MSC Trustgate Certificate Policy

Version 3.5

23 August 2019

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

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

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

Trademark Notices

MSC Trustgate and its associated logos are the registered trademarks of MSC Trustgate.com Sdn Bhd or its affiliates. Other names may be trademarks of their respective owners.

Without limiting the rights reserved above, and except as licensed below, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without prior written permission of MSC Trustgate.

Notwithstanding the above, permission is granted to reproduce and distribute this MSC Trustgate Certificate Policy on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete with attribution of the document to MSC Trustgate.

Requests for any other permission to reproduce this MSC Trustgate Certificate Policy must be addressed to MSC Trustgate.com Sdn Bhd, Suite 2-9, Level 2, Block 4801 CBD Perdana, Jalan Perdana, 63000 Cyberjaya, Selangor Darul Ehsan, Malaysia or via email at security@msctrustgate.com.

Revision History

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

No	Date	Changes	Version
1	April 8, 2019	To add Revision History and include several sections mentioned in Baseline Requirement to replace version 3.3 on 21st Feb 2019.	3.4
2	August 23, 2019	To amend the certificate validity period for DV, OV and AATL to 825 days in Section 6.3.2.	3.5

1. Introduction

This Certificate Policy (CP) document is the principal statement of policy governing MSC Trustgate.com Sdn Bhd ("Trustgate CA"). The CP sets forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the Trustgate CA ecosystem and providing associated trust services. These requirements protect the security and integrity of Trustgate CA and comprise a single set of rules that apply consistently, thereby providing assurances of uniform trust throughout the Trustgate CA ecosystem. This CP may be updated from time to time as outlined in *Section 1.5 Policy Administration*. The latest version may be found on the MSC Trustgate CA company repository at www.msctrustgate.com.

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

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

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

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

This CP is final and binding between MSC Trustgate.com Sdn Bhd, Suite 2-9, Level 2, Block 4801 CBD Perdana, Jalan Perdana, 63000 Cyberjaya, Selangor Darul Ehsan, Malaysia (hereinafter referred to as "Trustgate CA") and the Subscriber and/or Relying Party, who uses, relies upon or attempts to rely upon certification services made available by Trustgate CA.

1.1 Overview

This CP applies to the complete hierarchy of Certificates issued by Trustgate CA. The purpose of this CP is to present the Trustgate CA framework 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 CP aims to document the Trustgate CA delivery of certification services and management of the Certificate life cycle of any issued Subordinate CA, client, server and other purpose end entity Certificates.

This CP is specifically applicable to:

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

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

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

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

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

1.2 Document Name and Identification

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

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

1.2.1 Client Certificates

- 1.3.6.1.4.1.49530.1.1.1 Class 1 Certificates

- 1.3.6.1.4.1.49530.1.1.2 Class 2 Certificates (Generic)
- 1.3.6.1.4.1.49530.1.1.2.1 Class 2 Certificates (Government)
- 1.3.6.1.4.1.49530.1.1.2.2 Class 2 Certificates (Enterprise)
- 1.3.6.1.4.1.49530.1.1.3 Class 3 Certificates

1.2.2 Code Signing

- 1.3.6.1.4.1.49530.1.2.1 Code Signing Certificates

1.2.3 Time Stamping

- 1.3.6.1.4.1.49530.1.3.1 Time Stamping Certificates (Generic)

1.2.4 Domain Validation

- 1.3.6.1.4.1.49530.1.4.1 Domain Validation SSL Certificates

1.2.5 Organisation Validation

- 1.3.6.1.4.1.49530.1.5.1 Organisation Validation SSL Certificates

1.2.6 Extended Validation

- 1.3.6.1.4.1.49530.1.6.1 Extended Validation SSL Certificates
- 1.3.6.1.4.1.49530.1.6.2 Extended Validation Code Signing Certificates

1.2.7 Intranet Validation

- 1.3.6.1.4.1.49530.1.7.1 Intranet Validation SSL Certificates

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

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

The Trustgate CA certificates governed by this CP are:

Subject DN	Validity Period	Serial Number
CN = Trustgate Class 1 Root Certificate Authority O = MSC Trustgate.com Sdn. Bhd. C = MY	07/06/2012 00:00:00 GMT 07/05/2042 23:59:59 GMT	1b5ed8fca65cfcdeb0cc00e129023e3a
CN = Trustgate Class 2 Root Certificate Authority O = MSC Trustgate.com Sdn. Bhd. C = MY	07/06/2012 00:00:00 GMT 07/05/2042 23:59:59 GMT	0a8bc4060f5a6cd34d07805da007abf5
CN = Trustgate Class 3 Root Certificate Authority O = MSC Trustgate.com Sdn. Bhd. C = MY	07/06/2012 00:00:00 GMT 07/05/2042 23:59:59 GMT	703b113dcdb38e30f4e57dac18a5310f

