MSC Trustgate
Certification Practice Statement

Version 4.3.4

23 AUGUST 2019

MSC Trustgate.com Sdn. Bhd. (478231-X)
Suite 2-9, Level 2, Block 4801 CBD Perdana
Jalan Perdana, 63000 Cyberjaya
Selangor Darul Ehsan, Malaysia
Tel: +603 8318 1800
www.msctrustgate.com

Certification Authority License Number : LPBP-2/2015(2)

Certification of Recognition for Repository Number : PPR-2/2015(2)

Published date: 23 August 2019

TRADEMARK NOTICES

Revision History

This document is the Trustgate CA CPS. The following revisions have been made to the original document:

No	Date	Changes	Version
1	29 March 2019	This version replaces the MSC Trustgate.com CPS version 4.3.2 30 January 2019. It includes OID of Trustgate CA.	4.3.3
2	23 August 2019	To amend Class 1 require Applicant to demonstrate control of his/her email address or mobile number	4.3.4
3		To amend certificate validity period of DV, OV and AATL to 825 days in Section 6.3.2	4.3.4

1. Introduction

This Certification Practice Statement (CPS) applies to the products and services of MSC Trustgate.com Sdn Bhd ("Trustgate CA"). It outlines the principles and practises related to Trustgate CA's lifecycle of digital certificates management, including electronic signatures and validity checking services. This CPS may be updated from time to time as outlined in Section 1.5 *Policy Administration*. The latest version may be found on the MSC Trustgate CA company repository at www.msctrustgate.com.

Trustgate CA Certification Practice Statement (CPS) conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction. In additional, it conforms to current versions of the requirements of the following schemes:

- Malaysia Digital Signature Act 1997
- Malaysia Digital Signature Regulations 1998
- CPA Canada, WebTrust Principles and Criteria for Certification Authorities 2.1
- CPA Canada, WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.3
- CPA Canada, WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.6.2
- CA/Browser Forum - Network And Certificate System Security Requirements Version 1.1
- CA/Browser Forum - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Version 1.5.6
- CA/Browser Forum - Guidelines For The Issuance And Management Of Extended Validation Certificates Version 1.6.8
- CA/Browser Forum - Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates Version 1.4

While certain sections are included in this CPS according to the structure of RFC 3647, the topic may not necessarily apply to services of Trustgate CA. These sections state 'No stipulation'. Additional information is presented in subsections of the standard structure where necessary.

CA/Browser Forum requirements are published at www.cabforum.org. In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document.

This CPS is final and binding between MSC Trustgate.com Sdn Bhd, a company duly registered in Malaysia at Suite 2-9, Level 2, Block 4801 CBD Perdana, Jalan Perdana, 63000 Cyberjaya, Selangor Darul Ehsan, Malaysia or via email at security@msctrustgate.com (hereinafter referred to as "Trustgate CA") and the Subscriber and/or Relying Party, who uses, relies upon or attempts to rely upon certification services made available by Trustgate CA referring to this CPS. For Relying Parties, this CPS becomes binding by relying upon a Certificate issued under this CPS. In addition,

Subscribers are required by the Subscriber Agreement to inform their Relying Parties that the CPS is itself binding upon those Relying Parties.

1.1 Overview

This CPS applies to the complete hierarchy of Certificates issued by Trustgate CA. The purpose of this CPS is to present the Trustgate CA practices and procedures in managing Certificates and to demonstrate compliance with requirements pertaining to the issuance of Certificates according to Trustgate CA's own and industry requirements pursuant to the standards. Trustgate CA operates within the scope of the applicable sections of Malaysian Law when delivering its services. This CPS aims to document the Trustgate CA delivery of certification services and management of the Certificate life cycle of any issued Subordinate CA, client, server and other purpose end entity Certificates.

This CPS is specifically applicable to:

- Trustgate CA
- Trustgate CA Infrastructure
- Trustgate CA Administrators
- Trustgate CA's enterprise Customers

More generally, the CPS also governs the use of Trustgate CA services by all individuals and entities within Trustgate CA.

The Trustgate CA includes Three (3) classes of Certificates, Classes 1-3. These Certificates can be used:

- for encryption of data
- for authenticate web resources, such as servers and other devices;
- for signing data objects digitally
- for electronic signatures or digital signature to replace handwritten signatures for signing documents

Trustgate CA may publish Certificate Policy (CP) that are supplemental to this CPS in order comply with the specific policy requirements of Government, or other industry standards and requirements. These supplemental certificate policies shall be made available to subscribers for the certificates issued under the supplemental policies and their relying parties.

The CPS is only one of a set of documents relevant to Trustgate CA. These other documents include:

- ancillary confidential security and operational documents[1] that supplement the CP and CPS by providing more detailed requirements, such as:

[1] Although these documents are not publicly available their specifications are included in Trustgate CA's Annual WebTrust for Certification authorities audit and may be made available to customer under special Agreement

- Business continuity and disaster recovery;
- Security Policy;
- Personnel policies;
- Key management policies, and
- Registration procedures
- Privacy Policy

- ancillary agreements imposed by Trustgate CA. These agreements bind Customers, Subscribers, and Relying Parties to Trustgate CA. A Subscriber or Relying Party of a Trustgate CA Certificate must refer to this CPS in order to establish trust in a Certificate issued by Trustgate CA as well as for information about the practices of Trustgate CA.

In many instances, the CPS refers to these ancillary documents for specific, detailed practices implementing Trustgate CA Standards where including the specifics in the CPS could compromise the security of Trustgate CA.

All applicable Trustgate CA policies are subject to audit by authorised third parties, which Trustgate CA highlights on its public facing web site via a WebTrust Seal of Assurance.

1.2 Document Name and Identification

Trustgate CA Certificates contain object identifier values corresponding to the applicable Trustgate CA Class of Certificate. The OID for Trustgate CA is an iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) MSC Trustagte CA (45530). Trustgate issues certificates and time-stamp tokens containing the following OIDs arcs:

Digitally Signed Object	Object Identifier (OID)
Client Certificate	
Class 1 Client Certificates	1.3.6.1.4.1.49530.1.1.1
Class 2 Client Certificates (Generic)	1.3.6.1.4.1.49530.1.1.2
Class 2 Client Certificates (Government)	1.3.6.1.4.1.49530.1.1.2.1
Class 2 Client Certificates (Enterprise)	1.3.6.1.4.1.49530.1.1.2.2
Class 3 Client Certificates	1.3.6.1.4.1.49530.1.1.3
Code Signing Certificates	1.3.6.1.4.1.49530.1.2.1
Time Stamping Certificates (Generic)	1.3.6.1.4.1.49530.1.3.1
SSL Certificate	
Domain Validation SSL Certificates	1.3.6.1.4.1.49530.1.4.1
Organisation Validation SSL Certificates	1.3.6.1.4.1.49530.1.5.1
Extended Validation SSL Certificates	1.3.6.1.4.1.49530.1.6.1
Extended Validation Code Signing Certificates	1.3.6.1.4.1.49530.1.6.2
Intranet Validation SSL Certificates	1.3.6.1.4.1.49530.1.7.1

The Trustgate CA certificates governed by this CPS are:

Subject DN	Validity Period	Serial Number
CN = Trustgate Class 1 Root Certificate Authority O = MSC Trustgate.com Sdn. Bhd. C = MY	07/06/2012 00:00:00 GMT 07/05/2042 23:59:59 GMT	1b5ed8fca65cfcdeb0cc00e129023e3a
CN = Trustgate Class 2 Root Certificate Authority O = MSC Trustgate.com Sdn. Bhd. C = MY	07/06/2012 00:00:00 GMT 07/05/2042 23:59:59 GMT	0a8bc4060f5a6cd34d07805da007abf5
CN = Trustgate Class 3 Root Certificate Authority O = MSC Trustgate.com Sdn. Bhd. C = MY	07/06/2012 00:00:00 GMT 07/05/2042 23:59:59 GMT	703b113dcdb38e30f4e57dac18a5310f
CN = Trustgate RSA Certification Authority OU = Malaysia Licensed CA No: LPBP-2/2010 (1) O = MSC Trustgate.com Sdn. Bhd. C = MY	12/19/2016 00:00:00 GMT 12/18/2041 23:59:59 GMT	1f61b6a273937d89952bc4af8e86050e
CN = Trustgate Time Stamping Authority CA OU = Malaysia Licensed CA No: LPBP-2/2010 (1) O = MSC Trustgate.com Sdn. Bhd. C = MY	12/19/2016 00:00:00 GMT 12/18/2041 23:59:59 GMT	4139bac7f7f45005dcd7f76adebf17b1
CN = Trustgate Time Stamping Authority CA (ECC) OU = Malaysia Licensed CA No: LPBP-2/2010 (1) O = MSC Trustgate.com Sdn. Bhd. C = MY	12/19/2016 00:00:00 GMT 12/18/2041 23:59:59 GMT	51e80251ad3e7ff755cac506ddb64bde
CN= MyTrust Class 1 RSA Root CA OU= MyTrust Gateway O= MSC Trustgate.com Sdn. Bhd. C= MY	08/17/2017 00:00:00 GMT 08/16/2042 23:59:59 GMT	3606c60894f246dc130f2671463d11ea
CN= MyTrust Class 2 RSA Root CA OU= MyTrust Gateway O= MSC Trustgate.com Sdn. Bhd. C= MY	08/17/2017 00:00:00 GMT 08/16/2042 23:59:59 GMT	38be005b37d65a7204e7141a6d2262ce
CN= MyTrust Class 3 RSA Root CA OU= MyTrust Gateway O= MSC Trustgate.com Sdn. Bhd. C= MY	08/17/2017 00:00:00 GMT 08/16/2042 23:59:59 GMT	5682e857103ffd808b880488eb1127d0
CN= MyTrust Class 1 ECC Root CA OU=MyTrust Gateway O=MSC Trustgate.com Sdn. Bhd. C=MY	08/28/2017 00:00:00 GMT 08/27/2042 23:59:59 GMT	4fc238d27e35d1ddb4df977002a3efbf
CN= MyTrust Class 2 ECC Root CA OU=MyTrust Gateway O=MSC Trustgate.com Sdn. Bhd. C=MY	08/28/2017 00:00:00 GMT 08/27/2042 23:59:59 GMT	68d4f1dc28d868754c464f4b70123229

Subject DN	Validity Period	Serial Number
CN= MyTrust Class 3 ECC Root CA OU=MyTrust Gateway O=MSC Trustgate.com Sdn. Bhd. C=MY	08/28/2017 00:00:00 GMT 08/27/2042 23:59:59 GMT	3f9289237e806a1da7326edc082052d3

1.3 PKI Participants

1.3.1 Certification Authorities

Trustgate CA is a Malaysian licenced Certification Authority that issues Certificates in accordance with this CPS. As a Certification Authority, Trustgate CA performs functions related to Certificate lifecycle management such as Subscriber registration, Certificate issuance, Certificate renewal, Certificate distribution and Certificate revocation. Trustgate CA also provides Certificate status information using a Repository in the form of a Certificate Revocation List (CRL) and/or Online Certificate Status Protocol (OCSP) responder. Trustgate CA may also be described by the term *"Issuing Authority"* or *"Trustgate CA"* to denote the purpose of issuing Certificates at the request of a Registration Authority (RA) from a subordinate Issuing CA.

The Trustgate CA Policy Board, which is composed of members of the MSC Trustgate.com Sdn Bhd management team and appointed by its Board of Directors, is responsible for maintaining this Certificate Policy relating to all certificates in the hierarchy. Through its Policy Board, Trustgate CA maintains control over the lifecycle and management of the CA.

Some of the tasks associated with Certificate lifecycle are delegated to select Trustgate RAs, who operate on the basis of a service agreement with Trustgate CA.

1.3.2 Registration Authorities

In addition to identifying and authenticating applicants for Certificates, an RA may also initiate or pass along revocation requests for Certificates and requests for issuance and renewal of Certificates. Trustgate CA may delegate the performance of certain functions such as accepting, evaluating, approving or rejecting the registration of Certificate applications and initiating the process to revoke a Certificate to a third party to act as a Registration Authority (RA). The function of an RA may vary between entities, from gathering application information, verifying application information and approving application.

A third party must enter into a contractual relationship with Trustgate CA in order to operate as an RA and authorise the issuance of Certificates. The third party must abide with all the requirements of this CPS, the terms of their contract obligations and the policies and industry standards that are applicable to an RA. The third party may implement more restrictive vetting practices if its internal policy dictates.

Trustgate CA may designate an Enterprise RA to verify Certificate Requests from the Enterprise RA's own organisation. In Enterprise RA, the Subscriber's organisation shall be validated and pre-defined and shall be constrained by system configuration.

1.3.3 Subscribers

Subscribers are either legal entities or natural persons that successfully apply for and receive a Trustgate CA Certificate to support their use in transactions, communications and the application of Digital Signatures.

In most cases certificates are issued directly to individuals or entities for their own use. However, there are some situations where the party requiring a certificate is different from the subject to whom the credential applies. For example, an organization may require certificates for its employees to allow them to represent the organization in electronic transactions/business. In such situations the entity subscribing for the issuance of certificates (i.e. paying for them, either through subscription to a specific service, or as the issuer itself) is different from the entity which is the subject of the certificate (generally, the holder of the credential). Two different terms are used in this CPS to distinguish between these two roles: "Subscriber", is the entity which contracts with Trustgate CA for the issuance of credentials and; “Subject", is the person to whom the credential is bound. The Subscriber bears ultimate responsibility for the use of the credential but the Subject is the individual that is authenticated when the credential is presented.

When ‘Subject’ is used, it is to indicate a distinction from the Subscriber. When “Subscriber” is used it may mean just the Subscriber as a distinct entity but may also use the term to embrace the two. The context of its use in this CPS will invoke the correct understanding.

1.3.4 Relying Parties

Replying parties are entities that act in reliance on a Certificate issued by Trustgate CA. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate. A Relying party may or may not also be a Subscriber within Trustgate CA.

Adobe offers to the AATL platform from Acrobat® 9.12 and above in order to provide document recipients with improved assurances that certified PDF documents are authentic. Document recipients are Relying Parties who can use Adobe reader to verify the Subscriber’s signature on a certified PDF document.

1.3.5 Other Participants

Other participants include CAs that cross-certify Trustgate CA to provide trust among other PKI communities.

1.4 Certificate Usage

A Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction.

