TRUSTGATE

SECURE TRANSACTION. TRUSTED BUSINESS

MSC Trustgate Certificate Policy

Version 3.1

23 April 2018

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

Certification Authority License Number: LK0022000

Certification of Recognition for Repository Number: RK0022000

Published date: 23 April 2018

Trademark Notices

ACKNOWLEDGMENTS

This Trustgate CA Certificate Policy (CP) conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction.

This CP 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

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.

1. Introduction

This Certificate Policy (CP) document is the principal statement of policy governing MSC Trustgate.com Sdn Bhd ("Trustgate CA"). The CP sets forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the Trustgate CA ecosystem and providing associated trust services. These requirements protect the security and integrity of Trustgate CA and comprise a single set of rules that apply consistently, thereby providing assurances of uniform trust throughout the Trustgate CA ecosystem. The CP is not a legal agreement between Trustgate CA and participants; rather, contractual obligations between Trustgate CA and participants are to be established by means of agreements with such participants.

This CP addresses areas of policy and practice such as, but not limited to, technical requirements, security procedures, personnel and training needs which meet industry best practices. This CP applies to all Certificates issued by Trustgate CA, including its Root Certificates. Trustgate CA Root Certificates are used to manage Certificate hierarchies that may or may not be controlled directly by the same entity that manages Trustgate CA Root Certificate itself.

Depending on the class and type of certificate, digital certificates may be used by Subscribers to secure websites, digitally sign code or other content, digitally sign documents and/or e-mails. The person who ultimately receives a signed document or communication, or accesses a secured website is referred to as a relying party and has to make a decision on whether to trust it.

This CP is final and binding between MSC Trustgate.com Sdn Bhd, Suite 2-9, Level 2, Block 4801 CBD Perdana, Jalan Perdana, 63000 Cyberjaya, Selangor Darul Ehsan, Malaysia (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.

1.1 Overview

This CP applies to the complete hierarchy of Trustgate CA and all Certificates that it issues either directly through its own systems or indirectly through its trusted root programme. The purpose of this CP is to present Trustgate CA's practices and procedures in managing Root Certificates and to demonstrate Trustgate CA's compliance with industry accepted accreditations. In this regard, Trustgate CA operates within the scope of the applicable sections of Malaysian Law.

A Certification Practice Statement (CPS) complements this CP and states, *"how the Certification Authority adheres to the Certificate Policy"*. A CPS provides an end user with a summary of the processes, procedures and overall prevailing conditions that Trustgate CA *(i.e. the entity which provides the Subscriber its Certificate)* will use in creating and managing such Certificates.

In addition to this CP and the CPS, Trustgate CA maintains additional documented policies which address such issues as:

- Business continuity and disaster recovery
- Security policy
- Personnel policies
- Key management policies
- Registration procedures

All applicable Trustgate CA policies are subject to audit by Malaysian Communications and Multimedia Commission authorised third parties which Trustgate CA highlights on its public facing web site via a WebTrust Seal of Assurance. Additional information can be made available upon request.

Certificates allow entities that participate in an electronic transaction to prove their identities to other participants or sign data digitally. By means of a Certificate, a Certification Authority provides confirmation of the relationship between a named entity (Subscriber) and its Public Key. The purpose of entering Trustgate CA hierarchy is to enhance trust, as well as providing greater functionality within third party applications, such as web browsers.

The process to obtain a Certificate includes the identification, naming, authentication and registration of an Applicant as well as aspects of Certificate management such as issuance, revocation and expiration. By means of this policy, Trustgate CA provides confirmation of the identity of the Subject of a Certificate by binding the Public Key the Subscriber uses through the issuance of a Certificate. An entity in this instance might include an end user, a corporation or another Certification Authority. Trustgate CA makes available Certificates that can be used for non-repudiation, encryption and authentication.

1.2 Document Name and Identification

MSC Trustgate.com Sdn Bhd, acting as the certification authority, has assigned an object identifier (OID) value extension for each Class of Certificate issued under the Trustgate CA ecosystem. The OID for Trustgate CA is an iso (1) identified-organisation (3) dod (6) internet (1) private (4) enterprise (1) MSC Trustgate.com Sdn. Bhd. (49530).

Trustgate CA organises its OID arcs for the various Certificates and documents in this CP as follows:

1.2.1 Client Certificates

1.3.6.1.4.1.49530.1.1.1	Class 1 Certificates
1.3.6.1.4.1.49530.1.1.2	Class 2 Certificates (Generic)
1.3.6.1.4.1.49530.1.1.2.1	Class 2 Certificates (Government)
1.3.6.1.4.1.49530.1.1.2.2	Class 2 Certificates (Enterprise)
1.3.6.1.4.1.49530.1.1.2.3	Class 2 Certificates (AATL)
1.3.6.1.4.1.49530.1.1.3	Class 3 Certificates

1.2.2 Code Signing

1.3.6.1.4.1.49530.1.2.1	Code Signing Certificates

1.2.3 Time Stamping

1.3.6.1.4.1.49530.1.3.1	Time Stamping Certificates (Generic)
1.3.6.1.4.1.49530.1.3.2	Time Stamping Certificates (AATL)

1.2.4 Domain Validation

1.3.6.1.4.1.49530.1.4.1	Domain Validation SSL Certificates

1.2.5 Organisation Validation

1.3.6.1.4.1.49530.1.5.1	Organisation Validation SSL Certificates

1.2.6 Extended Validation

1.3.6.1.4.1.49530.1.6.1	Extended Validation SSL Certificates
1.3.6.1.4.1.49530.1.6.2	Extended Validation Code Signing Certificates

1.2.7 Intranet Validation

1.3.6.1.4.1.49530.1.7.1	Intranet Validation SSL Certificates

In addition to these identifiers, all Certificates that comply with the Baseline Requirements will include the following additional identifiers:

2.23.140.1.1	Extended Validation Certificate Policy
2.23.140.1.2.1	Domain Validation Certificates Policy
2.23.140.1.2.2	Organisation Validation Certificates Policy

The Trustgate CA certificates governed by this CP 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

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

As a licenced Certification Authority in Malaysia, Trustgate CA’s primary responsibility is to perform tasks related to Public Key Infrastructure (PKI) functions such as certificate lifecycle management, subscriber registration, certificate issuance, certificate renewal, certificate distribution and certificate revocation. Certificate status information is provided using a repository in the form of a Certificate Revocation List (CRL) distribution point and/or Online Certificate Status Protocol (OCSP) responder.

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.

Trustgate CA ensures the availability of all services relating to the management of Certificates issued. Appropriate publication is necessary to ensure that Relying Parties obtain notice or knowledge of revoked Certificates. Trustgate CA provide Certificate status information using a Repository in the form of a CRL distribution point and/or OCSP responder as indicated within the Certificate properties.

1.3.2 Registration Authorities

A Registration Authority is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for end-user certificates, and approves applications for renewal or re-keying certificates on behalf of a Trustgate CA. Trustgate CA and affiliates may act as RAs for certificates they issue.

Third parties, who enter into a contractual relationship with Trustgate CA, may operate their own RA and authorise the issuance of certificates by Trustgate CA. Third party RAs must abide by all the requirements of the Trustgate CA CP, the relevant CPS and any agreement entered into with Trustgate CA. RAs may, however implement a more restrictive practices based on their internal requirements.

In order to issue certain Certificate types, RAs may need to rely on Certificates issued by third party Certification Authorities or other third party databases and sources of information, such as government national identity cards. Relying Parties are advised to review additional information by referring to such third party's CPS.

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 include all end users (including entities) of certificates issued by a Trustgate CA. A subscriber is the entity named as the end-user Subscriber of a certificate. End-user Subscribers may be individuals, organisations or, infrastructure components such as firewalls, routers, trusted servers or other devices used to secure communications within an organisation.

In most cases certificates are issued directly to individuals or entities for their own use. 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 CP to distinguish between these two roles: "Subscriber", is the entity which contracts with Trustgate CA for the issuance of credentials and "Subject", is the entity to whom the credential is bound. The Subscriber bears ultimate responsibility for the use of the credential but the Subject is the entity that is authenticated when the credential is presented.

1.3.4 Relying Parties

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature issued under this CP. A Relying party may or may not also be a Subscriber within Trustgate CA.

1.3.5 Other Participants

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

1.4 Certificate usage

A Trustgate CA Certificate allows those taking part in an electronic transaction to prove their identity to other participants in such transaction. Certificates are used in commercial environments as a digital equivalent of their identity.

1.5 Appropriate Certificate Usage

Individual Certificates are used by individuals to encrypt an e-mail, to sign a transaction and to authenticate to applications (client authentication). An individual certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, by this CP or by any CPS under which the certificate has been issued and any agreements with Subscribers.

Organisational Certificates are issued to organisations after authentication that the Organisation legally exists and that other Organisation attributes included in the certificate are authenticated, such as through ownership of domain name and email address. An organisational certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, by this CP or by any CPS under which the certificate has been issued and any agreements with Subscribers.

1.6 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 nor intended for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance where failure could lead directly to death, personal injury, or severe environmental damage.

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.