Subject DN	Validity Period	Serial Number
CN = Trustgate RSA Certification Authority OU = Malaysia Licensed CA No: LPBP-2/2010 (1) O = MSC Trustgate.com Sdn. Bhd. C = MY	12/19/2016 00:00:00 GMT 12/18/2041 23:59:59 GMT	1f61b6a273937d89952bc4af8e86050e
CN = Trustgate Time Stamping Authority CA OU = Malaysia Licensed CA No: LPBP-2/2010 (1) O = MSC Trustgate.com Sdn. Bhd. C = MY	12/19/2016 00:00:00 GMT 12/18/2041 23:59:59 GMT	4139bac7f7f45005dcd7f76adebf17b1
CN = Trustgate Time Stamping Authority CA (ECC) OU = Malaysia Licensed CA No: LPBP-2/2010 (1) O = MSC Trustgate.com Sdn. Bhd. C = MY	12/19/2016 00:00:00 GMT 12/18/2041 23:59:59 GMT	51e80251ad3e7ff755cac506ddb64bde
CN= MyTrust Class 1 RSA Root CA OU= MyTrust Gateway O= MSC Trustgate.com Sdn. Bhd. C= MY	08/17/2017 00:00:00 GMT 08/16/2042 23:59:59 GMT	3606c60894f246dc130f2671463d11ea
CN= MyTrust Class 2 RSA Root CA OU= MyTrust Gateway O= MSC Trustgate.com Sdn. Bhd. C= MY	08/17/2017 00:00:00 GMT 08/16/2042 23:59:59 GMT	38be005b37d65a7204e7141a6d2262ce
CN= MyTrust Class 3 RSA Root CA OU= MyTrust Gateway O= MSC Trustgate.com Sdn. Bhd. C= MY	08/17/2017 00:00:00 GMT 08/16/2042 23:59:59 GMT	5682e857103ffd808b880488eb1127d0
CN= MyTrust Class 1 ECC Root CA OU=MyTrust Gateway O=MSC Trustgate.com Sdn. Bhd. C=MY	08/28/2017 00:00:00 GMT 08/27/2042 23:59:59 GMT	4fc238d27e35d1ddb4df977002a3efbf
CN= MyTrust Class 2 ECC Root CA OU=MyTrust Gateway O=MSC Trustgate.com Sdn. Bhd. C=MY	08/28/2017 00:00:00 GMT 08/27/2042 23:59:59 GMT	68d4f1dc28d868754c464f4b70123229
CN= MyTrust Class 3 ECC Root CA OU=MyTrust Gateway O=MSC Trustgate.com Sdn. Bhd. C=MY	08/28/2017 00:00:00 GMT 08/27/2042 23:59:59 GMT	3f9289237e806a1da7326edc082052d3

1.3 PKI participants

1.3.1 Certification Authorities

Trustgate CA is a Malaysian licenced Certification Authority that issues Certificates in accordance with this CPS. As a Certification Authority, Trustgate CA performs functions related to Certificate lifecycle management such as Subscriber registration, Certificate issuance, Certificate renewal, Certificate distribution and Certificate revocation. Trustgate CA also provides Certificate status

information using a Repository in the form of a Certificate Revocation List (CRL) and/or Online Certificate Status Protocol (OCSP) responder. Trustgate CA may also be described by the term *"Issuing Authority"* or *"Trustgate CA"* to denote the purpose of issuing Certificates at the request of a Registration Authority (RA) from a subordinate Issuing CA.

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

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

1.3.2 Registration Authorities

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

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

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

1.3.3 Subscribers

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

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

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

1.3.4 Relying Parties

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

1.3.5 Other Participants

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

1.4 Certificate usage

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

1.4.1 Appropriate Certificate Usage

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

- **Authentication:** The assurance of one's identity - who he/she/it claims to be.
- **Integrity:** The assurance to an entity that data has not been tempered with.
- **Confidentiality:** The assurance to an entity that only the intended recipient(s) can read a particular piece of data.
- **Non-repudiation:** A party cannot deny having digitally signed a data, a transaction or a document.

1.4.2 Prohibited Certificate Usage

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

Trustgate CA Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

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

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

Suite 2-9, Level 2,

Block 4801 CBD Perdana, Jalan Perdana, 63000 Cyberjaya

Selangor Darul Ehsan, Malaysia

Tel: +603 8318 1800

www.msctrustgate.com

security@msctrustgate.com

1.5.2 Contact Person

Compliance Officer

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

Suite 2-9, Level 2,

Block 4801 CBD Perdana, Jalan Perdana, 63000 Cyberjaya

Selangor Darul Ehsan, Malaysia

Tel: +603 8318 1800

www.msctrustgate.com

security@msctrustgate.com

1.5.3 Person Determining CP suitability for the Policy

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

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

1.5.4 CP Approval Procedures

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

1.6 Definitions

1.6.1 Definitions

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

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

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

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

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

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

1.6.2 Acronyms

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

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

2. Publication and Repository Responsibilities

Trustgate CA shall develop, implement, enforce, and annually update CP and/or CPS that describes in detail how the CA implements the latest version of these requirements.

2.1 Repositories

Trustgate CA shall publishes all Certificates-related and Certificate Revocation information for issued Certificates, CP, CPS and Relying Party agreements and Subscriber Agreements in public repositories. Trustgate CA shall ensures that revocation data for issued Certificates and its Root Certificates are available through a repository on 24 hours basis and is periodically updated as set forth in this CP.

2.2 Publication of Certificate Information

Trustgate CA shall make publicly available this CP and any CPS, CA Certificates, Relying Party agreements and CRLs through an appropriate and readily accessible online means that is available on a 24x7 basis.

Trustgate CA shall host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA shall host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired.

2.3 Time or Frequency of Publication

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

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

2.4 Access control on repositories

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

3. Identification and Authentication

Trustgate CA shall maintain documented practices and procedures to authenticate the identity and/or other attributes of an Applicant prior to inclusion of those attributes in a Certificate.

3.1 Naming

3.1.1 Types of Names

To identify a Subscriber, Trustgate CA shall follow naming and identification rules that include types of names assigned to the Subject, such as X.500 distinguished names, RFC-822 names and X.400 names.

3.1.2 Need for Names to be Meaningful

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

3.1.3 Anonymity or Pseudonymity of Subscribers

Unless prohibited by policy or law or requested by a State or Government authority to protect the identity of certain end user subscribers (e.g. minors or sensitive government employee information), Subscribers are not permitted to use pseudonyms (names other than a Subscriber's true personal or organizational name).

