MSC Trustgate.com-DigiCert Certification Practices Statement

Version 4.0.0

1 April 2020

MSC Trustgate.com Sdn. Bhd. (199901003331)
Suite 2-9, Level 2, Block 4801 CBD Perdana
Jalan Perdana, 63000 Cyberjaya
Selangor Darul Ehsan, Malaysia
Tel: +603 8318 1800
www.msctrustgate.com

MSC Trustgate.com-DigiCert Certification Practices Statement

Published date: **1st April 2020**

Important – Acquisition Notice

On October 31, 2017, DigiCert, Inc. completed the acquisition of Symantec Corporation's Website Security business unit. As a result, DigiCert is now the registered owner of this Certificate Policy document and the PKI Services described within this document.

However, a hybrid of references to "VeriSign," "Symantec," and "DigiCert" shall be evident within this document for a period of time until it is operationally practical to complete the re-branding of the Certification Authorities and services. Any references to VeriSign or Symantec as a corporate entity should be strictly considered to be legacy language that solely reflects the history of ownership.

Trademark Notices

MSC Trustgate.com Sdn. Bhd.
Suite 2-9, Level 2, CBD Perdana
Jalan Perdana, 63000 Cyberjaya
Selangor Darul Ehsan, Malaysia
Attn : Legal Advisor Email : legal@msctrustgate.com
Tel : +603 8318 1800 Fax : +603 8319 1800

Table of Contents

1 INTRODUCTION 1
1.1 OVERVIEW 1
1.2 DOCUMENT NAME AND IDENTIFICATION 3
1.3 PKI PARTICIPANTS 5
1.3.1 Certification Authorities 5
1.3.2 Registration Authorities 5
1.3.3 Subscribers 5
1.3.4 Relying Parties 6
1.3.5 Other Participants 6
1.4 CERTIFICATE USAGE 6
1.4.1 Appropriate Certificate Usages 6
1.4.2 Prohibited Certificate Uses 7
1.5 POLICY ADMINISTRATION 8
1.5.1 Organization Administering the Document 8
1.5.2 Contact Person 8
1.5.3 Person Determining CP Suitability for the Policy 8
1.5.4 CPS Approval Procedure 8
1.6 DEFINITIONS AND ACRONYMS 9
1.6.1 Definitions 9
1.6.2 Acronyms 10
1.6.3 References 10
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 11
2.1 REPOSITORIES 11
2.2 PUBLICATION OF CERTIFICATION INFORMATION 11
2.3 TIME OR FREQUENCY OF PUBLICATION 11
2.4 ACCESS CONTROLS ON REPOSITORIES 11
3 IDENTIFICATION AND AUTHENTICATION 12
3.1 NAMING 12
3.1.1 Types of Names 12
3.1.2 Need for Names to be Meaningful 14
3.1.3 Anonymity or Pseudonymity of Subscribers 14
3.1.4 Rules for Interpreting Various Name Forms 14
3.1.5 Uniqueness of Names 14
3.1.6 Recognition, Authentication, and Role of Trademarks 14
3.2 INITIAL IDENTITY VALIDATION 15
3.2.1 Method to Prove Possession of Private Key 15
3.2.2 Authentication of Organization and Domain/Email Control 15
3.2.3 Authentication of Individual Identity 18
3.2.4 Non-verified Subscriber Information 21
3.2.5 Validation of Authority 22
3.2.6 Criteria for Interoperation 22
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 23

3.3.1 Identification and Authentication for Routine Re-key 23
3.3.2 Identification and Authentication for Re-key After Revocation 23
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 23
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 25
4.1 CERTIFICATE APPLICATION 25
4.1.1 Who Can Submit a Certificate Application? 25
4.1.2 Enrollment Process and Responsibilities 25
4.2 CERTIFICATE APPLICATION PROCESSING 26
4.2.1 Performing Identification and Authentication Functions 26
4.2.2 Approval or Rejection of Certificate Applications 26
4.2.3 Time to Process Certificate Applications 26
4.3 CERTIFICATE ISSUANCE 27
4.3.1 CA Actions during Certificate Issuance 27
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 27
4.4 CERTIFICATE ACCEPTANCE 27
4.4.1 Conduct Constituting Certificate Acceptance 27
4.4.2 Publication of the Certificate by the CA 27
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 27
4.5 KEY PAIR AND CERTIFICATE USAGE 27
4.5.1 Subscriber Private Key and Certificate Usage 27
4.5.2 Relying Party Public Key and Certificate Usage 28
4.6 CERTIFICATE RENEWAL 28
4.6.1 Circumstance for Certificate Renewal 28
4.6.2 Who May Request Renewal 28
4.6.3 Processing Certificate Renewal Requests 29
4.6.4 Notification of New Certificate Issuance to Subscriber 29
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 29
4.6.6 Publication of the Renewal Certificate by the CA 30
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 30
4.7 CERTIFICATE RE-KEY 30
4.7.1 Circumstance for Certificate Rekey 30
4.7.2 Who May Request Certification of a New Public Key? 30
4.7.3 Processing Certificate Rekey Requests 30
4.7.4 Notification of Certificate Rekey to Subscriber 30
4.7.5 Conduct Constituting Acceptance of a Rekeyed Certificate 30
4.7.6 Publication of the Issued Certificate by the CA 30
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 30
4.8 CERTIFICATE MODIFICATION 31
4.8.1 Circumstances for Certificate Modification 31
4.8.2 Who May Request Certificate Modification 31
4.8.3 Processing Certificate Modification Requests 31
4.8.4 Notification of Certificate Modification to Subscriber 31
4.8.5 Conduct Constituting Acceptance of Modified Certificate 31
4.8.6 Publication of the Modified Certificate by the CA 31
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 31

4.9 CERTIFICATE REVOCATION AND SUSPENSION 32
4.9.1 Circumstances for Revocation 32
4.9.2 Who Can Request Revocation 34
4.9.3 Procedure for Revocation Request 34
4.9.4 Revocation Request Grace Period 34
4.9.5 Time within which CA Must Process the Revocation Request 35
4.9.6 Revocation Checking Requirement for Relying Parties 35
4.9.7 CRL Issuance Frequency 35
4.9.8 Maximum Latency for CRLs 36
4.9.9 On-line Revocation/Status Checking Availability 36
4.9.10 On-line Revocation Checking Requirements 36
4.9.11 Other Forms of Revocation Advertisements Available 36
4.9.12 Special Requirements Related to Key Compromise 36
4.9.13 Circumstances for Suspension 36
4.9.14 Who Can Request Suspension 36
4.9.15 Procedure for Suspension Request 36
4.9.16 Limits on Suspension Period 36
4.10 CERTIFICATE STATUS SERVICES 37
4.10.1 Operational Characteristics 37
4.10.2 Service Availability 37
4.10.3 Optional Features 37
4.11 END OF SUBSCRIPTION 37
4.12 KEY ESCROW AND RECOVERY 38
4.12.1 Key Escrow and Recovery Policy Practices 38
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 38
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 39
5.1 PHYSICAL CONTROLS 39
5.1.1 Site Location and Construction 39
5.1.2 Physical Access 39
5.1.3 Power and Air Conditioning 40
5.1.4 Water Exposures 40
5.1.5 Fire Prevention and Protection 40
5.1.6 Media Storage 40
5.1.7 Waste Disposal 40
5.1.8 Off-site Backup 40
5.1.9 Certificate Status Hosting, CMS and External RA Systems 41
5.2 PROCEDURAL CONTROLS 42
5.2.1 Trusted Roles 42
5.2.2 Number of Persons Required per Task 42
5.2.3 Identification and Authentication for each Role 43
5.2.4 Roles Requiring Separation of Duties 43
5.3 PERSONNEL CONTROLS 44
5.3.1 Qualifications, Experience, and Clearance Requirements 44
5.3.2 Background Check Procedures 44
5.3.3 Training Requirements 45
5.3.4 Retraining Frequency and Requirements 45