1.7 Policy Administration

1.7.1 Organisation Administering the Document

Requests for information on the compliance of Trustgate CA with any inquiry associated with this CP 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

1.7.2 Contact Person

Security and Compliance Manager
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

1.7.3 Person Determining CP Suitability for the Policy

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

In an effort to maintain credibility and promote trust in this CP and better correspond to accreditation and legal requirements, the Policy Board shall review this CP 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 CP.

1.7.4 CP Approval Procedures

Trustgate CA Policy Board reviews and approves any changes to the CP. Upon approval of a CP update by the Policy Board, the new CP is published in Trustgate CA Repository at www.msctrustgate.com/repository.

1.8 Definitions

Any terms used but not defined herein have the meaning attribute to them in the Baseline Requirements, the EV Guidelines, and/or the EV Code Signing Guidelines.

- **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:** The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Legal Entity is referred to as the Subscriber.
- **Application Software Supplier:** A supplier of Internet browser software or other Relying Party application software that displays or uses Certificates and incorporates 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, 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 Beneficiaries:** The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate, all Application Software Suppliers with whom Trustgate CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier, and all Relying Parties who reasonably rely on a Valid Certificate.
- **Certificate Data:** Certificate Requests and data related thereto (whether obtained from the Applicant or otherwise) in Trustgate CA's possession or control or to which Trustgate CA has access.
- **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 that issued the Certificates.
- **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:** A Certificate that is used to establish a trust relationship between two Root CAs.
- **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 Name:** The label assigned to a node in the Domain Name System.
- **Domain Name System:** An internet service that translates domain names into IP addresses.
- **Domain Namespace:** The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.
- **Domain Name Registrant:** Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
- **Domain Name Registrar:** A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Centre (including their affiliates, contractors, delegates, successors, or assigns).
- **Enterprise RA:** An employee or agent of an organisation unaffiliated with Trustgate CA who authorises issuance of Certificates to that organisation or its subsidiaries. An Enterprise RA may also authorise issuance of client authentication Certificates to partners, customers or affiliates wishing to interact with that organisation.
- **Expiry Date:** The "Not After" date in a Certificate that defines the end of a Certificate's Validity Period.
- **Fully-Qualified Domain Name:** A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
- **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.).
- **Hash (e.g. SHA1 or SHA256):** An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:
- A message yields the same result every time the algorithm is executed using the same message as input.
- It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.

- It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.
- **Internal Server Name:** A server name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.
- **Incorporate by Reference:** To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message have the same effect as if it had been fully stated in the message.
- **Individual:** A natural person.
- **Key Compromise:** A Private Key is said to be Compromised if its value has been disclosed to an unauthorised person, an unauthorised person has had access to it, or there exists a practical technique by which an unauthorised person may discover its value.
- **Key Pair:** The Private Key and its associated Public Key.
- **OCSP Responder:** An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.
- **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.
- **Practice Standards:** Defines the minimum requirements that must be met by Certification Authorities, the Certificates issued by those Certification Authorities and end entities that use those Certificates in order to comply with Trustgate CA standards.
- **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.
- **Registered Domain Name:** A Domain Name that has been registered with a Domain Name Registrar.
- **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, either in the form of a CRL or an OCSP response.
- **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 the Root CA, or another Subordinate 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 the 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.
- **Unregistered Domain Name:** A Domain Name that is not a Registered Domain Name.
- **Validity Period**: The period of time measured from the date when the Certificate is issued until the Expiry Date.
- **Valid Certificate:** A Certificate that passes the validation procedure specified in RFC 5280.
- **Vetting Agent:** Someone who performs the information verification duties specified by these Requirements.
- **WebTrust Programme for CAs:** The then-current version of the CPA Canada WebTrust Programme for Certification Authorities.
- **WebTrust Seal of Assurance:** An affirmation of compliance resulting from the WebTrust Programme 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.

2. Publication and Repository Responsibilities

2.1 Repositories

Trustgate CA shall publish all CA Certificates and Cross Certificates issued to and from Trustgate CA, revocation data for issued Certificates, CP, CPS and Relying Party agreements in a repository at www.msctrustgate.com/repository.

All parties who are related with the issuance, use or management of Trustgate CA Certificates are hereby notified that Trustgate CA may publish submitted information on publicly accessible directories for the provision of Certificate status information.

Trustgate CA may withhold from making publicly available certain sensitive and/or confidential documentation including security controls, operating procedures and internal security policies. These documents are, however, made available to Qualified Auditors as required during any WebTrust audit performed on Trustgate CA.

2.2 Publication of Certificate Information

Trustgate CA shall make publicly available this CP and any CPS, CA Certificates, Relying Party agreements and CRLs in the repository. CRLs contain entries for all revoked unexpired Certificates with a validity period that depends on the Certificate type.

2.3 Time or Frequency of Publication

Trustgate CA Certificates are published in a Repository via support pages as soon as possible after issuance. CRLs for end user Certificates shall be issued at least once per day. CRLs for CA Certificates shall be issued at least annually and within 24 hours if a Certificate is revoked. Each CRL includes an increasing sequence number for each CRL issued.

Trustgate CA reviews their CP and CPS at least annually and makes appropriate changes so that Trustgate CA operation remains accurate, transparent and complies with external requirements listed in the "*Acknowledgements*" section of this document. New or modified versions of this CP, the CPS, Subscriber Agreements or Relying Party agreements are published within seven days after being digitally signed by Trustgate CA.

2.4 Access control on repositories

Trustgate CA shall provide unrestricted read access to its Repositories and shall apply logical and physical controls to prevent unauthorised write access to such Repositories.

3. Identification and Authentication

Trustgate CA maintains documented practices and procedures to authenticate the identity and/or other allocate of the Applicant.

Trustgate CA uses approved procedures and criteria to accept applications from entities seeking to become part of Trustgate CA hierarchy, either as Subordinate CA seeking chaining services or as an RA, Enterprise RA or as an end entity Subscriber.

Trustgate CA validates the requests of parties wishing to perform revocation of Certificates under this CP.

3.1 Naming

3.1.1 Types of Names

To identify a Subscriber, Trustgate CA shall follow naming and identification rules that include types of names assigned to the Subject, such as X.500 distinguished names, RFC-822 names and X.400 names. Where DNs (Distinguished Names) are used, CNs (Common Names) must respect name space uniqueness and must not be misleading. RFC2460 (IP version 6) or RFC791 (IP version 4) addresses may be used.

3.1.2 Need for Names to be Meaningful

When applicable, Trustgate CA uses distinguished names to identify both the Subject and issuer name of the Certificate. When User Principal Names (UPN) are used, they must be unique and accurately reflect organisational structures.

3.1.3 Uniqueness of Names

Trustgate CA enforces the uniqueness within the DN or by requiring that each Certificate include a unique non-sequential serial number with at least 20 bits of entropy.

3.1.4 Recognition, Authentication and Role of Trademarks

Subscribers may not request Certificates with any content that infringes the intellectual property rights of another entity. This CP does not require that an Applicant's right to use a trademark be verified.

However, Trustgate CA may reject any applications or require revocation of any Certificate that is part of a debate.

3.2 Initial Identity Validation

Trustgate CA may perform identification of the Applicant or for services including CA chaining services using any legal means of communication or investigation necessary to identify the Legal Entity or individual.

Trustgate CA may use the result of a successful Subject DN initial identity validation process to create alternative product contributions by effectively combining elements of previously verified information with alternative, newly verified, information. A suitable account based challenge response mechanism must be used to authenticate any previously verified information for any returning Applicant or provided that reverification requirements are accurate.

3.2.1 Method to Prove Possession of Private Key

Subscribers must prove possession of the Private Key corresponding to the Public Key being registered with Trustgate CA. Such relationship can be proved by, for example, a Digital Signature in the Certificate Signing Request (CSR) in addition to an out-of-band confirmation.

Following an initial assessment and signing of a specific agreement with Trustgate CA, the applicant Subordinate CA must also prove possession of the Private Key. Trustgate CA chaining services do not mandate the physical appearance of the Subscriber representing the Subordinate CA so long as an agreement between the applicant organisation and Trustgate CA has been executed.

3.2.2 Authentication of Organisation Identity

For all Certificates that include an organisation identity, Applicants are required to indicate the organisation’s name and registered or business address. The legal existence, legal name, legal form (where included in the request or part of the legal name in the jurisdiction of incorporation) and provided address of the organisation must be verified and any methods used must be highlighted in the CPS.

The authority of the Applicant to request a Certificate on behalf of the organisation must be verified.

3.2.3 Authentication of Individual identity

Trustgate CA or RAs shall authenticate individuals depending upon the class of Certificate as indicated below.

3.2.3.1 Class 1

The Applicant is required to demonstrate control of the email address to which the Certificate relates. Trustgate CA or RAs are not required to authenticate any other information provided.

3.2.3.2 Class 2

For SSL certificate, the applicant is required to demonstrate control of the identity attributes included in the request, such as organisation name, domain name, email address and business address to which the Certificate relates.

For client certificate, the applicant certificate is required to submit a legible copy of a valid government issued identity document such as national identity or passport. Trustgate CA are required to verify to a reasonable level of assurance that the copy of the ID matches the requested name and that other Subject information are authenticated.

