique collection of data measurements of the Applicant's face captured "*live*" electronically via the

[1] A valid Singpass Account is one which is not terminated and not dormant.

Singpass app against such Applicant's facial data (which may include facial geometry, facial profiles and templates) previously enrolled with the RA; or

(b) where a Certificate Request is for a new Authentication Certificate before the expiry of the Authentication Certificate that has been previously issued, the RA may Authenticate the identity of an Applicant using the Authentication Certificate that has been previously issued.

Signing Certificate

The Applicant must possess an Authentication Certificate to submit a Certificate Request for a Signing Certificate.

RA Authenticates the identity of an Applicant of a Signing Certificate by any one of the following processes:

(a) through the Singpass app using the Authentication Certificate; or

(b) using the process that the RA uses to Authenticate an Applicant's identity for a Certificate Request for an Authentication Certificate.

After the RA Authenticates an Applicant's identity using the Authentication Certificate, the RA provides the identity information of the Authenticated Applicant for the CSR.

3.2.4 Non-Verified Subscriber Information

Not applicable.

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

Not applicable.

3.3 Identification and Authentication for Re-Key Requests

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

3.3.1 Identification and Authentication for Routine Rekey

Not applicable.

3.3.2 Identification and Authentication for Rekey After Revocation

Not applicable.

3.4 Identification and Authentication for Revocation Request

RA Authenticates a Subscriber's identity when a Subscriber logs into the Singpass Website to request for revocation of Certificates by deactivating the Singpass app.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

At present, only the Applicant who is a Specified Individual 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:

(a) Subscriber is required to accept and agree to the Subscriber Agreement (as may be amended from time to time) on the Singpass app;

(b) Subscriber generates Subscriber Key Pair on the Singpass app;

(c) RA delivers a CSR (including the Subscriber's Public Key) to the Issuer CA; and

(d) 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 Singpass app in a secure manner within a reasonable time. The Certificate is automatically installed on the Subscriber's device on which the Singpass app is installed. Upon successful issuance of the Certificate, the Singpass app 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 Singpass app.

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 or under Section 9.6.4.

4.6 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).

4.6.1 Circumstances for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.7 Certificate Re-Key

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

Not applicable.

4.7.2 Who May Request Certification of a New Public Key

Not applicable.

4.7.3 Processing Certificate Re-Keying Requests

Not applicable.

4.7.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Not applicable.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Not applicable.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.8 Certificate Modification

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

4.8.1 Circumstances for Certificate Modification

Not applicable.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

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

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

The Subscriber may request for the revocation of Certificates through the RA via the Singpass Website to deactivate the Singpass app. The Certificates will be revoked after the deactivation of the Singpass app.

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

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

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

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

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

(e) the Subscriber is deceased;

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

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

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

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

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

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

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

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

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

(o) the Subscriber is no longer entitled to hold the Certificate as the Subscriber does not have a valid Singpass Account.

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

4.9.2 Who Can Request Revocation

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

4.9.3 Procedure for Revocation Request

The Subscriber may request for the revocation of Certificates through the RA via the Singpass Website to deactivate the Singpass app. The Certificates will be revoked after the deactivation of the Singpass app.

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

Not applicable.

4.9.5 Time within Which CA Must Process the Revocation Request

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

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 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

Not applicable.

4.9.12 Special Requirements Regarding Key Compromise

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

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

4.9.13 Circumstances for Suspension

Not Applicable

4.9.14 Who Can Request Suspension

Not Applicable

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

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

Not applicable.

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

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

5.1 Physical Security Controls

Refer to the Certificate Policy.

5.2 Procedural Controls

Refer to the Certificate Policy.

5.3 Personnel Controls

Refer to the Certificate Policy.

5.4 Audit Logging Procedures

Refer to the Certificate Policy.

5.5 Records Archival

Refer to the Certificate Policy.

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

Refer to the Certificate Policy.

5.8 CA Termination

Before terminating its CA activities, the CA will:

(a) provide notice and information about the cessation of CA operations to its customers, Subscribers, and Relying Parties by sending emails or through such other reasonable method(s); and

(b) 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 or all Issuer CA 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

Refer to the Certificate Policy.

6.1.2 Private Key Delivery to Subscriber

Subscriber's Private Key is automatically generated on the Subscriber's device on which the Singpass app 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

Refer to the Certificate Policy.

6.1.6 Public Key Parameters Generation and Quality Checking

Refer to the Certificate Policy.

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.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Refer to the Certificate Policy.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The CA archives its Public Keys.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Root CA and Issuer CA Certificates have a validity period of 20 years and 10 years, respectively.

Certificates issued to Subscribers shall have a validity period as follows:

(a) Certificates issued to Subscribers by Issuer CA [Singapore NDI Intermediate CA 1 – B1] have a validity period of 1 year; and
(b) Certificates issued to Subscribers by Issuer CA [Singapore NDI Intermediate CA 1 – B2] have a validity period of 1 year.