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 shall ensure the uniqueness of name of Subscriber in issuance of Certificates. However, name uniqueness is not violated when multiple certificates are issued to the same Subcriber.

3.1.6 Recognition, Authentication and Role of Trademarks

Trustgate CA shall not approve any Certificate Application that infringes upon the Intellectual Property Rights of others. Trustgate CA, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark.

3.2 Initial Identity Validation

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

3.2.1 Method to Prove Possession of Private Key

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

3.2.2 Authentication of Organisation and Domain Identity

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

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

- determine that the organization exists by using at least one third party identity proofing service or database, or organizational documentation issued by or filed with the applicable government agency (e.g. QGIS, QTIS, QIIS) or competent authority that confirms the existence of the organization,
- confirm by telephone or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is

authorized to do so. When a certificate includes the name of an individual as an authorized representative of the Organization, the employment of that individual and his/her authority to act on behalf of the Organization shall also be confirmed.

3.2.2.1 Identity

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

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

Trustgate CA may use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address.

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

3.2.2.2 DBA/Tradename

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

Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence or recognition;

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

3.2.2.3 Verification of Country

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

a) the IP Address range assignment by country for either

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

(ii) the Applicant's IP address;

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

c) information provided by the Domain Name Registrar; or

d) a method identified in Section 3.2.2.1.

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

3.2.2.4 Validation of Domain Authorization or Control

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

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

Trustgate CA shall maintain a record of which domain validation method, including relevant BR version number used to validate every domain.

3.2.2.5 Authentication for an IP address

Trustgate CA shall confirm that prior to issuance, Trustgate CA or its RA has validated each IP address listed in the Certificate using at least one of the methods listed in Trustgate CA CPS.

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

3.2.2.6 Wildcard Domain Validation

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

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

3.2.2.7 Data Source Accuracy

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

1. The age of the information provided,
2. The frequency of updates to the information source,
3. The data provider and purpose of the data collection,

4. The public accessibility of the data availability, and
5. The relative difficulty in falsifying or altering the data.

Databases maintained by Trustgate CA, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is collect information for the purpose of fulfilling the validation require under this Section.

3.2.2.8 CAA record

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

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

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

CAs shall permit to treat a record lookup failure as permission to issue if:

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

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

3.2.3 Authentication of Individual identity

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

3.2.3.1 Class 1

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

3.2.3.2 Class 2

The Applicant is required to submit a legible copy of a valid government issued photographic identity such as national identity, passport, driver’s license, police ID, military ID or equivalent. A suitable non-

government issued identity document may also be required for additional proof. Trustgate CA verifies to a reasonable level of assurance that the copy of the identity matches the identity of the Applicant.

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

3.2.3.3 Class 3

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

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

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

3.2.5 Authentication of Domain Name

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

Trustgate CA or its RA may use the sources listed in section 3.2.2.1 to verify the Reliable Method of Communication. Provided that Trustgate CA or its RA uses a Reliable Method of Communication, Trustgate CA or its RA may establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate.

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

3.2.6 Criteria for Interoperation or Certification

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

3.3 Identification and Authentication for Re-key Request

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

3.3.1 Identification and Authentication for Routine Re-key

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

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. As an alternative to using a challenge phrase (or equivalent), Trustgate CA may send an e-mail message to the e-mail address associated with the verified corporate contact for the certificate being renewed, requesting confirmation of the Certificate renewal order and authorization to issue the Certificate. Upon receipt of confirmation authorizing issuance of the Certificate, Trustgate CA will issue the Certificate if the enrolment information (including Corporate and Technical contact information[1]) has not changed.

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

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

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

3.3.2 Identification and Authentication for Re-key After Revocation

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

- the Certificate (other than a Class 1 Certificate) was issued to a person other than the one named as the Subject of the Certificate, or
- the Certificate (other than a Class 1 Certificate) was issued without the authorization of the person or entity named as the Subject of such Certificate, or

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

- the entity approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false.
- For any other reason deemed necessary by Trustgate CA

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

3.4 Identification and Authentication for Revocation Request

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

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

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

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

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

4. Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

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

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

- Any authorized representative of an RA.

Trustgate CA shall maintain an internal database of al previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. Trustgate CA shall use this information to identify subsequent suspicious certificate requests.

4.1.2 Enrolment Process and Responsibilities

Prior to the issuance of a Certificate, Trustgate CA shall obtain the following documentation from the Applicant:

1. A certificate request, which may be electronic; and
2. An executed Subscriber Agreement or Terms of Use, which may be electronic.

Trustgate CA should obtain any additional documentation the CA determines necessary to meet these requirements.

One certificate request may suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in *Section 3.3.1*, provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant representative on behalf of the Applicant. The certificate request may be made, submitted and/or signed electronically.

The certificate request must contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The certificate request may include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for Trustgate CA to obtain from the Applicant in order to comply with Trustgate CA's CP and/or CPS. In cases where the certificate request does not contain all the necessary information about the Applicant, Trustgate CA shall obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. Trustgate CA shall establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

Applicant information must include, but not be limited to, at least one FQDN or IP address to be included in the Certificate's SubjectAltName extension.

Trustgate CA may use the documents and data provided in *Section 3.2* to verify certificate information, or may reuse previous validations themselves, provided that Trustgate CA obtains the data or document from a source specifiedunder *Section 3.2* or completed the validation itself no more than 825 days prior to issuing the Certificate.

In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.

Trustgate CA shall develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements.

If a RA fulfills any of the CA's obligations under this section, Trustgate CA shall verify that the process used by the RA to identify and further verify High Risk Certificate Requests provides at least the same level of assurance as Trustgate CA's own processes.