Trustgate CA or RAs are also required to authenticate the Applicant’s identity through one or more of the following methods:

- Performing a telephone challenge/response to the Applicant using a telephone number from a reliable source;
- Performing a fax challenge/response to the Applicant using a fax number from a reliable source; or

- Performing an email challenge/response to the Applicant using an email address from a reliable source; or
- Performing a postal challenge to the Applicant using an address obtained from a reliable source.

Further information may be requested 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

For EV Code Signing, the Applicant is required to demonstrate control of an email address to be included within a Certificate.

For EV SSL, the Applicant is required to demonstrate control of all domain names to be included in a Certificate.

For Class 3 Client Certificates, a face-to-face meeting is required to establish the individual's identity with an attestation from a trusted third party that they have met the individual and have inspected their government-issued national identity document, and that the application details are correct.

The Applicant is required to submit a legible copy of a valid government issued national identity document. Trustgate CA are required to verify to a reasonable level of assurance that the copy of the ID matches the requested name and that other Subject information are verified.

Trustgate CA or RAs are also required to verify the Applicant's authority to represent the organisation wishing to be named as the Subject in the Certificate, using reliable means of communication, verified by Trustgate CA as a reliable way of communicating with the Applicant in accordance with the EV Guidelines.

Further information may be requested from the Applicant or the Applicant's organisation.

3.2.4 Non Verified Subscriber Information

Trustgate CA must validate all information to be included within the Subject DN of a Certificate or clearly indicate within their CPS and within the issued Certificate itself any exceptions that may apply to specific product types or services offered. Trustgate CA may use the subject:organisationalUnitName as a suitable location to identify non-verified Subscriber information to Relying Parties or to provide any specific disclaimers/notices.

Specifically for SSL/TLS Certificates, Trustgate CA maintains a process to ensure that Applicants cannot add self-reported information to the subject:organisationalUnitName.

3.2.5 Authentication of Domain Name

For all SSL/TLS Certificates, the Applicant's ownership or control of all requested Domain Name(s) and IP address must be verified with methods to achieve this in accordance with the CPS.

Further information may be requested from the applicant and other information and/or methods may be utilised in order to achieve an equivalent level of confidence.

3.2.6 Authentication of Email addresses

Trustgate CA confirms that the Applicant has control of or right to use email addresses by having the Applicant demonstrate control over the email address via a challenge/response.

3.2.7 Identification and Authentication for Reissuance after Revocation

After a Certificate has been repeal, the Subscriber is required to go through the initial registration process described elsewhere in this CP to obtain a new Certificate.

3.2.8 Re-verification and Revalidation of Identity When Certificate Information Changes

If at any point any Subject name information include in a Certificate is changed in any way, the identity proofing procedures outlined in this requirement must be re-performed and a new Certificate issued with the validated information.

3.3 Identification and Authentication for Revocation Request

All revocation requests must be authenticated by Trustgate CA. Revocation requests from Subscribers may be granted following a suitable challenge response, such as logging into an account with a username and password or proving possession of unique elements incorporated into the Certificate, e.g. Domain Name or email address.

Trustgate CA may also perform revocation on behalf of Subscribers in accordance with the requirements of the applicable Subscriber Agreement. Examples of reasons for revocation include a breach of the Subscriber Agreement or non- payment of applicable fees.

4. Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Trustgate CA shall maintain their own blacklists for individuals from whom or entities from which they will not accept Certificate applications. Blacklists may be based on past history or other sources. In addition, other external sources, such as government lists, may be used to screen unwanted Applicants.

4.1.2 Enrolment Process and Responsibilities

Trustgate CA shall maintain systems and processes that sufficiently authenticate the Applicant's identify for all Certificate types that present the identity to Relying Parties. Applicants should submit sufficient information to allow Trustgate CA and RAs to successfully perform the required verification. Trustgate CA and RAs protects communications and securely store information presented by the Applicant during the application process.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Trustgate CA shall maintain systems and processes to sufficiently authenticate the Applicant's identify in compliance with its CPS. Initial identity validation shall be performed by Trustgate CA validation team or by RAs under contract with Trustgate CA. All communications shall be securely stored along with all information presented directly by the Applicant during the application process. Future identification of repeat Applicants and subsequent authentication checks may be addressed using single (username and password) or multi-factor (Certificate in combination with username/password) authentication principles.

Trustgate CA shall validate each server FQDN in publicly trusted SSL certificates against the domain's CAA records. If a CAA record exists that does not list msctrustgate.com as the CA, Trustgate CA shall not issue the certificate.

4.2.2 Approval or Rejection of Certificate Applications

Trustgate CA shall reject applications for Certificates where validation of all items cannot successfully be completed.

Assuming all validation steps can be completed successfully following appropriate best practice techniques Trustgate CA shall generally approve the Certificate Request. Trustgate CA may reject applications including for the following reasons:

- Based on potential brand damage to Trustgate CA in accepting the application;

- For Certificates from Applicants who have previously been rejected or have previously violated a provision of a Subscriber Agreement;

Trustgate CA are under no obligation to provide a reason to an Applicant for rejection of a Certificate Request.

4.2.3 Time to Process Certificate Applications

Trustgate CA ensures that all reasonable methods are used in order to process and evaluate Certificate applications.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Certificate issuance by Trustgate CA requires an authorised Trusted Role member from Trustgate CA to deliberately issue a direct command in order to perform a Certificate signing operation. Trustgate CA shall communicate with any RA administrators capable of Certificate issuance using multifactor authentication. RAs directly operated by Trustgate CA or RAs contracted by Trustgate CA to perform validation ensures that all information received is verified and authenticated in a secure manner.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

Trustgate CA shall notify the Subscriber of the issuance of a Certificate in a convenient and appropriate way based on information submitted during the enrolment process.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Trustgate CA shall inform the Subscriber that they may not use the Certificate until the Subscriber has reviewed and verified the accuracy of the data incorporated into the Certificate. To avoid this being an open ended stipulation, Trustgate CA may set a time limit by when the Certificate is deemed to be accepted.

4.4.2 Publication of the Certificate by Trustgate CA

Trustgate CA may publish a Certificate by sending the Certificate to the Subscriber and/or publishing in a suitable Repository, including to Certificate Transparency Logs.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

All Subscribers must protect their Private Key with care to avoid disclosure to third parties. Trustgate CA must maintain a suitable Subscriber Agreement which highlights the obligations of the Subscriber with respect to Private Key protection. Private Keys must only be used as specified in the appropriate key usage and extended key usage fields as indicated in the corresponding Certificate. Where it is possible to make a backup of a Private Key, Subscribers must use the same level of care and protection attributed to the live Private Key. At the end of the useful life of a Private Key, Subscribers must securely delete the Private Key and any fragments that it has been split into for the purposes of backup.

4.5.2 Relying Party Public Key and Certificate Usage

Trustgate CA shall describe the conditions under which Certificates may be relied upon by Relying Parties within their CPS including the appropriate mechanisms available to verify Certificate validity, such as the CRL or OCSP. Trustgate CA shall also offer a Relying Party agreement to Subscribers the content of which should be presented to the Relying Party prior to reliance upon a Certificate from Trustgate CA. Relying Parties should use the information to make a risk assessment and as such are solely responsible for performing the risk assessment prior to relying on the Certificate or any assurances made.

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 and the same Public Key. Trustgate CA may renew a Certificate so long as:

- The original Certificate to be renewed has not been revoked;
- The Public Key from the original Certificate has not been blacklisted for any reason; and
- All details within the Certificate remain accurate and no new or additional validation is required.

Trustgate CA may renew Certificates which have either been previously renewed or previously re-keyed (subject to the points above). The original Certificate may be revoked after renewal is complete; however, the original Certificate must not be further renewed or modified.

4.6.2 Who May Request Renewal

Trustgate CA may accept a renewal request provided that it is authorised by the original Subscriber through a suitable Certificate lifecycle account challenge response. A Certificate signing request is not mandatory, however if one is used then it may contain the same 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 Trustgate CA

As per 4.4.2

4.7 Certificate Modification

4.7.1 Circumstances for Certificate Modification

Certificate modification is defined as the production of a new Certificate that has details which differ from a previously issued Certificate. The new modified Certificate may or may not have a new Public Key and may or may not have a new ‘Not After’ date.

- Trustgate CA shall treat modification in the same was a ‘New’ issuance.
- Trustgate CA may modify Certificates that have either been previously renewed or previously re-keyed. The original Certificate may be revoked after modification is complete, however, the original Certificate must not be further renewed, re-keyed or modified.

