MSC Trustgate Certification Practice Statement (CPS)

Version 4.3.2

13 March 2019

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

Published date: 06 November 2018

TRADEMARK NOTICES

ACKNOWLEDGMENTS

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

This CPS 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 Certification Practice Statement (CPS) applies to the products and services of MSC Trustgate.com Sdn Bhd ("Trustgate CA"). Primarily this pertains to the issuance and lifecycle management of Certificates, including validity checking services. This CPS may be updated from time to time as outlined in Section 0 *Policy Administration*. The latest version may be found on the MSC Trustgate CA company repository at www.msctrustgate.com.

A CPS highlights the "procedures under which a Digital Certificate is issued to a particular community and/or class of application with common security requirements". This CPS meets the formal requirements of Internet Engineering Task Force (IETF) RFC 3647, dated November 2003 with regard to content, layout and format (RFC 3647 obsoletes RFC 2527). An RFC issued by IETF is an authoritative source of guidance with regard to standard practices in the area of electronic signatures and Certificate management. While certain section titles are included in this CPS according to the structure of RFC 3647, the topic may not necessarily apply to services of Trustgate CA. These sections state 'No stipulation'. Additional information is presented in subsections of the standard structure where necessary. Meeting the format requirements of RFC 3647 enhances and facilitates the mapping and interoperability with other third-party CAs and provides Relying Parties with advance notice of Trustgate CA's practices and procedures. Trustgate CA conforms to the current version of CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates (the "Baseline Requirements), the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates (the "EV Guidelines") as published at www.cabforum.org. In the event that of any inconsistency between this document and the Baseline Requirements, the Baseline Requirements shall take precedence over this document. Additional assertions on standards used in this CPS can be found under the "Acknowledgements" section on the previous page.

This CPS addresses the technical, procedural and personnel policies and practices of Trustgate CA during the complete lifecycle of Certificates issued by Trustgate CA. Trustgate CA operates within the scope of activities of MSC Trustgate.com Sdn Bhd. This CPS addresses the requirements of the CA that issues Certificates of various types. The chaining to any particular Root CA may well vary depending on the choice of intermediate Certificate and Cross Certificate used or provided by a platform or client.

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

1.1 Overview

This CPS applies to the complete hierarchy of Certificates issued by Trustgate CA. The purpose of this CPS is to present the Trustgate CA practices and procedures in managing Certificates and to

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

Trustgate CA Certificates:

- Can be used for electronic signatures in order to replace handwritten signatures where transacting parties choose;
- Can be used to authenticate web resources, such as servers and other devices;
- Can be used to digitally sign documents and other data objects; and
- Can be used for encryption of data.

This CPS identifies the roles, responsibilities and practices of all entities involved in the lifecycle, use, reliance upon and management of Trustgate CA Certificates. The provisions of this CPS with regard to practices, level of services, responsibilities and liability bind all parties involved, including Trustgate CA, Trustgate RAs, Subscribers and Relying Parties. A Trustgate Certificate Policy (CP) complements this CPS. The purpose of the Trustgate CP is to state the *"what is to be adhered to"* and, therefore, set out an operational framework for the broad range of Trustgate CA products and services.

This CPS states *"how Trustgate CA adheres to the Certificate Policy".* In doing so, this CPS features a greater amount of detail and provides the end user with an overview of the processes, procedures and conditions that Trustgate CA uses in creating and maintaining the Certificates that it manages. In addition to the CP and CPS, Trustgate CA maintains additional documented polices addressing such issues as:

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

Additionally, other relevant documents include:

- The Trustgate Warranty Policy that addresses issues on warranties offered by Trustgate;
- The Trustgate Privacy Policy on the protection of personal data; and
- The Trustgate Certificate Policy that addresses the trust objectives for the Trustgate Root Certificates.

A Subscriber or Relying Party of a Trustgate CA Certificate must refer to this CPS in order to establish trust in a Certificate issued by Trustgate CA as well as for information about the practices of Trustgate CA. It is also essential to establish the trustworthiness of the entire Certificate chain of the hierarchy.

This includes the Root CA Certificate as well as any operational Certificates. This can be established on the basis of the assertions within this CPS.

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

Certificates allow entities that participate in an electronic transaction to prove their identity to other participants or sign data digitally. By means of a Certificate, Trustgate CA provides confirmation of the relationship between a named entity (Subscriber) and its Public Key. The process to obtain a Certificate includes the identification, naming, authentication and registration of the Subscriber as well as aspects of Certificate management such as the issuance, revocation and expiration of the Certificate. By means of this procedure to issue Certificates, 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. Trustgate CA makes available Certificates that can be used for non-repudiation, encryption and authentication.

Trustgate CA expressly forbids the use of chaining services for MITM (Man in the Middle) SSL/TLS deep packet inspection.

1.2 PKI Participants

1.2.1 Certification Authorities

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

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

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

1.2.2 Registration Authorities

In addition to identifying and authenticating Applicants for Certificates, an RA may also initiate or pass along revocation requests for Certificates and requests for re-issuance and renewal of Certificates. Trustgate CA and affiliates may act as a Registration Authority (RA) for Certificates they issue in which case they are responsible for:

- Accepting, evaluating, approving or rejecting the registration of Certificate applications;
- Registering Subscribers for certification services;

- Providing systems to facilitate the identification of Subscribers (according to the type of Certificate requested);
- Using officially authorised documents or sources of information to evaluate and authenticate an Applicant's application;
- Requesting issuance of a Certificate via a multi-factor authentication process following the approval of an application; and
- Initiating the process to revoke a Certificate.

RAs who enter into a contractual relationship with Trustgate CA may operate their own RA and authorise the issuance of Certificates. Third parties comply with all the requirements of this CPS and the terms of their contract which may also refer to additional criteria. RA's may implement more restrictive vetting practices if their internal policy dictates.

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. Where the RA relies on Trustgate CA Certificates, 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.

1.2.3 Subscribers

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

A *Subscriber*, as used herein, refers to both the Subject of the Certificate and the entity that contracted with Trustgate CA for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, a Subscriber is an *Applicant*.

For all categories of Subscribers, additional credentials are required as explained in the process for application of a Certificate.

It is expected that a Subscriber organisation has a service agreement or other pre-existing contractual relationship with Trustgate CA authorising it to carry out a specific function within the scope of an application that uses Trustgate CA Certificate services. Issuance of a Certificate to a Subscriber organisation is only permitted pursuant to such an agreement between Trustgate CA and the subscribing end entity.

1.2.4 Relying Parties

To verify the validity of a Certificate, Relying Parties must always refer to Trustgate CA revocation information which is usually presented in the applicable end entity Certificate and appropriate chain of Certificates.

A Relying party may or may not also be a Subscriber within Trustgate CA.

Adobe offers to the AATL platform from Acrobat® 9.12 and above in order to provide document recipients with improved assurances that certified PDF documents are authentic. Document recipients are Relying Parties who use Adobe products on supported platforms to verify the Subscriber's signature on a certified PDF document. Such detail may be inspected by Relying Parties by using a suitable version of the Adobe PDF reader.

1.2.5 Other Participants

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

1.3 Certificate Usage

A Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Certificates are used in commercial environments as a digital equivalent of an identification card.

1.3.1 Appropriate certificate usage

End entity Certificate use is restricted by using Certificate extensions on key usage and extended key usage.

Certificates issued by Trustgate CA can be used for public domain transactions that require:

- **Non-repudiation:** A party cannot deny having engaged in the transaction or having sent the electronic message.
- **Authentication:** The assurance to one entity that another entity is who he/she/it claims to be.
- **Confidentiality (Privacy):** The assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended.
- **Integrity:** The assurance to an entity that data has not been altered (intentionally or unintentionally) from sender to recipient and from time of transmission to time of receipt.

A Digital (Electronic) Signature can only be used for specific transactions that support digital signing of electronic forms, electronic documents or electronic mail. A Certificate is used to verify the Digital Signature made by the Private Key that matches the Public Key within the Certificate and therefore only in the context of applications that support Certificates.

User authentication Certificates can be used for specific electronic authentication transactions that support accessing web sites and other online content, electronic mail and such. The authentication function of a Certificate is the result of a combination of tests on specific properties of the Certificate, such as the identity of the Subscriber bound to the Public Key.

Subscribers should choose an appropriate level of assurance in their identity that to present to Relying Parties, including:

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

- Medium assurance — (Class 2) Certificates are individual and organisational Certificates that are suitable for securing moderately risky inter and ,intra-organisational and commercial transactions.
- High assurance — (Class 3) Certificates are individual and organisational Certificates that provide a high level of assurance of the identity of the Subject as compared to Class 1 and 2.
- High assurance (EV) — Extended Validation Certificates are Class 3 Certificates issued by Trustgate CA in conformance with the EV Guidelines.