5.3.5 Job Rotation Frequency and Sequence 45
5.3.6 Sanctions for Unauthorized Actions 46
5.3.7 Independent Contractor Requirements 46
5.3.8 Documentation Supplied to Personnel 46
5.4 AUDIT LOGGING PROCEDURES 47
5.4.1 Types of Events Recorded 47
5.4.2 Frequency of Processing Log 47
5.4.3 Retention Period for Audit Log 48
5.4.4 Protection of Audit Log 48
5.4.5 Audit Log Backup Procedures 48
5.4.6 Audit Collection System (internal vs. external) 48
5.4.7 Notification to Event-causing Subject 48
5.4.8 Vulnerability Assessments 48
5.5 RECORDS ARCHIVAL 49
5.5.1 Types of Records Archived 49
5.5.2 Retention Period for Archive 49
5.5.3 Protection of Archive 50
5.5.4 Archive Backup Procedures 50
5.5.5 Requirements for Time-stamping of Records 50
5.5.6 Archive Collection System (internal or external) 50
5.5.7 Procedures to Obtain and Verify Archive Information 50
5.6 KEY CHANGEOVER 51
5.7 COMPROMISE AND DISASTER RECOVERY 51
5.7.1 Incident and Compromise Handling Procedures 51
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 51
5.7.3 Entity Private Key Compromise Procedures 51
5.7.4 Business Continuity Capabilities after a Disaster 52
5.8 CA OR RA TERMINATION 52
6 TECHNICAL SECURITY CONTROLS 53
6.1 KEY PAIR GENERATION AND INSTALLATION 53
6.1.1 Key Pair Generation 53
6.1.2 Private Key Delivery to Subscriber 53
6.1.3 Public Key Delivery to Certificate Issuer 54
6.1.4 CA Public Key Delivery to Relying Parties 54
6.1.5 Key Sizes 54
6.1.6 Key Usage Purposes (as per X.509 v3 key usage field) 55
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 56
6.2.1 Cryptographic Module Standards and Controls 56
6.2.2 Private Key (n out of m) Multi-person Control 56
6.2.3 Private Key Escrow 56
6.2.4 Private Key Backup 56
6.2.5 Private Key Archival 57
6.2.6 Private Key Transfer into or from a Cryptographic Module 57
6.2.7 Private Key Storage on Cryptographic Module 57
6.2.8 Method of Activating Private Keys 57
6.2.9 Method of Deactivating Private Keys 57

6.2.10 Method of Destroying Private Keys 58
6.2.11 Cryptographic Module Rating 58
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 58
6.3.1 Public Key Archival 58
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 58
6.4 ACTIVATION DATA 59
6.4.1 Activation Data Generation and Installation 59
6.4.2 Activation Data Protection 59
6.4.3 Other Aspects of Activation Data 59
6.5 COMPUTER SECURITY CONTROLS 60
6.5.1 Specific Computer Security Technical Requirements 60
6.5.2 Computer Security Rating 60
6.6 LIFE CYCLE TECHNICAL CONTROLS 61
6.6.1 System Development Controls 61
6.6.2 Security Management Controls 61
6.6.3 Life Cycle Security Controls 61
6.7 NETWORK SECURITY CONTROLS 61
6.8 TIME-STAMPING 62
7 CERTIFICATE, CRL, AND OCSP PROFILES 63
7.1 CERTIFICATE PROFILE 64
7.1.1 Version Number(s) 64
7.1.2 Certificate Extensions 64
7.1.3 Algorithm Object Identifiers 66
7.1.4 Name Forms 67
7.1.5 Name Constraints 67
7.1.6 Certificate Policy Object Identifier 67
7.1.7 Usage of Policy Constraints Extension 67
7.1.8 Policy Qualifiers Syntax and Semantics 67
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 67
7.2 CRL PROFILE 68
7.2.1 Version number(s) 68
7.2.2 CRL and CRL Entry Extensions 68
7.3 OCSP PROFILE 68
7.3.1 Version Number(s) 68
7.3.2 OCSP Extensions 68
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 69
8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 69
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 69
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 69
8.4 TOPICS COVERED BY ASSESSMENT 69
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 69
8.6 COMMUNICATION OF RESULTS 70
8.7 SELF-AUDITS 70

9 OTHER BUSINESS AND LEGAL MATTERS 71
9.1 FEES 71
9.1.1 Certificate Issuance or Renewal Fees 71
9.1.2 Certificate Access Fees 71
9.1.3 Revocation or Status Information Access Fees 71
9.1.4 Fees for Other Services 71
9.1.5 Refund Policy 71
9.2 FINANCIAL RESPONSIBILITY 72
9.2.1 Insurance Coverage 72
9.2.2 Other Assets 72
9.2.3 Insurance or Warranty Coverage for End-Entities 72
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 72
9.3.1 Scope of Confidential Information 72
9.3.2 Information Not Within the Scope of Confidential Information 72
9.3.3 Responsibility to Protect Confidential Information 72
9.4 PRIVACY OF PERSONAL INFORMATION 73
9.4.1 Privacy Plan 73
9.4.2 Information Treated as Private 73
9.4.3 Information Not Deemed Private 73
9.4.4 Responsibility to Protect Private Information 73
9.4.5 Notice and Consent to Use Private Information 73
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 73
9.4.7 Other Information Disclosure Circumstances 73
9.5 INTELLECTUAL PROPERTY RIGHTS 74
9.5.1 Property Rights in Certificates and Revocation Information 74
9.5.2 Property Rights in the CPS 74
9.5.3 Property Rights in Names 74
9.5.4 Property Rights in Keys and Key Material 74
9.5.5 Violation of Property Rights 74
9.6 REPRESENTATIONS AND WARRANTIES 75
9.6.1 CA Representations and Warranties 75
9.6.2 RA Representations and Warranties 75
9.6.3 Subscriber Representations and Warranties 75
9.6.4 Relying Party Representations and Warranties 76
9.6.5 Representations and Warranties of Other Participants 76
9.7 DISCLAIMERS OF WARRANTIES 76
9.8 LIMITATIONS OF LIABILITY 76
9.9 INDEMNITIES 77
9.9.1 Indemnification by MSC Trustgate.com 77
9.9.2 Indemnification by Subscribers 77
9.9.3 Indemnification by Relying Parties 77
9.10 TERM AND TERMINATION 78
9.10.1 Term 78
9.10.2 Termination 78
9.10.3 Effect of Termination and Survival 78

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 78
9.12 AMENDMENTS 78
9.12.1 Procedure for Amendment 78
9.12.2 Notification Mechanism and Period 79
9.12.3 Circumstances under which OID Must Be Changed 79
9.13 DISPUTE RESOLUTION PROVISIONS 79
9.13.1 Disputes among DigiCert, Affiliates, and Customers 79
9.13.2 Disputes with End-User Subscribers or Relying Parties 79
9.14 GOVERNING LAW 80
9.15 COMPLIANCE WITH APPLICABLE LAW 80
9.16 MISCELLANEOUS PROVISIONS 80
9.16.1 Entire Agreement 80
9.16.2 Assignment 80
9.16.3 Severability 80
9.16.4 Enforcement (attorneys' fees and waiver of rights) 80
9.16.5 Force Majeure 80
9.17 OTHER PROVISIONS 80

1 INTRODUCTION

1.1 OVERVIEW

This document is the MSC Trustgate.com-DigiCert Certification Practices Statement (CPS) that outlines the principles and practices related to MSC Trustgate.com's certification services operate under DigiCert PKI Platform (previously known as Symantec Trust Network (STN) and VeriSign Trust Network (VTN)).