4.7.2 Who May Request Certificate Modification

As per 4.1

4.7.3 Processing Certificate Modification 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 Modified Certificate

As per 4.4.1

4.7.6 Publication of the Modified Certificate by the CA

As per 4.4.2

4.8 Certificate Revocation and Suspension

4.8.1 Circumstances for Revocation

Certificate revocation is a process whereby the serial number of a Certificate is effectively blacklisted by adding the serial number and the date of the revocation to a Certificate Revocation List (CRL). The CRL itself will then be digitally signed with the same Private Key which originally signed the Certificate to be revoked. Adding a serial number allows Relying Parties to establish that the lifecycle of a Certificate has ended. Trustgate CA may remove serial numbers once a Certificate has normally expired to promote more efficient CRL file size management. Prior to performing a revocation Trustgate CA's will verify the authenticity of the revocation request. Revocation of a Subscriber's Certificate shall be performed within twenty-four (24) hours under the following circumstances:

- The Subscriber requests in writing (to the entity which provided the Certificate) that they wish to revoke the Certificate;
- The Subscriber notifies Trustgate CA that the original Certificate Request was not authorised and does not retroactively grant authorisation;
- Trustgate CA obtains reasonable evidence that the Subscriber's Private Key has been Compromised, no longer complies with the requirements for algorithm type and key size of the Baseline Requirements, or that the Certificate has otherwise been misused;
- Trustgate CA receives notice or otherwise becomes aware that the Subscriber violated any of its material obligations under the Subscriber Agreement or Terms of Use;
- Trustgate CA is made aware of any circumstance indicating that used of a Fully-Qualified Domain Name 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);
- The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- Trustgate CA receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
- Trustgate CA is made aware that the Certificate was not issued in accordance with the Baseline Requirements or Trustgate CA CP or CPS;
- If Trustgate CA determines that any of the information appearing in the Certificate is not accurate or is misleading;
- Trustgate CA is made aware of a possible Compromise of the Private Key of the Subordinate CA used for issuing the Certificate;
- Revocation is required by Trustgate CA's CP and/or CPS;

Revocation of a Subscriber Certificate may also be performed within a commercially reasonable period of time under the following circumstances:

- The Subscriber or organisation administrator requests revocation of the Certificate through an which controls the lifecycle of the Certificate;

- The Subscriber requests revocation of the Certificate via the revocation workflow process;
- The Subscriber requests revocation through an authenticated request to Trustgate CA's support team or Trustgate CA’s Registration Authority;
- Trustgate CA receives notice or otherwise become aware that the Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of Trustgate CA's jurisdiction of operation;
- Following the request for cancellation of a Certificate;
- If a Certificate has been reissued, Trustgate CA may revoke the previously issued Certificate;
- Under certain licensing arrangements, Trustgate CA may revoke Certificates following expiration or termination of the license agreement; and
- Trustgate CA determines the continued use of the Certificate is otherwise harmful to the business of Trustgate CA or third parties. When considering whether Certificate usage is harmful or a third party’s business or reputation, Trustgate CA should consider, amongst other things, the nature and number of complaints received, the identity of the complainant(s), relevant legislation in force, responses to the alleged harmful use by the Subscriber.

Revocation of a Subordinate CA Certificate shall be performed within seven (7) days under the following circumstances:

- The Subordinate CA requests in writing to Trustgate CA entity which provided the Subordinate CA Certificate, that Trustgate CA revoke the Certificate;
- The Subscriber notifies Trustgate CA that the original Certificate Request was not authorised and does not retroactively grant authorisation;
- Trustgate CA obtains reasonable evidence that the Subordinate CA’s Private Key has been Compromised, no longer complies with the requirements for algorithm type and key size of the Baseline Requirements, or that the Certificate has otherwise been misused;
- Trustgate CA is made aware that the Certificate was not issued in accordance with or that the Subordinate CA has not complied with the Baseline Requirements or the applicable CP or this CPS;
- Trustgate CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- Trustgate CA or Subordinate CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
- Trustgate CA’s or Subordinate CA’s right to issue Certificates expires or is revoked or terminated, unless Trustgate CA has made arrangements to continue maintaining the CRL Repository;
- Revocation is required by Trustgate CA’s CP and/or CPS;

4.8.2 Who Can Request Revocation

Trustgate CA and RAs shall accept authenticated requests for revocation. Authorisation for revocation shall be accepted if the revocation request is received from either the Subscriber or an affiliated organisation named in the Certificate. 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 a Certificate. Trustgate CA may also at their own discretion revoke Certificates including Certificates that are issued to other cross signed Trustgate CA.

4.8.3 Procedure for Revocation Request

Due to the nature of revocation requests and the need for efficiency, Trustgate CA and RAs may provide automated mechanisms for requesting and authenticating revocation requests; for example, through an account which issued the Certificate that is requested to be revoked. RAs may also provide manual backup processes in the event that automated revocation methods are not possible.

Trustgate CA and 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.

Trustgate CA and RAs shall prepare method for Subscribers, Relying Parties, Application Software Suppliers, and other third partied to submit Certificate Revocation request. Trustgate CA and RAs may or may not revoke in response to this request.

4.8.4 Revocation Request Grace Period

The ‘revocation request grace period’ is the time available for a Subscriber to take any necessary actions themselves in order to request revocation of a suspected Key Compromise, use of a weak key or discovery of inaccurate information within an issued Certificate. Trustgate CA should allow Subscribers a maximum of 48 hours to take appropriate action to revoke or take appropriate action on behalf of Subscribers.

4.8.5 Time Within Which Trustgate CA Must Process the Revocation Request

Trustgate CA shall begin investigating Certificate Problem Reports within twenty-four (24) hours of receipt of the report.

All revocation requests for end entity Certificates, both those generated automatically via user accounts and those initiated by Trustgate CA itself, must be processed within a maximum of 30 minutes of receipt.

Trustgate CA that cross sign other CAs should process a revocation request within 24 hours of a confirmation of Compromise and an ARL should be published within 12 hours of any off-line ARL key ceremony.

Trustgate CA and RAs shall conserve 24 x 7 ability to respond internally to a high-priority Certificate Problem Report through report abuse channel and, where appropriate, forward such a complaint to law enforcement authorities. Trustgate CA and RAs shall begin investigation procedures for a suspected Key Compromise or misuse of a Certificate within 24 hours of receipt of the report.

Trustgate CA and RAs shall decide whether revocation or other action is warranted based on at least following criteria:

- The nature of the alleged problem;
- The number of reports received about a particular Certificate or Subscriber;
- The entity making the complaint; and
- Relevant legislation.

4.8.6 Revocation Checking Requirements for Relying Parties

Prior to relying on a Certificate, Relying Parties must validate the suitability of the Certificate to the purpose intended and ensure the Certificate is valid. Relying Parties will need to consult CRL or OCSP information for each Certificate in the chain as well as validating that the Certificate chain itself is complete and follows IETF PKIX standards. This may include the validation of Authority Key Identifier (AKI) and Subject Key Identifier (SKI). Trustgate CA may include all applicable URLs within the Certificate to aid Relying Parties in performing the revocation checking process.

4.8.7 CRL Issuance Frequency

Trustgate CA meets the requirements of the Baseline Requirements and the EV Guidelines (if applicable).

For Subordinate CA Certificates, CRL is updated at least once every 12 months and within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field is not more than 12 months beyond the value of the thisUpdate field.

4.8.8 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation.

4.8.9 On-Line Revocation/Status Checking Availability

Online revocation and other Certificate status information are available via a web-based repository and, where offered, OCSP. Trustgate CA shall have a web-based repository that permits Relying Parties to make online inquiries regarding revocation and other Certificate status information.

4.8.10 On-Line Revocation Checking Requirements

Relying Parties must confirm revocation information.

4.8.11 Special Requirements Related to Key Compromise

Trustgate CA and related Registration Authorities uses commercially reasonable methods to inform Subscribers that their Private Key may have been Compromised. Where Key Compromise is not disputed Trustgate CA shall revoke Trustgate CA Certificates or Subscriber end entity Certificates and publish a revised CRL within 24 hours.

4.9 Certificate Status Services

4.9.1 Operational Characteristics

Trustgate CA shall provide a Certificate status service either in the form of a CRL distribution point or an OCSP responder or both. For other Certificate types, Trustgate CA shall not remove revocation entries on CRL until after the Expiry Date of the revoked Certificate.

4.9.2 Service Availability

Trustgate CA shall maintain 24x7 availability of Certificate status services and may choose to use additional content distribution network cloud based mechanisms to aid service availability.

4.9.3 End of Subscription

Subscribers may end their subscription to Certificate services by having their Certificate revoked or naturally letting it expire. Where Trustgate CA have issued in relation end entity issuance contracts between parties must be maintained unless revocation is used to terminate the contract.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

Trustgate CA have physical and environmental security policies for systems used for Certificate issuance and management which cover physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking & entering, and disaster recovery. Controls should be implemented to avoid loss, damage or Compromise of assets and interruption to business activities and theft of information and information processing facilities.

5.1.1 Site Location and Construction

Trustgate CA ensures that critical and sensitive information processing facilities are housed in secure areas with appropriate security barriers and entry controls. They should be physically protected from unauthorised access, damage and interference and the protections provided should be correspondent with the identified risks in risk analysis plans.

5.1.2 Physical Access

Trustgate CA ensures that the facilities used for Certificate lifecycle management are operated in an environment that physically protects the services from Compromise through unauthorised access to systems or data. An authorised employee should always accompany any unauthorised person entering a physically secured area. Physical protections should be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the systems hosting the CA operations. No parts of the CA premises shall be shared with other organisations within this perimeter.