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

Any other use of a Certificate is not supported by this CPS. When using a Certificate, the functions of electronic signature (non-repudiation) and authentication (Digital Signature) are permitted together within the same Certificate. The different terms relate to different terminologies used by IETF and the vocabulary adopted within the Malaysian legal framework.

1.3.2 Prohibited Certificate usage

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

Trustgate CA Certificates are not designed 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.

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.

1.4 Policy Administration

1.4.1 Organisation Administering the Document

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

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

1.4.2 Contact Person

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

1.4.3 Person Determining CPS Suitability for the Policy

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

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

1.4.4 CPS Approval Procedures

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

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

1.5 Definitions and acronyms

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

- **Adobe Approved Trust List (AATL):** A document signing certificate authority trust store created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 9.0
- **Affiliate:** A business, corporation, partnership, joint venture or other entity controlling, controlled by or under common control with another entity or an agency, department, political subdivision or any entity operating under the direct control of a Government Entity.
- **Applicant:** 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, businesses, general partnerships, unincorporated associations, sole proprietorships, etc.
- **CDS (Certified Document Services):** A document signing architecture created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 6.0.
- **Certificate:** An electronic document that uses a Digital Signature to bind a Public Key and an identity.
- **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 the 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.

- **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 Center (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.
- **Hardware Security Module (HSM):** An HSM is type of secure crypto processor targeted at managing digital keys, accelerating crypto processes in terms of digital signings/second and for providing strong authentication to access critical keys for server applications.
- **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 shall have the same effect as if it had been fully stated in the message.
- **Incorporating Agency:** In the context of a Private Organisation, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the entity is registered (e.g., the government agency that issues certificates of formation or incorporation). In the context of a Government Entity, the entity that enacts law, regulations or decrees establishing the legal existence of Government Entities.
- **Individual:** A natural person.
- **Internationalised Domain Name (IDN):** An internet domain name containing at least one language-specific script or alphabetic character which is then encoded for use in DNS which accepts only ASCII strings.
- **Issuing CA:** In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
- **Jurisdiction of Incorporation:** In the context of a Private Organisation, the country where the organisation's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country where the Entity's legal existence was created by law.
- **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.
- **Legal Entity:** An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a Country's legal system.
- **Object Identifier (OID):** A unique alphanumeric or numeric identifier registered under the International Organisation for Standardization's applicable standard for a specific object or object class.
- **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.
- **Place of Business:** The location of any facility (such as a factory, retail store, warehouse, etc.) where the Applicant's business is conducted.
- **Private Key:** The key of a Key Pair that is kept secret by the holder of the Key Pair and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
- **Public Key:** The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
- **Public Key Infrastructure (PKI):** A set of hardware, software, people, procedures, rules, policies and obligations used to facilitate the trustworthy creation, issuance, management and use of Certificates and keys based on Public Key cryptography.
- **Publicly-Trusted Certificate:** A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.
- **Qualified Auditor:** A natural person or Legal Entity that meets the requirements outlined by the relevant legislation.
- **Qualified Government Information Source:** A database maintained by a Government Entity.
- **Qualified Government Tax Information Source:** A Qualified Governmental Information Source that specifically contains tax information relating to Private Organisations, Business Entities or Individuals.
- **Qualified Independent Information Source:** A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for

which it is consulted and which is generally recognised as a dependable source of such information.

- **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 in the form of a CRL.
- **Root Certificate:** The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
- **Subject:** The natural person, device, system, unit or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
- **Subject Identity Information:** Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subjectAltName extension or the commonName field.
- **Subordinate CA:** A Certification Authority whose Certificate is signed by Trustgate CA.
- **Subscriber:** A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.
- **Subscriber Agreement**: An agreement between Trustgate CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
- **Terms of Use:** Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the Baseline Requirements when the Applicant/Subscriber is an Affiliate of the CA.
- **Trusted Third-party:** A service provider with a secure process used for individual identity verification based on Governmentally Accepted Form(s) of ID or whose service itself is considered to generate a Governmentally Acceptable Form of ID**.**
- **Trustworthy System:** Computer hardware, software and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.
- **Unregistered Domain Name:** A Domain Name that is not a Registered Domain Name.

- **Valid Certificate:** A Certificate that passes the validation procedure specified in RFC 5280.
- **Validity Period**: The period of time measured from the date when the Certificate is issued until the Expiry Date.
- **WebTrust Program for CAs:** The then-current version of the CPA Canada WebTrust Program for Certification Authorities.
- **WebTrust Seal of Assurance:** An affirmation of compliance resulting from the WebTrust Program for CAs.
- **Wildcard Certificate:** A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.
- **X.509:** The standard of the ITU-T (International Telecommunications Union-T) for Certificates.

2. Publication and Repository Responsibilities

2.1 Repositories

Trustgate CA publishes all CA Certificates and Cross Certificates, revocation data for issued Certificates, CP, CPS and Relying Party agreements and Subscriber Agreements in Repositories. Trustgate CA ensures that revocation data for issued Certificates and its Root Certificates are available through a Repository 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled downtime that does not exceed 0.5% annually.

Trustgate CA may publish submitted information on publicly accessible directories for the provision of Certificate status information.

Trustgate CA refrains from making publicly available 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 or ETSI audit performed on Trustgate CA.

2.2 Publication of Certificate Information

Trustgate CA publishes its CP, CPS, Subscriber Agreements and Relying Party agreements at www.msctrustgate.com. CRLs are published in online repositories. The CRLs contain entries for all revoked unexpired Certificates with a validity period that depends on Certificate type and/or position of the Certificate within the Certificate chain.

2.3 Time or Frequency of Publication

CA Certificates are published in a Repository via support pages as soon as possible after issuance. CRLs for end user Certificates are issued at least once per day. CRLs for CA Certificates are issued at least annually and within 24 hours if a Certificate is revoked. Each CRL includes a monotonically increasing sequence number for each CRL issued. If a Certificate listed in a CRL expires, it may be removed from later issued CRLs after the Certificate's expiration.

Trustgate CA reviews its 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 the CP, this 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

The repository is publicly accessible information. Read - only access to the repository is unrestricted. Logical and physical security measures are implemented to prevent unauthorised persons from adding, deleting or modifying repository entries.

3. Identification and Authentication

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

Applicants are prohibited from using names in their Certificate that infringe upon the intellectual property rights of others. Trustgate CA does not verify whether an Applicant has intellectual property rights in the name appearing in the Certificate application or arbitrate, mediate or otherwise resolve any dispute concerning the ownership of any Domain Name, trademark, trade name or service mark. Trustgate CA reserves the right, without liability to any Applicant, to reject an application because of such a dispute.

Trustgate RAs authenticate the requests of parties wishing to revoke Certificates.

3.1 Naming

3.1.1 Types of Names

Trustgate CA Certificates are issued with subject DNs (Distinguished Names) which meet the requirements of X.500 naming, RFC-822 naming and X.400 naming. CNs (Common Names) respect name space uniqueness and are not misleading. However, some Certificates such as IntranetSSL SSL Common Names and/or Trustgate CA may also include RFC2460 (IP version 6) or RFC791 (IP version 4) addresses.

Wildcard SSL Certificates include a wildcard asterisk character as the first character in a CN or SAN. Before issuing a Certificate with a wildcard character (*) in the CN or SAN, Trustgate CA follows best practices to determine if the wildcard character occurs in the first label position to the left of a "registry-controlled" label or "public suffix". (e.g. "*.com", see RFC 6454 Section 8.2 for further explanation.) and, if it does, it will reject the request if that Domain Namespace is not owned or controlled by the Subscriber.

3.1.2 Need for Names to be Meaningful

In cases where a Trustgate CA product allows the use of a role or departmental name and where the OU field is included in the DN, additional unique elements may be added to the DN within the OU field to allow Relying Parties to differentiate between Certificates with common DN elements.

3.1.3 Anonymity or Pseudonymity of Subscribers

Trustgate CA may issue end entity anonymous or pseudonymous Certificates provided that such Certificates are not prohibited by applicable policy and, where possible, name space uniqueness is preserved. Trustgate CA reserves the right to disclose the identity of the Subscriber if required by law. Requests for internationalised domain names (IDNs) in Certificates will be flagged for additional manual review. The decoded hostname will undergo additional review to attempt to mitigate the risk for phishing and other fraudulent usage and the decoded hostname may be compared with previously rejected Certificate Requests or revoked Certificates. Trustgate CAs may reject applications based on risk-mitigation criteria, including names at risk for phishing or other fraudulent usage, names listed on the Google Safe Browsing lists and names listed in the database maintained by the Anti-Phishing Working Group.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

Trustgate CA 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.