1.4.1 Appropriate certificate usage

Certificates issued by Trustgate CA complies to DSA 1997 and DSR 1998. These certificates can be used for public domain transactions that require:

- **Authentication:** The assurance of one’s identity - who he/she/it claims to be.
- **Integrity:** The assurance to an entity that data has not been tempered with.

- **Confidentiality:** The assurance to an entity that only the intended recipient(s) can read a particular piece of data.
- **Non-repudiation:** A party cannot deny having digitally signed a data, a transaction or a document.

This CPS covers several different types of certificates with varying levels of assurance.

Client Certificates

Client Certificates are normally used by individuals to digitally sign and encrypt online transactions, to authenticate for accessing online applications and to digitally sign electronic mails, forms and documents. The most common usages for client certificates are included in Table 1 below.

Client Certificates	**Usage**	**Assurance Level**
Class 1	Encryption Authentication	Low
Class 2	Encryption Authentication Digital Signature	Medium
Class 3`	Encryption Authentication Digital Signature	High

A Client Certificate of Class 3 can issued to an organization to digitally sign and encrypt electronic emails, forms and documents.

SSL Certificates

SSL certificates are intended for use in establishing web-based data communication conduits via TLS/SSL protocol. The types of SSL certificates are included in Table 2 below.

SSL Certificates	Usage	Assurance Level
Domain	Encryption Authentication	Low
Organization	Encryption Authentication	Medium
Extended Validation	Encryption Authentication	High

Assurance Level:

- Low assurance — (Class 1) Certificates are not suitable for identity verification as no authenticated identity information is included within the Certificate. These Certificates do not support non-repudiation.

- Medium assurance — (Class 2) Certificates are individual and organisational Certificates that are suitable for securing some inter and intra-organisational and commercial transactions.

- High assurance — (Class 3) Certificates are individual and organisational Certificates that provide a high level of assurance of the identity of the Subscriber as compared to Class 1 and 2. Extended validation certificates are high assurance certificates issued by Trustgate CA in conformance with the EV guidelines.

All Certificate types can be used to ensure the confidentiality of communications effected by means of Certificates. Confidentiality may apply to business and personal communications as well as personal data protection and privacy.

1.4.2 Prohibited Certificate usage

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

Trustgate CA Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. Also, Class 1 Certificates shall not be used as proof of identity or as support of non-repudiation of identity or authority. Trustgate CA Certificates may not be used for any functions except CA functions. In addition, end-user Subscriber Certificates shall not be used as CA Certificates.

Trustgate CA and its Participants shall not issue any certificate that can be used for man-in-the-middle (MITM) or traffic management of domain names or IP addresses that the certificate holder does not legitimately own or control. Such certificate usage is expressly prohibited.

Certificates do not guarantee that the Subject is trustworthy, operating a reputable business or that the equipment into which the Certificate has been installed is free from defect, malware or virus.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

Requests for information on the compliance of issuing CAs with accreditation schemes as well as any other inquiry associated with this CPS should be addressed to:

MSC Trustgate.com Sdn. Bhd. (478231-X)
Suite 2-9, Level 2,
Block 4801 CBD Perdana, Jalan Perdana, 63000 Cyberjaya
Selangor Darul Ehsan, Malaysia
Tel: +603 8318 1800

www.msctrustgate.com

security@msctrustgate.com

1.5.2 Contact Person

Compliance Officer

MSC Trustgate.com Sdn. Bhd. (478231-X)

Suite 2-9, Level 2,

Block 4801 CBD Perdana, Jalan Perdana, 63000 Cyberjaya

Selangor Darul Ehsan, Malaysia

Tel: +603 8318 1800

www.msctrustgate.com

security@msctrustgate.com

1.5.3 Person Determining CPS Suitability for the Policy

The Trustgate CA policy board determines the suitability and applicability of the CP and the conformance of this CPS based on the results and recommendations received from a Qualified Auditor.

In an effort to maintain credibility and promote trust in this CPS and better correspond to accreditation and legal requirements, the Trustgate CA policy board shall review this CPS at least annually and may make revisions and updates to policies as it sees fit or as required by other circumstances. Any updates become binding for all Certificates that have been issued or are to be issued upon the date of the publication of the updated version of this CPS.

1.5.4 CPS Approval Procedures

The Trustgate CA policy board reviews and approves any changes to CPS. The updated CPS is reviewed against the CP in order to check for consistency. CP changes are also added on a as-needed basis. Upon approval of a CPS update by the policy board, the new CPS is published in the Trustgate CA Repository at www.msctrustgate.com.

The updated version is binding upon all Subscribers including the Subscribers and parties relying on Certificates that have been issued under a previous version of the CPS.

1.6 Definitions and acronyms

Any terms used but not defined herein shall have the meaning ascribed to them in the Baseline Requirements and the EV Guidelines.

1.6.1 Definitions

- **Adobe Approved Trust List :** A document signing certificate authority trust store created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 9.0
- **Affiliate:** A business, corporation, partnership, joint venture or other entity controlling, controlled by or under common control with another entity or an agency, department, political subdivision or any entity operating under the direct control of a Government Entity.

- **Applicant:** A natural person or an entity that applies for (or seeks renewal of) a Certificate.
- **Application Software Supplier:** A supplier of Internet browser software or other Relying Party application software that displays or uses Trustgate Certificates and distributes Trustgate's Root Certificates.
- **Attestation Letter:** A letter attesting that Subject Identity Information is correct.
- **Business Entity:** Any entity that is not a Private Organisation, Government Entity or non-commercial entity as defined in the EV Guidelines. Examples include, but are not limited to, businesses, general partnerships, unincorporated associations, sole proprietorships, etc.
- **Certificate:** An electronic document that uses a Digital Signature to bind a Public Key and an identity.
- **Certificate Application:** An application form requested by an RA operating under Trustgate CA and submitted by an application when application for issuance of a Trustgate Certificate.
- **Certificate Approver:** A Trustgate employee or an authorized administrator to approve a request for a Trustgate Certificate.
- **Certificate Management Process:** Processes, practices and procedures associated with the use of keys, software and hardware, by which Trustgate CA verifies Certificate Data, issues Certificates, maintains a Repository and revokes Certificates.
- **Certificate Policy:** A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
- **Certificate Problem Report:** A complaint of suspected Key Compromise, Certificate misuse or other types of fraud, compromise, misuse or inappropriate conduct related to Certificates.
- **Certificate Revocation List:** A regularly updated timestamped list of revoked Certificates that is created and digitally signed by Trustgate CA.
- **Certification Practice Statement:** One of several documents forming the governance framework in which Certificates are created, issued, managed and used.
- **Compromise:** A violation of a security policy that results in loss of control over sensitive information.
- **Country:** Either a member of the United Nations OR a geographic region recognised as a sovereign nation by at least two UN member nations.
- **Cross Certificate:** as defined in the Baseline Requirement.
- **Digital Signature:** To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's Public Key can accurately determine whether the transformation was created using the Private Key

that corresponds to the signer's Public Key and whether the initial message has been altered since the transformation was made.

- **Domain Contact:** as defined in the Baseline Requirement.
- **Domain Name:** as defined in the Baseline Requirement.
- **Domain Name Registrant:** as defined in the Baseline Requirement.
- **Domain Name Registrar:** as defined in the Baseline Requirement.
- **DNS CAA Email Contact:** as defined in the Baseline Requirement.
- **DNS TXT Record Email Contact:** as defined in the Baseline Requirement.
- **DNS TXT Record Phone Contact:** as defined in the Baseline Requirement.
- **Enterprise RA:** as defined in the Baseline Requirement.
- **Expiry Date:** The "Not After" date in a Certificate that defines the end of a Certificate's Validity Period.
- **Fully-Qualified Domain Name:** as defined in the Baseline Requirement.
- **Government Accepted Form of ID:** A physical or electronic form of ID issued by the government or a form of ID that the government accepts for validating identities of individuals for its own official purposes.
- **Government Entity:** A government-operated legal entity, agency, department, ministry, branch or similar element of the government of a Country or political subdivision within such Country (such as a municipality, city or state, etc.).
- **Hardware Security Module (HSM):** An HSM is type of secure crypto processor targeted at managing digital keys, accelerating crypto processes in terms of digital signings/second and for providing strong authentication to access critical keys for server applications.
- **Issuing CA:** In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
- **Key Compromise:** as defined in the Baseline Requirement.
- **Key Pair:** The Private Key and its associated Public Key.
- **Legal Entity:** An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a Country's legal system.
- **Object Identifier (OID):** A unique alphanumeric or numeric identifier registered under the International Organisation for Standardization's applicable standard for a specific object or object class.
- **Online Certificate Status Protocol (OCSP):** An online Certificate-checking protocol that enables Relying Party application software to determine the status of an identified Certificate. See also OCSP Responder.

- **Private Key:** The key of a Key Pair that is kept secret by the holder of the Key Pair and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
- **Public Key:** The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
- **Public Key Infrastructure (PKI):** A set of hardware, software, people, procedures, rules, policies and obligations used to facilitate the trustworthy creation, issuance, management and use of Certificates and keys based on Public Key cryptography.
- **Publicly-Trusted Certificate:** A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.
- **Qualified Auditor:** A natural person or Legal Entity that meets the requirements outlined by the relevant legislation.
- **Qualified Government Information Source:** as defined in the Baseline Requirement.
- **Qualified Government Tax Information Source:** as defined in the Baseline Requirement.
- **Qualified Independent Information Source:** as defined in the Baseline Requirement.
- **Registration Authority (RA):** Any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA and hence does not sign or issue Certificates. An RA may assist in the Certificate application process or revocation process or both. When “RA” is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
- **Relying Party:** Any natural person or Legal Entity that relies on a Valid Certificate.
- **Repository:** An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information in the form of a CRL.
- **Root Certificate:** The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
- **Subject:** The natural person, device, system, unit or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
- **Subject Identity Information:** Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subjectAltName extension or the commonName field.
- **Subordinate CA:** A Certification Authority whose Certificate is signed by Trustgate CA.

- **Subscriber:** A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.
- **Subscriber Agreement**: An agreement between Trustgate CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
- **Terms of Use:** Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the Baseline Requirements when the Applicant/Subscriber is an Affiliate of the CA.
- **Trusted Third-party:** A service provider with a secure process used for individual identity verification based on Governmentally Accepted Form(s) of ID or whose service itself is considered to generate a Governmentally Acceptable Form of ID**.**
- **Trustworthy System:** Computer hardware, software and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.
- **Valid Certificate:** A Certificate that passes the validation procedure specified in RFC 5280.
- **Validity Period**: The period of time measured from the date when the Certificate is issued until the Expiry Date.
- **WebTrust Program for CAs:** The then-current version of the CPA Canada WebTrust Program for Certification Authorities.
- **WebTrust Seal of Assurance:** An affirmation of compliance resulting from the WebTrust Program for CAs.
- **Wildcard Certificate:** A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.
- **X.509:** The standard of the ITU-T (International Telecommunications Union-T) for Certificates.

1.6.2 Acronyms

AATL	Adobe Approved Trust List
CA	Certificate Authority or Certification Authority
CAA	Certification Authority Authorization
CAB	CA/Browser as in CAB Forum
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
DNS	Domain Name Service
DV	Domain Validated

ETSI European Telecommunications Standards Institute
EU European Union
EV Extended Validation
FIPS Federal Information Processing Standard
FQDN Fully Qualified Domain Name
FTP File Transfer Protocol
HSM Hardware Security Module
HTTP Hypertext Transfer Protocol
IANA Internet Assigned Numbers Authority
ICANN Internet Corporation for Assigned Names and Numbers
IDN Internationalized Domain Name
ISSO Information System Security Officer
IETF Internet Engineering Task Force
IGTF International Grid Trust Federation
ITU International Telecommunication Union
NIST National Institute of Standards and Technology
OCSP Online Certificate Status Protocol
OID Object Identifier
OSU Online Sign-Up (Wi-Fi Alliance Hotspot 2.0)
OV Organization Validated
PIN Personal Identification Number (e.g. a secret access code)
PKI Public Key Infrastructure
RA Registration Authority
RFC Request for Comments
SAN Subject Alternative Name
SHA Secure Hashing Algorithm
SSL Secure Sockets Layer
TLD Top-Level Domain
TLS Transport Layer Security
TSA Time Stamping Authority
TST Time-Stamp Token
TTL Time To Live
UTC Coordinated Universal Time
X.509 The ITU-T standard for Certificate and their corresponding authentication framework

2. Publication and Repository Responsibilities

2.1 Repositories

Trustgate CA publishes all Certificates-related and Certificate Revocation information for issued Certificates, CP, CPS and Relying Party agreements and Subscriber Agreements in public repositories. Trustgate CA ensures that revocation data for issued Certificates and its Root

Certificates are available through a repository on 24 hours basis and is periodically updated as set forth in this CPS.

The repository can be accessed at https://www.msctrustgate.com/respository.

2.2 Publication of Certificate Information

Trustgate CA publishes its CP, CPS, Subscriber Agreements, Relying Party agreements and CRLS at https://www.msctrustgate.com/repository.

2.3 Time or Frequency of Publication

Trustgate CA reviews its CP and CPS at least once per year and makes appropriate changes to comply with external requirements listed in the "*Introduction*" section of this document. Updates to Subscriber Agreements and Relying Party Agreements are published as necessary.

Certificates are published in a Repository upon issuance. CRLs are updated every 24 hours. CRLs for CA Certificates are issued at least once a year and within 24 hours if a Certificate is revoked.

2.4 Access control on repositories

Information published in the repository of Trustgate CA web site is publicly-accessible. Read only access to such information is unrestricted. Trustgate CA has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3. Identification and Authentication

Trustgate CA verifies and authenticates the identity and/or other attributes of an Applicant prior to inclusion of those attributes in a Certificate.

3.1 Naming

3.1.1 Types of Names

Trustgate CA Certificates are issued with subject DNs (Distinguished Names) which meet the requirements of X.500 naming, RFC-822 naming and X.400 naming.