5.1.3 Power and Air Conditioning

Trustgate CA ensures that the power and air conditioning facilities are sufficient to support the operation of the CA system.

5.1.4 Water Exposure

Trustgate CA ensures that the CA system is protected from water exposure.

5.1.5 Fire Prevention and Protection

Trustgate CA ensures that the CA system is protected with a fire suppression system.

5.1.6 Media Storage

Trustgate CA ensures that any media used is securely handled to protect it from damage, theft and unauthorised access. Media management procedures should be protected against obsolescence and deterioration of the media within a defined period of time. Records are required to be retained. All media should be handled securely in accordance with requirements of the information asset classification scheme and media containing sensitive data must be securely disposed of when no longer required.

5.1.7 Waste Disposal

Trustgate CA ensures that all media used for the storage of information is declassified or destroyed in a generally accepted manner before being released for disposal.

5.1.8 Off-Site Backup

Trustgate CA ensures that full system backups of the Certificate issuance system are sufficient to recover from system failures and are made periodically, as defined in Trustgate CA’s CPS. Back-up copies of essential business information and software must be taken regularly. Adequate back-up facilities are provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems should be regularly tested to ensure that they meet the requirements of business continuity plans. Backups should be stored at a site with physical and procedural controls commensurate to that of the operational facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trustgate CA should ensure that all operators and administrators including Vetting Agents are acting in the capacity of a trusted role. Trusted roles are such that no conflict of interest is possible and the roles are distributed such that no single person can circumvent the security of the CA system.

Trusted roles include but are not limited to the following:

- **Developers**: Responsible for development of CA systems.
- **Security Manager:** overall responsibility for administering the implementation of Trustgate CA's security practices, cryptographic key life cycle management functions (e.g., key component custodians);
- **Administrator:** approval of the generation, revocation and suspension of certificates;
- **System Engineer:** installation, configuration and maintenance of the CA systems, viewing and maintenance of CA system archives and audit logs;
- **Operator:** day-to-day operation of CA systems and system backup and recovery;

- **Key Manager:** cryptographic key life cycle management functions (e.g., key component custodians).

5.2.2 Number of Persons Required per Task

Trustgate CA shall state the number of persons required per task within their CPS. The goal is to guarantee the trust for all CA services (Key Pair generation, Certificate generation, revocation) so that any malicious activity would require collusion. Where multiparty control is required, at least one of the participants shall be an Administrator. All participants shall serve in a trusted role as defined in Section 5.2.1 above.

5.2.3 Identification and Authentication for Each Role

Before appointing a person to a trusted role, Trustgate CA shall run 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. The CPS should describe the mechanisms that are used to identify and authenticate people appointed to trusted roles.

5.2.4 Roles Requiring Separation of Duties

Trustgate CA shall enforce role separation either by the CA equipment or procedurally or by both means. Individual CA personnel are specifically designated to the roles defined in Section 5.2.1 above. It is not permitted for any one person to serve in the following roles at the same time:

- Security officer and System Engineer or Operator;
- System Engineer and Operator or Administrator.

No individual shall be assigned more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Trustgate CA shall employ a sufficient number of personnel that possess the expert knowledge, experience and qualifications necessary for the offered services, as appropriate to the job function. Trustgate CA personnel should fulfil the requirement of expert knowledge, experience and qualifications through formal training and education, actual experience, or a combination of the two. Trusted roles and responsibilities, as specified in Trustgate CA's CPS, are documented in job descriptions. Trustgate CA personnel (both temporary and permanent) have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. Trustgate CA personnel shall be formally appointed to trusted roles by senior management responsible for security.

The job descriptions include skills and experience requirements. Managerial personnel are employed who possess experience or training in electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

5.3.2 Background Check Procedures

All Trustgate CA personnel in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the CA operations. Trustgate CA shall not appoint to a trusted role any person who is known to have a conviction for a serious crime or another offence, is such conviction affects his/her suitability for the position. Personnel do not have access to the trusted functions until any necessary checks are completed and results analysed, provided such checks are permitted by the jurisdiction in which the person will be employed. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation.

Any use of information revealed by background checks by Trustgate CA shall be in compliance with applicable laws of jurisdiction where the person is employed.

5.3.3 Training Requirements

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

- CA/RA security principles and mechanisms;
- Software versions in use on the CA system;
- Duties they are expected to perform; and
- Disaster recovery and business continuity procedures.

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

5.3.4 Retraining Frequency and Requirements

Individuals responsible for trusted roles shall be aware of changes in Trustgate CA or RA operations, as applicable. Any significant change to the operations have a training (awareness) plan with at least annual training on information security, and the execution of such plan shall be documented.

5.3.5 Job Rotation Frequency and Sequence

Trustgate CA should ensure 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 sanctions shall be applied to personnel violating provisions and policies within the CP, CPS or CA related operational procedures.

5.3.7 Independent Contractor Requirements

Contractor personnel employed for Trustgate CA operations must be subjected to the same process, procedures, assessment, security control and training as permanent CA personnel.

5.3.8 Documentation Supplied to Personnel

Trustgate CA should make available to its personnel this CP, any corresponding CPS and any relevant statutes, policies or contracts. Other technical, operational and administrative documents (e.g., administrator manuals, user manuals, etc.) are provided in order for the trusted personnel to perform their duties.

Documentation is maintained identifying all personnel who received training and the level of training completed.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Audit log files shall be generated for all events relating to the security and services of Trustgate CA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

Trustgate CA should ensure all events relating to the lifecycle of Certificates are logged in a manner to ensure the traceability to a person in a trusted role for any action required for CA services. At a minimum, each audit record includes the following (either recorded automatically or manually) elements:

- The type of event;
- The date and time the event occurred;
- Success or failure where appropriate;

- The identity of the entity and/or operator that caused the event;
- The identity to which the event was targeted; and
- The cause of the event.

5.4.2 Frequency of Processing Log

Audit logs are reviewed periodically for any evidence of malicious activity and following each important operation.

5.4.3 Retention Period for Audit Log

Audit log records must be held for a period of time as appropriate to provide necessary legal evidence in accordance with any applicable legislation. Records may be required at least as long as any transaction relying on a Valid Certificate can be questioned.

5.4.4 Protection of Audit Log

The events must be logged in a way that they cannot be deleted or destroyed (except for transfer to long term media) for any period of time that they are retained.

The events must be logged in a manner to ensure that only individuals with authorised trusted access are able to perform any operations regarding their profile without modifying integrity, authenticity and confidentiality of the data.

The records of events are protected in a manner to prevent alteration and detect tampering.

The records of events must be date stamped in a secure manner that guarantees, from the date of creation of the record to the end of the archive period that there is a trusted link between the event and the time of its realisation.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries must be backed-up in a secure location (for example, a fire proof safe), under the control of an authorised trusted role, and separated from their component source generation. Audit log backup should be protected to the same degree as originals.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection systems is an internal component of Trustgate CA. Audit processes must be initiated at system start up and may finish only at system shutdown. The audit collection system should ensure the integrity and availability of the data collected. The audit collection system protects the data confidentiality.

5.4.7 Vulnerability Assessments

Trustgate CA shall perform regular vulnerability assessments covering all Trustgate CA assets related to Certificate issuance products and services. Assessments should focus on internal and external threats that could result in unauthorised access, tampering, modification, alteration or destruction of the Certificate issuance process.

5.5 Records Archival

5.5.1 Types of Records Archived

Trustgate CA and RAs archive records with enough detail to establish the validity of a signature and of the proper operation of the CA system. At a minimum, the following data is archived:

CA key lifecycle management events, including:

- Key generation, backup, storage, recovery, archival, and destruction;
- Cryptographic device lifecycle management events; and
- CA system equipment configuration.

CA and Subscriber Certificate lifecycle management events, including:

- Certificate Requests, renewal, and re-key requests, and revocation for both successful and unsuccessful attempts;
- All verification activities stipulated in this CP;
- Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
- Acceptance and rejection of Certificate Requests;
- Issuance, revocation, expiration of Certificates; and
- Generation of Certificate Revocation Lists and OCSP entries including failed read-and-write operations on the Certificate and CRL directory as well as the actual CRL.

Security events, including:

- Successful and unsuccessful PKI system access attempts;
- PKI and security system actions performed;
- Security profile changes;
- System crashes, hardware failures, and other anomalies;
- Firewall and router activities; and
- Entries to and exits from the CA facility.

5.5.2 Retention Period for Archive

The minimum retention period for archive data for Trustgate CA is ten (10) years.

5.5.3 Protection of Archive

The archives is created in such a way that they cannot be deleted or destroyed (except for transfer to long term media) within the period of time for which they are required to be held. Archive protections should ensure that only authorised trusted access is able to make operations without modifying integrity, authenticity and confidentiality of the data. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site.

5.5.4 Archive Collection System (Internal or External)

The archive collection system complies with the security requirements defined in Section 5.3.

5.5.5 Procedures to Obtain and Verify Archive Information

Media storing of Trustgate CA archive information are checked upon creation. Only authorised Trustgate CA equipment, trusted role and other authorised persons are allowed to access the archive.