3.1.6 Recognition, Authentication and Role of Trademarks

Subscribers may not request Certificates with any content that infringes the intellectual property rights of a third-party. Trustgate CA does not require that an Applicant's right to use a trademark be verified. Trustgate CA reserves the right to revoke any Certificate that is involved in a dispute. 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 uses the results of successful initial identity validation processes to create alternative product offerings by effectively combining elements of previously verified information with alternative, newly verified information. A Trustgate Certificate Centre (Trustgate CA) account is used to authenticate the use of any previously verified information for returning Applicants provided that that the re-verification requirements of Section 3.3.1 are complied with by the Trustgate CA account holder.

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 either as a Certificate Signing Request (CSR) in PKCS#10 format or as a Signed Public Key and Challenge (SPKAC).

Trustgate CA accepts other Issuing CAs wishing to enter its hierarchy through its Trusted Root program. Following an initial assessment and signing of an agreement with Trustgate CA, the Issuing CA must also prove possession of the Private Key. CA chaining services do not mandate the physical appearance of the Subscriber representing the Issuing CA so long as an agreement between the Applicant organisation (which has been authenticated) and Trustgate CA has been executed.

3.2.2 Authentication of Organisation Identity

Trustgate CA maintains internal policies and procedures which are reviewed regularly in order to comply with the requirements of the various root programs that Trustgate CA is a member of, as well as the Baseline Requirements, the EV Guidelines and EV Code Signing Guidelines. These policy and procedure documents are under the control of Policy Authority fulfilling the criteria of Principle 6 of the WebTrust 2.0. The method by which Trustgate CA verifies the organisation identity is generally consistent across all product types, however alternative methods, in line with accepted alternatives, may be used where authentication is not possible through the more commonly used QGIS method outlined below.

For all Certificates that include an organisation identity, Applicants are required to provide the organisation's name and registered or trading address. For all Certificates, the legal existence, legal name, assumed name, legal form (where included in the request or part of the legal name in the jurisdiction of incorporation) and requested address of the organisation are verified using one of the following:

- A government agency (QGIS) in the jurisdiction of the Applicant or a superior governing governmental agency if the Applicant claims they are a government agency themselves;
- A third-party database that is periodically updated and has been evaluated by Trustgate CA to determine that it is reasonably accurate and reliable;
- An attestation letter confirming that Subject Identity Information is correct written by an accountant, a lawyer, a government official, a judge or other reliable third-party customarily relied upon for such information; or
- A Qualified Governmental Tax Information Source

Except for Extended Validation (which does not allow this method for verification of the address), Trustgate CA may verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document or other form of identification that has been determined by Trustgate CA to be reasonably accurate and reliable.

The authority of the Applicant to request a Certificate on behalf of the organisation is verified in accordance with Section 3.2.5 below.

3.2.2.1 Local Registration Authority Authentication

Trustgate CA sets authenticated organisational details in the form of a *Profile.* Suitably authenticated account administrators acting in the capacity of a Local Registration Authority authenticate individuals affiliated with the organisation and/or any sub-domains owned or controlled by the organisation.

3.2.2.2 Role Based Certificate Authentication (DepartmentSign)

Trustgate CA ensures that requests for machine, device, department or role based Certificates are authenticated. LRAs are contractually obligated to ensure that machine, device, department or role based names relating to the organisation profile and its business are accurate and correct.

3.2.3 Authentication of Individual identity

Trustgate CA authenticates individuals depending upon the class of Certificate as indicated below.

3.2.3.1 Class 1

The Applicant is required to demonstrate control of his/her email address to which the Certificate relates. Trustgate CA does not authenticate additional information/attributes which may be provided by the Applicant during the application and enrolment process.

3.2.3.2 Class 2

The Applicant is required to demonstrate control of certain identity attributes included in the request, such as his/her physical credential to which the Certificate relates if included in the Certificate Request.

The Applicant is required to submit a legible copy of a valid government issued identity such as national identity, passport, driver's license, military ID or equivalent. A suitable non-government issued identity document or photo ID may also be required for additional proof. Trustgate CA verifies to a reasonable level of assurance that the copy of the ID matches the requested name and that other Subject information such as Country and/or state and locality fields are correct.

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

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

- Receiving an attestation from a customer to validate the identities of its own end customers based on a verification of a Governmentally accepted form of identity, while the customer maintains a secure auditable trail of these verifications.
- The Applicant's seal impression (in jurisdictions that permit their use to legally sign a document) is included with any application received in writing.

Trustgate CA may request further information from the Applicant. Other information and/or methods may be utilised in order to demonstrate an equivalent level of confidence.

If an email address is to be included in the Certificate Request, Trustgate CA or LRA shall verify the validity and ownership of that email address.

3.2.3.3 Class 3

The Applicant is required to submit a legible copy of a valid government issued identity such as national ID, passport, driver's license, military ID or equivalent. A suitable non-government issued identity document or photo ID may also be required for additional proof. Where the submission of a copy of a government issued identity is prohibited by local law or regulation, Trustgate CA shall accept attestation or documentation from a Trusted Third-party authorised to conduct identity verification. Trustgate CA or a trusted third-party verifies to a reasonable level of assurance that the copy of the ID matches the requested name and that other Subject information such as Country and/or state and locality fields are correct.

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

- Performing an SMS challenge/response to the Applicant using his/her mobile number or receiving a fund transfer payment from the Applicant's banking account via a channel (e.g FPX, IBG) that provides the name of the applicant;
- Performing face to face verification against the Applicant's valid government issued identity such as national ID, passport, driver's license, military ID or equivalent;
- Performing a biometric verification (e.g. fingerprint and face recognition)

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

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

3.2.4 Non-Verified Subscriber Information

Trustgate CA validates all information to be included within the Subject DN of a Certificate except as stated otherwise in this section of the CPS. Trustgate CA uses the Subject: organisationalUnitName as a suitable location to identify non-verified Subscriber information to Relying Parties or to provide any specific disclaimers/notices. In the case of individuals, a unique identifier such as mobile number may be used in conjunction with the individual's legal name.

- For all Certificate types where Trustgate CA can explicitly identify a name, DBA, tradename, trademark, address, location or other text that refers to a specific natural person or Legal Entity Trustgate CA verifies the information and omits any disclaimer notice.
- For all Certificate types where Trustgate CA cannot explicitly verify the identity, e.g. a generic term such as “Marketing”, Trustgate CA omits any disclaimer that this item is classified as non-verified Subscriber information as described herein. For IntranetSSL SSL/TLS Certificates only, Trustgate CA relies upon information provided by the Applicant to be included within the subjectAlternativeName such as internal or non-public DNS names, hostnames and RFC 1918 IP addresses. The Baseline Requirements define the time frame for an industry wide deadline at which time these objects may no longer be included within OV Certificates. Until such time, these items are classified as non-verified Subscriber information as ownership cannot reasonably be validated.

Specifically for SSL/TLS Certificates and code signing Certificates, Trustgate CA maintains an enrolment process which ensures that Applicants cannot add self-reported information to the subject: organisationalUnitName.

Trustgate CA through its EPKI service provides certificates used most commonly used for client authentication, document signing and secure messaging for end users, roles and devices. Local Registration Authorities are contractually obligated to perform validation of device names and/or roles and/or names. The following Policy OID (1.3.6.1.4.1.4146.1.40.10) is added in the Certificate in order to indicate that data included within the Certificate’s Subject: organisationalUnitName and/or the common name has been verified by a LRA.