Client Certificate Class 1

Attribute	Value
Common Name (CN)	The Subscriber's name
E-Mail Address (E)	The Subscriber's E-mail address

Client Certificate Class 2

Attribute	Value
Country (C)	The two letter ISO 3166 code for the country in which the Subscriber is located
Organization (O)	MSC Trustgate.com or The legal name of the Subscriber's organization

Attribute	Value
Organizational Unit (OU)	Trustgate CA end-user Subscriber Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: • Subscriber organizational unit (for organizational Certificates and individual Certificates that have an organization affiliation) • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate • A copyright notice • "Authenticated by Trustgate CA" and "Member" in Certificates whose applications were authenticated by Trustgate • "Persona Not Validated" for Class 1 Individual Certificates • Text to describe the type of Certificate.
State or Province (S)	Not used.
Locality (L)	Not used.
Common Name (CN)	This attribute includes the CA Name (if the CA Name is not specified in an OU attribute) or is not used.
E-Mail Address (E)	The Subscriber's E-mail address

Client Certificate Class 3

Attribute	Value
Country (C)	The two letter ISO 3166 code for the country in which the Subscriber is located
Organization (O)	MSC Trustgate.com or The legal name of the Subscriber's organization
Organizational Unit (OU)	Trustgate CA end-user Subscriber Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: • Subscriber organizational unit (for organizational Certificates and individual Certificates that have an organization affiliation) • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate • A copyright notice

Attribute	Value
	• "Authenticated by Trustgate CA" and "Member" in Certificates whose applications were authenticated by Trustgate • "Persona Not Validated" for Class 1 Individual Certificates • Text to describe the type of Certificate.
State or Province (S)	Not used.
Locality (L)	Not used.
Common Name (CN)	This attribute includes the CA Name (if the CA Name is not specified in an OU attribute) or is not used.
E-Mail Address (E)	The Subscriber's E-mail address

Domain Certificates

Attribute	Value
Country (C)	The two letter ISO 3166 code for the country in which the Subscriber is located
Organization (O)	The legal name of the Subscriber's organization
Organizational Unit (OU)	Trustgate CA end-user Subscriber Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: • Subscriber organizational unit (for organizational Certificates and individual Certificates that have an organization affiliation) • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate • A copyright notice • "Authenticated by Trustgate CA" and "Member" in Certificates whose applications were authenticated by Trustgate • Text to describe the type of Certificate.
State or Province (S)	Not used.
Locality (L)	Not used.
Common Name (CN)	Domain Name of the server which the Applicant intend to install the SSL Certificate

Attribute	Value
E-Mail Address (E)	The Subscriber's E-mail address

Organization Certificates

Attribute	Value
Country (C)	The two letter ISO 3166 code for the country in which the Subscriber is located
Organization (O)	The legal name of the Applicant's organization
Organizational Unit (OU)	Trustgate CA SSL Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: • Subscriber organizational unit • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate • A copyright notice • "Authenticated by Trustgate CA" and "Member" in Certificates whose applications were authenticated by Trustgate • Text to describe the type of Certificate.
State or Province (S)	Not used.
Locality (L)	Not used.
Common Name (CN)	Domain Name of the server which the Applicant intend to install the SSL Certificate.
E-Mail Address (E)	The Subscriber's E-mail address
serialNumber	The registration number of the organization

EV Certificates

Attribute	Value
Country (C)	The two letter ISO 3166 code for the country in which the Subscriber is located
Organization (O)	The legal name of the Applicant's organization
Organizational Unit (OU)	Trustgate CA Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following:

Attribute	Value
	• Subscriber organizational unit • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate • A copyright notice • "Authenticated by Trustgate CA" and "Member" in Certificates whose applications were authenticated by Trustgate • Text to describe the type of Certificate.
State or Province (S)	Not used.
Locality (L)	Not used.
Common Name (CN)	Domain Name of the server which the Applicant intend to install the SSL Certificate.
E-Mail Address (E)	The Subscriber's E-mail address
serialNumber	The registration number of the organization
Business Category	The business category of the Organization

3.1.2 Need for Names to be Meaningful

Class 2 and 3 Certificates contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the Certificate.

Trustgate CA certificates contain names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

Unless prohibited by policy or law or requested by a State or Government authority to protect the identity of certain end user subscribers (e.g. minors or sensitive government employee information), Subscribers are not permitted to use pseudonyms (names other than a Subscriber's true personal or organizational name). Each request for anonymity in a certificate will be evaluated on its merits by Trustgate CA and, if allowed the certificate will indicate that identity has been authenticated but is protected.

Trustgate CAs may reject applications based on risk-mitigation criteria, including names at risk for phishing or other fraudulent usage, names listed on the Google Safe Browsing lists and names listed in the database maintained by the Anti-Phishing Working Group.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished names in Certificates are interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in Certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5 Uniqueness of Names

Trustgate CA ensures that Subject Distinguished Names of Subscriber are unique within the domain of a specific CA through automated components of the Subscriber enrolment process. It is possible for a Subscriber to have two or more certificates with the same Subject Distinguished Name.

3.1.6 Recognition, Authentication and Role of Trademarks

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. Trustgate CA, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark.

Trustgate CA reserves the right to reject any applications and to revoke any Certificate that is involved in a dispute.

3.2 Initial Identity Validation

Trustgate CA may use any legal means of communication or investigation necessary to identify a legal entity or individual. Trustgate CA may refuse to issue a Certificate in its sole discretion.

3.2.1 Method to Prove Possession of Private Key

The certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be PKCS #10 format, another cryptographically equivalent demonstration, or Trustgate-approved method. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber, for example where pre-generated keys are placed on smart cards.

3.2.2 Authentication of Organisation and Domain Identity

Trustgate CA maintains internal policies and procedures which are reviewed regularly in order to comply with the requirements of the various root programs that Trustgate CA is a member of, as well as the Baseline Requirements, the EV Guidelines and EV Code Signing Guidelines.

Whenever a certificate contains an organization name, the identity of the organization and other enrolment information (e.g. registered number, business address, domain name) provided by Certificate Applicants is confirmed in accordance with the procedures set forth in Trustgate CA's documented Validation Procedures. Trustgate CA shall:

- determine that the organization exists by using at least one third party identity proofing service or database, or organizational documentation issued by or filed with the applicable government agency (e.g. QGIS, QTIS, QIIS) or competent authority that confirms the existence of the organization,

- confirm by telephone or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so. When a certificate includes the name of an individual as an authorized representative of the Organization, the employment of that individual and his/her authority to act on behalf of the Organization shall also be confirmed.

3.2.2.1 Identity

If the Subject Identity Information is to include the name or address of an organization, Trustgate CA shall verify the identity and address of the organization and that the address is the Applicant's address of existence or operation. Trustgate CA shall verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1. A government agency (e.g, QGIS) in the jurisdiction of the Applicant's legal creation, existence or recognition;
2. An third party database (e.g. SSM) that is periodically updated, which Trustgate CA has evaluated and determine that it is reasonably accurate and reliable;
3. A site visit by the Trustgate CA or a third party who is acting as an agent of Trustgate CA; or
4. An attestation letter confirming that Subject Identity Information is correct written by a profession body, a lawyer, a government official, a judge or other reliable third-party customarily relied upon for such information.

Alternatively, Trustgate CA may verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document (e.g. QGTIS), or other form of identification that Trustgate CA determines to be reliable.

3.2.2.2 DBA/Tradename

If the Subject Identity Information includes a DBA or tradename, Trustgate CA shall verify the Applicant's right to use the DBA/tradename using at least one of the following:

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence or recognition;
2. A Reliable Data Source;
3. Communication with a government agency responsible for the management of such DBAs or tradenames;
4. An Attestation Letter written by a lawyer, a government official, a judge or other reliable third-party customarily accompanied by documentary support; or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that Trustgate CA determines to be reliable.

3.2.2.3 Verification of Country

If the Applicant requests require the subject:countryName field to be presented, then Trustgate CA shall verify the country associated with the Subject using one of the following:

a) the IP Address range assignment by country for either

   (i) the web site's IP address, as indicated by the DNS record for the web site or

   (ii) the Applicant's IP address;

b) the two-letter country code (ccTLD) of the requested Domain Name;

c) information provided by the Domain Name Registrar; or

d) a method identified in Section 3.2.2.1.

Trustgate CA should implement a process to screen proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.

3.2.2.4 Validation of Domain Authorization or Control

Trustgate CA confirms that prior to issuance, Trustgate CA or its RA has validated each FQDN listed in the Certificate using at least one of the methods listed below.

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. For purposes of domain validation, the term Applicant includes the Applicant's Parent company, subsidiary company or affiliate.

3.2.2.4.1 Validating the Applicant as a Domain Contact

No stipulation.

3.2.2.4.2 Email, Fax, SMS or Postal Mail to Domain Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value must be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact.

Each email, fax, SMS, or postal mail may confirm control of multiple Authorization Domain Names.

Trustgate CA may send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email, fax, SMS, or postal mail.

The Random Value shall be unique in each email, fax, SMS, or postal mail.

Trustgate CA may resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.4.3 Phone Contact with Domain Contact

Confirming the Applicant's control over the FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. Trustgate CA must place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.

Each phone call shall be made to a single number and may confirm control of multiple FQDNs, provided that the phone number is identified by the Domain Registrar as a valid contact method for every Base Domain Name being verified using the phone call.

Trustgate CA shall not perform validations using this method after May 31, 2019. Completed validations using this method SHALL continue to be valid for subsequent issuance per the applicable certificate data reuse periods.

3.2.2.4.4 Construct Email to Domain Contact

Confirm the Applicant's control over the FQDN by (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at- sign ("@"), followed by an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

Each email may confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed

The Random Value shall be unique in each email.

The email may be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient shall remain unchanged.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.4.5 Domain Authorization Document

No stipulation.

3.2.2.4.6 Agreed-Upon Change to Website

Confirming the Applicant's control over the FQDN by confirming one of the following under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of Domain Validation, on the Authorization Domain Name that is accessible by Trustgate CA via HTTP/HTTPS over an Authorized Port:

The presence of Required Website Content contained in the content of a file. The entire Required Website Content MUST NOT appear in the request used to retrieve the file or web page, or

The presence of the Request Token or Random Value contained in the content of a file where the Request Token or Random Value must not appear in the request.

If a Random Value is used, Trustgate CA shall provide a Random Value unique to the certificate request and shall not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant

submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate (such as in Section 4.2.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).

3.2.2.4.7 DNS Change

Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

If a Random Value is used, Trustgate CA shall provide a Random Value unique to the Certificate request and shall not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate (such as in Section 3.3.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).

3.2.2.4.8 IP Address

Confirming the Applicant's control over the FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with section 3.2.2.5.

Once the FQDN has been validated using this method, Trustgate CA also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.9 Test Certificate

No stipulation.

3.2.2.4.10 TLS Using a Random Number

No stipulation.

3.2.2.4.11 Any Other Method

No stipulation.

3.2.2.4.12 Validating Applicant as a Domain Contact

No stipulation.

3.2.2.4.13 Email to DNS CAA Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value must be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set must be found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065 (Appendix A).

Each email may confirm control of multiple FQDNs, provided that each email address is a DNS CAA Email Contact for each Authorization Domain Name being validated. The same email may be sent to multiple recipients as long as all recipients are DNS CAA Email Contacts for each Authorization Domain Name being validated.

The Random Value shall be unique in each email. The email may be re-sent in its entirety, including the re- use of the Random Value, provided that its entire contents and recipient(s) remain unchanged. The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.4.14 Email to DNS TXT Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value must be sent to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN.

Each email may confirm control of multiple FQDNs, provided that each email address is DNS TXT Record Email Contact for each Authorization Domain Name being validated. The same email may be sent to multiple recipients as long as all recipients are DNS TXT Record Email Contacts for each Authorization Domain Name being validated.

The Random Value shall be unique in each email. The email may be re-sent in its entirety, including the re- use of the Random Value, provided that its entire contents and recipient(s) shall remain unchanged. The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.4.15 Phone Contact with Domain Contact

Confirm the Applicant's control over the FQDN by calling the Domain Contact’s phone number and obtain a confirming response to validate the ADN. Each phone call may confirm control of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

In the event that someone other than a Domain Contact is reached, Trustgate CA may request to be transferred to the Domain Contact.

In the event of reaching voicemail, Trustgate CA may leave the Random Value and the ADN(s) being validated. The Random Value must be returned to Trustgate CA to approve the request.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

Confirm the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact’s phone number and obtain a confirming response to validate the ADN. Each phone call may confirm control of multiple ADNs provided that the same DNS TXT Record Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

Trustgate CA may not knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation.

In the event of reaching voicemail, Trustgate CA may leave the Random Value and the ADN(s) being validated. The Random Value must be returned to Trustgate CA to approve the request.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.5 Authentication of IP address

For each IP address listed in a Certificate, the CA or RA shall confirm that the Applicant has control over the IP address by the method listed below:

a. Agreed-Upon Change to Website under *Section 3.2.2.4.6*,

b. Email, Fax, SMS or Portal Mail to IP Address Contact under *Section 3.2.2.4.2*, or

c. Perform a reverse-IP address lookup and then verifying control over the resulting Domain Name under *Section 3.2.2.4*.

3.2.2.6 Wildcard Validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, Trustgate CA must establish and follow a documented procedure that determines if the wildcard character occurs in the first label position to the left of a “registry-controlled” label or “public suffix” (e.g. “*.com”, “*.co.uk”, see RFC 6454 Section 8.2 for further explanation).

If a wildcard falls within the label immediately to the left of a registry-controlled or public suffix, Trustgate CA must refuse issuance unless the applicant proves its rightful control of the entire Domain Namespace.

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, Trustgate CA shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification.

3.2.2.8 CAA record

As part of the issuance process, Trustgate CA must check for CAA records and follow the processing instructions found, for each dNSName in the subjectAltName extension of the certificate to be issued, as specified in RFC 6844. If Trustgate CA issues, Trustgate CA must do so within the TTL of the CAA record, or 8 hours, whichever is greater.

For issuances conforming to these Baseline Requirements, Trustgate CA must not rely on any exceptions specified in its CP or CPS unless they are one of the following:

- for certificates for which a Certificate Transparency pre -certificate was created and logged in a least two public logs, and which CAA was checked.
- for certificates issued by a Technically Constrained Subordinate CA Certificate as set out in *Section 7.1.5*, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.
- if the CA or an Affiliate of the CA is the DNS Operator (as defined in RFC 7719) of the domain's DNS.

Trustgate CA treats a record lookup failure as permission to issue if:

- the failure is outside the CA's infrastructure;

- the lookup has been retried at least once; and
- the domain's zone does not have a DNSSEC validation chain to the ICANN root.

Trustgate CA must document potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CAB Forum on the circumstances, and should dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s), if present. CAs are not expected to support URL schemes in the iodef record other than mailto: or https:.