5.6 Compromise and Disaster Recovery

5.6.1 Incident and Compromise Handling Procedures

Trustgate CA has established business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data that could disturb or compromise Trustgate CA services. Trustgate CA carries out risk assessments to evaluate business risk and determine the necessary security requirements and operational procedures to be taken as a consequence of its disaster recovery plan. This risk analysis is regularly reviewed and revised if necessary *(threat evolution, vulnerability evolution, etc.).*

Trustgate CA personnel that serve in a trusted role and operational role are specially trained to operate according to procedures defined in the disaster recovery plan for business critical operations.

If Trustgate CA detects a potential hacking attempt or another form of compromise, it performs an investigation in order to determine the nature and the degree of damage. Otherwise, Trustgate CA assesses the scope of potential damage in order to determine if Trustgate CA or RA system needs to be rebuilt, if only some Certificates need to be revoked, and/or if a CA hierarchy needs to be declared as Compromised. The CA disaster recovery plan should highlight which services should be maintained *(for example revocation and Certificate status information).*

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

If any equipment is damaged or rendered inoperative, but the Private Keys are not destroyed, the operation should be re-established as quickly as possible, giving priority to the ability to generate Certificate status information according to Trustgate CA's disaster recovery plan.

5.6.3 Entity Private Key Compromise Procedures

In the event Trustgate CA Private Key is Compromised, lost, destroyed or suspected to be Compromised:

- Trustgate CA shall, after investigation of the problem, decide whether the Trustgate CA Certificate should be revoked. If so, then:
- All the Subscribers who have been issued a Certificate will be notified at the earliest feasible opportunity; and
- A new Trustgate CA Key Pair shall be generated or an alternative existing CA hierarchy shall be used to create new Subscriber Certificates.

5.6.4 Business Continuity Capabilities After a Disaster

The disaster recovery plan deals with the business continuity of Trustgate CA. Certificate status information systems are deployed so as to provide 24 hours per day, 365 days per year availability.

5.7 CA or RA Termination

In the event of termination of Trustgate CA or RA, Trustgate CA shall provide notice to all customers prior to the termination and:

- Stop delivering Certificates according to and referring to this CP;
- Archive all audit logs and other records prior to termination;
- Destroy all Private Keys upon termination;
- Ensure archive records are transferred to an appropriate authority such as another Trustgate CA that delivers identical services; and
- Use secure means to notify customers to delete all trust anchors.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Trustgate CA generates all issuing Key Pairs in a physically secure environment by personnel in trusted roles under, at least, dual control. External witnesses (Ideally an independent auditor who normally performs audits on a regular basis) may be present or the ceremony, as a whole, must be videotaped/recorded. Trustgate CA key generation is carried out within a device which is at least certified to FIPS 140-2 level 3 or above.

6.1.2 Private Key Delivery to Subscriber

Trustgate CA creates Private Keys on behalf of Subscribers only when sufficient security is maintained within the key generation process and any onward issuance process to the Subscriber.

The cryptographic algorithms regarding Public/Private key generation (encryption, sign, cryptographic hash, RNG or PRNG etc.) were approved by FIPS, the Public/Private key generation algorithm is also specified in FIPS 186-4.

The generated Public/Private key is encrypted with PIN code which was provided by the Subscriber. The encrypted Public/Private key will be delivered in TLS session, authenticated by the password preregistered by an administrator of the Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

Trustgate CA shall only accept Public Keys from RAs that have been protected during transit and have had the authenticity and integrity of their origin from the RA suitably verified.

6.1.4 CA Public Key Delivery to Relying Parties

Trustgate CA ensures that Public Key delivery to Relying Parties is undertaken in such a way as to prevent substitution attacks. This may include working with commercial browsers and platform operators to embed Root Certificate Public Keys into root stores and operating systems. Trustgate CA Public Keys may be delivered by the Subscriber in the form of a chain of Certificates or via a Repository operated by Trustgate CA and referenced within the profile of the issued Certificate.

6.1.5 Key Sizes

Trustgate CA follows NIST Special Publication 800-133 (2012) - Recommendation for Cryptographic Key Generation - for recommended timelines and best practices in the choice of Key Pairs for Root CAs, Trustgate CA and end entity Certificates delivered to Subscribers. Any Subordinate CAs in the Trusted Root programme, outside of the direct control of Trustgate CA are contractually obligated to use the same best practices. Trustgate CA selects from the following Key Sizes/Hashes for Root Certificates, Trustgate CA Certificates and end entity Certificates as well as CRL/OCSP Certificate status responders. These choices align with the Baseline Requirements and EV Guidelines:

RSA

- 2048 bit RSA key with Secure Hash Algorithm 1 (SHA-1)
- 2048 bit RSA key with Secure Hash Algorithm 2 (SHA-256)
- 4096 bit RSA key with Secure Hash Algorithm 2 (SHA-384)

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

Trustgate CA generates Key Pairs in accordance with FIPS 186 and uses reasonable techniques to validate the suitability of Public Keys presented by Subscribers. Known weak keys shall be tested for and rejected at the point of submission.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Trustgate CA shall set key usage of Certificates depending on their proposed field of application via the v3 Key Usage Field for X.509 v3.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Trustgate CA ensures that all systems signing Certificates and CRLs or generating OCSP responses use FIPS 140-2 level 3 as the minimum level of cryptographic protection. Trustgate CA certificates that require Subscribers to use FIPS 140-2 level 2 or above systems for Private Key protection must contractually obligate the Subscriber to use such a system or provide a suitable mechanism to guarantee protection. This can be achieved, for example, through limitation to a suitable CSP (Cryptographic Service Provider) tied to a known FIPS compliant hardware platform as part of the enrolment process.

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

Trustgate CA activates Private Keys for cryptographic operations with multi-person control (using CA activation data) performing duties associated with their trusted roles. The trusted roles permitted to participate in this Private Key multi-person controls are strongly authenticated (i.e. token with PIN code).

6.2.3 Private Key Escrow

Trustgate CA shall not escrow CA Private Keys for any reason.

6.2.4 Private Key Backup

Trustgate CA shall back up Private Keys under the same multi-person control as the original Private Key for disaster recovery plan purposes.

6.2.5 Private Key Archival

With the exception of Digital Signing Service, Trustgate CA shall not archive Private Keys and must ensure that any temporary location where a Private Key may have existed in any memory location during the generation process is purged.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Trustgate CA Private Keys must be generated, activated and stored in Hardware Security Modules. When Private Keys are outside of a Hardware Security Module (either for storage or transfer), they must be encrypted.

6.2.7 Private Key Storage on Cryptographic Module

Trustgate CA shall store Private Keys on at least a FIPS 140-2 level 3 device.

6.2.8 Method of Activating Private Key

Trustgate CA are 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 form of a Subscriber Agreement or Terms of Use.

6.2.9 Method of Deactivating Private Key

Trustgate CA ensures that Hardware Security Modules that have been activated are not left unattended or otherwise available to unauthorised access. During the time Trustgate CA's Hardware Security Module is online and operational it is only used to sign Certificates and CRL/OCSPs from an authenticated RA. When a CA is no longer operational, its Private Keys are removed from the Hardware Security Module.

6.2.10 Method of Destroying Private Key

Trustgate CA Private Keys must be destroyed when they are no longer needed or when the Certificate to which they correspond have expired or are revoked. Destroying Private Keys requires Trustgate CA to destroy all associated CA secret activation data in security world in such a manner that no information can be used to deduce any part of the Private Key.

Private Keys generated by Trustgate CA are stored in PKCS 12 format until the Key Pairs are picked up by the Subscriber. When the Subscriber acknowledge the receipt of the Key Pair or when 30 days has passed after the key generation, the Subscriber Key Pair is automatically deleted from GCC. Subscriber Private Keys are not stored in any other systems.

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 complies with the Baseline Requirements with respect to the maximum validity period, in some cases thereby reducing the effective available Certificate term. In some cases, the maximum validity period may not be realised by the Subscriber in the event the current or future Baseline Requirements impose requirements on Certification Authorities relative to Certificate issuance that were not in place at the time the Certificate was originally issued, particularly in the case of a request for reissuance, e.g., additional requirements are included for identification and authentication for certain Certificate type, or maximum Validity Period is decreased.

In no event shall Trustgate CA issue an SSL/TLS Certificate with a validity period greater than 825 days whether as initial issue, re-key, reissue or otherwise.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation and use of Trustgate CA activation data used to activate Trustgate CA Private Keys shall be made during a key ceremony (Refer to Section 6.1.1). Activation data shall be generated automatically by the appropriate HSM and delivered to a shareholder who must be a person in trusted role. The delivery method must maintain the confidentiality and the integrity of the activation data.

6.4.2 Activation Data Protection

Trustgate CA activation data are protected from disclosure through a combination of cryptographic and physical access control mechanisms. Trustgate CA activation data must be stored on secure cryptographic devices.