4.2.2 Approval or Rejection of Certificate Applications

Trustgate CA should not issue Certificates containing a new gTLD under consideration by ICANN. Trustgate CA will revoke the Certificate unless the applicant promptly registers the Domain Name.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

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

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

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

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Trustgate CA shall inform the Subscriber that he/she may not use the Certificate until the Subscriber has reviewed and verified the accuracy of the data incorporated into the Certificate. Unless the Subscriber notifies Trustgate CA may set a time limit when the Certificate is deemed accepted.

4.4.2 Publication of the Certificate by the CA

No stipulation.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

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

accepted the certificate. The certificate shall be used lawfully in accordance with Trustgate CA's Subscriber Agreement the terms of the Trustgate CA CP and this CPS.

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

4.5.2 Relying Party Public Key and Certificate Usage

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

Trustgate CA shall describe the mechanisms available for Relying Parties to verify Certificate validity such as CRLs or OCSP.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

Certificate renewal is defined as the production of a new Certificate that has the same details as a previously issued Certificate. Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to renew a new certificate to maintain continuity of Certificate usage. A certificate may also be renewed after expiration provided the existing Certificate has not been revoked and all details within the Certificate remain accurate.

4.6.2 Who May Request Renewal

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

4.6.3 Processing Certificate Renewal Requests

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

4.6.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As per 4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

As per 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

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

4.7.2 Who May Request Certificate a New Public Key

As per 4.1

4.7.3 Processing Certificate Re-Key Requests

As per 4.2

4.7.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.7.5 Conduct Constituting Acceptance of Re-Key Certificate

As per 4.4.1

4.7.6 Publication of the Re-Key Certificate by the CA

As per 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

No stipulation.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

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

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

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

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

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
2. The CA obtains evidence that the Certificate was misused;
3. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. The CA obtains evidence that the validation of the domain authorization or control for any FQDN or IP address in the Certificate should not be relied upon;
5. The CA is made aware of any circumstance indicating that use of a FQDN or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
6. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
7. The CA is made aware of a material change in the information contained in the Certificate;
8. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's CP or CPS;
9. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate or misleading;
10. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;

11. Revocation is required by the CA's CP and/or CPS;
12. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed;
13. The affiliation between an Enterprise Customer with a Subscriber is terminated or has otherwise ended;
14. The Subscriber has not made payment when due;
15. The technical content of format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties;
16. Any other reason that may be reasonably expected to affect the integrity, security or trustworthiness of a Certificate or CA; or
17. The continued use of the Certificate is harmful to the Trustgate CA

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

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

4.9.1.2 Revoking a Subscriber Certificate

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

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies Trustgate CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. Trustgate CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
4. Trustgate CA obtains evidence that the Certificate was misused;
5. Trustgate CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable CP or CPS;
6. Trustgate CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. Trustgate CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;

8. Trustgate CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the Issuing CA's CP and/or CPS.

4.9.2 Who Can Request Revocation

The Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.

4.9.3 Procedure for Revocation Request

The CA shall provide a process for Subscribers to request revocation of their own Certificates. The CA shall maintain a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports.

The CA shall provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA shall publicly disclose the instructions through a readily accessible online means and in *Section 1.5.2* of its CPS.

4.9.4 Revocation Request Grace Period

No stipulation.

4.9.5 Time Within Which CA Must Process the Revocation Request

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

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

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

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

5. Relevant legislation.

4.9.6 Revocation Checking Requirements for Relying Parties

No stipulation.

4.9.7 CRL Issuance Frequency

For the status of Subscriber Certificates:

If the CA publishes a CRL, then the CA shall update and reissue CRLs at least once every seven days, and the value of the nextUpdate field must not be more than ten days beyond the value of the thisUpdate field.

For the status of Subordinate CA Certificates:

The CA shall update and reissue CRLs at least (i) once every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field must not be more than twelve months beyond the value of the thisUpdate field.

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9 On-Line Revocation/Status Checking Availability

Trustgate CA supports OCSP responses in addition to CRLs. Response times are generally within reasonable time under normal network operating conditions.

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

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

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

4.9.10 On-Line Revocation Checking Requirements

For the status of Subscriber Certificates, Trustgate CA shall update information provided via an OCSP at least every 4 days. OCSP responses from this service must be a maximum expiration time of 10 days.

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

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

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation

4.9.12 Special Requirements Related to Key Compromise

See Section 4.9.1.

4.9.13 Circumstances for Suspension

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

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

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

4.10.2 Service Availability

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

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

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

4.10.3 Operational Features

No stipulation.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Management, Operational and Physical Controls

The CA shall develop, implement, and maintain a comprehensive security program designed to:

a. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;

b. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;

c. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;

d. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and

e. Comply with all other security requirements applicable to the CA by law.

The Certificate Management Process must include:

a. Physical security and environmental controls such as system integrity controls, including configuration management, integrity maintenance of trusted code, audit logging and malware detection/prevention,

b. Network security and firewall management, including port restrictions and IP address filtering;

c. Personnel Controls such as user management, separate trusted-role assignments, education, awareness, and training; and

d. logical access controls, activity logging, and inactivity time-outs to provide individual accountability,

e. Business continuity including incident and compromise handling and disaster recovery procedures

The CA's security program must include an annual Risk Assessment that:

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

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

c. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Based on the Risk Assessment, the CA shall develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan must include administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan must also take into account then-available technology and the cost of implementing the

specific measures, and shall implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

No stipulation.

5.1.2 Physical Access

No Stipulation.

5.1.3 Power and Air Conditioning

No Stipulation.

5.1.4 Water Exposures

No Stipulation.

5.1.5 Fire Prevention and Protection

No Stipulation.