MSC Trustgate.com is an affiliate of DigiCert, having own PKI system to issue digital certificate. This means MSC Trustgate.com has established a secure facility housing, among other things, CA systems, including the cryptographic modules holding the private keys used for the issuance of Certificates. MSC Trustgate.com acts as a subordinate CA in the DigiCert PKI and performs all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates.

This CPS is specifically applicable to:

- Digicert's Public Primary Certification Authorities (PCAs),
- MSC Trustgate.com Infrastructure CAs, and MSC Trustgate.com Administrative CAs supporting the DigiCert PKI Platform
- MSC Trustgate.com's Public CAs who issue Certificates within MSC Trustgate.com's sub-domain of the DigiCert PKI

More generally, the CPS also governs the use of DigiCert PKI services within MSC Trustgate.com's Sub-domain of the DigiCert PKI by all individuals and entities within MSC Trustgate.com's Sub-domain (collectively, MSC Trustgate.com Sub-domain Participants"). Private CAs and hierarchies managed by MSC Trustgate.com are outside the scope of this CPS.

The DigiCert PKI includes four levels of Certificates, Level 1-4. The CP is a single document that defines these certificate policies, one for each of the Level, and sets DigiCert PKI Standards for each Level.

MSC Trustgate.com offers three Level of Certificates within its Sub-domain of the DigiCert PKI and refer it to as Class 1-3. This CPS describes how MSC Trustgate.com meets the CP requirements for each Class within its Sub-domain. Thus, the CPS, as a single document, covers practices and procedures concerning the issuance and management of all three Certificate Classes.

MSC Trustgate.com may publish Certificate Practices Statements that are supplemental to this CPS in order comply with the specific policy requirements of Government, or other industry standards and requirements.

These supplemental certificate policies shall be made available to subscribers for the certificates issued under the supplemental policies and their relying parties.

This CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction. To preserve the outline specified by RFC 3647, section headings that do not apply are accompanied with the statement "Not applicable" or "No stipulation".

This CPS describes the practices used to comply with the current versions of the following law, policies, guidelines, and requirements:

Name of Law / Policy / Guideline / Requirement Standard	Location of Source Document
Malaysia Digital Signature Act 1997	http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20562.pdf
Malaysia Digital Signature Regulation 1998	https://www.mcmc.gov.my/en/legal/acts/digital-signature-act-1997-reprint-2002/digital-signature-regulations-1998
WebTrust for CA Principle and Criteria	https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria
DigiCert Certificate Policy version 5.0	https://www.digicert.com/legal-repository/
Certification Authority / Browser Forum ("CAB Forum") Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements")	https://cabforum.org/baseline-requirements-document/
CAB Forum Network and Certificate System Security Requirements	https://cabforum.org/network-security-requirements/
Microsoft Trusted Root Store (Program Requirements)	https://docs.microsoft.com/en-us/security/trusted-root/program-requirements
Mozilla Root Store Policy	https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/
Mozilla CA/Forbidden or Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices
Apple Root Store Program	https://www.apple.com/certificateauthority/ca_program.html
Chromium Project Root Store Certificate Policy	https://www.chromium.org/Home/chromium-security/root-ca-policy

If any inconsistency exists between this CPS and the normative provisions of the foregoing policies, guidelines, and requirements ("Applicable Requirements"), then the Applicable Requirements take precedence over this CPS.

The CPS is only one of a set of documents relevant to MSC Trustgate.com's Sub-domain of the DigiCert PKI. Other important documents include both private and public documents, such as the CP, MSC Trustgate.com's agreements with its customers, Relying Party agreements, and MSC Trustgate.com's privacy policy. MSC Trustgate.com may provide additional certificate policies or certification practice statements. These supplemental policies and statements are available to applicable users or relying parties.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the MSC Trustgate.com-DigiCert Certification Practices Statement and was first approved for publication on 1st April 2020 by MSC Trustgate.com Policy Management Authority (PMA) and endorsed by DigiCert Policy Authority (DCPA). The following revisions have been made to the original document:

Date	Changes	Version
1st April 2020	This version 4.0.0 replaces the MSC Trustgate.com-DigiCert Certification Practices Statement, Version 3.9.0 dated 30 January 2019	4.0.0

The OID for MSC Trustgate.com is iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) MSC Trustgate.com Sdn. Bhd. (49530). The OID-arc for this version 4 of the CPS is 1.3.6.14.1.49530.1.2.4. Subsequent revisions to this CPS might have new OID assignments.

MSC Trustgate.com issues Certificates under DigiCert PKI containing the following OIDs:

Digitally Signed Object	Object Identifier (OID)
Class 1 Certificates	2.16.840.1.113733.1.7.23.1
Class 2 Certificates	2.16.840.1.113733.1.7.23.2
Class 3 Certificates	2.16.840.1.113733.1.7.23.3

All OIDs mentioned above belong to their respective owners. The specific OIDs used when objects are signed pursuant to this CPS are indicated in the object's respective Certificate Policies extension. For instance, when MSC Trustgate.com issues a Certificate containing one of the above-specified policy identifiers it asserts that the Certificate was issued and is managed in accordance with those applicable requirements and policies for the PKI participant.

The MSC Trustgate.com CA certificates governed by this CPS are:

Subject CN	Issuer CN	Serial Number	Validity Period
MSC Trustgate.com Class 2 CA - G2	VeriSign Class 2 Public Primary Certification Authority - G2	54f4e89c500793c7246ecd56eeb2194b	Sep 29 00:00:00 2011 GMT Sep 28 23:59:59 2021 GMT
Bank Negara Malaysia Class 2 CA - G2	MSC Trustgate.com Class 2 CA - G2	74bc0e0674f43469ddae0e3d6befa0ab	Sep 29 00:00:00 2011 GMT Sep 27 23:59:59 2021 GMT
MSC Trustgate.com Class 1 Consumer Individual Subscriber CA-G3	Symantec Class 1 Public Primary Certification Authority - G6	1b19a3cb8fdf464c7e673bbb397b68f6f7f5ec34	Apr 4 00:00:00 2017 GMT Apr 3 23:59:59 2022 GMT
MSC Trustgate.com Class 2 Consumer Individual Subscriber CA-G3	Symantec Class 2 Public Primary Certification Authority - G6	504ff8221f2065377dbd664042ce0b99	Apr 4 00:00:00 2017 GMT Apr 3 23:59:59 2022 GMT

Subject CN	Issuer CN	Serial Number	Validity Period
MSC Trustgate.com Class 2 MPKI Individual Subscriber CA-G3	Symantec Class 2 Public Primary Certification Authority - G6	2657d43610d3472f6f908dcb6219d412	Mar 23 00:00:00 2017 GMT Mar 22 23:59:59 2022 GMT
MSC Trustgate.com Class 2 CA-G3	Symantec Class 2 Public Primary Certification Authority - G6	35629fa5234394d5d2120c9f8f7c25e5	Apr 4 00:00:00 2017 GMT Apr 3 23:59:59 2027 GMT
MyTrust ID Public Basic CA	MSC Trustgate.com Class 2 CA-G3	6c2f088d169db78d2d97e4cdaa37ac40	Apr 4 00:00:00 2017 GMT Apr 3 23:59:59 2022 GMT
MyTrust ID Public CA	MSC Trustgate.com Class 2 CA-G3	79829bd93d502cb61746f97483d7e4cc	Apr 4 00:00:00 2017 GMT Apr 3 23:59:59 2022 GMT
MSC Trustgate.com Class 3 Private MPKI Enterprise Admin CA	Symantec Class 3 Internal Root CA	2eac26cf04c8941a2218561f25380251	May 23 00:00:00 2013 GMT May 22 23:59:59 2023 GMT
MSC Trustgate.com Class 3 Private MPKI Operational Admin CA	Symantec Class 3 Internal Root CA	1a7597984c8e7872059e3d2977b1e508	May 23 00:00:00 2013 GMT May 22 23:59:59 2023 GMT

1.3 PKI PARTICIPANTS

1.3.1 Certification Authorities

MSC Trustgate.com are external subordinate CAs of DigiCert PKI that issue digital certificates using its own PKI. As the operator of several CAs, MSC Trustgate.com performs its functions associated with Public Key operations, including receiving certificate requests, issuing, revoking and renewing a digital Certificate, and maintaining, issuing, and publishing CRLs and OCSP responses. General information about MSC Trustgate.com's products and services are available at www.msctrustgate.com.