3.2.5 Authentication of Domain Name

For all SSL/TLS Certificates, authentication of the Applicant’s (or the Applicant’s parent company’s, subsidiary company’s or Affiliate’s, collectively referred to as “Applicant’s” for the purposes of this section) ownership or control of all requested Domain Name(s) is done using one of the following methods:

- Confirming the Applicant’s control over the FQDN by validating the Applicant is the Domain Contact directly with the Domain Name Registrar where the Applicant’s identity is verified and the authority of the Applicant representative is validated (BR section 3.2.2.4.1); or
- Having the Applicant demonstrate control over the requested FQDN by sending a Random Value to a Domain Contact via email and then receiving a confirming response utilizing the Random Value. (BR section 3.2.2.4.2); or
- Having the Applicant demonstrate control over the requested FQDN by calling the Domain Contact’s (the Registrant’s) phone number and obtaining a response confirming the Applicant's request for validation of the FQDN (BR section 3.2.2.4.3); or

- Having the Applicant demonstrate control over the requested FQDN by sending a Random Value to an email address created by prepending ‘admin’, ‘administrator’, ‘webmaster’, ‘hostmaster’ or ‘postmaster’ in the local part, followed by the at-sign (“@”), followed by an Authorisation Domain Name and obtaining a response utilizing the Random Value (BR section 3.2.2.4.4); or
- Having the Applicant demonstrate control over the requested FQDN by confirming the presence of a Random Value within a file under the "/well-known/pki-validation" directory on an Authorisation

Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorised Port. (BR section 3.2.2.4.6); or

- Having the Applicant demonstrate control over the requested FQDN by confirming the presence of a Random Value in a DNS TXT record on an Authorisation Domain Name (BR section 3.2.2.4.7); or
- Having the applicant demonstrate control over the requested FQDN by confirming the presence of a non-expired Test Certificate issued by the CA on the Authorisation Domain Name and which is accessible by the CA via TLS over an Authorised Port for the purpose of issuing a Certificate with the same Public Key as in the Test Certificate (BR section 3.2.2.4.9).

Trustgate CA uses the following methods to confirm that the Applicant has control of or right to use IP addresses:

- Having the Applicant demonstrate practical control over the IP Address by making an agreed - upon change to information found on an online Web page identified by a uniform resource identifier containing the IP Address; or
- Obtaining documentation of IP address assignment from the Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC); or,
- Performing a reverse - IP address lookup and then verifying control over the resulting Domain Name; or
- Email challenge based on email address or via phone information listed in the IANA or similar repository; or
- Using any other method of confirmation, provided that the CA maintains documented evidence that the method of confirmation establishes that the Applicant has control over the requested IP address.

3.2.6 Authentication of Email addresses

Trustgate uses the following methods to confirm that the Applicant has control of or right to use email addresses:

- Having the Applicant demonstrate control over the email address by sending an URL including a Random Value to the email address and then receiving a confirming access to the web page utilizing the Random Value URL; or
- Having the Applicant demonstrate control over or right to use the FQDN using one of the Domain Validation processes listed above. Once verified, an Enterprise RA can issue Certificates containing accurate email addressed under that FQDN.

3.2.7 Identification and Authentication for Reissuance after Revocation

After a Certificate has been revoked, the Subscriber is required to go through the initial registration process described elsewhere in this document 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 embodied 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.

3.2.9 Identification and Authentication for Re-key After Revocation

A routine re-key after revocation is not supported. Re-key after revocation of a Certificate requires the Subscriber to follow the initial validation process that was previously completed to allow the initial issuance of the Certificate.

3.3 Identification and Authentication for Revocation Request

All revocation requests are authenticated by Trustgate CA. Revocation requests may be granted following a suitable challenge response such as, logging into an account with the username and password, proving possession of unique elements incorporated into the Certificate E.g. Domain Name or email address or authentication of specific information from within the account which is authenticated out of band.

4. Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Trustgate CA maintains its own blacklists of individuals from whom and entities from which it will not accept Certificate applications. In addition, other external sources such as government denied lists or internationally recognised denied persons lists which are applicable to the jurisdictions in which Trustgate CA operates are used to screen out unwanted Applicants.

Trustgate CA does not issue Certificates to entities that reside in Countries where the laws of a Trustgate CA office location prohibit doing business.

EV Guidelines highlight the specific rules to follow in order to obtain an Extended Validation SSL / Extended Validation Code Signing Certificate. Applicants must submit and agree to a Certificate Request and Subscriber Agreement, which may be electronic or pre-authorised depending upon the nature of the service required from Trustgate CA.

Applications are accepted via one of four methods:

- **On-line –** Via a web interface over an https session. An Applicant must submit an application via a secure ordering process according to a procedure maintained by Trustgate CA. The majority of direct customers use this method, known as Trustgate CA. It requires users to maintain an account with a suitably strong username and password for ongoing maintenance of the lifecycle of the Certificate. The account may be classified as MSSL, EPKI, retail, partner or reseller.
- **API –** Resellers, partners and large enterprises may submit an appropriately formatted Certificate Request via an approved API (Application Programming Interface) to Trustgate CA with a suitably strong username and password. The source IP address of the Applicant may be required by Trustgate CA if no other constraints are applicable. The account may be classified as API or SAPI (Simple API).
- **Manual –** Applicants wishing to enter the Trusted Root program, issue timestamping certificates or those requiring a greater number of SubjectAlternativeName entries in a Certificate are required to submit applications both electronically in the form of an email and out of band such that the request can be sufficiently authenticated and verified.

4.1.2 Enrolment Process and Responsibilities

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

Generally, the application process includes the following steps (but not necessarily in this order as some workflow processes generate Key Pairs after the validation has been completed):

- Generating a suitable Key Pair using a suitably secure platform;
- Generating a Certificate Signing Request (CSR) using an appropriately secure tool;
- Submitting a request for a Certificate type and appropriate application information;
- Agreeing to a Subscriber Agreement or other applicable terms and conditions; and
- Paying any applicable fees.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Trustgate CA maintains systems and processes to sufficiently authenticate the Applicant's identity in compliance with this CPS. Initial identity vetting may be performed by Trustgate CA's validation team as set forth in Section 3.2 or by Registration Authorities under contract. All communications sent through as faxes/email are securely stored along with all information presented directly by the Applicant via the Trustgate web interface or API. Future applications for Certificates are

authenticated using single (username and password) or multi-factor (Certificate in combination with username/password) authentication techniques.

4.2.2 Approval or Rejection of Certificate Applications

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

Assuming all validation steps can be completed successfully following the procedures in this CPS then Trustgate CA shall generally approve the Certificate Request. Trustgate CA may reject applications including for the following reasons:

- Trustgate CA may reject requests based on potential brand damage to Trustgate CA in accepting the request.
- Trustgate CA may also reject applications for Certificates from Applicants who have previously been rejected or have previously violated a provision of their Subscriber Agreement.

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

For Extended Validation Certificates, separation of duties requires two members of the validation team to approve the request. Trustgate CA operates in many jurisdictions; however, it may choose to outsource a pre-vetting function to suitably trained and experienced external RA partners who have additional relevant language and local jurisdiction knowledge to be able to process and/or translate documentation that is not in a language that Trustgate CA itself can process internally.

4.2.3 Time to Process Certificate Applications

Trustgate CA shall ensure that all reasonable methods are used in order to evaluate and process Certificate applications. Where issues outside of the control of Trustgate CA occur, Trustgate CA shall strive to keep the Applicant duly informed.

For Extended Validation Certificates, Trustgate CA first validates that all information provided by the Applicant is correct before requesting the contract signer to approve the Subscriber Agreement.

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 issue a direct command in order for the Root CA to perform a certificate signing operation.

Trustgate CA shall ensure it communicates with any RA accounts capable of causing Certificate issuance using multi-factor authentication. This includes RAs directly operated by Trustgate CA or RAs contracted by Trustgate CA. Enterprise or local RA capabilities do not directly communicate with the CA and therefore multi-factor authentication is optional. RAs shall perform validation of all information sent to the CA and ensure that any database used to store any information is suitably protected from unauthorised modification or tampering.

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

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the CA

Trustgate CA publishes the Certificate by delivering it to the Subscriber and may publish them to one or more Certificate Transparency Logs. In addition, for Enterprise PKI customers Trustgate CA may publish the Certificate into a directory such as LDAP.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RAs, local RA or partners/resellers or Trustgate CA may be informed of the issuance if they were involved in the initial enrolment.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers must protect their Private Key taking care to avoid disclosure to third parties. Trustgate CA's Subscriber Agreement identifies 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.

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

4.5.2 Relying Party Public Key and Certificate Usage

Within this CPS Trustgate CA provides the conditions under which Certificates may be relied upon by Relying Parties including the appropriate Certificate services available to verify Certificate validity such as CRL and/or OCSP. Trustgate CA provides 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.

Software used by Relying Parties should be fully compliant with X.509 standards including best practice for chaining decisions around policies and key usage.

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 with the exception of NAESB Certificates which must rely on rekeying but contains a new 'Not After' date.

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 limitations above). The original Certificate may be revoked after renewal is complete; however, the original Certificate must not be further renewed, re-keyed or modified.

4.6.2 Who May Request Renewal

Trustgate CA may accept a renewal request, provided that the original Subscriber, through a suitable Certificate lifecycle account challenge response authorises it. For IETF RFC definition of renewal a Certificate signing request is not mandatory, however Trustgate CA uses the term renewal to support a second application for a Certificate which is technically a re-key, however, the same Public Key may be used.