6.4.3 Other Aspects of Activation Data

Trustgate CA activation data is only held by Trustgate CA personnel in trusted roles.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards. Trustgate CA PKI components include the following functions:

- Require authenticated logins for trusted role;
- Provide discretionary access control with least privilege;
- Provide security audit capability (protected in integrity);
- Prohibit object re-use;
- Require use of strong password policy;
- Require use of cryptography for session communication;
- Require trusted path for identification and authentication;
- Provide means for malicious code protection;
- Provide means to maintain software and firmware integrity;
- Provide domain isolation and partitioning different systems and processes; and
- Provide self-protection for the operating system.

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

The system development controls for Trustgate CA are as follows:

- Use software that has been designed and developed under a formal, documented development methodology;
- Hardware and software procured are purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase);
- Hardware and software are developed in a controlled environment, and the development processes are defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software;
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location;
- The hardware and software are dedicated to performing CA activities. There are no other applications, hardware devices, network connections, or component software installed which are not part of the

CA operation;

- Proper care is taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the CA operations are installed on the equipment and are obtained from sources authorised by local policy. Trustgate CA hardware and software are scanned for malicious code on first use and periodically thereafter; and
- Hardware and software updates are purchased or developed in the same manner as original equipment; and are installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of Trustgate CA system as well as any modifications and upgrades are documented and controlled by Trustgate CA management. There is a mechanism for detecting unauthorised modification to Trustgate CA software or configuration. A formal configuration management methodology is used for installation and on-going maintenance of Trustgate CA system. Trustgate CA software, when first loaded, is checked as being that supplied from the vendor, with no modifications, and is the version intended for use.

6.6.3 Lifecycle Security Controls

Trustgate CA monitors the maintenance scheme requirements in order to maintain the level of trust of software and hardware that are evaluated and certified.

6.7 Network Security Controls

Trustgate CA PKI components implement appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of security guards, firewalls and filtering routers. Unused network ports and services are turned off. Any boundary control devices used to protect the network on which PKI equipment are hosted deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 Timestamping

All Trustgate CA components are regularly synchronized with a time service such as an atomic clock or Network Time Protocol (NTP) service. A dedicated authority, such as a timestamping authority, may be used to provide this trusted time. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates; and
- Issuance of Subscriber end entity Certificates.

Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

Trustgate CA shall issue Certificates in compliance with X.509 Version 3.

7.1.2 Certificate Extensions

Trustgate CA shall issue Certificates in compliance with RFC 5280 and applicable best practice. Criticality shall also follow best practice and where possible prevent unnecessary risks to Relying Parties when applied to name constraints.

7.1.3 Algorithm Object Identifiers

Trustgate CA shall issue Certificates with algorithms indicated by the following OIDs

- **SHA1WithRSAEncryption** {iso(1) member - body(2) us(840) rsadsi (113549) pkcs(1) pkcs - 1(1) 5}
- **SHA256WithRSAEncryption** {iso(1) member - body(2) us(840) rsadsi (113549) pkcs(1) pkcs - 1(1) 11}
- **ECDSAWithSHA1** {iso(1) member - body(2) us(840) ansi - X9 - 62 (10045) signatures(4) 1 }
- **ECDSAWithSHA224** {iso(1) member - body(2) us(840) ansi - X9 - 62 (10045) signatures(4) ecdsa - with - SHA2(3) 1 }
- **ECDSAWithSHA256** {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

Trustgate CA shall issue Certificates with name forms compliant to RFC 5280. Within the domain of each Trustgate CA, Issuer CAs shall include a unique non-sequential Certificate serial number greater than zero (0) containing at least 64 bits of output from a CSPRNG.

The content of the Certificate Issuer Distinguished Name field shall match the Subject DN of Trustgate CA to support Name chaining as specified in RFC 5280, section 4.1.2.4.

7.1.5 Name Constraints

Trustgate CA may issue Subordinate CA Certificates with Name Constraints and mark as critical where necessary. In case of Name Constraints are NOT set on a Subordinate CA, such CA must be subject for full audit specified in section 8.0 of this document.

Trustgate CA may issue Certificates with a policy qualifier and suitable text to aid Relying Parties in determining applicability.

7.2 CRL Profile

7.2.1 Version Number(s)

Trustgate CA shall issue Version 2 CRLs in compliance with RFC 5280.

7.3 OCSP Profile

Trustgate CA may operate an Online Certificate Status Profile (OCSP) responder in compliance with RFC 2560 or RFC5019.

7.3.1 Version Number(s)

Trustgate CA shall issue Version 1 OCSP responses.

8. Compliance Audit and Other Assessments

The policies within this CP encompass all relevant portions of currently applicable PKI standards for the various vertical PKI industries in which Trustgate CA are required to operate. Trustgate CA Certificates that are not constrained by dNSNameConstraints are audited for compliance to one or more of the following standards:

- CPA Canada Trust Service Principles and Criteria for Certification Authorities
- CPA Canada WebTrust for Certification Authorities – Extended Validation Audit Criteria
- CPA Canada, WebTrust 2.0 Programme for Certification Authorities
- CPA Canada, WebTrust SSL Baseline with Network Security v2.0 for Certification Authorities
- CPA Canada, WebTrust Extended Validation SSL v1.4.5 for Certification Authorities
- Malaysia Digital Signature Act 1997
- Malaysia Digital Signature Regulations 1998

8.1 Frequency and Circumstances of Assessment

Trustgate CA are required to complete a compliance via a Qualified Auditor on at least an annual basis. The audit must cover Trustgate CA and its associated RA.

8.2 Identity/Qualifications of Assessor

Applicable audits of Trustgate CA shall be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess 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 Scheme such as stipulated in 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 by the Malaysia Communications and Multimedia Commission (MCMC);
- Bound by law, government regulation, or professional code of ethics

8.3 Assessor's Relationship to Assessed Entity

Trustgate CA chooses an auditor/assessor who is completely independent from Trustgate CA.

8.4 Topics Covered by Assessment

The audit meets the requirements of the audit scheme under which the assessment is being made. These requirements may vary as audit schemes are updated. An audit scheme will be applicable to Trustgate CA in the year following the adoption of the updated scheme.

8.5 Actions Taken as a Result of Deficiency

Trustgate CA follows the same process if presented with a material non-compliance by external auditors and creates a suitable corrective action plan to remove the deficiency.

8.6 Communications of Results

Results of the audit are reported to the Trustgate CA Policy Board for analysis and resolution of any deficiency through a subsequent corrective action plan.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Trustgate CA charges fees for Certificate issuance or renewal. Fees and any associated terms and conditions are made clear to Applicants.

9.1.2 Certificate Access Fees

Trustgate CA may charge for access to any database which stores issued Certificates.

9.1.3 Fees for Other Services

Trustgate CA may charge for other additional services.

9.1.4 Refund Policy

Trustgate CA may offer a refund policy to Subscribers. Refund policy (if any) may be place in company website, Subscriber Agreements and in CPSs.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Trustgate CA maintains Ringgit Two Million bank guarantee as required under its licence from the Malaysian Communications and Multimedia Commission as a licenced Malaysian Certification Authority.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Trustgate CA defines the scope of confidential information within its CPS.

9.3.2 Information Not Within the Scope of Confidential Information

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

9.3.3 Responsibility to Protect Confidential Information

Trustgate CA protects confidential information. Trustgate CA shall enforce protection of confidential information through training and contracts with employees, agents and contractors.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Trustgate CA protects personal information in accordance with a privacy policy published on a suitable Repository along with this CP.

9.4.2 Information Treated as Private

Trustgate CA shall treat all information received from Applicants that will not ordinarily be placed into a Certificate as private. This applies both to those Applicants who are successful in being issued a Certificate and those who are unsuccessful and rejected. Trustgate CA should periodically train all

RA and vetting staff as well as anyone who has access to the information about due care and attention that must be applied.

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 are responsible for securely storing private information in accordance with a published privacy policy document and may store information received in either paper or digital form. Any backup of private information must be encrypted when transferred to suitable backup media.

9.4.5 Notice and Consent to Use Private Information

Personal information obtained from Applicants during the application and enrolment process is deemed private and permission is required from the Applicant to allow the use of such information. Trustgate CA should incorporate the relevant provisions within an appropriate Subscriber Agreement including any additional information obtained from third parties that may be applicable to the validation process for the product or service being offered by Trustgate CA.

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.

9.5 Intellectual Property rights

Trustgate CA shall 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 retain ownership of Certificates however, they shall grant permission to reproduce and distribute Certificates on a non-exclusive, royalty free basis, provided that they are reproduced and distributed in full.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Trustgate CA use this CP and applicable Subscriber Agreements to convey legal conditions of usage of issued Certificates to Subscribers and Relying Parties. Participants may make representations and warranties include Trustgate CA, RAs, Subscribers, Relying Parties, and any other participants as it might become necessary. All parties including Trustgate CA, any RAs and Subscribers warrant the integrity of their respective Private Key(s). If any such party suspects that a Private Key has been Compromised they will immediately notify the Trustgate CA.