5.1.6 Media Storage

No Stipulation.

5.1.7 Waste Disposal

No Stipulation.

5.1.8 Off-Site Backup

No Stipulation.

5.2 Procedural Controls

5.2.1 Trusted Roles

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

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

Trusted roles include but are not limited to the following:

- Customer Service/Vetting Personnel,
- CA operations personnel,
- Information Security personnel,

- System Administration/Engineer personnel,
- Developer personnel,
- Internal Auditor,
- Infrastructure personnel, and
- RA administrator

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

5.2.2 Number of Persons Required per Task

Trustgate CA Private Key shall be backed up, stored and recovered only by personnel in Trusted roles using dual control in a physically secured environment.

5.2.3 Identification and Authentication for Each Role

No Stipulation.

5.2.4 Roles Requiring Separation of Duties

No Stipulation.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience and Clearance Requirements

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor of the CA, the CA SHALL verify the identity and trustworthiness of such person.

5.3.2 Background Check Procedures

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

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

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

5.3.3 Training Requirements

The CA shall provide all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements.

The CA shall maintain records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

The CA shall document that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

The CA shall require all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in these Requirements.

5.3.4 Retraining Frequency and Requirements

All personnel in Trusted roles shall maintain skill levels consistent with the CA's training and performance programs.

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanctions for Unauthorised Actions

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

5.3.7 Independent Contractor Requirements

The CA shall verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3.3 and the document retention and event logging requirements of *Section 5.4.1.*

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

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

Trustgate CA shall record at least the following events:

1. CA key lifecycle management events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction; and
    b. Cryptographic device lifecycle management events.
2. CA and Subscriber Certificate lifecycle management events, including:
    a. Certificate requests, renewal, and re-key requests, and revocation;
    b. All verification activities stipulated in these Requirements and the CA's CPS;
    c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    d. Acceptance and rejection of certificate requests;
    e. Issuance of Certificates; and
    f. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
    a. Successful and unsuccessful PKI system access attempts;
    b. PKI and security system actions performed;
    c. Security profile changes;
    d. System crashes, hardware failures, and other anomalies;
    e. Firewall and router activities; and
    f. Entries to and exits from the CA facility.

Log entries MUST include the following elements:

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

5.4.2 Frequency of Processing Log

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

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.

5.4.4 Protection of Audit Log

Events are logged with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, tampering or destroyed. The audit log files

are protected to ensure that only individuals with authorised trusted access are able to perform any operations without modifying integrity, authenticity and confidentiality of the data.

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (Internal vs. External)

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

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

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

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

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

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

5.5 Records Archival

5.5.1 Types of Records Archived

No Stipulation.

5.5.2 Retention Period for Archive

The CA SHALL retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid.

5.5.3 Protection of Archive

No Stipulation.

5.5.4 Archive Backup Procedures

No Stipulation.

5.5.5 Requirements for Timestamping of Records

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

5.5.6 Archive Collection System (Internal or External)

The archive collection system shall comply with the requirements in Section 5.

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.6 Key Changeover

No Stipulation.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

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

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

The business continuity plan includes:

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

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

In the event of the corruption of computing resources, software, and/or data, Trustgate CA's incident response handling procedures shall be enacted.

5.7.3 Recovery Procedure After Key Compromise

In the event a Trustgate CA Private Key is Compromised, Trustgate CA shall revoke the CA Certificate and communicate to all the Subscribers who have been issued a Certificate on the revoke status at the earliest feasible time.

5.7.4 Business Continuity Capabilities After a Disaster

Trustgate CA shall create and maintain business continuity plan so that in the event of a disruption, critical business functions will be resumed.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

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

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

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

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

In all cases, the CA shall:

1. generate the keys in a physically secured environment as described in the CA's CP and/or CPS;
2. generate the CA keys using personnel in trusted roles under the principles of multiple person control and split knowledge;
3. generate the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's CP and/or CPS;
4. log its CA key generation activities; and

5. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its CP and/or CPS and (if applicable) its Key Generation Script.

6.1.1.2 RA Key Pair Generation

No Stipulation

6.1.1.3 Subscriber Key Pair Generation

The CA shall reject a certificate request if the requested Public Key does not meet the requirements set forth in *Sections 6.1.5* and *Section 6.1.6* or if it has a known weak Private Key.

6.1.2 Private Key Delivery to Subscriber

Parties other than the Subscriber shall not archive the Subscriber Private Key.

If the CA or any of its designated RAs generated the Private Key on behalf of the Subscriber, then the CA shall encrypt the Private Key for transport to the Subscriber.

If the CA or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then the CA shall revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

Trustgate CA shall ensure that Public Key delivery to Relying Parties is undertaken in such a way as to prevent substitution attacks.

6.1.5 Key Sizes

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

6.1.5.1 RSA

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

6.1.5.2 ECC

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

6.1.6 Public Key Parameters Generation and Quality Checking

For RSA, the CA shall confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent should be in the range between 2^{16} + 1 and 2^{256} – 1. The modulus should also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752.

For DSA, although FIPS 800-57 says that domain parameters may be made available at some accessible site, compliant DSA certificates must include all domain parameters. This is to insure maximum interoperability among relying party software. The CA must confirm that the value of the public key has the unique correct representation and range in the field, and that the key has the correct order in the subgroup.

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

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

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

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates, and OCSP Response verification Certificates); and
4. Certificates issued solely for the purpose of testing products with Certificates issued by a Root CA.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

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

6.2.1 Cryptographic Module Standards and Controls

No Stipulation.

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

No Stipulation.

6.2.3 Private Key Escrow

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

6.2.4 Private Key Backup

See Section 5.2.2.