3.2.3 Authentication of Individual identity

Trustgate CA shall use the method s set out below to verify any individual identities that are submitted by an Applicant or Subscriber.

3.2.3.1 Class 1

Trustgate CA does not authenticate the identity of the Applicant except required the Applicant to demonstrate control of his/her email address or mobile number to which the Certificate relates.

3.2.3.2 Class 2

The Applicant is required to submit a legible copy of a valid government issued photographic identity such as national identity, passport, driver's license, police ID, military ID or equivalent. A suitable non-government issued identity document may also be required for additional proof. Trustgate CA verifies to a reasonable level of assurance that the copy of the identity matches the identity of the Applicant.

Trustgate CA may also authenticate the Applicant's identity through one or more of the following methods:

- Performing a telephone challenge/response to the Applicant using a published office number; or
- Performing a fax challenge/response to the Applicant using a published office fax number; or
- Performing an email challenge/response to the Applicant using an email address from reliable source; or
- Performing an SMS challenge/response to the Applicant using his/her mobile number from reliable source; or
- Receiving a fund transfer from the Applicant's banking account via a secure channel (e.g FPX, IBG) that provides the name of the Applicant; or
- Receiving an attestation from an appropriate notary or Trusted Third-party that they have verified the individual identity based on a form of photographic identity issued by a government
- In the case of individuals affiliated with an organisation, Trustgate CA may rely on the relevant company incorporation documents (e.g. Form 9, Form49, Company's resolution), letter of appointment that can associate the individual with the organisation and/or attestations from the approved RA.

Trustgate CA may request further information such as utility bills, bank and credit card statement from the Applicant. Other information and/or methods may be utilised in order to demonstrate an equivalent level of confidence.

3.2.3.3 Class 3

The Applicant is required to submit a legible copy of a valid government issued photographic identity such as national identity, passport, driver's license, police ID, military ID or equivalent. A suitable non-government issued identity document may also be required for additional proof. Trustgate CA verifies to a reasonable level of assurance that the copy of the identity matches the identity of the Applicant.

Trustgate CA shall authenticate the Applicant's identity through two or more of the following methods:

- Performing an SMS challenge/response to the Applicant using his/her mobile number and receiving a fund transfer from the Applicant's banking account via a secure channel (e.g FPX, IBG) that provides the name of the applicant;
- Performing face to face verification against the Applicant's valid government issued photographic identity such as national ID, passport, driver's license, military ID or equivalent before an agent of the CA or RA, before a notary public or other official with comparable authority within the Certificate Applicant's jurisdiction;
- Performing a biometric verification (e.g. fingerprint and face recognition) against the Applicant's valid government issued photographic identity such as national ID, passport, driver's license, military ID or equivalent

Trustgate CA also authenticates the Applicant's authority to represent the organisation wishing to be named as the Subject in the Certificate using reliable means of communication in accordance with the EV Guidelines.

Further information may be requested from the Applicant or the Applicant's organisation. Other information and/or methods may be utilised in order to demonstrate an equivalent level of confidence.

3.2.4 Non-Verified Subscriber Information

Trustgate CA validates all information to be included within the Subject DN of a Certificate except as stated otherwise in this section of the CPS. Non-verified subscriber information includes:

- Subscriber's name in Class 1 certificates
- Any other information designated as non-verified in the certificate according to Baseline Requirement and EV guideline.

3.2.5 Validation of Authority

If the Applicant for a Certificate containing Subject Identity Information is an organization, Trustgate CA or its RA shall use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request.

Trustgate CA or its RA may use the sources listed in section 3.2.2.1 to verify the Reliable Method of Communication. Provided that Trustgate CA or its RA uses a Reliable Method of Communication,

Trustgate CA or its RA may establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate.

In addition, Trustgate CA or its RA shall establish a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then Trustgate CA or its RA shall not accept any certificate requests that are outside this specification. Trustgate CA shall provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

3.2.6 Criteria for Interoperation or Certification

Trustgate CA shall disclose all Cross Certificates that identify Trustgate CA as the Subject.

3.3 Identification and Authentication for Re-key Request

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. Trustgate CA generally requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey"). However, in certain cases (i.e., for web server certificates) Subscribers may request a new certificate for an existing key pair (technically defined as "renewal").

Generally speaking, both "Rekey" and "Renewal" are commonly described as "Certificate Renewal", focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasizing whether or not a new key pair is generated. For all Classes and Types of Trustgate CA Certificates, except for Class 3 Server Certificates, this distinction is not important as a new key pair is always generated as part of Trustgate CA's Client Certificates replacement process. However, for Class 3 Server Certificates, because the Subscriber key pair is generated on the web server and most web server key generation tools permit the creation of a new Certificate Request for an existing key pair, there is a distinction between "rekey" and "renewal."

3.3.1 Identification and Authentication for Routine Re-key

Re-key procedures ensure that the person or organization seeking to rekey an end-user Subscriber Certificate is in fact the Subscriber of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrolment information a Challenge Phrase. Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's re-enrolment information, and the enrolment information (including Corporate and Technical contact information) has not changed, a renewal Certificate is automatically issued.

As an alternative to using a challenge phrase (or equivalent), Trustgate CA may send an e-mail message to the e-mail address associated with the verified corporate contact for the certificate being renewed, requesting confirmation of the Certificate renewal order and authorization to issue the Certificate. Upon receipt of confirmation authorizing issuance of the Certificate, Trustgate CA will

issue the Certificate if the enrolment information (including Corporate and Technical contact information[2]) has not changed.

After rekeying or renewal in this fashion, and on at least alternative instances of subsequent rekeying or renewal thereafter, Trustgate CA or the RA reconfirms the identity of the Subscriber in accordance with the identification and authentication requirements of an original Certificate Application.[3]

In particular, for retail Class 3 Organizational certificates, Trustgate CA re-authenticates the Organization name and domain name included in the certificate at intervals described in ***Section 6.3.2***. In circumstances where:

- The challenge phrase is correctly used for the subsequent renewal certificate and:
- The certificate Distinguished Name has not been changed, and
- The Corporate and Technical Contact information remains unchanged from that which was previously verified,

Trustgate CA will not have to reconfirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so.

Rekey after 30-days from expiration of the Certificate are re-authenticated as an original Certificate Application and are not automatically issued.

3.3.2 Identification and Authentication for Re-key After Revocation

Re-key/renewal after revocation is not permitted if the revocation occurred because:

- the Certificate (other than a Class 1 Certificate) was issued to a person other than the one named as the Subject of the Certificate, or
- the Certificate (other than a Class 1 Certificate) was issued without the authorization of the person or entity named as the Subject of such Certificate, or
- the entity approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false.
- For any other reason deemed necessary by Trustgate CA

Subject to the foregoing paragraph, renewal of an organizational or CA Certificate following revocation of the Certificate is permissible as long as renewal procedures ensure that the organization or CA seeking renewal is in fact the Subscriber of the Certificate. Renewed organizational Certificates

[2] The authentication of a request to rekey/renew a Class 3 Organizational Certificate, however, requires the use of a Challenge Phrase as well as the same identification and authentication as for the original Certificate Application.

[3] The authentication of a request to rekey/renew a Class 3 Organizational Certificate, however, requires the use of a Challenge Phrase as well as the same identification and authentication as for the original Certificate Application.

shall contain the same Subject distinguished name as the Subject distinguished name of the organizational Certificate being renewed.

Renewal of an individual Certificate following revocation must ensure that the person seeking renewal is, in fact, the Subscriber. One acceptable procedure is the use of a Challenge Phrase (or the equivalent thereof). Other than this procedure or another Trustgate CA -approved procedure, the requirements for the identification and authentication of an original Certificate Application shall be used for renewing a Certificate following revocation.

3.4 Identification and Authentication for Revocation Request

Prior to the revocation of a Certificate, Trustgate CA verifies that the revocation has been requested by the Certificate's Subscriber, the entity that approved the Certificate Application.

Acceptable procedures for authenticating the revocation requests of a Subscriber include:

- Having the Subscriber for certain certificate types submit the Subscriber's Challenge Phrase (or the equivalent thereof), and revoking the Certificate automatically if it matches the Challenge Phrase (or the equivalent thereof) on record. (Note that this option may not be available to all customers.)
- Receiving a message from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked,
- Communication with the Subscriber providing reasonable assurances in light of the Class of Certificate that the person or organization requesting revocation is, in fact the Subscriber. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

Trustgate CA Administrators are entitled to request the revocation of Client Certificates within Trustgate CA's Sub domain. Trustgate CA authenticates the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions, or another Trustgate CA-approved procedure.

RAs using an Automated Administration Software Module may submit bulk revocation requests to Trustgate CA. Such requests shall be authenticated via a digitally signed request signed with the private key in the RA's Automated Administration hardware token.

4. Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Below is a list of people who may submit certificate applications:

- Any individual who is the subject of the certificate;
- Any authorized representative of an Organization or legal entity;
- Any authorized representative of a CA; or

- Any authorized representative of an RA.

Trustgate CA does not issue Certificates to any persons or entities blacklisted (e.g. previously revoked Certificates and rejected Certificate requests due to suspected phishing) by Trustgate CA, other external sources such as government denied lists, internationally recognised denied persons lists or that is located in a country with which the law of Malaysia prohibit doing business.

4.1.2 Enrolment Process and Responsibilities

Trustgate CA maintains systems and processes that sufficiently authenticate the Applicant's identity for all Certificate types that present the identity to Relying Parties. Applicants must submit sufficient information to allow Trustgate CA and its RA to successfully perform the required verification. Trustgate CAs and its RAs shall protect communications and securely store information presented by the Applicant during the application process in compliance with the Trustgate CA Privacy Policy.

The enrolment process includes:

- Agreeing to the Subscriber Agreement or other applicable terms and conditions,
- Submitting a valid Certificate request form with true and correct information,
- Generating a suitable key pair,
- Delivering his, her, or its public key, directly or through an RA, to Trustgate CA, and
- Paying any applicable fees.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Trustgate CA or an RA shall perform identification and authentication of all required Subscriber information in terms of ***Section 3.2*** or complete the validation no more than 825 days prior to issuing the Certificate.

Trustgate CA maintain procedures that identity and require additional verification information for high risk Certificate requests prior to Certificate issuance. Trustgate CA ensure that its RAs provides at least the same level of assurance when identify and verify high risk Certificate requests as Trustgate CA's own processes.

4.2.2 Approval or Rejection of Certificate Applications

Trustgate CA or an RA will approve an application for a certificate if the following criteria are met:

- Successful identification and authentication of all required Subscriber information in terms of ***Section 3.2***.
- Payment has been received

Trustgate CA or an RA will reject a certificate application if:

- identification and authentication of all required Subscriber information in terms of ***Section 3.2*** cannot be completed, or
- The Subscriber fails to furnish supporting documentation upon request, or
- The Subscriber fails to respond to notices within a specified time, or
- Payment has not been received, or
- The RA believes that issuing a certificate to the Subscriber may bring the Trustgate CA into disrepute.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Certificate issuance by Trustgate CA requires an authorised Trusted role member of TrustgateCA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for Trustgate CA to perform a certificate signing operation. Trustgate CA creates and issues to an Applicant a Certificate based on the information provided in the Certificate Application following approval of such Certificate Application.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

Trustgate CA notifies the Subscriber of the issuance of a Certificate at an email address which was supplied by the Subscriber during the enrolment process or by any other equivalent method. The email may contain the Certificate itself or a link to download depending upon the work flow of the Certificate requested.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Trustgate CA informs the Subscriber that he/she may not use the Certificate until the Subscriber has reviewed and verified the accuracy of the data incorporated into the Certificate. Unless the Subscriber notifies Trustgate CA within seven (7) days from receipt, the Certificate is deemed to be accepted.

4.4.2 Publication of the Certificate by the CA

No stipulation.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Use of the private key corresponding to the public key in the certificate shall only be permitted once the Subscriber has agreed to the Subscriber agreement, other applicable terms and condition and

accepted the certificate. The certificate shall be used lawfully in accordance with Trustgate CA's Subscriber Agreement the terms of the Trustgate CA CP and this CPS. Certificate use must be consistent with the key usage and extended key usage fields as indicated in the corresponding Certificate (e.g., if Digital Signature is not enabled then the certificate must not be used for signing).

Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate. Parties other than the Subscriber shall not archive the Subscriber Private Key except as set forth in ***Section 4.12***.

In the case of Trustgate CA's digital signing service and with the consent of the Subscriber, Trustgate shall host, secure and manage Certificates and corresponding Private Keys.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall assent to the terms of the applicable Relying Parties agreement as a condition of relying on the Certificate. Reliance on a Certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Parties must obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties shall independently assess:

- The appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CPS. Trustgate CA is not responsible for assessing the appropriateness of the use of a Certificate.
- That the certificate is being used in accordance with the key usage and extended key usage fields included in the Certificate (e.g., if Digital Signature is not enabled then the certificate may not be relied upon for validating a Subscriber's signature).
- The status of the Certificate and all the CAs in the chain that issued the Certificate. If any of the Certificate in the Certificate Chain have been revoked, the Relying Parties are solely responsible to investigate whether reliance on a digital signature performed by a Subscriber with a Client Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain.

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilize the software and/or hardware that fully compliant with X.509 standards including best practice to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

Certificate renewal is defined as the production of a new Certificate that has the same details as a previously issued Certificate. Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to renew a new certificate to maintain continuity of Certificate usage. A

certificate may also be renewed after expiration provided the existing Certificate has not been revoked and all details within the Certificate remain accurate.

4.6.2 Who May Request Renewal

The Subscribers or an authorized representative of the Subscribers may request certificate renewal. Certificate may be reissued using the previously accepted Public Key.

4.6.3 Processing Certificate Renewal Requests

Trustgate CA may request additional information before processing a renewal request.

4.6.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As per 4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

As per 4.4.2

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3

4.7 Certificate Re-key

Certificate rekey is the application for the issuance of a new Certificate with details which differ from a previously issued Certificate or a new Public Key. Certificate rekey is supported for all certificate Classes.

4.7.1 Circumstances for Certificate Re-Key

Prior to the expiration of an existing Subscriber's Certificate, it may be necessary for the Subscriber to re-key the certificate to maintain continuity of Certificate usage. A certificate may also be re-keyed after expiration.