Certificates issued under MSC Trustgate.com Issuer CAs crossed sign with DigiCert owned Public Root Cas, MSC Trustgate.com maintains and has physical control of its Private Key associated with these CA Certificates. All MSC Trustgate.com Issuer CAs under DigiCert PKI are prohibited from issuing Certificates to SSL/TLS Server Certificates.

1.3.2 Registration Authorities

A Registration Authority is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewal or re-keying certificates on behalf of MSC Trustgate.com CA. MSC Trustgate.com may act as an RA for certificates it issues (MSC Trustgate.com does not issue TLS or Code Signing certificate under DigiCert PKI).

Third parties, who enter into a contractual agreement relationship with MSC Trustgate.com, may operate as RAs and authorize the issuance of certificates by MSC Trustgate.com CA. Third party RAs must abide by all the requirements of the DigiCert PKI CP, the MSC Trustgate.com CPS and the terms of their enterprise services agreement with MSC Trustgate.com. RAs may, however implement more restrictive practices based on their internal requirements[1].

1.3.3 Subscribers

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

In some cases certificates are issued directly to individuals or entities for their own use. However, there commonly exist other 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 MSC Trustgate.com for the issuance of credentials and; "Subject", is the person to whom the credential is bound. The Subscriber bears ultimate responsibility for the usage 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] An example of a third party RA is a customer of Managed PKI services customer

CAs are technically also subscribers of certificates within the DigiCert PKI, either as a PCA issuing a self-signed Certificate to itself, or as a CA issued a Certificate by a superior CA. References to "end entities" and "subscribers" in this CPS, however, apply only to end-user Subscribers.

1.3.4 Relying Parties

Relying Parties are entities that act in reliance on a Certificate and/or digital signature issued by MSC Trustgate.com. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate. The location of the CRL distribution point is detailed within the Certificate. A Relying party may, or may not also be a Subscriber within the DigiCert PKI.

1.3.5 Other Participants

Not applicable.

1.4 CERTIFICATE USAGE

A digital Certificate (or Certificate) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital Certificate that allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital Certificates are used in commercial environments as a digital equivalent of an identification card.

1.4.1 Appropriate Certificate Usages

Certificates issued pursuant to this CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the Certificate. However, the sensitivity of the information processed or protected by a Certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a Certificate issued under this CPS.

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

Certificate Class	Assurance Level			Usage		
	Low	Medium	High	Signing	Encryption	Client Authentication
Class 1 Certificates	√			√	√	
Class 2 Certificates		√		√	√	√
Class 3 Certificates			√	√	√	√

Table 1 - Individual Certificate Usage

Organizational Certificates are issued to organizations after the process of authentication that the Organization legally exists and that the other Organization attributes included in the certificate (excluding the non- verified subscriber information) are also authenticated e.g. ownership of an Internet or e-mail domain. It is not the intention of this CPS to limit the types of usages for Organizational Certificates. While an organizational certificate may be used for other purposes as well, provided that the Relying Party is able to reasonably rely on that certificate and

the usage is not otherwise prohibited by law, by the DigiCert CP, by any CPS (including this one) under which the certificate has been issued and any agreements with Subscribers.

Certificate Class	Assurance Level			Usage		
	Low	Medium	High	Signing	Encryption	Authentication
Class 2 Certificates[2]		√		√	√	√
Class 3 Certificates			√	√	√	√

Table 2 - Organizational Certificate Usage

1.4.1.1 Assurance Levels

Low assurance certificates are certificates that should not be used for authentication purposes or to support Non-repudiation. The digital signature provides modest assurances that the e-mail originated from a sender with a certain e-mail address. The Certificate, however, provides no proof of the identity of the Subscriber. The encryption application enables a Relying Party to use the Subscriber's Certificate to encrypt messages to the Subscriber, although the sending Relying Party cannot be sure that the recipient is in fact the person named in the Certificate.

Medium assurance certificates are certificates that are suitable for securing some inter- and intra-organizational, commercial, and personal e-mail requiring a medium level of assurances of the Subscriber identity.

High assurance Certificates are individual and organizational Certificates that provide a high level or class of assurance of the identity of the Subscriber in comparison with lower assurance level or class certificates.

1.4.2 Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, safe to do business with, or compliant with any laws. A Certificate only establishes that the information in the Certificate was verified in accordance with this CPS when the Certificate issued.

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.

CA Certificates subject to the Mozilla Root Store Policy will not be used for any functions except CA functions. In addition, end-user Subscriber Certificates cannot not be used as CA Certificates.

Digicert and MSC Trustgate.com periodically rekey Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been rekeyed. MSC Trustgate.com therefore does not warrant the use of Intermediate CAs as root certificates and recommends that Intermediate CAs not be embedded into applications and/or platforms as root certificates. MSC Trustgate.com recommends the use of PCA Roots as root certificates.

[2] "In limited circumstances Class 2 certificates may be issued by a Managed MPKI customer to an affiliated organization (and not an individual within the organization). Such certificate may be used for organization authentication and application signing only. Except as expressly authorized by MSC Trustgate.com through an Enterprise Service Agreement imposing authentication and practice requirements consistent with the security standards of this CPS, Subscribers are prohibited from using this certificate for code and content signing, SSL encryption and S/MIME signing and such key usage will be disabled for these certificates."

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

MSC Trustgate.com Policy Management Authority.
Suite 2-9, Level 2, CBD Perdana
Jalan Perdana, 63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia.
Tel: +603 8318 1800
Fax: +603 8319 1800
Email: legal@msctrustgate.com

1.5.2 Contact Person

Attn: Legal Advisor
MSC Trustgate.com Policy Management Authority.
Suite 2-9, Level 2, CBD Perdana
Jalan Perdana, 63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia.
Tel: +603 8318 1800
Fax: +603 8319 1800
Email: legal@msctrustgate.com

1.5.2.1 Revocation Reporting Contact Person

Attn: MPKI Support
MSC Trustgate.com MPKI Support
Suite 2-9, Level 2, CBD Perdana
Jalan Perdana, 63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia.
Tel: +603 8318 1800
Fax: +603 8319 1800
Email: revoke@msctrustgate.com

1.5.3 Person Determining CP Suitability for the Policy

The organization identified in Section 1.5.2 is responsible for determining whether this CPS and other documents in the nature of certification practice statements that supplement or are subordinate to this CPS are suitable under the CP and this CPS.

1.5.4 CPS Approval Procedure

The PMA approves the CPS and any amendments. Amendments are made after the PMA has reviewed the amendments' consistency with the CP, by either updating the entire CPS or by publishing an addendum. The PMA determines whether an amendment to this CPS is consistent with the CP, requires notice, or an OID change. See also Section 9.10 and Section 9.12 below.

Amended versions or updates is publicly available at MSC Trustgate.com Repository located at: https://www.msctrustgate.com/repository.htm. Updates supersede any designated or conflicting provisions of the referenced to the previous version of the CPS.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

"**Applicant**" means an entity applying for a Certificate.

"**Application Software Vendor**" means a software developer whose software displays or uses DigiCert Certificates and distributes DigiCert's root Certificates.

"**CAB Forum**" is defined in section 1.1.