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 4.6.1

4.6.6 Publication of the Renewal Certificate by the CA

As per 4.6.2

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

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 treats modification the same as 'New' issuance.
- Trustgate CA may modify Certificates that have either been previously renewed or previously rekeyed. The original Certificate may be revoked after modification is complete, however, the original Certificate cannot 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 4.6.1

4.7.6 Publication of the Modified Certificate by the CA

As per 4.6.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

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 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 when revoked Certificates pass their expiration date to promote more efficient CRL file size management. Prior to performing a revocation Trustgate CA will verify the authenticity of the revocation request. Revocation of a Subscriber Certificate shall be performed within twenty-four (24) hours under the following circumstances:

- The Subscriber requests in writing to the Trustgate CA 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);
- Trustgate 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's CP or this CPS;
- If Trustgate CA determines that any of the information appearing in the Certificate is not accurate or is misleading;
- Trustgate CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
- Trustgate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless Trustgate CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- 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;
- The technical content of format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/B Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time);

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 a Trustgate CA account which controls the lifecycle of the Certificate;

- The Subscriber requests revocation of the Certificate via a OneClickSSL 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;
- Overdue payment of applicable fees by the Subscriber;
- 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;
- 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 to Trustgate CA's or a third-party's business or reputation, Trustgate CA will consider, among other things, the nature and number of complaints received, the identity of the complainant(s), relevant legislation in force and 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 the Trustgate CA entity which provided the Subordinate CA Certificate or the authority detailed in Section 1.5.2 of this CPS, that Trustgate CA revoke the Certificate;
- The Subscriber notifies the Issuing CA that the original Certificate Request was not authorised and does not retroactively grant authorisation;
- The Issuing 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;
- The Issuing 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;
- The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The Issuing CA or Subordinate CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;

- The Issuing CA's or Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless the issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by the Issuing CA's CP and/or CPS;
- The technical content of format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/B Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

For any Trusted Root CA, Trustgate CA may revoke the Issuing CA if the Trusted Root CA no longer meets the contractual terms and conditions of the agreement between the two parties.

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 the Certificate. Trustgate CA may also at its own discretion revoke Certificates including Certificates that are issued to other cross signed CAs.

4.8.3 Procedure for Revocation Request

Due to the nature of revocation requests and the need for efficiency, Trustgate CA provides automated mechanisms for requesting and authenticating revocation requests. The primary method is through the Trustgate CA account used to issue the Certificate that is requested to be revoked. Alternative out of band methods may be used, such as receipt of a fax/letter/phone call, the origins of which must be authenticated using shared secrets from the Trustgate CA account. Alternatively, where Trustgate CA accounts are not provided, methods may be used which rely on a demonstration of control of one or more elements of the Subject DN of the Certificate. For SSL/TLS, this could involve using the OneClickSSL protocol to demonstrate control/ownership of the dNSDomainName. For SMIME Certificates, it could include demonstration of control of the email address. Trustgate CA and its RAs will record each request for revocation and authenticate the source, taking appropriate action to revoke the Certificate if the request is authentic and approved.

Subscribers, Relying Parties, Application Software Suppliers and other third parties may submit Certificate Revocation request via support@msctrustgate.com. Trustgate CA may or may not revoke in response to this request. See section 4.9.5 for detail of actions performed by Trustgate CA for making this decision.

Once revoked, the serial number of the Certificate and the date and time shall be added to the appropriate CRL. CRL reason codes may be included. CRLs are published according to this CPS.

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. Subscribers are given 48 hours to take appropriate actions, otherwise Trustgate CA may revoke the Certificate. A risk analysis shall be completed and recorded for any revocations that cannot be processed by either party for any reason.

4.8.5 Time Within Which CA Must Process the Revocation Request

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 24 hours of receipt.

Trustgate CA through its Trusted Root program processes revocation requests within 24 hours of a confirmation of Compromise and an ARL is published within 12 hours of its creation.

Trustgate CA maintains 24 x 7 ability to respond internally to a high-priority Certificate Problem Report and, where appropriate, forward such a complaint to law enforcement authorities and/or revoke a Certificate that is the subject of such a complaint. Trustgate CA will begin investigation procedures for a suspected Key Compromise or misuse of a Certificate within 24 hours of receipt of the report.

Trustgate CA decides whether revocation or other action is warranted based on at least the 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 legislations.

4.8.6 Revocation Checking Requirements for Relying Parties

Prior to relying upon 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 the 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 will include all applicable URLs within the Certificate to aid Relying Parties in performing the revocation checking process such as:

- http://crl.msctrustgate.com
- http://ocsp.msctrustgate.com

PDF signing Certificates also require Relying Parties to check the status of the Adobe Root CRL. This CRL is outside the scope of this CPS but is located at http://crl.adobe.com/cds.crl

4.8.7 CRL Issuance Frequency

If an End Entity certificate contains a CDP (CRL Distribution Point) then that CRL is updated every 24 hours and is valid for seven (7) days.

If a CA certificate contains a CDP, then that 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

Trustgate CA supports OCSP responses in addition to CRLs. Response times are generally no longer than 10 seconds under normal network operating conditions.

For the status of Subscriber Certificates:

- Trustgate CA updates information provided via an OCSP at least every four days. OCSP responses from this service will not exceed an expiration time of ten days.

For the status of Subordinate CA Certificates:

- Trustgate CA updates information provided via an OCSP at least (i) every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate.

OCSP responders for CAs which are not Technically Constrained in line with Section 7.1.5 will not respond with a "good" status for such Certificates.

Trustgate CA requires OCSP requests to contain the following data:

- Protocol version
- Service request
- Target Certificate identifier

4.8.10 On-Line Revocation Checking Requirements

Relying Parties must confirm revocation information otherwise all warranties become void.

4.8.11 Other Forms of Revocation Advertisements Available

No stipulation

4.8.12 Special Requirements Related to Key Compromise

Trustgate CA and any of its Registration Authorities shall use commercially reasonable methods to inform Subscribers that their Private Key may have been Compromised. This includes cases where new vulnerabilities have been discovered or where Trustgate CA at its own discretion decides that evidence suggests a possible Key Compromise has taken place. Where Key Compromise is not disputed, Trustgate CA shall revoke Issuing CA Certificates or Subscriber end entity Certificates within 24 hours and publish online CRLs within 30 minutes of creation and ARLs within 12 hours.

4.8.13 Circumstances for Suspension

Certificate suspension is allowed in ePKI customers. Certificate suspension can be used when an ePKI administrator wants to disable client certificates temporarily. Such situations may include temporary loss of certificates and temporary leave of users from organisation, etc. Unlike certificate revocation which disables a Certificate permanently, Certificate suspension status can be lifted by an ePKI administrator to reactivate the Certificate.

4.8.14 Who Can Request Suspension

ePKI administrators can request suspension and lifting of Certificate suspension through Trustgate CA. Trustgate CA does not process Certificate suspension which are not requested through Trustgate CA.

4.8.15 Procedure for Suspension Request

ePKI administrators can request Certificate suspension in Trustgate CA. After the request is submitted in Trustgate CA, such information is synced with RA and CA to process the suspension request. Certificate suspension is listed in the CRL with reason code of “on hold”.

4.8.16 Limits on Suspension Period

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

4.9 Certificate Status Services

4.9.1 Operational Characteristics

Trustgate CA provides a Certificate status service either in the form of a CRL distribution point or an OCSP responder or both. For Code Signing Certificates, Trustgate CA does not remove revocation entries on CRL or OCSP until 10 years after the Expiry Date of the revoked Certificate. For other Certificate types, Trustgate CA does not remove revocation entries on CRL or OCSP until after the Expiry Date of the revoked Certificate.

4.9.2 Service Availability

Trustgate CA maintains 99.9% availability on a 24x7 basis of Certificate status services and may choose to use additional content distribution network cloud based mechanisms to aid service availability.

4.9.3 Operational Features

No stipulation.

4.9.4 End of Subscription

Subscribers may end their subscription to Certificate services by having their Certificate revoked or naturally letting it expire. For Trusted Root, contracts between Trustgate CA and the Trusted Root Subscriber must be maintained throughout the life of the Certificate, unless Certificate revocation is used by Trustgate CA as a method to terminate the contract.

4.10 Key Escrow and Recovery

4.10.1 Key Escrow and Recovery Policy and Practices

CA Private Keys are never escrowed. Trustgate CA does not offer key escrow services to Subscribers.

4.10.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Facility, Management and Operational Controls

5.1 Physical Controls

Trustgate CA maintains 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 is located within a secure data centre. The data centre is a purpose built facility made of concrete and steel construction.