6.2.5 Private Key Archival

Parties other than the Subordinate CA shall not archive the Subordinate CA Private Keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

If the Issuing CA generated the Private Key on behalf of the Subordinate CA, then the Issuing CA shall encrypt the Private Key for transport to the Subordinate CA. If the Issuing CA becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then the Issuing CA shall revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.2.7 Private Key Storage on Cryptographic Module

The CA shall protect its Private Key in a system or device that has been validated as meeting at least FIPS 140 level 3 or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats.

6.2.8 Activating Private Key

Trustgate CA shall 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 Deactivating Private Key

No Stipulation.

6.2.10 Destroying Private Key

No Stipulation.

6.2.11 Cryptographic Module Capabilities

6.2.12 No Stipulation. Cryptographic Module Capabilities

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Trustgate CA archives Public Keys from Certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

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

5	AATL Certificates		No stipulation		825 days (27 months)
6	Timestamping Certificates		11 years		133 months

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

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

6.4.2 Activation Data Protection

No stipulation.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

6.5.2 Computer Security Rating

No stipulation.

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

No Stipulation.

6.6.2 Security Management Controls

No Stipulation.

6.6.3 Lifecycle Security Controls

No stipulation.

6.7 Network Security Controls

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

6.8 Time Stamping

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

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The CA shall meet the technical requirements set forth in *Section 2.2* – Publication of Information, *Section 6.1.5* – Key Sizes, and *Section 6.1.6* – Public Key Parameters Generation and Quality Checking.

The CA shall generate non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

7.1.1 Version Number(s)

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

7.1.2 Certificate Content and Extensions; Application of RFC 5280

Trustgate CA shall issue Certificates in compliance with RFC 5280 and applicable best practice.

7.1.2.1 Root CA Certificate

a. basicConstraints

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

b. keyUsage

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

c. certifcatePolicies

   This extension must not be present.

d. extendedKeyUsage

   This extension must not be present.

7.1.2.2 Subordinate CA Certificate

a. CertificatePolicies

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

   certificatePolicies:policyIdentifier (Required)

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

   certificatePolicies:policyQualifiers:policyQualifierId (Optional)

- id-qt 1 [RFC 5280].

certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

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

b. cRLDistributionPoints

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

c. authorityInformationAccess

With the exception of stapling, which is noted below, this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It SHOULD also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

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

d. basicConstraints

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

e. keyUsage

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

f. nameConstraints (optional)

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

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

g. extkeyUsage (optional)

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

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

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

7.1.2.3 Subscriber Certificate

a. certificatePolicies

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

certificatePolicies:policyIdentifier (Required)

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

The following extensions MAY be present:

certificatePolicies:policyQualifiers:policyQualifierId (Recommended)

- id-qt 1 [RFC 5280].

certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

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

b. cRLDistributionPoints

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

c. authorityInformationAccess

With the exception of stapling, which is noted below, this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It SHOULD also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

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

d. basicConstraints (optional)

The cA field MUST NOT be true.

e. keyUsage (optional)

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

f. extKeyUsage (required)

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

7.1.2.4 All Certificate

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

The CA SHALL NOT issue a Certificate with:

a. Extensions that do not apply in the context of the public Internet (such as an extendedKeyUsage value for a service that is only valid in the context of a privately managed network), unless:

   i. such value falls within an OID arc for which the Applicant demonstrates ownership, or

   ii. the Applicant can otherwise demonstrate the right to assert the data in a public context; or

b. semantics that, if included, will mislead a Relying Party about the certificate information verified by the CA (such as including extendedKeyUsage value for a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

7.1.2.5 Application of RFC 5280

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

7.1.3 Algorithm Object Identifiers

The CA shall not issue Subscriber Certificates utilizing the SHA-1 algorithm. The CA may continue to use their existing SHA-1 Root Certificates. However, SHA-2 Subscriber certificates should not chain up to a SHA-1 Subordinate CA Certificate.

7.1.4 Name Forms

7.1.4.1 Issuer Information

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

7.1.4.2 Subject Information – Subscriber Certificate

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

7.1.4.2.1 Subject Alternative Name Extension

Certificate Field: extensions:subjectAltName

Required/Optional: Required

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

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

7.1.4.2.2 Subject Distinguished Name Fields

Certificate Field: subject:commonName (OID 2.5.4.3)

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

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

Certificate Field: subject:organizationName (OID 2.5.4.10)

Required/Optional: Optional

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

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

Required/Optional: Optional

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

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

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

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

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

Certificate Field: subject:localityName (OID: 2.5.4.7)

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

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

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

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

Certificate Field: subject:stateOrProvinceName (OID: 2.5.4.8)

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

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

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

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

Certificate Field: subject:postalCode (OID: 2.5.4.17)

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

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

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

Certificate Field: subject:countryName (OID: 2.5.4.6)

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

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

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

Certificate Field: subject:organizationalUnitName

Required/Optional: Optional

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

Other Subject Attributes

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

7.1.4.3 Subject Information – Root Certificate and Subordinate CA Certificate

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

7.1.5 Name Constraint

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

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

1. For each dNSName in permittedSubtrees, the CA MUST confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of *Section 3.2.2.4*.
2. For each iPAddress range in permittedSubtrees, the CA MUST confirm that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf. (c) For each DirectoryName in permittedSubtrees the CA MUST confirm the Applicants and/or Subsidiary's Organizational name and location such that end entity certificates issued from the subordinate CA Certificate will be in compliancy with *Section 7.1.2.4* and *7.1.2.5*.