"**Certificate**" means an electronic document that uses a digital signature to bind a Public Key and an identity.

"**Key Pair**" means a Private Key and associated Public Key.

"**OCSP Responder**" means an online software application operated under the authority of DigiCert and connected to its repository for processing certificate status requests.

"**Private Key**" means 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**" means 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.

"**Qualified Certificate**" means a Certificate that meets the requirements of EU law and is provided by an Issuer CA meeting the requirements of EU law.

"**Relying Party**" means an entity that relies upon either the information contained within a Certificate or a time-stamp token.

"**Relying Party Agreement**" means an agreement which must be read and accepted by the Relying Party prior to validating, relying on or using a Certificate or accessing or using DigiCert's Repository. The Relying Party Agreement is available for reference through a DigiCert online repository.

"**Subscriber**" means either the entity identified as the subject in the Certificate or the entity that is receiving DigiCert's time-stamping services.

"**Subscriber's Agreement**" means an agreement that governs the issuance and use of a Certificate that the Applicant must read and accept before receiving a Certificate.

"**WebTrust**" means the current version of CPA Canada's WebTrust Program for Certification Authorities.

1.6.2 Acronyms

CA	Certificate Authority or Certification Authority
CAB	”CA/Browser” as in “CAB Forum”
CMS	Card Management System
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DBA	Doing Business As (also known as “Trading As”)
ETSI	European Telecommunications Standards Institute
EU	European Union
FIPS	(US Government) Federal Information Processing Standard
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IGTF	International Grid Trust Federation
ISSO	Information System Security Officer
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
IV	Individual Validated
LEI	Legal Entity Identifier
MICS	Member-Integrated Credential Service (IGTF)
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number (e.g. a secret access code)
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
RFC	Request for Comments (at IETF.org)
RPS	Registration Practice Statement
SHA	Secure Hashing Algorithm
TSA	Time Stamping Authority
TST	Time-Stamp Token
UTC	Coordinated Universal Time
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

1.6.3 References

If not listed in section 1.1:

- CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (“Baseline Requirements”)
- Mozilla Root Store Policy v.2.7

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

MSC Trustgate.com makes its CA Certificates, revocation data for issued digital Certificates, CPs, CPSs, Relying Party Agreements, and standard Subscriber Agreements available in public repositories. MSC Trustgate.com develops, implements, enforces, and annually updates this CPS to meet the compliance standards of the documents listed in Sections 1.1 and 1.6.3. These updates also describe how the latest version of the Baseline Requirements are implemented. As Baseline Requirements are updated, MSC Trustgate.com reviews the changes to determine their impact on these practices. Each section impacted by the Baseline Requirements will be updated and provided to the PMA for approval and implementation.

MSC Trustgate.com's legal repository for most services is located at https://www.msctrustgate.com/repository.htm

MSC Trustgate.com's CA Certificates and its CRLs and OCSP responses are regularly accessible online with systems described in Section 5 to minimize downtime.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The MSC Trustgate.com certificate services and the repository are accessible through several means of communication:

- On the web: https://www.msctrustgate.com (and via URIs included in the certificates themselves)
- By email to mpki-support@msctrustgate.com
- By mail addressed to: MSC Trustgate.com Sdn Bhd, Suite 2-9, Block 4801, CBD Perdana, 63000 Cyberjaya, Selangor, Malaysia
- By telephone: +603-8318 1800
- By fax: +603-8319 1800

2.3 TIME OR FREQUENCY OF PUBLICATION

CA Certificates are published in a repository as soon as possible after issuance. CRLs for end-user Certificates are issued at least once per day. CRLs for CA Certificates are issued at least annually, and also within eighteen (18) hours if a CA Certificate is revoked. Under special circumstances, MSC Trustgate.com may publish new CRLs prior to the scheduled issuance of the next CRL. (See Section 4.9 for additional details.)

If a Certificate listed in a CRL expires, it may be removed from later issued CRLs after the Certificate's expiration.

New or modified versions of the CP, this CPS, Subscriber Agreements, or Relying Party Warranties are typically published within seven days after their approval.

2.4 ACCESS CONTROLS ON REPOSITORIES

Read-only access to the repository is unrestricted. Logical and physical controls prevent unauthorized write access to repositories.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

Unless where indicated otherwise in the DigiCert CP, this CPS or the content of the digital certificate, names appearing in Certificates issued under DigiCert PKI platform are authenticated.

3.1.1 Types of Names

For S/MIME certs, Certificates are issued with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards except that MSC Trustgate.com CA may issue a Level 1 Certificate with a null subject DN if it includes at least one alternative name form that is marked critical. When DNs are used, common names must respect namespace uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous Certificates, except where stated otherwise under Section 3.1.3.

MSC Trustgate.com CA Certificates contain X.500 Distinguished Names in the Issuer and Subject fields. MSC Trustgate.com CA Distinguished Names consist of the components specified in Table 3 below.

Attribute	Value
Country (C) =	"MY", "US" or not used.
Organization (O) =	"DigiCert, Inc." or MSC Trustgate.com Sdn. Bhd. or <organization name>[3]
Organizational Unit (OU) =	MSC Trustgate.com CA Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: • CA Name • DigiCert PKI Platform • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate • A copyright notice. • Text to describe the type of Certificate.
State or Province (S) =	Not used.
Locality (L) =	Not used.
Common Name (CN) =	This attribute includes the CA Name (if the CA Name is not specified in an OU attribute) or is not used.

Table 3 - Distinguished Name Attributes in CA Certificates

[3] For a CA dedicated to a customer organization, the (o=) component shall be the legal name of the organization

End-user Subscriber Certificates contain an X.500 distinguished name in the Subject name field and consist of the components specified in Table4 below.

Attribute	Value
Country (C) =	"MY" or not used
Organization (O) =	The Organization attribute is used as follows: • "MSC Trustgate.com Sdn. Bhd." for MSC Trustgate.com OCSP Responder and optionally for individual Certificates that do not have an organization affiliation. • Subscriber organizational name for individual Certificates that have an organization affiliation.
Organizational Unit (OU) =	MSC Trustgate.com end-user Subscriber Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: • Subscriber organizational unit (for organizational Certificates and individual Certificates that have an organization affiliation) • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate • A copyright notice • "Authenticated by MSC Trustgate.com" and "Member, DigiCert PKI Platform" in Certificates whose applications were authenticated by Digicert • "Persona Not Validated" for Class 1 Individual Certificates • Text to describe the type of Certificate.
State or Province (S) =	Indicates the Subscriber's State or Province (State is not a required field in certificates issued to individuals).
Locality (L) =	Indicates the Subscriber's Locality (Locality is not a required field in certificates issued to individuals).
Common Name (CN) =	This attribute includes: • The OCSP Responder Name (for OCSP Responder Certificates) • Organization name (for organizational Certificates) • Person's name (for individual Certificates issued to individuals).
E-Mail Address (E) =	E-mail address for Class 1 individual Certificates and generally for MPKI Subscriber Certificates
SERIALNUMBER =	National Identity Number (If the certificate is required to be verified against national identity document)

Table 4 - Distinguished Name Attributes in End User Subscriber Certificates

The Common Name (CN=) component of the Subject distinguished name of end-user Subscriber Certificates is authenticated in the case of Class 2-3 Certificates.

- The authenticated common name value included in the Subject distinguished names of organizational Certificates is the legal name of the organization or unit within the organization.
- The common name value included in the Subject distinguished name of individual Certificates represents the individual's generally accepted personal name.

3.1.2 Need for Names to be Meaningful

MSC Trustgate.com uses distinguished names that identify both the entity (i.e. person, organization, device, or object) that is the subject of the Certificate and the entity that is the issuer of the Certificate. MSC Trustgate.com only allows directory information trees that accurately reflect organization structures.