5.1.2 Physical Access

Trustgate CA operates within a secure data centre that provides premise security with biometric scanners and card access systems. A 24x7 Closed Circuit TV (CCTV) monitoring system as well as digital recording is provided. Qualified security guards secure the physical premises and only security cleared and authorised personnel are allowed into the premises.

5.1.3 Power and Air Conditioning

Trustgate CA operates within a secure data centre that is equipped with redundant power and cooling system. UPS and failover to power generator are in place in the unlikely event of power outage.

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

Storage of backup media is off-site, physically secured and protected from fire and water damage.

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 performs regular off-site backup of critical data. The backed up data is stored at a physically secured off-site location.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trustgate CA ensures that all 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:

- **Developer**: Responsible for development of CA systems.
- **Security Officer/Head of Information Security:** Overall responsibility for administering the implementation of the CA's security practices;
- **Vetting Agents**: Responsible for validating the authenticity and integrity of data to be included within Certificates via a suitable RA system and approve the generation/revocation/suspension of Certificates;
- **Infra System Engineer**: Authorised to install, configure and maintain the CA systems used for Certificate lifecycle management;
- **Infra Operator**: Responsible for operating the CA systems on a day to day basis. Authorised to perform system backup / recovery, viewing / maintenance of CA system archives and audit logs;
- **Auditor**: Authorised to view archives and audit logs of the CA Trustworthy Systems;
- **CA activation data holder**: Authorised person that holds CA activation data that is necessary for CA hardware security module operation;

5.2.2 Number of Persons Required per Task

Trustgate CA requires at least two people per task. The goal is to guarantee the trust for all CA services (Key Pair generation, Certificate generation and 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 performs a background check. Each role described above is identified and authenticated in a manner to guarantee that the right person has the right role to support the CA.

5.2.4 Roles Requiring Separation of Duties

Trustgate CA enforces role separation either by the CA equipment or procedurally or by both means. Individual CA personnel are specifically assigned 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.

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

Trustgate CA employs 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 fulfil the requirement through expert knowledge, experience and qualifications with formal training and education, actual experience or a combination of the two. Trusted roles and responsibilities, as specified in Section 5.2.1 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 are 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 are free from conflict of interests that might prejudice the impartiality of the CA operations. Trustgate CA does not appoint to a trusted role any person who is known to have a conviction for a serious crime or another offence if 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 where permitted by law.

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

5.3.3 Training Requirements

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

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

5.3.4 Retraining Frequency and Requirements

Individuals responsible for trusted roles are aware of changes in the Trustgate CA or RA operations, as applicable. Any significant change to the operations has a training (awareness) plan and the execution of such plan is documented.

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

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanctions for Unauthorised Actions

Appropriate disciplinary sanctions are applied to personnel violating provisions and policies within the CP, this CPS or CA related operational procedures.

5.3.7 Independent Contractor Requirements

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

5.3.8 Documentation Supplied to Personnel

Trustgate CA makes available to its personnel this CPS, any corresponding CP 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 the CA. Where possible, the security audit logs shall be automatically generated. 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 ensures 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 are 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 are 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 records of events are protected to prevent alteration and detect tampering and to ensure that only individuals with authorised trusted access are able to perform any operations without modifying integrity, authenticity and confidentiality of the data.

The records of events are 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 are 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 is protected to the same degree as originals.

5.4.6 Audit Collection System (Internal vs. External)

Audit processes are initiated at system start up and finish only at system shutdown. The audit collection system ensures the integrity and availability of the data collected. If necessary, the audit collection system protects the data confidentiality. In the case of a problem occurring during the process of the audit collection Trustgate CA determines whether to suspend Trustgate CA operations until the problem is resolved, duly informing the Trustgate impacted asset owners.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

Trustgate CA performs regular vulnerability assessments covering all Trustgate CA assets related to Certificate issuance, products and services. Assessments 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 CAs 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:

Trustgate CA key life cycle management events, including:

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

Trustgate CA and Subscriber Certificate life cycle management events, including:

- Certificate Requests, renewal and re-key requests and revocation for both successful and unsuccessful attempts;
- All Certificates issued including revoked and expired Certificates;
- All verification activities stipulated in this CPS;
- Date, time, phone number used, persons spoken to and end results of verification telephone calls;
- Acceptance and rejection of Certificate Requests;
- Issuance 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 actual CRLs.

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 is 10 years, however a Trustgate LRA (for EPKI) may retain records for a shorter period of time.

5.5.3 Protection of Archive

The archives are 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 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 Backup Procedures

Archive backups are made which are either of the online Trustgate CA system or the offline system. Online backups are duplicated weekly and each backup is stored in a location which is different from the original online system. One backup is stored in a fire rated media safe. An offline backup is taken at the end of any key ceremony (with the exception of any encrypted material which is store separately in line with key ceremony procedures) and stored in an off-site location within 30 days of the ceremony.

5.5.5 Requirements for Timestamping of Records

If a timestamping service is used to date the records, then it has to comply with the requirements defined in Section 6.8. Irrespective of timestamping methods, all logs must have data indicating the time at which the event occurred.

5.5.6 Archive Collection System (Internal or External)

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

5.5.7 Procedures to Obtain and Verify Archive Information

Media storing of Trustgate CA archive information is checked upon creation. Periodically, statistical samples of archived information are tested to check the continued integrity and readability of the information. Only authorised Trustgate CA equipment, trusted role and other authorised persons are allowed to access the archive. Requests to obtain and verify archive information are coordinated by operators in trusted roles (internal auditor, the manager in charge of the process and the security officer).

5.6 Key Changeover

Trustgate CA may periodically change over key material for Issuing CAs in accordance with Section 6.3.2. Certificate Subject information may also be modified and Certificate profiles may be altered to adhere to best practices. Private Keys used to sign previous Subscriber Certificates are maintained until such time as all Subscriber Certificates have expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Trustgate CA handles incident and compromise according to incident and compromise handling procedures in order to minimise the impact of such events.

5.7.2 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.

5.7.3 Entity Private Key Compromise Procedures

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

Trustgate CA, after investigation of the problem, shall decide if 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. A new Trustgate CA Key Pair shall be generated or an alternative existing CA hierarchy shall be used to create new Subscriber Certificates.

5.7.4 Business Continuity Capabilities After a Disaster

The disaster recovery plan deals with the business continuity as described in Section 5.7.1. Certificate status information systems should be deployed so as to provide 24 hours per day, 365 days per year availability.

5.8 CA or RA Termination

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

- Stops delivering Certificates according to and referring to this CPS;
- Archives all audit logs and other records prior to termination;
- Destroys all Private Keys upon termination;
- Ensures archive records are transferred to an appropriate authority such as another Trustgate CA that delivers identical services;
- Uses secure means to notify customers and Application Software Suppliers to delete all trust anchors.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Root, Intermediate and Issuing CA 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) is present or the ceremony, as a whole, is videotaped/recorded. Trustgate CA key generation is carried out within a device which is certified at least to FIPS 140-2 level 3 or above.

Subscriber key generation provided by Trustgate CA is performed in a secure cryptographic device that meets FIPS 140-2 using key generation algorithm and key size as specified in Section 6.1.5 and 6.1.6.

6.1.2 Private Key Delivery to Subscriber

Trustgate CAs that create Private Keys on behalf of Subscribers do so only when sufficient security is maintained within the key generation process and any onward issuance process to the Subscriber. For SSL/TLS Certificates, this is achieved through the use of PCKS#12 (.pfx) files containing Private

Keys and Certificates encrypted by at least sixteen (16) character password. At least eight (8) characters are system generated and provided to the Subscriber during the enrolment process and the Subscriber specifies at least eight (8) characters. For SMIME certificates, this is again achieved through the use of PCKS#12 (.pfx) files containing Private Keys and Certificates encrypted by a minimum twelve (12) alpha-numeric character Subscriber-selected password.

Trustgate CA ensures the integrity of any Public/Private Keys and the randomness of the key material through a suitable RNG or PRNG. If Trustgate CA detects or suspects that the Private Key has been communicated to an unauthorised person or an organisation not affiliated with the Subscriber, then Trustgate CA revokes all Certificates that include the Public Key corresponding to the communicated Private Key.

6.1.3 Public Key Delivery to Certificate Trustgate CA

Trustgate CA only accepts 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. RA's shall only accept Public Keys from Subscribers in accordance with Section 3.2.1 of this CPS.