4.7.2 Who May Request Certificate of a New Public Key

As per 4.1

4.7.3 Processing Certificate Re-Key Requests

As per 4.2

4.7.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.7.5 Conduct Constituting Acceptance of Re-Key Certificate

As per 4.4.1

4.7.6 Publication of the Re-Key Certificate by the CA

As per 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3

4.8 Certificate Modification

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

4.9.1.1 Reasons for Revoking a Subscriber Certificate

Trustgate CA shall entitled to revoke or may revoke a Subscriber's Certificate if Trustgate CA or its RAs have been notified that any of the events listed in this section has occurred.

Trustgate CA shall revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate;
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or
4. The CA obtains evidence that the validation of domain authorization or control for any FQDN or IP address in the Certificate should not be relied upon.

Trustgate CA should revoke a certificate within 24 hours and must revoke a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
2. The CA obtains evidence that the Certificate was misused;
3. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. The CA obtains evidence that the validation of the domain authorization or control for any FQDN or IP address in the Certificate should not be relied upon;
5. The CA is made aware of any circumstance indicating that use of a FQDN or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
6. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
7. The CA is made aware of a material change in the information contained in the Certificate;
8. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's CP or CPS;
9. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate or misleading;
10. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
11. Revocation is required by the CA's CP and/or CPS;
12. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed;
13. The affiliation between an Enterprise Customer with a Subscriber is terminated or has otherwise ended;
14. The Subscriber has not made payment when due;
15. The technical content of format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties;
16. Any other reason that may be reasonably expected to affect the integrity, security or trustworthiness of a Certificate or CA; or
17. The continued use of the Certificate is harmful to the Trustgate CA

When considering whether certificate usage is harmful to the Trustgate CA, Trustgate CA considers, among other things, the following:

- The nature and number of complaints received
- The identity of the complainant(s)
- Relevant legislation in force
- Responses to the alleged harmful use from the Subscriber

4.9.1.2 Revoking a Subscriber Certificate

Trustgate CA shall revoke a Subordinate CA Certificate within 7 days if one or more of the following occurs

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies Trustgate CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. Trustgate CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
4. Trustgate CA obtains evidence that the Certificate was misused;
5. Trustgate CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable CP or CPS;
6. Trustgate CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. Trustgate CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. Trustgate CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the Issuing CA's CP and/or CPS.

4.9.2 Who Can Request Revocation

The Subscriber, RA, or Trustgate CA can initiate revocation. In the case of an affiliated organization name in the Certificate(s), a duly authorized representative of the organization shall be entitled to request the revocation of Certificates. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports to notify Trustgate CA of a suspected reasonable cause to revoke the Certificate. Trustgate CA may also at its own discretion revoke Certificates.

4.9.3 Procedure for Revocation Request

The primary method for requesting revocation request is to submit a written request by either the Subscriber or an authorised representative of the Subscriber. Trustgate CA may provide automated mechanisms for requesting and authenticating revocation requests. Trustgate CA and its RAs will

record each request for revocation and authenticate the source, taking appropriate action to revoke the Certificate if the request is authentic and approved.

Subscribers, Relying Parties, Application Software Suppliers and other third parties may submit Certificate revocation request or Certificate Problem Report via support@msctrustgate.com. Trustgate CA may or may not revoke in response to this request. Nevertheless, Trustgate CA will maintain an ability to accept and respond to a high-priority Certificate Problem Report revocation and where appropriate, forward such a complaint to law enforcement authorities and/or revoke a Certificate that is the subject of such a complaint.

4.9.4 Revocation Request Grace Period

No stipulation.

4.9.5 Time Within Which CA Must Process the Revocation Request

Within 24 hours after receiving a Certificate Problem Report, Trustgate CA shall investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, Trustgate CA shall work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which Trustgate CA will revoke the certificate. The period from receipt of the Certificate

Problem Report or revocation-related notice to published revocation must not exceed the time frame set forth in *Section 4.9.1.1*. The date selected by Trustgate CA should consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
5. Relevant legislation.

4.9.6 Revocation Checking Requirements for Relying Parties

No stipulation.

4.9.7 CRL Issuance Frequency

For the status of Subscriber Certificates:

Trustgate CA updates and reissues CRLs every 24 hours and is valid for 7 days.

For the status of Subordinate CA Certificates:

Trustgate CA updates and reissues CRLs at least (i) once every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field is not more than twelve months beyond the value of the thisUpdate field.

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9 On-Line Revocation/Status Checking Availability

Trustgate CA supports OCSP responses in addition to CRLs. Response times are generally no longer than 15 seconds under normal network operating conditions.

Trustgate CA's OCSP responses conform to RFC6960 and/or RFC5019. The OCSP responses either:

1. Be signed by Trustgate CA that issued the Certificate whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose Certificate is signed by Trustgate CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 On-Line Revocation Checking Requirements

For the status of Subscriber Certificates, Trustgate CA updates information provided via an OCSP at least every four days. OCSP responses from this service is valid for 10 days.

For the status of Subordinate CA Certificates, Trustgate CA updates information provided via an OCSP at least (i) every 12 months and (ii) within 24 hours after revoking a Subordinate CA Certificate.

If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder should not respond with a "good" status. Trustgate CA monitors the responder for such requests as part of its security response procedures.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation

4.9.12 Special Requirements Related to Key Compromise

See Section 4.9.1.

4.9.13 Circumstances for Suspension

The Repository does not include entries that indicate that a Certificate is suspended.

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

Trustgate CA does not remove revocation entries on CRL or OCSP until after the Expiry Date of the revoked Certificate.

4.10.2 Service Availability

Trustgate CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of 10 seconds or less under normal operating conditions.

Trustgate CA maintains an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by Trustgate CA.

Trustgate CA maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3 Operational Features

No stipulation.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

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 Controls

5.1.1 Site Location and Construction

Trustgate CA's computer systems for CA services is located within a secure data centre in Cyberjaya, Malaysia. The data centre is a purpose built facility made of concrete and steel construction. Trustgate CA maintains physical and environmental security policies for systems used for CA services and management which cover physical access control, protection against thief and breaking, fire safety factors, failure of supporting utilities (e.g. power, telecommunications) and disaster recovery.

5.1.2 Physical Access

Trustgate CA systems are protected by a minimum of four tiers of physical security, with access to the lower tier required before gaining access to the higher tier.

Progressively restrictive physical access privileges control access to each tier. Sensitive CA operational activities, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Access to each tier requires the use of a proximity card employee badge. Physical access is automatically logged and video recorded. Additional tiers enforce individual access control through the use of two factor authentication including biometrics. Unescorted personnel, including untrusted employees or visitors, are not allowed into such secured areas.

The physical security system includes additional tiers for key management security which serves to protect both online and offline storage of CSUs and keying material. Areas used to create and store cryptographic material enforce dual control, each through the use of two factor authentication including biometrics. Online CSUs are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material is restricted in accordance with Trustgate CA's segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes.

5.1.3 Power and Air Conditioning

Trustgate CA's secure facilities are equipped with primary and backup:

- power systems to ensure continuous, uninterrupted access to electric power and
- heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

Trustgate CA is secure data centre is located on a higher floor with raised flooring. In addition, a water detection alarm system is in place and on site data centre operations staff are ready to respond to any unlikely water exposure.

5.1.5 Fire Prevention and Protection

Trustgate CA operates within a secure data centre that is equipped with a fire detection and suppression system.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

5.1.7 Waste Disposal

All sensitive documents and material are shredded before disposal. Trustgate CA ensures that all media used for the storage of information is rendered unreadable before being released for disposal.

5.1.8 Off-Site Backup

Trustgate CA performs routine off-site backup of critical data, audit log data and other information. The backed up data is stored at a physically secured off-site location.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trustgate CA ensures that all employees including vetting agents who have access to or perform the CA operations below are acting in the capacity of a trusted role:

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests;
- the issuance or revocation of Certificates, including personnel having access to restricted portions of its repository;
- the handling of Subscriber information or requests.

Trusted roles include but are not limited to the following:

- Customer Service/Vetting Personnel,
- CA operations personnel,
- Information Security personnel,
- System Administration/Engineer personnel,
- Developer personnel,
- Internal Auditor,
- Infrastructure personnel, and
- RA administrator

Trustgate CA considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements set out in this CPS.

5.2.2 Number of Persons Required per Task

Trustgate CA has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (e.g. CSU) and associated key material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and

logical access to the device. Persons with physical access to modules do not hold “Secret Shares” and vice versa.

Other manual operations such as the validation and issuance of Class 3 Certificates, not issued by an automated validation and issuance system, require the participation of at least 2 Trusted Persons, or a combination of at least one trusted person and an automated validation and issuance process. Manual operations for Key Recovery may optionally require the validation of two (2) authorized Administrators.

5.2.3 Identification and Authentication for Each Role

Before appointing a person to a trusted role, Trustgate CA performs a background check. Each role described above is identified and authenticated in a manner to guarantee that the right person has the right role to support the CA.

5.2.4 Roles Requiring Separation of Duties

Trustgate CA enforces role separation either by the CA equipment or procedurally or by both means. Roles requiring Separation of duties include (but are not limited to)

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, recovery requests or renewal requests, or enrolment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository;
- the handling of Subscriber information or requests
- the generation, issuing or destruction of a CA certificate
- the loading of a CA to a Production environment

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience and Clearance Requirements

Trustgate CA requires that personnel seeking to become Trusted Persons present proof of the requisite background and possess the expert knowledge, experience and qualifications necessary to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts. Trustgate CA personnel fulfil the requirement through expert knowledge, experience and qualifications with formal training and education, actual experience or a combination of the two.

5.3.2 Background Check Procedures

Prior to commencement of employment in a Trusted Role, Trustgate CA conducts background checks which include the following:

- confirmation of previous employment,
- check of professional reference,

- confirmation of the highest or most relevant educational degree obtained,
- search of criminal records (local, state or provincial, and national),
- check of credit/financial records,
- search of driver's license records, and
- search of QIIS records

To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, Trustgate CA will utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted roles or for taking action against an existing Trusted Person generally include (but are not limited to) the following:

- misrepresentations made by the candidate or Trusted Person,
- highly unfavourable or unreliable professional references,
- certain criminal convictions, and
- indications of a lack of financial responsibility.

Reports containing such information are evaluated by human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behaviour uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

The use of information revealed in a background check to take such actions is subject to the applicable federal, state, and local laws.

5.3.3 Training Requirements

Trustgate CA ensures that all personnel performing duties with respect to the operation of the CA receive comprehensive training in:

- Public Key Infrastructure knowledge;
- CA/RA security principles and mechanisms;
- Software versions in use on the CA system;
- Duties they are expected to perform such as authentication and vetting policies including CP and CPS; and
- Disaster recovery and business continuity procedures.

Trustgate CA and RA personnel are retrained when changes occur in Trustgate CA or RA systems. Refresher training is conducted as required and Trustgate CA shall review refresher training requirements at least once per year.

5.3.4 Retraining Frequency and Requirements

Trustgate CA provides refresher training and updates to its personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

Trustgate CA provides information security and privacy training at least once a year to all employees.

5.3.5 Job Rotation Frequency and Sequence

Trustgate CA ensures that any change in the staff will not affect the operational effectiveness of the service or the security of the system.

5.3.6 Sanctions for Unauthorised Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of Trustgate CA's policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Roles. Any such contractor or consultant is held to the same functional and security criteria that apply to a Trustgate CA's employees in a comparable position.

5.3.8 Documentation Supplied to Personnel

Trustgate CA provides its employees the requisite training, this CPS, CP and all relevant documentations such as technical operational and administrative needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Trustgate CA and its RA shall record details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. Trustgate CA shall make these records available to its Qualified Auditor as proof of the CA's compliance with these Requirements.

Trustgate CA shall record at least the following events:

1. CA key lifecycle management events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction; and
    b. Cryptographic device lifecycle management events.
2. CA and Subscriber Certificate lifecycle management events, including:
    a. Certificate requests, renewal, and re-key requests, and revocation;
    b. All verification activities stipulated in these Requirements and the CA's CPS;

c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;

d. Acceptance and rejection of certificate requests;

e. Issuance of Certificates; and

f. Generation of Certificate Revocation Lists and OCSP entries.

3. Security events, including:

a. Successful and unsuccessful PKI system access attempts;

b. PKI and security system actions performed;

c. Security profile changes;

d. System crashes, hardware failures, and other anomalies;

e. Firewall and router activities; and

f. Entries to and exits from the CA facility.

Log entries MUST include the following elements:

1. Date and time of entry;
2. Identity of the person making the journal entry; and
3. Description of the entry.

5.4.2 Frequency of Processing Log

The CA system and audit logs are continuously monitored to provide real time alerts of significant security and operational events. In addition, Trustgate CA periodically reviews its audit logs for suspicious or evidence of malicious activity in response to alerts generated based on irregularities and incidents within Trustgate CA and RA systems.

Audit log processing consists of a review of the audit logs and documentation for all significant events in an audit log summary. Audit log reviews include a verification that the log has not been tampered with, an inspection of all log entries, and an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also documented.

5.4.3 Retention Period for Audit Log

Log records related to transaction are held for a period of time as appropriate to provide necessary legal evidence in accordance with any applicable legislation. Other logs such as system or access are held for a period time as appropriate.

5.4.4 Protection of Audit Log

Events are logged with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, tampering or destroyed. The audit log files are protected to ensure that only individuals with authorised trusted access are able to perform any operations without modifying integrity, authenticity and confidentiality of the data.

5.4.5 Audit Log Backup Procedures

Incremental backups of audit logs are created daily and full backups are performed weekly by authorised Trusted Personnel. The backup are stored in a secure location (e.g. file proof safe).

5.4.6 Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by Trustgate CA personnel.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

Trustgate CA's security program includes an annual Risk Assessment that:

a. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;

b. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and

c. Assesses the sufficiency of the policies, procedures, information

5.5 Records Archival

5.5.1 Types of Records Archived

Trustgate CA archives audit log files, system information and network information but not limited to the following:

- All audit data collected in terms of ***Section 5.4***
- Certificate application information
- Documentation supporting certificate applications and verification
- Certificate lifecycle information e.g., revocation, rekey and renewal application information

5.5.2 Retention Period for Archive

Records shall be retained for minimum periods set forth below following the date the Certificate expires or is revoked.

Five (5) years for Class 1 Certificates,

Ten (10) years for all other Certificates

5.5.3 Protection of Archive

Trustgate CA protects the archive so that only authorized Trusted Persons are able to obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a trustworthy system. The media holding the archive data and the

applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CPS.