3.1.3 Anonymity or Pseudonymity of Subscribers

The identity of Class 1 individual Subscribers is not authenticated. Class 1 subscribers may use pseudonyms. Unless when required by 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), Class 2 and 3 Subscribers are not permitted to use pseudonyms (names other than a Subscriber's true personal or organizational name). Each request for anonymity in a certificate will be evaluated on its merits by the PMA and, if allowed the certificate will indicate that identity has been authenticated but is protected.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax.

3.1.5 Uniqueness of Names

The uniqueness of each subject name in a Certificate is enforced as follows:

Certificate	Uniqueness Requirement
Client Certificates	Requiring a unique email address or a unique organization name combined/associated with a unique serial integer
Device Certificates	For device Certificates, an FQDN is included in the appropriate fields. For other Certificates, DigiCert may append a unique ID to a name listed in the Certificate.

The names of Subscribers shall be unique within a subordinate Issuer CA's and Customer's Sub-domain for a specific type of Certificate. Name uniqueness is not violated when multiple certificates are issued to the same entity.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. MSC Trustgate.com, 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.

MSC Trustgate.com is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 INITIAL IDENTITY VALIDATION

MSC Trustgate.com may use any legal means of communication or investigation to ascertain the identity of an organizational or individual Applicant. MSC Trustgate.com 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, another cryptographically equivalent demonstration, or another MSC Trustgate.com-approved and DigiCert-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 Organization and Domain/Email Control

Certificate	Validation
Domain-related Certificates	MSC Trustgate.com validates the Applicant's right to use or control each domain name that will be listed in the Subject Alternative Name field of a Certificate by using at least one of the following procedures from section 3.2.2.4 of the Baseline Requirements: i. This method (BR Section 3.2.2.4.1) is no longer used because it was deprecated as of 1-August-2018; ii. Email, Fax, SMS, or Postal Mail to the Domain Contact by sending a unique Random Value (valid for no more than 30 days from its creation) through email, fax, SMS, or postal mail, to the Domain Contact and receiving confirmation by their use of the Random Value, performed in accordance with BR Section 3.2.2.4.2; iii. (BR Section 3.2.2.4.3) is no longer used because it was deprecated as of 31-May-2019; iv. Constructed Email to Domain Contact establishing the Applicant's control over the FQDN by sending an email created by using 'admin', 'administrator', 'webmaster', 'hostmaster' or 'postmaster' as the local part followed by the ("@") sign, followed by an Authorization Domain name, including a Random Value in the email, and receiving a response using the Random Value, performed in accordance with BR Section 3.2.2.4.4; v. (BR Section 3.2.2.4.5) is no longer used because it was deprecated as of 1-August-2018; vi. An Agreed-Upon Change to the Website by the Applicant placing an agreed-upon Request Token or Random Value in the "/.well-known/pki-validation" directory, performed in accordance with BR Section 3.2.2.4.6; vii. Domain Name Service (DNS) Change by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT, or CAA record for either an Authorization Domain Name or an Authorization Domain Name prefixed with a label that begins with an underscore character, performed in accordance BR Section 3.2.2.4.7; viii. IP Address - by confirming the Applicant's control over the FQDN through control of an IP address returned from a DNS lookup for

Certificate	Validation
	A or AAAA records for the FQDN, performed in accordance with BR Sections 3.2.2.5 and 3.2.2.4.8; ix. (BR Section 3.2.2.4.9) is no longer used because it was deprecated upon publication of v.4.16 of this CPS; x. (BR Section 3.2.2.4.10) is no longer used because it was deprecated upon publication of v.4.16 of this CPS; xi. (BR Section 3.2.2.4.11) is no longer used because it was deprecated as of 5-February-2018; xii. Confirming that the Applicant is the Domain Contact for the Base Domain Name (provided that the CA or RA is also the Domain Name Registrar or an Affiliate of the Registrar), performed in accordance with BR Section 3.2.2.4.12; xiii. Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value will be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set is found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065 performed in accordance with BR Section 3.2.2.4.13; xiv. Confirming the Applicant's control over the FQDN by sending a Random Value via email to the DNS TXT Record Email Contact for the Authorization Domain Name for the FQDN and then receiving a confirming response utilizing the Random Value, performed in accordance with BR Section 3.2.2.4.14; xv. Confirming the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same Domain Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with BR Section 3.2.2.4.15; and xvi. Confirming the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same DNS TXT Record Phone Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with BR Section 3.2.2.4.16. All of the above methods for validation, except IP Address (BR Section 3.2.2.4.8) may be used for Wildcard Certificate Domain Name validation along with current best practice of consulting a public suffix list. MSC Trustgate.com verifies an included country code using (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 ccTLD of the requested Domain Name; or (c) information provided by the Domain Name Registrar.

Certificate	Validation
Device Certificates	MSC Trustgate.com validates the Applicant's right to use or control the Domain Name(s) and the country code that will be listed in the Certificate using the Domain-related Certificates validation procedures above. MSC Trustgate.com also verifies the identity and address of the Applicant using the procedures found in section 3.2.2.1 or section 3.2.3 of the Baseline Requirements. MSC Trustgate.com verifies any DBA included in a Certificate using a third party or government source, attestation letter, or reliable form of identification in accordance with section 3.2.2.2 of the Baseline Requirements.
S/MIME Certificates issued as Class 1-4 Client Certificates.	MSC Trustgate.com verifies an individual's or organization's right to use or control an email address to be contained in a Certificate that will have the "Secure Email" EKU by doing one of the following: i. By verifying domain control over the email domain using one of the procedures listed above in this table under the heading "DV SSL/TLS Server Certificates"; or ii. By sending an email message containing a Random Value to the email address to be included in the Certificate and receiving a confirming response through use of the Random Value to indicate that the Applicant and/or Organization owns or controls that same email address.

MSC Trustgate.com maintains and utilizes a scoring system to flag certificate requests that potentially present a higher risk of fraud. Those certificate requests that are flagged "**high risk**" receive additional scrutiny or verification prior to issuance, which may include obtaining additional documentation from or additional communication with the Applicant.

MSC Trustgate.com uses a documented internal process to check the accuracy of information sources and databases to ensure that the data acquired is acceptable, including by reviewing the database provider's terms of use.

MSC Trustgate.com uses data from databases and information sources after MSC Trustgate.com determines that the sources are:

- not self-reported; and
- the database or the information sources that demonstrate transparent efforts and reported methods to be accurate which can then be verified by MSC Trustgate.com through analysis of the resource against other known reliable resources.

3.2.3 Authentication of Individual Identity

If a Certificate will contain the identity of an individual, then MSC Trustgate.com or an RA validates the identity of the individual using the following procedures:

Certificate Type	Validation
Device Certificate	See section 3.2.3.3
Class 1 Client Certificates – Personal (email Certificates)[4]	As specified in Section 3.2.2 (no identity verification other than control of the email address listed in the Certificate)
Class 1 Client Certificates – Enterprise (email certificates)	Any one of the following: i. In-person appearance before a person performing identity proofing for a Registration Authority or a Trusted Agent with presentment of an identity credential (e.g., driver's license or birth certificate). ii. Using procedures similar to those used when applying for consumer credit and authenticated through information in consumer credit databases or government records, such as: a. the ability to place or receive calls from a given number; or b. the ability to obtain mail sent to a known physical address. iii. Through information derived from an ongoing business relationship with the credential provider or a partner company (e.g., a financial institution, airline, employer, or retail company). Acceptable information includes: a. the ability to obtain mail at the billing address used in the business relationship; b. verification of information established in previous transactions (e.g., previous order number); or c. the ability to place calls from or receive phone calls at a phone number used in previous business transactions. iv. Any method used to verify the identity of an Applicant for a Class 2, 3, or 4 Client Certificate.