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

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

X509v3 Name Constraints:
Permitted:
DNS:example.com
DirName: C=US, ST=MA, L=Boston, O=Example LLC
Excluded:
IP:0.0.0.0/0.0.0.0
IP:0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0

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

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Reserved Certificate Policy Identifiers

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

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

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

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

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2), if the Certificate complies with these Requirements and includes Subject Identity Information that is verified in accordance with *Section 3.2.2.1*.

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

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

i. either organizationName or givenName and surname,

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

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

7.1.6.2 Root CA Certificates

A Root CA Certificate SHOULD NOT contain the certificatePolicies extension.

7.1.6.3 Subordinate CA Certificates

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

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

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

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

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

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

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

7.1.6.4 Subscriber Certificates

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

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

7.1.7 Usage of Policy Constraints Extension

No Stipulation.

7.1.8 Policy Qualifier Syntax and Semantics

No Stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No Stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

Trustgate CA shall issue X.509 Version 2 CRLs in compliance with RFC 5280.

7.2.2 CRL and CRL entry extensions

No Stipulation.

7.3 OCSP Profile

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

7.3.1 Version Number(s)

No Stipulation.

7.3.2 OCSP extensions

No Stipulation.

8. Compliance Audit and Other Assessments

The CA SHALL at all times:

1. Issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates;
2. Comply with these Requirements;
3. Comply with the audit requirements set forth in this section; and
4. Be licensed as a CA in each jurisdiction where it operates, if licensing is required by the law of such jurisdiction for the issuance of Certificates.

8.1 Frequency and Circumstances of Assessment

Certificates that are capable of being used to issue new certificates MUST either be Technically Constrained in line with *Section 7.1.5* and audited in line with *Section 8.7* only, or Unconstrained and fully audited in line with all remaining requirements from this section. A Certificate is deemed as capable of being used to issue new certificates if it contains an X.509v3 basicConstraints extension, with the cA boolean set to true and is therefore by definition a Root CA Certificate or a Subordinate CA Certificate.

The period during which the CA issues Certificates SHALL be divided into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration.

If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 8.1, then no pre-issuance readiness assessment is necessary.

If the CA does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in *Section 8.1*, then, before issuing Publicly-Trusted Certificates, the CA SHALL successfully complete a point-in-time readiness assessment performed in accordance with applicable

standards under one of the audit schemes listed in *Section 8.1*. The point-in-time readiness assessment SHALL be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.

8.2 Identity/Qualifications of Assessor

The CA's audit SHALL be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.1);
3. 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;
4. For audits conducted in accordance with any one of the ETSI standards - accredited in accordance with ETSI TS 119 403, or accredited to conduct such audits under an equivalent national scheme, or accredited by a national accreditation body in line with ISO 27006 to carry out ISO 27001 audits;
5. For audits conducted in accordance with the WebTrust standard - licensed by WebTrust;
6. Bound by law, government regulation, or professional code of ethics; and
7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

The CA SHALL undergo an audit in accordance with one of the following schemes:

1. WebTrust for Certification Authorities v2.0;
2. A national scheme that audits conformance to ETSI TS 102 042;
3. A scheme that audits conformance to ISO 21188:2006; or
4. If a Government CA is required by its Certificate Policy to use a different internal audit scheme, it MAY use such scheme provided that the audit either (a) encompasses all requirements of one of the above schemes or (b) consists of comparable criteria that are available for public review.

Whichever scheme is chosen, it MUST incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit MUST be conducted by a Qualified Auditor, as specified in Section 8.2.

If a Delegated Third Party is not currently audited in accordance with Section 8 and is not an Enterprise RA, then prior to certificate issuance the CA SHALL ensure that the domain control validation process required under Section 3.2.2.4 or IP address verification under 3.2.2.5 has been properly performed by the Delegated Third Party by either (1) using an out-of-band mechanism involving at least one human who is acting either on behalf of the CA or on behalf of the Delegated Third Party to confirm the authenticity of the certificate request or the information supporting the certificate request or (2) performing the domain control validation process itself.

If the CA is not using one of the above procedures and the Delegated Third Party is not an Enterprise RA, then the CA SHALL obtain an audit report, issued under the auditing standards that underlie the accepted audit schemes found in Section 8.1, that provides an opinion whether the Delegated Third Party's performance complies with either the Delegated Third Party's practice statement or the CA's Certificate Policy and/or Certification Practice Statement. If the opinion is that the Delegated Third Party does not comply, then the CA SHALL not allow the Delegated Third Party to continue performing delegated functions.

The audit period for the Delegated Third Party SHALL NOT exceed one year (ideally aligned with the CA's audit). However, if the CA or Delegated Third Party is under the operation, control, or supervision of a Government Entity and the audit scheme is completed over multiple years, then the annual audit MUST cover at least the core controls that are required to be audited annually by such scheme plus that portion of all non-core controls that are allowed to be conducted less frequently, but in no case may any non-core control be audited less often than once every three years.

8.5 Actions Taken as a Result of Deficiency

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

8.6 Communications of Results

The Audit Report SHALL state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in *Section 7.1.6.1*. The CA SHALL make the Audit Report publicly available. The CA is not required to make publicly available any general audit findings that do not impact the overall audit opinion. For both government and commercial CAs, the CA SHOULD make its Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, and if so requested by an Application Software Supplier, the CA SHALL provide an explanatory letter signed by the Qualified Auditor.

8.7 Self-Audits

During the period in which the CA issues Certificates, the CA SHALL monitor adherence to its CP, CPS and these Requirements and strictly control its service quality by performing self audits on at

least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken. Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in *Section 8.1*, the CA SHALL strictly control the service quality of Certificates issued or containing information verified by a Delegated Third Party by having a Validation Specialist employed by the CA perform ongoing quarterly audits against a randomly selected sample of at least the greater of one certificate or three percent of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last sample was taken. The CA SHALL review each Delegated Third Party's practices and procedures to ensure that the Delegated Third Party is in compliance with these Requirements and the relevant CP and/or CPS.