6.4 Activation Data

Refer to the Certificate Policy.

6.5 Computer Security Controls

Refer to the Certificate Policy.

6.6 Life Cycle Technical Controls

Refer to the Certificate Policy.

6.7 Network Security Controls

Refer to the Certificate Policy.

6.8 Time-Stamping

Refer to the Certificate Policy.

7 CERTIFICATE, CRL, AND OCSP PROFILES

Applicants who are Specified Individuals may be issued Certificates from the following Issuer CAs:

(a) Singapore NDI Intermediate CA 1 – B1; and

(b) Singapore NDI Intermediate CA 1 – B2.

7.1 Certificate Profile

(a) Certificates issued by Issuer CA [Singapore NDI Intermediate CA 1 – B1]

AUTHENTICATION CERTIFICATE		
Attribute	**Value**	**Description**
Version	V3	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 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 - B1	Name of Issuer CA.
Organization (O)	Government Technology Agency	Organization of the Issuer CA.
Country	SG	Country of the Issuer CA.
Subject DN		
Serial Number	<UUID>	Unique serial number linking the Subscriber to the Subscriber's Singpass Account.
Given Name	<Given name>	Subscriber's given name provided by the RA.
Surname	<Surname>	Subscriber's surname provided by the RA.
Common Name (CN)	<Either NRIC or FIN > <Name>	<Either NRIC or FIN> - The NID number of the Subscriber provided by the RA. <Name> - Full name of the Subscriber provided by the RA.
Organization (O)	Singpass	-
Organization Unit (OU)	Singpass Account (Individual)	-
Organization Unit (OU)	Authentication Certificate	-
Country	SG	Country of the Subscriber.
Subject Public Key	ECDSA 256 bit subject public key	Public Key of the Subscriber.
Signature	<computed signature value>	Certificate computed signature value by Issuer CA.

(b) Certificates issued by Issuer CA [Singapore NDI Intermediate CA 1 – B2]

SIGNING CERTIFICATE		
Attribute	**Value**	**Description**
Version	V3	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 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 - B2	Name of Issuer CA.
Organization (O)	Government Technology Agency	Organization of the Issuer CA.
Country	SG	Country of the Issuer CA.
Subject DN		
Serial Number	<UUID>	Unique serial number linking the Subscriber to the Subscriber's Singpass Account.
Given Name	<Given name>	Subscriber's given name provided by the RA.
Surname	<Surname>	Subscriber's surname provided by the RA.
Common Name (CN)	<Name>	<Name> - Full name of the Subscriber provided by the RA.
Organization (O)	Singpass	-
Organization Unit (OU)	Singpass Account (Individual)	-
Organization Unit (OU)	Signing Certificate	-
Country	SG	Country of the Subscriber.
Subject Public Key	ECDSA 256-bit subject public key	Public Key of the Subscriber.
Signature	<computed signature value>	Certificate computed signature value by Issuer CA.

7.1.1 Version Number(s)

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

7.1.2 Certificate Extensions

(a) Certificates issued by Issuer CA [Singapore NDI Intermediate CA 1 – B1]

AUTHENTICATION CERTIFICATE		
Attribute	**Value**	**Description**
Basic Constraints	critical CA: FALSE	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	TLS Web Client Authentication	Certificate additional key usage/purpose.
Authority Key Identifier	<Issuer CA Certificate hash value>	
Subject Key Identifier	<Subscriber Certificate hash value>	
Certificate Policies	CPS=https://repository.nca.gov.sg	
Certificate Policy OID	1.2.702.0.1009.100.1	
CRL Distribution Points	URL=http://crl.nca.gov.sg/crl/<CA-ID>.crl	
Authority Information Access		
OCSP	URL=http://ocsp2.nca.gov.sg	

(b) Certificates issued by Issuer CA [Singapore NDI Intermediate CA 1 – B2]

SIGNING CERTIFICATE		
Attribute	**Value**	**Description**
Basic Constraints	critical CA: FALSE	Certificate type and constraint. This is a critical extension.
Key Usage	Digital Signature Non-Repudiation	Certificate key usage/purpose. This is a critical extension.
Authority Key Identifier	<Issuer CA Certificate hash value>	
Subject Key Identifier	<Subscriber Certificate hash value>	
Certificate Policies	CPS=https://repository.nca.gov.sg/	
Certificate Policy OID	1.2.702.0.1009.100.1	
CRL Distribution Points	URL=http://crl.nca.gov.sg/crl/<CA-ID>.crl	
Authority Information Access		
OCSP	URL=http://ocsp2.nca.gov.sg	

7.1.3 Signature Algorithm

Certificates are signed using one of the following algorithms:

(a) ECDSAWithSHA256

(b) ECDSAWithSHA384

(c) ECDSAWithSHA512

7.1.4 Name Forms

Refer to Section 7.1 Certificate Profile above.