5.5.4 Archive Backup Procedures

Trustgate CA incrementally backs up electronic archives of its issued Certificate information on a daily basis and performs full backups on a weekly basis. Copies of paper-based records shall be maintained in an off-site secure facility.

5.5.5 Requirements for Timestamping of Records

All entries in the log files shall contain time and date information at which the event occurred.

5.5.6 Archive Collection System (Internal or External)

The archive collection system complies with the requirements in Section 5.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified by checking the readability of the information.

5.6 Key Changeover

Trustgate CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in Section 6.3. Trustgate CA Certificates may be renewed as long as the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs will be generated, for example to replace CA key pairs that are being retired, to supplement existing, to support the continuation of CA services.

Prior to the expiration of the CA Certificate, the CA key changeover procedures are enacted to facilitate a smooth transition and minimal disruption to Subscribers and Relaying Parties.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Trustgate CA handles incident and compromise according to Incident Response Plan and Disaster Recovery plan in order to minimise the impact of such events. Trustgate CA's incident and compromise handling procedures designed to notify and reasonably protect ASS, Subscribers, and Relying Parties in the event of a disaster.

Trustgate CA does not disclose its business continuity plans but shall make its business continuity plan and security plans available to its auditors upon request.

The business continuity plan includes:

1. The conditions for activating the plan,
2. Emergency procedures,
3. Fallback procedures,
4. Resumption procedures,

5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans.
10. The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time
13. How frequently backup copies of essential business information and software are taken;
14. The distance of recovery facilities to the CA's main site; and
15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

5.7.2 Recovery Procedures if Computing Resources, Software and/or Data Are Corrupted

In the event of the corruption of computing resources, software, and/or data, Trustgate CA's incident response handling procedures are enacted. Such procedures require incident investigation and incident response. If necessary, Disaster Recovery procedures will be enacted to quickly re-establish the CA services.

5.7.3 Recovery Procedure After Key Compromise

In the event a Trustgate CA Private Key is Compromised:

Trustgate CA shall revoke the CA Certificate and communicate to all the Subscribers who have been issued a Certificate on the revoke status at the earliest feasible time. A new Trustgate CA Key Pair shall be generated or an alternative existing CA hierarchy shall be used to create new Subscriber Certificates.

5.7.4 Business Continuity Capabilities After a Disaster

Trustgate CA has created and maintains business continuity plan so that in the event of a disruption, critical business functions will be resumed. Trustgate CA maintains a disaster recovery facility located at a separate secure location from the primary production facility. Trustgate CA maintains redundant hardware and backups of its CA and infrastructure system software at its disaster recovery facility. In addition, CA private keys are backed up and maintained for disaster recovery purposes in accordance with ***Section 6.2.4***.

5.8 CA or RA Termination

In the event that it is necessary for a Trustgate CA, or Enterprise Customer CA to cease operation, Trusgate CA makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, Trustgate CA will develop a termination plan to minimize disruption to Customers, Subscribers, and Relying Parties. Such termination plans may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA;
- The revocation of the Certificate issued to the CA by Trustgate CA;
- The preservation of the CA's archives and records for the time periods required in this CPS;
- The continuation of Subscriber and customer support services;
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services;
- The revocation of unexpired unrevoked Certificates of end-user Subscribers and subordinate CAs, if necessary;
- Disposition of the CA's private key and the hardware tokens containing such private key, and
- Provisions needed for the transition of the CA's services to a qualified successor CA.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

For Root CA Key Pairs created after the Effective Date that are either (i) used as Root CA Key Pairs or (ii) Key Pairs generated for a subordinate CA that is not the operator of the Root CA or an Affiliate of the Root CA, the CA shall:

1. prepare and follow a Key Generation Script,
2. have a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process, and
3. have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

For other CA Key Pairs created after the Effective Date that are for the operator of the Root CA or an Affiliate of the Root CA, the CA should:

1. prepare and follow a Key Generation Script and
2. have a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process.

In all cases, the CA shall:

1. generate the keys in a physically secured environment as described in the CA's CP and/or CPS;
2. generate the CA keys using personnel in trusted roles under the principles of multiple person control and split knowledge;
3. generate the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's CP and/or CPS;
4. log its CA key generation activities; and
5. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its CP and/or CPS and (if applicable) its Key Generation Script.

6.1.1.2 RA Key Pair Generation

No stipulation.

6.1.1.3 Subscriber Key Pair Generation

Generation of a secure key pairs is generally performed by the Subscriber or Applicant to be used in association with the Subscriber's Certificate. However, there are occasion where Subscriber's key pairs are generated by Trustgate CA. For Client Certificate, the Subscriber and Trustgate CA typically use a certified cryptographic device that meets or exceeds the requirement defined in ***Section 6.2.11*** for key generation. For server Certificates, the Subscriber typically uses the key generation utility provided with the web server software.

Trusgate CA will reject a Certificate request if the requested Public key does not meet the requirements set forth in Section 6.1.5 and 6.1.6 or if it has a known weak Private key (e.g. Debian weak key).

6.1.2 Private Key Delivery to Subscriber

Trustgate CA may generate and deliver Key pair one behalf of the Subscribers for Client Certificate only. In the case where the Key pair is created on behalf of Subscribers by Trustgate CA, the Private key shall be delivered to the Subscribers in a secure manner. The data required to activate the device is communicated to the Subscriber using an out of band process. The distribution of such devices is logged by Trustgate CA.

6.1.3 Public Key Delivery to Certificate Trustgate CA

Subscribers and RAs submit their public keys to Trustgate CA as part of Certificate Application process through the use of a PKCS#10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Secure Sockets Layer (SSL). The signature of the CSR will be verified by Trustgate CA prior to issuance of Certificates.

6.1.4 CA Public Key Delivery to Relying Parties

Trustgate CA publishes its root CAs at www.msctrustgate.com/respository for Subscribers and Relying Parties to download. For Root Certificate Public-Keys, Trustgate CA makes available through their inclusion in web browser software or operating system. As new Root Certificates Public Keys

are generated, Trustgate CA provides such new Certificates to the browser manufacturers for inclusion in new browser releases and updates.

6.1.5 Key Sizes

Trustgate CA follows Baseline Requirements and EV Guideline – Key Sizes - for recommended timelines and best practices in the choice of Key Pairs for Root CAs, Subordinate CAs and Certificates delivered to Subscribers. Any Subordinate CAs in the Trusted Root program, outside of the direct control of Trustgate CA are contractually obligated to use the same best practices.

6.1.5.1 RSA

- 2048 bit RSA key with Secure Hash Algorithm 2 (SHA-256)
- 4096 bit RSA key with Secure Hash Algorithm 2 (SHA-384)
- 6144 bit RSA key with Secure Hash Algorithm 2 (SHA-512)

6.1.5.2 ECC

- 256 bit ECDSA key with Secure Hash Algorithm 2 (SHA-256)
- 384 bit ECDSA key with Secure Hash Algorithm 2 (SHA-384)
- 521 bit ECDSA key with Secure Hash Algorithm 2 (SHA-512)

6.1.6 Public Key Parameters Generation and Quality Checking

For RSA, Trustgate CA shall confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent should be in the range between 216+1 and 2256-1. The modulus should also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752.

For ECC, Trustgate CA should confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine.

Trustgate CA sets key usage of Certificates depending on their proposed field of application via the v3 Key Usage Field for X.509 v3 (see Section 7.1).

6.1.7 Key usage Purposes

Private Keys corresponding to Root Certificates must not be used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and
4. Certificates for OCSP Response verification.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Trustgate CA implements physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the validated system or device specified above consists of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA Private Key. Trustgate CA encrypts its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic Module Standards and Controls

Trustgate CA ensures that all CA systems signing Certificates use minimum FIPS 140-2 level 3 requirement or higher of cryptographic protection. Trustgate CA requires Subscribers to use FIPS 140-2 level 2 requirement or above for Private Key protection.

6.2.2 Private Key (n out of m) Multi-Person Control

Trustgate CA has implemented technical and procedural mechanisms that require the participation of multiple Trusted Persons to perform sensitive CA cryptographic operations. Trustgate CA uses “Secret Sharing” to split the activation data needed to make use of a CA private key into separate parts called “Secret Shares” which are held by trained and Trusted Persons called “Shareholders.” A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a CA private key stored on the module. The threshold number of shares needed to sign a CA certificate is 3.

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

See ***Section 5.2.2***.

6.2.5 Private Key Archival

Upon expiration of a CA Certificate, the key pairs associated with the CA Certificates will be securely arhived to HSMs that meet the requirements of this CPS. These CA key pairs shall not be used for any signing events after the expiration date of the corresponding CA Certificates, unless the CA Certificates have been renewed in terms of this CPS.

Trustgate CA does not archive copies of RA and Subscriber private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Trustgate CA generates CA key pairs on the HSM in which the keys will be used. In addition, Trustgate CA makes copies of such CA key pairs for routine recovery and disaster recovery purposes. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

If Trustgate CA becomes aware that a Subordinate CA’s Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then Trustgate CA

shall revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.2.7 Private Key Storage on Cryptographic Module

Trustgate CA private keys held on HSM which meets FIPS 140-2 level 3 requirement or above.

6.2.8 Activating Private Key

Trustgate CA is responsible for activating the Private Key in accordance with the instructions and documentation provided by the manufacturer of the hardware security module. Subscribers are responsible for protecting Private Keys in accordance with the obligations that are presented in the Subscriber Agreement or Terms of Use.

6.2.9 Deactivating Private Key

Trustgate CA Private Keys shall be deactivated when they are no longer needed or when the Certificates to which they correspond have expired or have been revoked. Trustgate CA is responsible for deactivatng the Private Key in accordance with the instructions and documentation provided by the manufacturer of the hardware security module.

6.2.10 Destroying Private Key

Trustgate CA Private Keys are destroyed when they are no longer needed or when the Certificates to which they correspond have expired or have been revoked. Trustgate CA utilizes the zeroization function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys. When performed, CA key destruction activities are logged.

6.2.11 Cryptographic Module Capabilities

See Section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Trustgate CA archives Public Keys from Certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Trustgate CA Certificates and renewed Certificates have a maximum Validity Period of:

Type			Private Key Usage		Max Validity Period
1	Root Certificates		20 years		30 years
2	DV SSL		No stipulation		825 days (27 months)
3	OV SSL		No stipulation		825 days (27 months)
4	EV SSL		No stipulation		27 months
5	AATL Certificates		No stipulation		825 days (27 months)
6	Timestamping Certificates		11 years		133 months

Trustgate CA complies with the Baseline Requirements with respect to the maximum Validity Period. In the event that a Subscriber's Certificate has a reduced validity period, subsequent reissues may be used to regain that lost validity period.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation Activation data (Secret Shares) used to protect tokens containing Trustgate CA private keys is generated in accordance with the requirements of ***Section 6.1.1*** and the Key Ceremony Reference Guide. Activation data is either generated automatically by the appropriate HSM or in such a way that meets the same needs. The creation and distribution of Activation data is logged.

6.4.2 Activation Data Protection

No stipulation.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Trustgate CA ensures that the systems maintaining CA software and data files are secure from unauthorized access. Access to production CA systems by those with authorization are required to use hardware token in conjunction with a PIN.

Trustgate CA's computer security control include the following:

- physical security and environmental controls;
- system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
- network security and firewall management, including port restrictions and IP address filtering;
- user management, separate trusted-role assignments, education, awareness, and training; and
- logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

Trustgate CA enforces multi-factor authentication for all account capable of issuance Certificate.

6.5.2 Computer Security Rating

No stipulation.

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

Trustgate CA make use of Commercial Off The Shelf products for hardware, software and network components. Applications developed and implemented by Trustgate CA in accordance with Trustgate

CA systems development and change management standards. Trustgate CA also provides software to its Enterprise Customers for performing RA and certain CA functions. Such software is developed in accordance with Trustgate CA system development standards.

6.6.2 Security Management Controls

The configuration of the Trustgate CA system as well as any modifications and upgrades are documented and controlled. There is a mechanism for detecting unauthorised modification to the Trustgate CA software or configuration to ensure the integrity of CA system. A formal configuration management methodology is used for installation and on-going maintenance of the Trustgate CA system.

6.6.3 Lifecycle Security Controls

No stipulation.

6.7 Network Security Controls

Trustgate CA performs all its CA functions using networks secured in accordance with its security policy to prevent unauthorized access and other malicious activities such as denial of service and intrusion attacks. Trustgate CA protects its communications of sensitive information through the use of encryption, firewall and filtering routers. Unused network ports and services are turned off.

6.8 Time Stamping

Trustgate CA provides a Time Stamp Authority (TSA) service for use with document signing Certificates. The TSA complies to RFC 3161. For more information, please refer to Trusgate CA's TSA Policy.

7. Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

Trustgate CA Certificates generally conform to (a) ITU-T Recommendation X.509 version 3 and (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. As applicable to the Certificate type, Trustgate CA Certificates conform to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

Trustagte CA generates non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits.

7.1.1 Version Number(s)

Trustgate CA issues Certificates in compliance with X.509 Version 3.

7.1.2 Certificate Extensions

Trustgate CA issues Certificates in compliance with RFC 5280, Baseline Requirements section 7.1.2.1 to section 7.1.2.5 and applicable best practice.

7.1.2.1 Root CA Certificate

a. basicConstraints

This extension must appear as a critical extension. The cA field must be set to true. The pathLenConstraint field should not be present.

b. keyUsage

This extension must be present and must be marked as critical. Bit positions for keyCertSign and cRLSign must be set. If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit must be set

c. certifcatePolicies

This extension must not be present.

d. extendedKeyUsage

This extension must not be present.

7.1.2.2 Subordinate CA Certificate

a. CertificatePolicies

This extension must be present and should not be marked as critical.

certificatePolicies:policyIdentifier (Required)

The following fields may be present if the Subordinate CA is not an Affiliate of the entity that controls the Root CA.

certificatePolicies:policyQualifiers:policyQualifierId (Optional)

- id-qt 1 [RFC 5280].

certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

- HTTP URL for the Root CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the CA.

b. cRLDistributionPoints

This extension must be present and must not be marked as critical. It must contain the HTTP URL of the CA's CRL service

c. authorityInformationAccess

With the exception of stapling, which is noted below, this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It SHOULD also contain the HTTP URL of the Issuing CA's

certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

The HTTP URL of the Issuing CA's OCSP responder MAY be omitted, provided that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshakes [RFC4366].

d. basicConstraints

This extension MUST be present and MUST be marked as critical. The cA field MUST be set to true. The pathLenConstraint field MAY be present

e. keyUsage

This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.

f. nameConstraints (optional)

If present, this extension SHOULD be marked as critical*.