6.1.4 CA Public Key Delivery to Relying Parties

Trustgate CA ensures that its Public Keys are delivered to Relying Parties in such a way as to prevent substitution attacks. The Certificates highlighted in Section 1.1 are available for download via https:// URLs and this CPS document is protected by a Certificate issued under the Adobe CDS program, protecting the integrity and authenticity of content (i.e. the serial numbers highlighted in Section 1.1). Commercial web browsers and platform operators are encouraged to embed Root Certificate Public Keys into their root stores and operating systems. Issuing CA Public Keys are 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 through AIA (Authority Information Access).

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, Issuing CAs and end entity Certificates delivered to Subscribers. Any Subordinate CAs in the Trusted Root program, outside of the direct control of Trustgate CA are contractually obligated to use the same best practices. Trustgate CA selects from the following Key Sizes/Hashes for Root Certificates, Issuing CA Certificates and end entity Certificates as well as CRL/OCSP Certificate status responders. These choices align with the Baseline Requirements and EV Guidelines:

6.1.5.1 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)

6.1.5.2 ECC

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

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

6.1.6 Public Key Parameters Generation and Quality Checking

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

6.2 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 requires 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. A suitable mechanism used by Trustgate CA is the 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). The Root Certificate Private Key is always protected through 3 of X.

6.2.3 Private Key Escrow

Trustgate CA does not escrow Private Keys for any reason.

6.2.4 Private Key Backup

If required for business continuity Trustgate CA backs up Root and Subordinate Private Keys under the same multi-person control as the original Private Key. Trustgate CA does not backup Subscriber Private Keys.

6.2.5 Private Key Archival

With the exception of Trustgate CA's digital signing service, Trustgate CA does not archive Subscriber Private Keys and ensures 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 are generated, activated and stored in Hardware Security Modules. When Private Keys are outside of a Hardware Security Module (either for storage or transfer), they are encrypted. Private Keys never exist in plain text outside of a cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

Trustgate CA is responsible for activating the Private Key in accordance with the instructions and documentation provided by the manufacturer of the hardware security module. Subscribers are responsible for protecting Private Keys in accordance with the obligations that are presented in the 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 a Trustgate CA's Hardware Security Module is on-line and operational, it is only used to sign Certificates and CRL/OCSPs from an authenticated RA. When a CA is no longer operational, Private Keys are removed from the Hardware Security Module.

6.2.10 Method of Destroying Private Key

Trustgate CA Private Keys are destroyed when they are no longer needed or when the Certificates to which they correspond have expired or have been revoked. Destroying Private Keys means that Trustgate CA destroys all associated CA secret activation data in the 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 Trustgate CA in PKCS 12 format until the Key Pair is picked up by the Subscriber. When the Subscriber acknowledges the receipt of Key Pair or when 30 days has passed after the key generation, the Subscriber Key Pair is automatically deleted from Trustgate CA. Subscriber Private Keys are not stored in any other Trustgate CA systems.

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Trustgate CA archives Public Keys from Certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

Type			Private Key Usage		Max Validity Period
1	Root Certificates		20 years		30 years
2	TPM Root Certificates		30 years		40 years
3	Issuing CA		11 years		15 years
4	Trusted Root		No stipulation		10 years
5	CA for AATL Certificates		No stipulation		181 months
6	AATL Certificate		No stipulation		39 months
7	DV SSL Certificates		No stipulation		39 months
8	OV SSL		No stipulation		39 months

9	Intranet SSL		No stipulation		5 years
10	EV SSL Certificates		No stipulation		27 months
11	Timestamping Certificates		11 years		133 months
12	PDF Signing for Adobe		No stipulation		39 months

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

Effective March 1, 2018, in no event will Trustgate CA issue an SSL/TSL 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 are made during a key ceremony (Refer to Section 6.1.1). Activation data is either generated automatically by the appropriate HSM or in such a way that meets the same needs. It is then delivered to a holder of a share of the key who is a person in a trusted role. The delivery method maintains the confidentiality and the integrity of the activation data.

6.4.2 Activation Data Protection

Issuing CA activation data is protected from disclosure through a combination of cryptographic and physical access control mechanisms. Trustgate CA activation data is stored on smart cards.

6.4.3 Other Aspects of Activation Data

Trustgate CA activation data may only be 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. The Trustgate CA PKI components must 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 for 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;
- All hardware will be inspected during commissioning process to ensure conformity to supply and no evidence of tampering found. 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;
- 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 approved personnel in a defined manner.

6.6.2 Security Management Controls

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

All Trustgate CA components are regularly synchronised with a reliable time service. Trustgate CA uses one GPS source & one DCF77 source & three non-authenticated NTP source clocks to establish the correct time for:

- 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.

6.8.1 PDF Signing Time Stamping Services

All Digital Signatures created by PDF Signing Certificates have the ability to include a trusted timestamp issued from an RFC 3161 compliant Time Stamp Authority (TSA) server chained to an Adobe Root Certificate. The TSA Certificate shall be located in a FIPS 140-2 level 2 or higher HSM. Timestamping services may be provided by Trustgate CA or by a Trustgate CA outsource agent. In the event that a timestamping service is managed by an outsource agent, then Trustgate CA will issue a timestamping Certificate in compliance with this CPS.

7. Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

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

7.1.2 Certificate Extensions

Trustgate CA issues Certificates in compliance with RFC 5280 and applicable best practice. Criticality also follows best practice to prevent unnecessary risks to Relying Parties when applied to name constraints.

7.1.3 Algorithm Object Identifiers

Trustgate CA issues 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 }
- **ECDSAWithSH256** {iso(1) member - body(2) us(840) ansi - X9 - 62 (10045) signatures(4) ecdsa - with - SHA2(3) 2 }
- **ECDSAWithSHA384** {iso(1) member - body(2) us(840) ansi - X9 - 62 (10045) signatures(4) ecdsa - with - SHA2(3) 3 }
- **ECDSAWithSHA512** {iso(1) member - body(2) us(840) ansi - X9 - 62 (10045) signatures(4) ecdsa - with - SHA2(3) 4 }

7.1.4 Name Forms

Trustgate CA issues Certificates with name forms compliant to RFC 5280.

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

7.1.5 Name Constraints

Trustgate CA may issue Subordinate CA Certificates with name constraints where necessary and mark as critical where necessary as part of the Trusted Root program. When 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.

7.1.6 Certificate Policy Object Identifier

No stipulation.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

7.2.1 Version Number(s)

Trustgate CA issues Version 2 CRLs in compliance with RFC 5280. CRLs have the following fields:

Issuer	The Subject DN of the issuing CA

Effective date	Date and Time
Next update	Date and Time
Signature Algorithm	sha1RSA, sha256RSA etc. (Depending upon product)
Signature Hash Algorithm	sha1, sha256 etc. (Depending upon product)
Serial Number(s)	List of revoked serial numbers
Revocation Date	Date of Revocation

7.2.2 CRL and CRL Entry Extensions

CRLs have the following extensions:

- **CRL Number** Monotonically increasing serial number for each CRL
- **Authority Key Identifier** AKI of the issuing CA for chaining/validation requirements

7.3 OCSP Profile

Trustgate CA operates an Online Certificate Status Profile (OCSP) responder in compliance with RFC 2560 and RFC5019 and highlights this within the AIA extension via an OCSP responder URL.

7.3.1 Version Number(s)

Trustgate CA issues Version 1 OCSP responses with following fields:

Responder ID	SHA-1 Hash of responder's Public Key
Produced Time	the time at which this response was signed
Certificate Status	Certificate status referenced (good/revoked/unknown)
ThisUpdate/NextUpdate	Recommended validity interval for the response
Signature Algorithm	SHA1 RSA, SHA256 RSA etc. (depending upon product)
Signature	Signature value generated by the responder
Certificates	the OCSP responder's Certificate

An OCSP request must contain the following data:

- Protocol version
- Service request
- Target Certificate identifier

7.3.2 OCSP Extensions

If OCSP request has a nonce field, then the corresponding response also has the same nonce value in the response.

8. Compliance Audit and Other Assessments

The procedures within this CPS encompass all relevant portions of currently applicable PKI standards for the various vertical PKI industries in which Trustgate CA operates. Trusted Root CAs that are not constrained by dNSNameConstraints are audited for compliance to one or more of the following standards:

- AICPA/CICA Trust Service Principles and Criteria for Certification Authorities
- AICPA/CICA WebTrust for Certification Authorities – Extended Validation Audit Criteria
- AICPA/CICA WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing
- AICPA/CICA WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security

8.1 Frequency and Circumstances of Assessment

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

8.2 Identity/Qualifications of Assessor

The audit of Trustgate CA is performed by a "Qualified Auditor" that possesses the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit as stipulated in section 8.0 of this document;
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing and the third-party attestation function;
- Certified, accredited, licensed or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme; and
- Bound by law, government regulation or professional code of ethics.