7.1.5 Name Constraints

Not applicable.

7.1.6 Certificate Policy Object Identifier

Object	OID
CPS for Singpass Account (Individual) Certificates	1.2.702.0.1009.100.1

7.1.7 Usage Of Policy Constraints Extension

Not applicable.

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

Not applicable.

7.2 CRL Profile

(a) CRL for Singapore NDI Intermediate CA 1 – B1

Attribute	Value	Description
Version	2	Certificate format version
Issuer	CN = Singapore NDI Intermediate CA 1 – B1 O = Government Technology Agency C = SG	Entity that has signed and issued the CRL
Effective date	CRL issue date	Issuance date of the CRL
Next update	CRL next update date	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

(b) CRL for Singapore NDI Intermediate CA 1 – B2

Attribute	Value	Description
Version	2	Certificate format version
Issuer	CN = Singapore NDI Intermediate CA 1 – B2 O = Government Technology Agency C = SG	Entity that has signed and issued the CRL
Effective date	CRL issue date	Issuance date of the CRL
Next update	CRL next update date	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

Currently, the OCSP is signed directly by the Root CA and Issuer CA.

7.3.1 Version Number(s)

The CA's OCSP responders conform to RFC 5019.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Types of Assessment

The CA conducts compliance audit at such frequency as may be required under the Governing Law.

8.2 Frequency or Circumstances of Assessment

Refer to Section 8.1 above.

8.3 Identity/Qualifications of Assessor

An auditor performing compliance audit shall have such qualifications as required under the Governing Law.

8.4 Assessor's Relationship to Assessed Entity

The auditor performing compliance audit shall meet such independence requirements as required under the Governing Law.

8.5 Topics Covered by Assessment

The compliance audit shall cover such topics as may be required under the Governing Law.

8.6 Actions Taken as a Result of Deficiency

The CA will take appropriate measures to address any shortcomings identified through the compliance audit.

8.7 Communication of Results

The results of each assessment are reported to the CA's PKIPA. The CA will 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

Not applicable.

9.1.2 Certificate Access Fees

Not applicable.

9.1.3 Revocation or Status Information Access Fees

Not applicable.

9.1.4 Fees for Other Services

Not applicable.

9.1.5 Refund Policy

Not applicable.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Not applicable.

9.2.2 Other Assets

Not applicable.

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:

(a) CA's Private Keys;

(b) personal information of Subscribers (not including such information as may be publicly available on the Subscriber's Certificate);

(c) internal documentation relating to the CA's operations;

(d) security practices used to protect the confidentiality, integrity, or availability of information;

(e) audit logs and archived records, including Certificate application records and documentation submitted in support of Certificate applications whether successful or rejected; and

(f) 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:

(a) personal information of Subscribers (not including such information as may be publicly available on the Subscriber's Certificate);

(b) internal documentation on the RA's operations;

(c) security practices used to protect the confidentiality, integrity, or availability of information;

(d) audit logs and archived records, including Certificate application records and documentation submitted in support of Certificate applications whether successful or rejected; and

(e) 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 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 all applicable laws and regulations. Please refer to the CA's Privacy Statement available at https://repository.nca.gov.sg/ (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.

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

Not applicable.

9.5 Intellectual Property Rights

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

(a) this CPS and CP;

(b) Certificates;

(c) revocation information;

(d) the CA's logos, trademarks and service marks;

(e) the Root CA and Issuer CA Key Pairs; and

(f) 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:

(a) only use or rely on a Certificate for uses that are consistent with the key usage extension fields stated in the Certificate;

(b) not use or rely on a Certificate:

(i) 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;

(ii) for hazardous or unlawful (including tortious) activities; and

(iii) 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; and

(c) not:

(i) 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;

(ii) 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

(iii) 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

Not applicable.

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:

(a) THAT ANY CRYPTOGRAPHIC TECHNIQUES OR METHODS USED IN CONDUCTING ANY ACT, TRANSACTION, OR PROCESS INVOLVING OR UTILIZING A CERTIFICATE IS RELIABLE;

(b) 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

(c) 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; and (b) 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 change. 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

Not applicable.

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:

(a) state the specific dispute, difference, or claim to be resolved and the nature of such dispute, difference, or claim; and

(b) 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:

(a) the seat of the arbitration shall be Singapore;

(b) 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;

(c) the language of the arbitration shall be English; and

(d) 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 2001 for the time being in force. The application of Part II of the International Arbitration Act 1994, 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 ("**Governing Law**").

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

9.16.1 Entire Agreement

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

9.16.2 Assignment

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

9.16.3 Severability

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

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

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

9.16.5 Force Majeure

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

9.17 Other Provisions

Not applicable.