*Non-critical Name Constraints are an exception to RFC 5280 (4.2.1.10), however, they MAY be used until the Name Constraints extension is supported by Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide

g. extkeyUsage (optional)

For Subordinate CA Certificates to be Technically constrained in line with *Section 7.1.5*, then either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present**.

Other values MAY be present. If present, this extension SHOULD be marked non-critical.

** Generally Extended Key Usage will only appear within end entity certificates (as highlighted in RFC 5280 (4.2.1.12)), however, Subordinate CAs MAY include the extension to further protect relying parties until the use of the extension is consistent between Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide

7.1.2.3 Subscriber Certificate

a. certificatePolicies

This extension MUST be present and SHOULD NOT be marked critical.

certificatePolicies:policyIdentifier (Required)

A Policy Identifier, defined by the issuing CA, that indicates a Certificate Policy asserting the issuing CA's adherence to and compliance with these Requirements.

The following extensions MAY be present:

certificatePolicies:policyQualifiers:policyQualifierId (Recommended)

- id-qt 1 [RFC 5280].

certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

- HTTP URL for the Subordinate CA's Certification Practice Statement, Relying Party Agreement or other pointer to online information provided by the CA

b. cRLDistributionPoints

This extension MAY be present. If present, it MUST NOT be marked critical, and it MUST contain the HTTP URL of the CA's CRL service.

c. authorityInformationAccess

With the exception of stapling, which is noted below, this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It SHOULD also contain the HTTP URL of the Issuing CA's

certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

The HTTP URL of the Issuing CA's OCSP responder MAY be omitted provided that the Subscriber "staples" OCSP responses for the Certificate in its TLS handshakes [RFC4366].

d. basicConstraints (optional)

The cA field MUST NOT be true.

e. keyUsage (optional)

If present, bit positions for keyCertSign and cRLSign MUST NOT be set.

f. extKeyUsage (required)

Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present. id-kp-emailProtection [RFC5280] MAY be present. Other values SHOULD NOT be present.

7.1.2.4 All Certificate

All other fields and extensions MUST be set in accordance with RFC 5280. The CA SHALL NOT issue a Certificate that contains a keyUsage flag, extendedKeyUsage value, Certificate extension, or other data not specified in *Section 7.1.2.1*, *7.1.2.2*, or *7.1.2.3* unless the CA is aware of a reason for including the data in the Certificate.

The CA SHALL NOT issue a Certificate with:

a. Extensions that do not apply in the context of the public Internet (such as an extendedKeyUsage value for a service that is only valid in the context of a privately managed network), unless:
    i. such value falls within an OID arc for which the Applicant demonstrates ownership, or
    ii. the Applicant can otherwise demonstrate the right to assert the data in a public context; or
b. semantics that, if included, will mislead a Relying Party about the certificate information verified by the CA (such as including extendedKeyUsage value for a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

7.1.2.5 Application of RFC 5280

For purposes of clarification, a Precertificate, as described in RFC 6962 – Certificate Transparency, shall not be considered to be a "certificate" subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile under the Baseline Requirements.

7.1.3 Algorithm Object Identifiers

Trustgate CA issues Certificates with algorithms indicated by the following OIDs:

- **SHA256WithRSAEncryption** {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
- **SHA284WithRSAEncryption** {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}
- **ECDSAWithSH256** {iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 2 }
- **ECDSAWithSHA384** {iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 3 }
- **ECDSAWithSHA512** {iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 4 }

7.1.4 Name Forms

7.1.4.1 Issuer Information

The content of the Certificate Issuer Distinguished Name field MUST match the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280, *Section 4.1.2.4*.

7.1.4.2 Subject Information – Subscriber Certificate

By issuing the Certificate, the CA represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate. CAs SHALL NOT include a Domain Name or IP Address in a Subject attribute except as specified in *Sections 3.2.2.4* or *3.2.2.5*.

7.1.4.2.1 Subject Alternative Name Extension

Certificate Field: extensions:subjectAltName

Required/Optional: Required

Contents: This extension MUST contain at least one entry. Each entry MUST be either a dNSName containing the FQDN or an iPAddress containing the IP ad- dress of a server. The CA MUST confirm that the Applicant controls the FQDN or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate. Wildcard FQDNs are permitted.

As of the Effective Date of these Requirements, prior to the issuance of a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name, the CA SHALL notify the Applicant that the use of such Certificates has been

deprecated by the CA / Browser Forum and that the practice will be eliminated by October 2016. Also as of the Effective Date, the CA SHALL NOT issue a certificate with an Expiry Date later than 1 November 2015 with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name. Effective 1 October 2016, CAs SHALL revoke all unexpired Certificates whose subjectAlternativeName extension or Subject commonName field contains a Reserved IP Address or Internal Name. Effective May 1, 2015, each CA SHALL revoke all unexpired Certificates with an Internal Name using onion as the right-most label in an entry in the subjectAltName Extension or commonName field unless such Certificate was issued in accordance with Appendix F of the EV Guidelines.

7.1.4.2.2 Subject Distinguished Name Fields

Certificate Field: subject:commonName (OID 2.5.4.3)

Required/Optional: Deprecated (Discouraged, but not prohibited)

Contents: If present, this field MUST contain a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension (see Section 7.1.4.2.1).

Certificate Field: subject:organizationName (OID 2.5.4.10)

Required/Optional: Optional

Contents: If present, the subject:organizationName field MUST contain either the Subject's name or DBA as verified under Section 3.2.2.2. The CA may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name". Because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, the CA MAY use the subject:organizationName field to convey a natural person Subject's name or DBA.

Certificate Field: subject:givenName (2.5.4.42) and subject:surname (2.5.4.4)

Required/Optional: Optional

Contents: If present, the subject:givenName field and subject:surname field MUST contain an natural person Subject's name as verified under Section 3.2.3. A Certificate containing a sub- ject:givenName field or subject:surname field MUST contain the (2.23.140.1.2.3) Certificate Policy OID.

Certificate Field: Number and street: subject:streetAddress (OID: 2.5.4.9)

Optional if the subject:organizationName field, subject: givenName field, or subject:surname field are present.

Prohibited if the subject:organizationName field, subject:givenName, and subject:surname field are absent.

Contents: If present, the subject:streetAddress field MUST contain the Subject's street address information as verified under Section 3.2.2.1.

Certificate Field: subject:localityName (OID: 2.5.4.7)

Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and the subject:stateOrProvinceName field is absent.

Optional if the subject:stateOrProvinceName field and the subject:organizationName field, subject:givenName field, or subject:surname field are present.

Prohibited if the subject:organizationName field, subject:givenName, and subject:surname field are absent.

Contents: If present, the subject:localityName field MUST contain the Subject's locality information as verified under Section 3.2.2.1. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2(g), the localityName field MAY contain the Subject's locality and/or state or province information as verified under Section 3.2.2.1.

Certificate Field: subject:stateOrProvinceName (OID: 2.5.4.8)

Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and subject:localityName field is absent.

Optional if the subject:localityName field and the subject:organizationName field, and subject:givenName field , or subject:surname field are present.

Prohibited if the subject:organizationName field, subject:givenName field , or subject:surname field are absent.

Contents: If present, the subject:stateOrProvinceName field MUST contain the Subject's state or province information as verified under Section 3.2.2.1. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2(g), the subject:stateOrProvinceName field MAY contain the full name of the Subject's country information as verified under Section 3.2.2.1.

Certificate Field: subject:postalCode (OID: 2.5.4.17)

Optional if the subject:organizationName, subject:givenName field, or subject:surname fields are present.

Prohibited if the subject:organizationName field, subject:givenName field, or subject:surname field are absent.

Contents: If present, the subject:postalCode field MUST contain the Subject's zip or postal information as verified under Section 3.2.2.1

Certificate Field: subject:countryName (OID: 2.5.4.6)

Required if the subject:organizationName field, subject:givenName, or subject:surname field are present.

Optional if the subject:organizationName field, subject:givenName field, and subject:surname field are absent.

Contents: If the subject:organizationName field is present, the subject:countryName MUST contain the two-letter ISO 3166-1 country code associated with the location of the Subject verified under Section 3.2.2.1. If the subject:organizationName field is absent, the subject:countryName field MAY contain the two-letter ISO 3166-1 country code associated with the Subject as verified in accordance with Section 3.2.2.3. If a Country is not represented by an official ISO 3166-1 country code, the CA MAY specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

Certificate Field: subject:organizationalUnitName

Required/Optional: Optional

The CA SHALL implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with Section 3.2 and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 3.2.2.1.

Other Subject Attributes

All other optional attributes, when present within the subject field, MUST contain information that has been verified by the CA. Optional attributes MUST NOT contain metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.4.3 Subject Information – Root Certificate and Subordinate CA Certificate

By issuing a Subordinate CA Certificate, the CA represents that it followed the procedure set forth in its CP and/or CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.5 Name Constraints

For a Subordinate CA Certificate to be considered Technically Constrained, the certificate must include an Extended Key Usage (EKU) extension specifying all extended key usages that the Subordinate CA Certificate is authorized to issue certificates for. The anyExtendedKeyUsage KeyPurposeId must not appear within this extension.

If the Subordinate CA Certificate includes the id-kp-serverAuth extended key usage, then the Subordinate CA Certificate must include the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:

1. For each dNSName in permittedSubtrees, Trustgate CA must confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of *Section 3.2.2.4*.
2. For each iPAddress range in permittedSubtrees, Trustgae CA MUST confirm that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf. (c) For each DirectoryName in permittedSubtrees, Trustgate CA must confirm the Applicants and/or Subsidiary's Organizational name and location such that

end entity certificates issued from the subordinate CA Certificate will be in compliancy with *Section 7.1.2.4* and *7.1.2.5*.

If the Subordinate CA Certificate is not allowed to issue certificates with an iPAddress, then the Subordinate CA Certificate must specify the entire IPv4 and IPv6 address ranges in excluded-Subtrees. The Subordinate CA Certificate must include within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4 address range of 0.0.0.0/0). The Subordinate CA Certificate must also include within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0). Otherwise, the Subordinate CA Certificate MUST include at least one iPAddress in permittedSubtrees.

A decoded example for issuance to the domain and sub domains of example.com by organization: Example LLC, Boston, Massachusetts, US would be:

X509v3 Name Constraints:

Permitted:

DNS:example.com

DirName: C=US, ST=MA, L=Boston, O=Example LLC

Excluded:

IP:0.0.0.0/0.0.0.0

IP:0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0

If the Subordinate CA is not allowed to issue certificates with dNSNames, then the Subordinate CA Certificate MUST include a zero-length dNSName in excludedSubtrees. Otherwise, the Sub- ordinate CA Certificate MUST include at least one dNSName in permittedSubtrees.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Reserved Certificate Policy Identifiers

This section describes the content requirements for the Root CA, Subordinate CA, and Subscriber Certificates, as they relate to the identification of this CP.

The following Certificate Policy identifiers are reserved for use by CAs as an optional means of asserting compliance with these Requirements as follows:

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1), if the Certificate complies with these Requirements but lacks Subject Identity Information that is verified in accordance with *Section 3.2.2.1* or *Section 3.2.3*.

If the Certificate asserts the policy identifier of 2.23.140.1.2.1, then it MUST NOT include organizationName, givenName, surname, streetAddress, localityName, stateOrProvinceName, or postal- Code in the Subject field.

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2), if the Certificate

complies with these Requirements and includes Subject Identity Information that is verified in accordance with *Section 3.2.2.1*.

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) individual-validated(3)} (2.23.140.1.2.3), if the Certificate complies with these Requirements and includes Subject Identity Information that is verified in accordance with *Section 3.2.3*.

If the Certificate asserts the policy identifier of 2.23.140.1.2.2, then it MUST also include organizationName, localityName (to the extent such field is required under *Section 7.1.4.2.2*), stateOrProvinceName (to the extent such field is required under *Section 7.1.4.2.2*), and countryName in the Subject field. If the Certificate asserts the policy identifier of 2.23.140.1.2.3, then it MUST also include

i. either organizationName or givenName and surname,

ii. localityName (to the extent such field is required under *Section 7.1.4.2.2*),

iii. stateOrProvinceName (to the extent required under Section 7.1.4.2.2), and (iv) countryName in the Subject field.

7.1.6.2 Root CA Certificates

A Root CA Certificate SHOULD NOT contain the certificatePolicies extension.

7.1.6.3 Subordinate CA Certificates

A Certificate issued after the Effective Date to a Subordinate CA that is not an Affiliate of the Issuing CA:

a. MUST include one or more explicit policy identifiers that indicates the Subordinate CA's adherence to and compliance with these Requirements (i.e. either the CA/Browser Forum reserved identifiers or identifiers defined by the CA in its CP and/or CPS) and

b. MUST NOT contain the "anyPolicy" identifier (2.5.29.32.0).

A Certificate issued after the Effective Date to a Subordinate CA that is an affiliate of the Issuing CA:

1. MAY include the CA/Browser Forum reserved identifiers or an identifier defined by the CA in its CP and/or CPS to indicate the Subordinate CA's compliance with these Requirements and

2. MAY contain the "anyPolicy" identifier (2.5.29.32.0) in place of an explicit policy identifier.

A Subordinate CA SHALL represent, in its CP and/or CPS, that all Certificates containing a policy identifier indicating compliance with these Requirements are issued and managed in accordance with these Requirements.

7.1.6.4 Subscriber Certificates

A Certificate issued to a Subscriber MUST contain one or more policy identifier(s), defined by the Issuing CA, in the Certificate's certificatePolicies extension that indicates adherence to and compliance with these Requirements. CAs complying with these Requirements MAY also assert one of the reserved policy OIDs in such Certificates.

The issuing CA SHALL document in its CP or CPS that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with these Requirements..