8.3 Assessor's Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

The audit meets the requirements of the audit schemes highlighted in Section 8.0 under which the assessment is being made. These requirements may vary as audit schemes are updated. An audit scheme is applicable to Trustgate CA in the year following the adoption of the updated scheme.

8.5 Actions Taken as a Result of Deficiency

Trustgate CA, including cross-signed Issuing CAs that are not technically constrained, follow the same process if presented with a material non-compliance by auditors and create a suitable corrective action plan to remove the deficiency. Corrective action plans which directly affect policy and procedure as dictated by the CP and CPS are referred to the Trustgate CA policy authority.

8.6 Communications of Results

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

8.7 Self Audit

Trustgate CA monitors its adherence to Certificate Policy, Certification Practice Statement and other external requirements specified in the “Acknowledgements” section and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected samples at least 3 percent (6% for EV SSL Certificate and EV Code Signing Certificates) of the Certificates issued.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Trustgate CA charges fees for Certificate issuance and renewal. Trustgate CA does not charge for reissuance (re-key during the lifetime of the Certificate). Fees and any associated terms and conditions are made clear to Applicants both by the enrolment process through a web interface or in the sales and marketing materials on Trustgate CA’s web site.

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

Trustgate CA may charge additional fees to Subscribers who have a large Relying Party community and choose not to use OCSP stapling or other similar techniques to reduce the load on the Trustgate CA’s Certificate status infrastructure.

9.1.4 Fees for Other Services

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

9.1.5 Refund Policy

Trustgate CA offers a refund to Subscribers in accordance with the refund policy published on Trustgate CA’s web site www.msctrustgate.com. Subscribers who choose to invoke the refund policy will have all issued Certificates revoked.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Enterprise Customers are encouraged to maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention. Trustgate CA maintains commercial general liability insurance with policy limits of at least Five Hundred Ringgit Malaysia (MYR500) and a maximum One million Ringgit Malaysia (MYR1,000,000) in coverage. Trustgate CA's insurance policies include coverage for (1) claims for damages arising out of an act, error or omission, unintentional breach of contract or neglect in issuing or maintaining Certificates and (2) claims for damages arising out of infringement of the proprietary rights of any third-party (excluding copyright, patent and trademark infringement), invasion of privacy and advertising injury.

9.2.2 Other Assets

Enterprise Customers shall have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to Subscribers and Relying Parties.

9.2.3 Insurance or Warranty Coverage for End Entities

Trustgate CA offers a Warranty Policy to Subscribers published on Trustgate CA's web site at www.msctrustgate.com.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following items are classified as being confidential information and therefore are subject to reasonable care and attention by Trustgate CA staff including Vetting Agents and administrators:

- Personal Information as detailed in Section 9.4;
- Audit logs from CA and RA systems;
- Activation data used to active CA Private Keys as detailed in Section 6.4;
- Internal Trustgate CA business process documentation including Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP); and
- Audit Reports from an independent auditor as detailed in Section 8.0.

9.3.2 Information Not Within the Scope of Confidential Information

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

9.3.3 Responsibility to Protect Confidential Information

Trustgate CA protects confidential information through training and enforcement 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 Trustgate CA's web site at www.msctrustgate.com.

9.4.2 Information Treated as Private

Trustgate CA treats all information received from Applicants that will not ordinarily be placed into a Certificate 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 periodically trains 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 is 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. The Privacy Policy is published on Trustgate CA's web site at www.msctrustgate.com.

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 includes any required consents in the Subscriber Agreement, including any permission required for additional information to be 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.

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property rights

Trustgate CA does not knowingly violate the intellectual property rights of third parties. Public and Private Keys remain the property of Subscribers who legitimately hold them. Trustgate CA retains ownership of Certificates; however, it grants permission to reproduce and distribute Certificates on a non-exclusive, royalty free basis, provided that they are reproduced and distributed in full.

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Trustgate CA uses this CPS and applicable Subscriber Agreements to convey legal conditions of usage of issued Certificates to Subscribers and Relying Parties. 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 appropriate RA.

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 (see Section 3.2);
- **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 (see Sections 3.2.3, 3.2.3, 3.2.4);
- **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 (see Sections 3.2.3, 3.2.3, 3.2.4);
- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA (i) implemented a procedure to verify the identity of the Applicant; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in Trustgate CA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);
- **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 (see Section 4.5.1);

- **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, EV Guidelines and/or EV Code Signing Guidelines (as applicable) (see Section 4.9.1).

In addition, Trustgate CA represents and warrants to Certificate Beneficiaries for NAESB Certificates that, 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:

- Trustgate CA has issued and will manage, the Certificate in accordance with the NAESB WEQ PKI Standards.
- There are no misrepresentations of fact in the Certificate actually known to or reasonably knowable by Trustgate CA and Trustgate CA has verified information in the Certificate.
- Information provided by the Applicant for inclusion in the Certificate has been accurately transcribed to the Certificate.

In lieu of the warranties set forth above, Trustgate CA represents and warrants to Certificate Beneficiaries for EV Certificates and EV Code Signing 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 and/or EV Code Signing 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:** For EV Certificates only, 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

RAs warrant that:

- Issuance processes are in compliance with this CPS and the relevant CP;
- All information provided to Trustgate CA does not contain any misleading or false information; and all translated material provided by the RA is accurate.

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 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; and
- Subscriber shall respond to Trustgate CA's instructions concerning Compromise or Certificate misuse within forty-eight (48) hours.

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 an Trustgate CA's Certificate warrants to:

- Have the technical capability to use Certificates;
- Receive notice of the Issuing CA and associated conditions for Relying Parties;
- Validate an Issuing CA's Certificate by using Certificate status information (e.g. a CRL or OCSP) published by the Issuing CA in accordance with the proper Certificate path validation procedure;
- Trust an Issuing 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 an Issuing 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 CPS; and
- Take any other precautions prescribed in the Issuing 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

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

9.8 Limitations of Liability

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

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

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

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

9.9 Indemnities

9.9.1 Indemnification by Trustgate CA

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

9.9.2 Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify Trustgate CA, its partners and any Trusted Root entities and their respective directors, officers, employees, agents and contractors against any loss, damage or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this CPS or applicable law; (iii) the Compromise or unauthorised use of a Certificate or Private Key caused by the Subscriber's negligence; or (iv) Subscriber's misuse of the Certificate or Private Key.

9.9.3 Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify Trustgate CA, its partners and any cross-signed entities and their respective directors, officers, employees, agents and contractors against any loss, damage or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, this CPS or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate's status prior to use.

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

Trustgate CA will communicate the conditions and effect of this CPS termination via the appropriate Repository.

9.11 Individual Notices and Communications with Participants

Trustgate CA accepts notices related to this CPS 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 to the sender. Individual communications made to Trustgate CA must be addressed to support@msctrustgate.com or by post to Trustgate CA in the address provided in Section 1.5.2.

9.12 Amendments

9.12.1 Procedure for Amendment

Changes to this CPS are indicated by appropriate numbering.

9.12.2 Notification Mechanism and Period

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

9.12.3 Circumstances Under Which OID Must be Changed

No stipulation

9.13 Dispute Resolution Provisions

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 of 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 the Trustgate CA executive management. The Trustgate CA executive management may subsequently communicate the proposed settlement to the complaining party.

If the dispute is not resolved within twenty (20) business days after initial notice pursuant to CPS, parties submit the dispute to arbitration.

There will be three (3) arbitrators of whom each party proposes one while both parties of the dispute choose the third arbitrator. The place of the arbitration is Kuala Lumpur, Malaysia and the arbitrators determine all associated costs.

9.14 Governing Law

This CPS is governed, construed and interpreted in accordance with the laws of Malaysia. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of Trustgate CA Certificates or other products and services. The law of Malaysia applies also to all Trustgate CA commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to Trustgate CA products and services where Trustgate CA acts as a provider, supplier, beneficiary receiver or otherwise.

Each party, including Trustgate CA partners, Subscribers and Relying Parties, 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 Malaysian jurisdiction and regulatory framework. Trustgate CA's infrastructure is based in Malaysia. 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 CPS 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 CPS cannot assign their rights or obligations without the prior written consent of Trustgate CA.

9.16.4 Severability

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

9.16.5 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 CPS does not waive Trustgate CA's right to enforce the same provisions later or right to enforce any other provisions of this CPS. To be effective any waivers must be in writing and signed by Trustgate CA.

9.17 Other Provisions

No Stipulation