Trustgate CA represents and warrants to Certificate Beneficiaries , during the period when the Certificate is valid, Trustgate CA has complied with its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate:

- **Right to Use Domain Name or IP Address**: That, at the time of issuance, Trustgate 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 Trustgate CA's Certificate Policy and/or Certification Practice Statement;
- **Authorisation for Certificate:** That, at the time of issuance, Trustgate 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 Trustgate CA's Certificate Policy and/or Certification Practice Statement (see Section 3.2.5);

- **Accuracy of Information:** That, at the time of issuance, Trustgate 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 Trustgate CA's Certificate Policy and/or Certification Practice Statement;
- **No Misleading Information:** That, at the time of issuance, Trustgate 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 Trustgate CA's Certificate Policy and/or Certification Practice Statement;
- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, Trustgate 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 Trustgate CA's Certificate Policy and/or Certification Practice Statement;
- **Subscriber Agreement:** That, if Trustgate 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 Trustgate CA and Subscriber are Affiliates, the Applicant Representative acknowledged and accepted the Terms of Use;
- **Status:** That Trustgate CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
- **Revocation:** That Trustgate CA will revoke the Certificate for any of the reasons specified in the Baseline Requirements and/or EV Guidelines.

In lieu of the warranties set forth above, Trustgate CA represents and warrants to Certificate Beneficiaries for EV Certificates that, during the period when the Certificate is valid, Trustgate CA has followed the Guidelines and its Certification Practice Statement in issuing and managing the Certificate and in verifying the accuracy of the information contained in the EV Certificate:

- **Legal Existence:** Trustgate CA has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the Certificate was issued, the Subject named in the Certificate legally exists as a valid organisation or entity in the Jurisdiction of Incorporation or Registration;
- **Identity:** Trustgate CA has confirmed that, as of the date the Certificate was issued, the legal name of the Subject named in the Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;
- **Right to Use Domain Name:** Trustgate CA has taken all steps reasonably necessary to verify that, as of the date the Certificate was issued, the Subject named in the Certificate has the right to use all the Domain Name(s) listed in the Certificate;
- **Authorisation for EV Certificate:** Trustgate CA has taken all steps reasonably necessary to verify that the Subject named in the Certificate has authorised the issuance of the Certificate;
- **Accuracy of Information:** Trustgate CA has taken all steps reasonably necessary to verify that all of the other information in the Certificate is accurate, as of the date the Certificate was issued;
- **Subscriber Agreement:** The Subject named in the Certificate has entered into a legally valid and enforceable Subscriber Agreement with the CA that satisfies the requirements of these Guidelines or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use;

- **Status:** Trustgate CA will follow the requirements of the EV Guidelines (as applicable) and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the Certificate as Valid or revoked; and
- **Revocation:** Trustgate CA will follow the requirements of the EV Guidelines and revoke the Certificate for any of the revocation reasons specified in the EV and/or EV Code Signing Guidelines.

9.6.2 RA Representations and Warranties

Trustgate CA 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

Subscribers and/or Applicants warrant that:

- Subscriber will provide accurate and complete information at all times to Trustgate CA, both in the Certificate Request and as otherwise requested by Trustgate CA in connection with issuance of a Certificate;
- Applicant shall take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key to be included in the requested Certificate(s) and any associated activation data or device, e.g. password or token;
- Subscriber shall review and verify the Certificate contents for accuracy;
- Subscriber shall install the SSL/TLS Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
- Subscriber shall (a) promptly request revocation of the certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate; and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
- Subscriber shall promptly cease use of Private Key associated with the Public Key in the Certificate upon revocation of that Certificate;
- Subscriber shall respond to Trustgate CA's instructions concerning Compromise or Certificate misuse within forty-eight (48) hours; and
- Applicant acknowledges and accepts that Trustgate CA is entitled to revoke the Certificate immediately if the Applicant violates the terms of the Subscriber Agreement or Terms of Use or if Trustgate 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 Warranties

A party relying on Trustgate CA's Certificate warrants to:

- Have the technical capability to use Certificates;
- Receive notice of Trustgate CA and associated conditions for Relying Parties;
- Validate Trustgate CA's Certificate by using Certificate status information using CRL or OCSP published by Trustgate CA in accordance with the proper Certificate path validation procedure;
- Trust Trustgate CA's Certificate only if all information featured on such Certificate can be verified via such a validation procedure as being correct and up to date;

- Rely on Trustgate CA's Certificate, only as it may be reasonable under the circumstances; and
- Notify the appropriate RA immediately, if the Relying Party becomes aware of or suspects that a Private Key has been Compromised.

The obligations of the Relying Party, if it is to reasonably rely on a Certificate, are to:

- Verify the validity or revocation of the CA Certificate using current revocation status information as indicated to the Relying Party;
- Take account of any limitations on the usage of the Certificate indicated to the Relying Party either in the Certificate or this CP;
- Take any other precautions prescribed in Trustgate CA's Certificate as well as any other policies or terms and conditions made available in the application context a Certificate might be used.

Relying Parties must at all times establish that it is reasonable to rely on a Certificate under the circumstances taking into account circumstances such as the specific application context a Certificate is used in.

9.7 Disclaimers of Warranties

Trustgate CA makes statements in their CPS that they do not warrant:

- The accuracy of any unverifiable piece of information contained in Certificates except as it may be stated in the relevant product description below in this CP and in a warranty policy, if available.
- The accuracy, authenticity, completeness or fitness of any information contained in, free, test or demo Certificates.

9.8 Limitations of Liability

The total liability of Trustgate CA is limited in accordance with this warranty policy and any limitations set forth in the Trustgate CA CPS.

9.8.1 Exclusion of Certain Elements of Damages

Trustgate CA states that in no event (except for fraud or wilful misconduct) is Trustgate CA liable for:

- Any loss of profits;
- Any loss of data;
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of Certificates or Digital Signatures;
- Any transactions or services offered or within the framework of this CP;
- Any other damages except for those due to reliance on the verified information in a Certificate; and
- Any liability incurred in any case if the error in such verified information is the result of fraud or wilful misconduct of the Applicant.

9.9 Indemnities

9.9.1 Indemnification by Trustgate CA

Trustgate CA's indemnification obligations are set forth in its CPS, Subscriber Agreement or Relying Party Agreement including any obligation to third party beneficiaries.

9.9.2 Indemnification by Subscribers

Trustgate CA includes its indemnification requirements for Subscribers in the CPS and in its Subscriber Agreements.

9.9.3 Indemnification by Relying Parties

Trustgate CA includes its indemnification requirements for Relying Parties in its CPS.

9.10 Term and Termination

9.10.1 Term

This CP 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. Following publications, changes become applicable 30 days thereafter.

9.10.3 Effect of Termination and Survival

Trustgate CA communicates the conditions and effect of this CP's termination via their appropriate Repository.

9.11 Individual Notices and Communications with Participants

Trustgate CA accepts notices related to this CP by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from Trustgate CA the sender of the notice deems its communication effective. The sender must receive such acknowledgment within twenty (20) business days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows. Individuals communications made to Trustgate CA must be addressed to MSC Trustgate.com Sdn Bhd, Suite 2-9, Level 2, Block 4801 CBD Perdana, Jalan Perdana, 63000 Cyberjaya, Selangor Darul Ehsan, Malaysia or via email at security@msctrustgate.com.

9.12 Amendments

9.12.1 Procedure for Amendment

Changes to this CP are indicated by appropriate numbering.

9.12.2 Notification Mechanism and Period

Trustgate CA shall post appropriate notice on their web site at www.msctrustgate.com/repository of major or significant changes to this CP as well as any appropriate period by when the revised CP is deemed to be accepted.

9.13 Dispute Resolution Provisions

Before resorting to any dispute resolution mechanism including adjudication or any type of alternative dispute resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) complaining parties agree to notify Trustgate CA of the dispute in an effort to seek dispute resolution.

Upon receipt of a dispute notice, Trustgate CA convenes a dispute committee that advises Trustgate CA management on how to proceed with the dispute. The dispute committee convenes within twenty (20) business days from receipt of a dispute notice. The dispute committee is composed by a counsel, a data protection officer, a member of Trustgate CA operational management and a security officer. The counsel or data protection officer chair the meeting. In its resolutions the dispute committee proposes a settlement to Trustgate CA executive management. Trustgate CA executive management may subsequently communicate the proposed settlement to the complaining party.

9.14 Governing Law

This CP is governed, construed and interpreted in accordance with the laws of Malaysia. Each party irrevocably submit to the jurisdiction of the courts of Malaysia.

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 Compelled Attacks

Trustgate CA is subject to Malaysia jurisdiction and regulatory framework. Trustgate CA will use all reasonable legal defence against being compelled by a third party to issue Certificates in violation of the CP and CPS.

9.16.2 Entire Agreement

Trustgate CA will contractually obligate every RA involved with Certificate issuance to comply with this CP and all applicable Industry guidelines. No third party may rely on or bring action to enforce any such agreement.

9.16.3 Assignment

Entities operating under this CP must not assign their rights or obligations without the prior written consent of MSC Trustgate.com Sdn Bhd.

9.16.4 Severability

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

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

Trustgate CA may seek indemnification and attorneys' fees from a party for damages, losses and expenses related to that party's conduct. Trustgate CA's failure to enforce a provision of this CP does not waive MSC Trustgate.com Sdn Bhd's right to enforce the same provisions later or right to enforce any other provisions of this CP. To be effective any waivers must be in writing and signed by MSC Trustgate.com Sdn Bhd.