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No Stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

7.2.1 Version Number(s)

As applicable to the Certificate type, corresponding CRLs conform to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

X.509 Version 2 CRLs conform to RFC 5280 and contain the basic fields and contents specified in table below:

Field	Value or Value constraint
Issuer	Entity who has signed and issued the CRL.
Effective Date	Issue date of the CRL. CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued. CRL issuance frequency is in accordance with the requirements of ***Section 4.4.7***.
Signature Algorithm	Algorithm used to sign the CRL in accordance with RFC 3279.
Signature Hash Algorithm	Depend on Products (e.g. SHA256)
Serial Number(s)	List of revoked serial numbers
Revoked Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

CRL Profile Basic Fields

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.3 OCSP Profile

Online Certificate Status Protocol (OCSP) is a way to obtain timely information about the revocation status of a particular certificate. Trustgate CA operates an OCSP responder in compliance with RFC 2560 and RFC 5019.

7.3.1 Version Number(s)

Version 1 of the OCSP specification as defined by RFC 2560 and Version 1 of the OCSP specification as defined by RFC 5019 are supported.

7.3.2 OCSP Extensions

No stipulation.

8. Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

Trustgate CA maintains its compliance with the CPA Canada WebTrust for CA standards identified above via a Qualified Auditor on an annual basis. The audit covers all of Trustgate CA's activities.

8.2 Identity/Qualifications of Assessor

The audit of Trustgate CA is performed by a "Qualified Auditor". A Qualified Auditor means a natural person, Legal entity, or group of natural persons or Legal Entities that collectively posses the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit as stipulated in section 8.0 of this document;
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing and the third-party attestation function;
- Certified, accredited, licensed or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme; and
- Bound by law, government regulation or professional code of ethics.
- Except in the case of Internal Government Auditng Agency, maintain Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

Trustgate CA has selected an auditor/assessor who is completely independent from Trustgate CA and approved by Malaysian Communications Multimedia Commission, an authority that licensed CA in Malaysia.

8.4 Topics Covered by Assessment

Trustgate CA shall undergo an audit in accordance with one of the following schemes:

1. Trustgate CA's CPS
2. WebTrust for CAs v2.1 or newer
3. WebTrust for CAs SSL Baseline with Network Security v2.3 or newer;
4. WebTrust for CAs Extended Validation SSL v1.6.2 or newer

If a Government CA is required by its Certificate Policy to use a different internal audit scheme, it may use such scheme provided that: (a) the audit either (i) encompasses all requirements of one of the above schemes or (ii) consists of comparable criteria that are available for public review, and (b) the audit is performed by a Qualified Auditor, who is separate from the CA. An audit scheme is applicable to Trustgate CA in the year following the adoption of the updated scheme.

8.5 Actions Taken as a Result of Deficiency

With respect to compliance audits of CA's operations, significant exceptions or deficiencies identified during the Compliance Audit, Trustgate CA shall use commercially reasonable effort to develop and implement a suitable corrective action plan.

8.6 Communications of Results

Trustgate CA shall make the Audit Report publicly available. Trustgate CA may not make publicly available any general audit findings that do not impact the overall audit opinion. Trustgate CA makes its Audit Report publicly available no later than three months after the end of the audit period.

8.7 Self Audit

Trustgate CA monitors its adherence to Certificate Policy, Certification Practice Statement and other external requirements specified ***Section 1*** by performing self audits on at least a quarterly basis against a randomly selected samples at least 3 percent (6% for EV SSL Certificate and EV Code Signing Certificates) of the Certificates issued since the last audit.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Trustgate CA charges Subscribers for the issuance, management, and renewal of Certificates. Fees are made know to Applicants via enrolment form or on Trustgate CA's website.

9.1.2 Certificate Access Fees

Trustgate CA may charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

.

9.1.3 Revocation or Status Information Access Fees

Trustgate CA may charge a fee as a condition of making the CRLs available in a repository or otherwise available to Relying Parties. Trustgate CA is, however, entitled to charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services.

9.1.4 Fees for Other Services

Trustgate CA may charge for other additional services, such as timestamping.

9.1.5 Refund Policy

Except for formal written agreement, no refunds for Certificates or services shall be provided by Trustgate CA.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Enterprise Customers are encouraged to maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention. Trustgate CA maintains general liability insurance of a maximum One million US dollars (USD1,000,000) in coverage.

9.2.2 Other Assets

No Stipulation.

9.2.3 Insurance or Warranty Coverage for End Entities

No Stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following records of Subscribers shall, subject to *Section 9.3.2*, be kept confidential and private ("Confidential/Private Information"):

- CA application records, whether approved or disapproved,
- Certificate Application records,
- Private keys held by enterprise Customers using Managed PKI Key Manager and information needed to recover such Private Keys,
- Transactional records (both full records and the audit trail of transactions),
- Audit trail records created or retained by Trustgate CA or a Customer,
- Audit reports created by Trustgate CA or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public),
- Contingency planning and disaster recovery plans, and

- Security measures controlling the operations of Trustgate CA hardware and software and the administration of Certificate services and designated enrolment services.

9.3.2 Information Not Within the Scope of Confidential Information

Any information not defined as confidential within this CPS shall be deemed public. Certificate status information and Certificates themselves are deemed public.

9.3.3 Responsibility to Protect Confidential Information

Trustgate CA' employees, agents and contractors are responsible for protecting cofidential information and are contractually to do so.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Trustgate CA protects personal information in accordance with a Privacy Policy published on Trustgate CA's web site at www.msctrustgate.com.

9.4.2 Information Treated as Private

Trustgate CA treats all information received from Applicants that will not ordinarily be placed into a Certificate, CRLs or OCSP as private. This applies both to those Applicants who are successful in being issued a Certificate and those who are unsuccessful and rejected.

9.4.3 Information Not Deemed Private

Certificate status information and any Certificate content is deemed not private.

9.4.4 Responsibility to Protect Private Information

Trustgate CA stores private information securely in accordance with a published Privacy Policy document and may store information received in either paper or digital form.

9.4.5 Notice and Consent to Use Private Information

Unless where otherwise stated in this CPS, the applicable Privacy Policy or by agreement, private information will not be used without the consent of the party to whom that information applies.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Trustgate CA may disclose private information without notice to Applicants or Subscribers where required to do so by law or regulation.

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property rights

Trustgate CA does not knowingly violate the intellectual property rights of third parties. Public and Private Keys remain the property of Subscribers who legitimately hold them. Trustgate CA retains all Intellectual Property Rights in and to the Certificates and revocation information that Trustgate CA

issue. Turtsgate CA grant Subscribers permission to reproduce and distribute Certificates on a non-exclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate.

Trustgate CA and the Trustgate logo are the registered trademarks of MSC Trustgate.com Sdn Bhd.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

By issuing a Certificate, the CA makes the certificate warranties listed herein to the following Certificate Beneficiaries:

1. The Subscriber that is a party to the Subscriber or Terms of Use Agreement for the Certificate;
2. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
3. All Relying Parties who reasonably rely on a Valid Certificate.

The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with Baseline Requirements and its CP and/or CPS in issuing and managing the Certificate.

The Certificate Warranties specifically include, but not limited to, the following:

- **Right to Use Domain Name or IP Address**: That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's Subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's CP and/or CPS;
- **Authorisation for Certificate:** That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Subject authorised the issuance of the Certificate and that the Applicant Representative is authorised to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's CP and/or CPS;
- **Accuracy of Information:** That, at the time of issuance, the CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organisationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's CP and/or CPS;
- **No Misleading Information:** That, at the time of issuance, the CA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organisationalUnitName attribute would be misleading; (ii) followed the procedure

when issuing the Certificate; and (iii) accurately described the procedure in the CA's CP and/or CPS;

- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA (i) implemented a procedure to verify the identity of the Applicant; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's CP and/or CPS;
- **Subscriber Agreement:** That, if the CA and Subscriber are not Affiliates, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the Baseline Requirements, or, if the CA and Subscriber are Affiliates, the Applicant Representative acknowledged and accepted the Terms of Use;
- **Status:** That theCA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
- **Revocation:** That the CA will revoke the Certificate for any of the reasons specified in the Baseline Requirements and/or EV Guidelines.

The Root CA SHALL be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with the Baseline Requirements, and for all liabilities and indemnification obligations of the Subordinate CA under the Baseline Requirements, as if the Root CA were the Subordinate CA issuing the Certificates .

9.6.2 RA Representations and Warranties

Trustgate CA shall require all RAs to warrant that they are in compliance with this CP and the relevant CPS and may choose to include additional representations within its CPS or RA agreement.

9.6.3 Subscriber Representations and Warranties

The CA SHALL require, as part of the Subscriber or Terms of Use Agreement, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries. Prior to the issuance of a Certificate, the CA SHALL obtain, for the express benefit of the CA and the Certificate Beneficiaries, either:

a. The Applicant's agreement to the Subscriber Agreement with the CA, or

b. The Applicant's agreement to the Terms of Use agreement.

The CA SHALL implement a process to ensure that each Subscriber or Terms of Use Agreement is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. The CA may use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber or Terms of Use Agreement. The Subscriber or Terms of Use Agreement MUST contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. **Accuracy of Information**: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;
2. **Protection of Private Key**: An obligation and warranty by the Applicant to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
3. **Acceptance of Certificate**: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. **Use of Certificate**: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber or Terms of Use Agreement;
5. **Reporting and Revocation**: An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request the CA to revoke the Certificate, in the event that: (a) any information in the Certificate is, or becomes, incorrect or inaccu- rate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate;
6. **Termination of Use of Certificate**: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
7. **Responsiveness**: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. **Acknowledgment and Acceptance**: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Agreement or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

9.6.4 Relying Party Representations and Warrantie

Relying Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CPS.

9.6.5 Representations and Warranties of Other Participants

No Stipulation.

9.7 Disclaimers of Warranties

EXCEPT TO THE EXTENT PROHIBITED BY LAW OR AS OTHERWISE PROVIDED HEREIN, TRUSTGATE CA DISCLAIMS ALL WARRANTIES INCLUDING ANY WARRANTY OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE.

9.8 Limitations of Liability

To the extent Trustgate CA has issued and managed the certificates in accordance with the baseline requirements and this CPS, Trustgate CA shall not be liable to the subscriber, relying party or any third parties for any losses suffered as a result of use or reliance on such certificates. Otherwise, Trustgate CA's liability to the subscriber, relying party or any third parties for any such losses shall in no event exceed the following:

Class	Liability Caps
Class 1	Ringgit Malaysia Five Hundred (RM 500.00)
Class 2	Ringgit Malaysia Twenty Five Thousand (RM25,000.00)
Class 3	Ringgit Malaysia Four Hundred Thousand (RM400,000.00)

In no event shall Trustgate CA be liable for any indirect, incidental, special or consequential damages or for any loss of profits, loss of data or other indirect, incidental, consequential damages arising from or in connection with the use, delivery, reliance upon, license, performance or non-performance of certificates, digital signatures or any other transactions or services offered or contemplated by this CPS.

Note: The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber agreements. The liability (and/or limitation thereof) of enterprise RAs and the applicable CA shall be set out in the agreement(s) between them. The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.9 Indemnities

9.9.1 Indemnification by Trustgate CA

Trustgate CA shall indemnify each application software supplier against any claim, damage or loss suffered by the application software supplier related to an SSL Certificate issued by Trustgate CA, regardless of the cause of action or legal theory involved, except where the claim, damage or loss suffered by the application software supplier was directly caused by the application software supplier's software displaying either (1) a valid and trustworthy Certificate as not valid or trustworthy or (2) displaying as trustworthy (i) a Certificate that has expired or (ii) a revoked Certificate where the revocation status is available online but the application software supplier's software failed to check or ignored the status.

9.9.2 Indemnification by Subscribers

To the extent permitted by applicable law, Subscribers are required to indemnify Trustgate CA for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

The applicable Subscriber Agreement may include additional indemnity obligations.

9.9.3 Indemnification by Relying Parties

To the extent permitted by applicable law, Relying Party Agreements shall require Relying Parties to indemnify Trustgate CA for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

The applicable Relying Party Agreement may include additional indemnity obligations.

9.10 Term and Termination

9.10.1 Term

This CPS remains in force until such time as communicated otherwise by Trustgate CA on its web site or Repository.

9.10.2 Termination

Notified changes are appropriately marked by an indicated version. Changes become effective immediately upon publication.

9.10.3 Effect of Termination and Survival

Upon termination of this CPS, Trustgate sub-domain participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, Trustgate CA sub-domain participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication. Individual communications made to Trustgate CA must be addressed to support@msctrustgate.com or by post to Trustgate CA in the address provided in *Section 1.5.2*.

9.12 Amendments

9.12.1 Procedure for Amendment

Changes to this CPS are indicated by appropriate numbering.

9.12.2 Notification Mechanism and Period

Trustgate CA will post appropriate notice on its web sites of any major or significant changes to this CPS as well as any appropriate period by when the revised CPS is deemed to be accepted.

9.12.3 Circumstances Under Which OID Must be Changed

No stipulation

9.13 Dispute Resolution Provisions

Disputes among Trustgate CA sub-domain participants shall be resolved pursuant to provisions in the applicable agreements among the parties.

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. Disputes involving Trustgate require an initial negotiation period of sixty (60) days followed by litigation in court of Malaysia.

9.14 Governing Law

Subject to any limits appearing in applicable law, the laws of Malaysia shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in Malaysia. This choice of law is made to ensure uniform procedures and interpretation for all Trustgate CA sub-domain participants, no matter where they are located.

This governing law provision applies only to this CPS. Agreements incorporating the CPS by reference may have their own governing law provisions, provided that this *Section 9.14* governs the enforceability, construction, interpretation, and validity of the terms of the CPS separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

9.15 Compliance with Applicable Law

Trustgate CA complies with applicable laws of Malaysia. Export of certain types of software used in certain Trustgate CA public Certificate management products and services may require the approval of appropriate public or private authorities. Parties (including Trustgate CA, Subscribers and Relying Parties) agree to comply with applicable export laws and regulations as pertaining in Malaysia.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No Stipulation.

9.16.2 Assignment

Certificates, Subscriber Agreements, Relaying Party Agreement and any rights granted under this CPS cannot be assigned, transferred or otherwise disposed of without prior written consent of Trustgate CA. Trustgate CA reserves the rights to assign, transfer and dispose any Subscriber Agreement and Relying Party Agreement to its affiliate, subsidiary or a third party as part of business transaction.

9.16.3 Severability

If any provision of this CPS, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CPS will be interpreted in such manner as to effect the original intention of the parties.

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

No Stipulation.

9.17 Other Provisions

No Stipulation