[4] MSC Trustgate.com do not delegate validation of the domain portion of an e-mail address in S/MIME certificates. MSC Trustgate.com will use a process the CA/B Forum authorized to meet this requirement as listed in this section.

Certificate Type	Validation
Class 2 Client Certificates	The CA or an RA confirms that the following are consistent with the application and sufficient to identify a unique individual: a) the name on the government-issued photo-ID referenced below; b) date of birth; and c) current address or personal telephone number. i. In-person appearance before a person performing identity proofing for a Registration Authority or a Trusted Agent (or entity certified by a state, federal, or national entity as authorized to confirm identities) with presentment of a reliable form of current government-issued photo ID. ii. The Applicant must possess a valid, current, government-issued, photo ID. The Registration Authority or Trusted Agent performing identity proofing must obtain and review, which may be through remote verification, the following information about the Applicant: (i) name, date of birth, and current address or telephone number; (ii) serial number assigned to the primary, government-issued photo ID; and (iii) one additional form of ID such as another government-issued ID, an employee or student ID card number, telephone number, a financial account number (e.g., checking account, savings account, loan or credit card), or a utility service account number (e.g., electricity, gas, or water) for an address matching the applicant's residence. Identity proofing through remote verification may rely on database record checks with an agent/institution or through credit bureaus or similar databases. MSC Trustgate.com or an RA may confirm an address by issuing credentials in a manner that confirms the address of record or by verifying knowledge of recent account activity associated with the Applicant's address and may confirm a telephone number by sending a challenge-response SMS text message or by recording the applicant's voice during a communication after associating the telephone number with the applicant in records available to MSC Trustgate.com or the RA. iii. Where MSC Trustgate.com or an RA has a current and ongoing relationship with the Applicant, identity may be verified through the exchange of a previously exchanged shared secret (e.g., a PIN or password) that meets or exceeds NIST SP 800-63 Class 2 entropy requirements, provided that: (a) identity was originally established with the degree of rigor equivalent to that required in 1 or 2 above using a government-issued photo-ID, and (b) an ongoing relationship exists sufficient to ensure the Applicant's continued personal possession of the shared secret. iv. Any of the methods used to verify the identity of an applicant for a MSC Trustgate.com Class 3 or 4 Client Certificate.

Certificate Type	Validation
Class 3 Client Certificates	In-person proofing before an RA, Trusted Agent, or an entity certified by a State, Federal, or National Agencies that is authorized to confirm identities. The information must be collected and stored in a secure manner. Required identification consists of one unexpired government-issued Photo I.D and one other identification credential. Acceptable forms of Government-issued Photo ID include a national identity card, driver's license, state-issued photo ID card, passport, permanent resident card, military/police ID, or similar photo identification document. The person performing identity proofing examines the credentials and determines whether they are authentic and unexpired and checks the provided information (name, date of birth, and current address) to ensure legitimacy. MSC Trustgate.com also employs the in-person antecedent process. In-Person Definition, to meet this in-person identity proofing requirement. Under this definition, historical in-person identity proofing is sufficient if (1) it meets the thoroughness and rigor of in-person proofing described above, (2) supporting ID proofing artifacts exist to substantiate the antecedent relationship, and (3) mechanisms are in place that bind the individual to the asserted identity. In one use case, MSC Trustgate.com may uses a third party Identity Verification Provider that constructs a real-time, five-question process, based on multiple historic antecedent databases, and the applicant is given two minutes to answer at least four of the five questions correctly. The identity of the Applicant must be established no earlier than 30 days prior to initial certificate issuance. The authentication of Class 3 Administrator certificates is based on authentication of the organization and a confirmation from the organization of the identity and authorization of the person to act as Administrator. MSC Trustgate.com may also have occasion to approve Certificate Applications for their own Administrators. Administrators are “Trusted Persons” within an organization. In this case, authentication of their Certificate Applications shall be based on confirmation of their identity in connection with their employment or retention as an independent contractor and background checking procedures[5].

[5] MSC Trustgate.com may approve Administrator Certificates to be associated with a non-human recipient such as a device, or a server. Authentication of a Class 3 Administrator Certificate Applications for a non-human recipient shall include:

- Authentication of the existence and identity of the service named as the Administrator in the Certificate Application
- Authentication that the service has been securely implemented in a manner consistent with it performing an Administrative function
- Confirmation of the identity and authorization of the person enrolling for the Administrator certificate for the service named as Administrator in the Certificate Application.

If in-person identity verification is required and the Applicant cannot participate in face-to-face registration alone (e.g. because Applicant is a network device, minor, or person not legally competent), then the Applicant may be accompanied by a person already certified by the PKI or who has the required identity credentials for a Certificate of the same type applied for by the Applicant. The person accompanying the Applicant (i.e. the "**Sponsor**") will present information that is sufficient for registration at the level of the Certificate being requested, for himself or herself, and for the Applicant.

For in-person identity proofing for Class 3 Certificates, MSC Trustgate.com may rely on an entity certified by a State, Federal, or National Agencies as authorized to confirm identities may perform the authentication on behalf of the RA. The certified agencies should forward the information collected from the applicant directly to the RA in a secure manner.

The RA also may establish a technology based in person identity proofing (e.g. video conference, biometric authentication with Government-issued photo ID) to confirm the identities of the Applicant.

3.2.3.1 Authentication for Role-based Client Certificates

Not applicable.

3.2.3.2 Authentication for Group Client Certificates

Not applicable.

3.2.3.3 Authentication of Devices with Human Sponsors

MSC Trustgate.com issues Class 1, 2, or 3 Certificates for use on computing or network devices, provided that the entity owning the device is listed as the subject. In all cases, the device has a human sponsor who provides:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name);
- Equipment Public Keys;
- Equipment authorizations and attributes (if any are to be included in the Certificate); and
- Contact information.

If the Certificate's sponsor changes, the new sponsor is required to review the status of each device to ensure it is still authorized to receive Certificates. Each sponsor is required to provide proof that the device is still under the sponsor's control or responsibility on request. Sponsors are contractually obligated to notify MSC Trustgate.com if the equipment is no longer in use, no longer under their control or responsibility, or no longer requires a Certificate. All registration is verified commensurate with the requested certificate type.

3.2.4 Non-verified Subscriber Information

Non-verified subscriber information includes:

- Organization Unit (OU) (with certain exceptions)
- Subscriber's name in Class 1 certificates
- Any other information designated as non-verified in the certificate.

3.2.5 Validation of Authority

Certificate Type	Verification
Device Certificate	The request is verified using a Reliable Method of Communication, in accordance with section 3.2.5 of the Baseline Requirements.
Class 1 Client Certificates Personal (email Certificates) and Enterprise (email Certificates)	The authority of the request is verified through the email address listed in the Certificate or with a person who has technical or administrative control over the domain or the email address to be listed in the Certificate.
Client Certificates Class 2, 3 and 4 Certificates	The organization named in the Certificate confirms to MSC Trustgate.com or an RA that the individual is authorized to obtain the Certificate. The organization is required to request revocation of the Certificate when that affiliation ends.

An organization may limit who is authorized to request Certificates by sending a request to MSC Trustgate.com. A request to limit authorized individuals is not effective until approved by MSC Trustgate.com. MSC Trustgate.com will respond to an organization's verified request for MSC Trustgate.com's list of its authorized requesters.

3.2.6 Criteria for Interoperation

MSC Trustgate.com may provide interoperation services that allow a non-DigiCert PKI CA to be able to interoperate with the DigiCert PKI by unilaterally certifying that CA. CAs enabled to interoperate in this way will comply with the DigiCert CP as supplemented by additional policies when required.