The CA SHALL internally audit each Delegated Third Party's compliance with these Requirements on an annual basis.

During the period in which a Technically Constrained Subordinate CA issues Certificates, the CA which signed the Subordinate CA SHALL monitor adherence to the CA's Certificate Policy and the Subordinate CA's Certification Practice Statement. On at least a quarterly basis, against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by the Subordinate CA, during the period commencing immediately after the previous audit sample was taken, the CA SHALL ensure all applicable CP are met.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

No Stipulation.

9.1.2 Certificate Access Fees

No Stipulation.

9.1.3 Fees for Other Services

No Stipulation.

9.1.4 Refund Policy

No Stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

No Stipulation.

9.2.2 Other assets

No Stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

No Stipulation.

9.3.2 Information Not Within the Scope of Confidential Information

No Stipulation.

9.3.3 Responsibility to Protect Confidential Information

No Stipulation.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

Trustgate CA shall treat all information received from Applicants as Private except for those information to be placed into a Certificate.

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

No Stipulation.

9.4.5 Notice and Consent to Use Private Information

No Stipulation.

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 shall not knowingly violate the intellectual property rights of third parties.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

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

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

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

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

- **Right to Use Domain Name or IP Address**: That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's Subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's CP and/or CPS;
- **Authorisation for Certificate:** That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Subject authorised the issuance of the Certificate and that the Applicant Representative is authorised to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's CP and/or CPS;
- **Accuracy of Information:** That, at the time of issuance, the CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organisationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's CP and/or CPS;
- **No Misleading Information:** That, at the time of issuance, the CA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organisationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's CP and/or CPS;
- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA (i) implemented a procedure to verify the identity of the Applicant; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's CP and/or CPS;
- **Subscriber Agreement:** That, if the CA and Subscriber are not Affiliates, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the Baseline Requirements, or, if the CA and Subscriber are Affiliates, the Applicant Representative acknowledged and accepted the Terms of Use;
- **Status:** That theCA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
- **Revocation:** That the CA will revoke the Certificate for any of the reasons specified in the Baseline Requirements and/or EV Guidelines.

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

9.6.2 RA Representations and Warranties

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

9.6.3 Subscriber Representations and Warranties

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

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

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

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

1. **Accuracy of Information**: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;
2. **Protection of Private Key**: An obligation and warranty by the Applicant to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
3. **Acceptance of Certificate**: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. **Use of Certificate**: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber or Terms of Use Agreement;
5. **Reporting and Revocation**: An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request the CA to revoke the Certificate, in

the event that: (a) any information in the Certificate is, or becomes, incorrect or inaccu- rate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate;

6. **Termination of Use of Certificate**: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
7. **Responsiveness**: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. **Acknowledgment and Acceptance**: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Agreement or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

9.6.4 Relying Party Representations and Warranties

No Stipulation.

9.6.5 Representations and Warranties of other Participants

No Stipulation.

9.7 Disclaimers of Warranties

No Stipulation.

9.8 Limitations of Liability

For delegated tasks, the CA and any Delegated Third Party MAY allocate liability between themselves contractually as they determine, but the CA SHALL remain fully responsible for the performance of all parties in accordance with these Requirements, as if the tasks had not been delegated.

If the CA has issued and managed the Certificate in compliance with these Requirements and its CP and/or CPS, the CA may disclaim liability to the Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such Certificate beyond those specified in the CA's CPS. If the CA has not issued or managed the Certificate in compliance with applicable requirements and its CPS, the CA may seek to limit its liability to the Subscriber and to Relying Parties, regardless of the cause of action or legal theory involved, for any and all claims, losses or damages suffered as a result of the use or reliance on such Certificate by any appropriate means that the CA desires. If the CA chooses to so limit its liability, then the CA SHALL include the limitations on liability in the its CPS.

9.9 Indemnities

9.9.1 Indemnification by CAs

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Root CA do not assume any obligation or potential liability of the CA

under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, except in the case where the CA is a government entity, the CA SHALL defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.2 Indemnification by Subscribers

No Stipulation.

9.9.3 Indemnification by Relying Parties

No Stipulation.

9.10 Term and Termination

9.10.1 Term

No Stipulation.

9.10.2 Termination

No Stipulation.

9.10.3 Effect of Termination and Survival

No Stipulation.

9.11 Individual Notices and Communications with Participants

No Stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

No Stipulation.

9.12.2 Notification Mechanism and Period

No Stipulation.

9.12.3 Circumstances under which OID must be Changed

No Stipulation.

9.13 Dispute Resolution Provisions

No Stipulation.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

The CA shall comply with applicable laws of Malaysia. Export of certain types of software used in certain the CA public Certificate management products and services may require the approval of appropriate public or private authorities.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No Stipulation.

9.16.2 Assignment

No Stipulation.

9.16.3 Severability

In the event of a conflict between these Requirements and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which a CA operates or issues certificates, a CA MAY modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law. In such event, the CA SHALL immediately (and prior to issuing a certificate under the modified requirement) include in *Section 9.16.3* of the CA's CPS a detailed reference to the Law requiring a modification of these Requirements under this section, and the specific modification to these Requirements implemented by the CA.

The CA MUST also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to these Requirements accordingly.

Any modification to CA practice enabled under this section MUST be discontinued if and when the Law no longer applies, or these Requirements are modified to make it possible to Baseline Requirements accordingly.

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

No Stipulation.

9.16.5 Force Majeure

No Stipulation.

9.17 Other Provision

No Stipulation.