MSC Trustgate.com shall only allow interoperation with the DigiCert PKI of a non-DigiCert PKI CA in circumstances where the CA, at a minimum:

- Enters into a contractual agreement with MSC Trustgate.com;
- Operates under a CPS that meets DigiCert PKI requirements for the classes of certificates it will issue;
- Passes a compliance assessment before being allowed to interoperate; and
- Passes an annual compliance assessment for ongoing eligibility to interoperate.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

Subscribers may request re-key of a Certificate prior to a Certificate's expiration. After receiving a request for re-key, MSC Trustgate.com creates a new Certificate with the same certificate contents except for a new Public Key and, optionally, an extended validity period. If the Certificate has an extended validity period, MSC Trustgate.com may perform some revalidation of the Applicant but may also rely on information previously provided or obtained.

Subscribers re-establish their identity as follows:

Certificate	Routine Re-Key Authentication	Re-Verification Required
Device Certificates	Username and password	According to Baseline Requirements
Class 1 Client Certificates	Username and password or a challenge phrase	At least every nine years
Class 2 Client Certificates	Current signature key or multi-factor authentication meeting NIST SP 800-63 Level 3 or a challenge phrase	At least every nine years
Class 3 and 4 Client Certificates	Current signature key or multi-factor authentication meeting NIST SP 800-63 Level 3	At least every nine years
Device Certificates	Current signature key or multi-factor authentication meeting NIST SP 800-63 Level 3	At least every nine years

MSC Trustgate.com does not re-key a Certificate without additional authentication if doing so it would allow the Subscriber to use the Certificate beyond the limits described above.

3.3.2 Identification and Authentication for Re-key After Revocation

If a Certificate was revoked for any reason other than a renewal, update, or modification action, then the Subscriber must undergo the initial registration process (described in Section 3.2) prior to rekeying the Certificate.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Prior to the revocation of a Certificate, MSC Trustgate.com 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.

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

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

The requests to revoke a CA Certificate shall be authenticated by the MSC Trustgate.com to ensure that the revocation has in fact been requested by the CA.

4 CERTIFICATE LIFE-CYCLE 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 entity,
- Any authorized representative of a CA,
- Any authorized representative of an RA.

No individual or entity listed on a government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the Malaysia may submit an application for a Certificate. Applicants or individuals authorized to request Certificates, who are not included in any of the previous lists, may apply for a Certificate.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 End-User Certificate Subscribers

All end-user Certificate Subscribers shall manifest assent to the relevant Subscriber Agreement that contains representations and warranties described in Section 9.6.3 and undergo an enrollment process (in no particular order) consisting of:

1. Completing a Certificate Application and providing true and correct information;
2. Generating, or arranging to have generated, a key pair;
3. Delivering his, her, or its public key, directly or through an RA, to MSC Trustgate.com;
4. Demonstrating possession and/or exclusive control of the private key corresponding to the public key delivered to MSC Trustgate.com;
5. Agreeing to the applicable Subscriber Agreement; and
6. Paying any applicable fees.

4.1.2.2 CA and RA Certificates

Subscribers of CA and RA Certificates enter into a contract with MSC Trustgate.com. CA and RA Applicants shall provide their credentials to demonstrate their identity and provide contact information during the contracting process.

During this contracting process or, at the latest, prior to the Key Generation Ceremony to create a CA or RA key pair, the applicant shall cooperate with MSC Trustgate.com to determine the appropriate distinguished name and the content of the Certificates to be issued by the applicant.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

MSC Trustgate.com or an RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2.

If an RA assists in the verification, the RA must create and maintain records sufficient to establish that it has performed its required verification tasks and communicate the completion of such performance to MSC Trustgate.com. After verification is complete, MSC Trustgate.com evaluates the corpus of information and decides whether or not to issue the Certificate.

MSC Trustgate.com considers a source's availability, purpose, and reputation when determining whether a third-party source is reasonably reliable. MSC Trustgate.com does not consider a database, source, or form of identification reasonably reliable if MSC Trustgate.com or the RA is the sole source of the information.

4.2.2 Approval or Rejection of Certificate Applications

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

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

MSC Trustgate.com or an RA will reject a certificate application if:

- Identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or
- The Subscriber fails to furnish supporting documentation upon request, or
- The Subscriber fails to respond to notices within a specified time, or
- Payment has not been received, or
- The RA believes that issuing a certificate to the Subscriber could damage or diminish MSC Trustgate.com or DigiCert's reputation or business.

MSC Trustgate.com is not liable for any rejected Certificate and is not obligated to disclose the reasons for a rejection. Rejected Applicants may re-apply. Subscribers are required to check the Certificate's contents for accuracy prior to using the certificate.

4.2.3 Time to Process Certificate Applications

Under normal circumstances, MSC Trustgate.com verifies an Applicant's information and issues a digital Certificate within a reasonable time frame. Issuance time frames are greatly dependent on when the Applicant provides the details and documentation necessary to complete validation. MSC Trustgate.com will usually complete the validation process and issue or reject a certificate application within three (3) working days after receiving all of the necessary details and documentation from the Applicant, although such events outside of the control of MSC Trustgate.com can delay the issuance process.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

MSC Trustgate.com confirms the source of a certificate request before issuance. Databases and CA processes occurring during certificate issuance are protected from unauthorized modification. After issuance is complete, the Certificate is stored in a database and sent to the Subscriber.

MSC Trustgate.com does not issue end entity Certificates directly from its root Certificates. CA Certificate issuance by the Root CA requires an individual authorized by MSC Trustgate.com (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

MSC Trustgate.com shall, either directly or through an RA, notify Subscribers within a reasonable time that they have created such Certificates, and provide Subscribers with access to the Certificates by notifying them that their Certificates are available.

Certificates shall be made available to end-user Subscribers, either by allowing them to download them from a web site or via a message sent to the Subscriber containing the Certificate.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

Subscribers are solely responsible for installing the issued Certificate on the Subscriber's computer or hardware security module. Certificates are considered accepted thirty (30) days after the Certificate's issuance, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

Failure of the Subscriber to object to the certificate or its content constitutes certificate acceptance.

4.4.2 Publication of the Certificate by the CA

MSC Trustgate.com publishes all CA Certificates and the Certificates in its publicly accessible repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of a Certificate's issuance if the RA was involved in the issuance process.

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 is only permitted once the Subscriber agrees to the Subscriber Agreement and accepted the certificate. The certificate shall be used lawfully in accordance with MSC Trustgate.com's Subscriber Agreement, the terms of this CP and the relevant CPS.

Subscribers are contractually obligated to protect their Private Keys from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated Certificate, and use Certificates in accordance with their intended purpose.

Parties other than the Subscriber shall not archive the Subscriber Private Key except as set forth in Section 4.12.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties may only use software that is compliant with X.509, IETF RFCs, and other applicable standards. MSC Trustgate.com does not warrant that any third party software will support or enforce the controls and requirements found herein.

A Relying Party should use discretion when relying on a Certificate and should consider the totality of the circumstances and risk of loss prior to relying on a Certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate. Any warranties provided by MSC Trustgate.com are only valid if a Relying Party's reliance was reasonable and if the Relying Party adhered to the Relying Party Agreement set forth in the MSC Trustgate.com repository.

A Relying Party should rely on a digital signature only if:

1. the digital signature was created during the operational period of a valid Certificate and can be verified by referencing a valid Certificate,
2. the Certificate is not revoked and the Relying Party checked the revocation status of the Certificate prior to the Certificate's use by referring to the relevant CRLs or OCSP responses, and
3. the Certificate is being used for its intended purpose and in accordance with this CPS.

4.6 CERTIFICATE RENEWAL

Certificate renewal is the issuance of a new certificate to the subscriber with new serial number and new validity period but without changing the public key or any other information in the certificate.

4.6.1 Circumstance for Certificate Renewal

MSC Trustgate.com may renew a Certificate if:

1. the associated Public Key has not reached the end of its validity period,
2. the Subscriber and attributes are consistent,
3. the associated Private Key remains uncompromised, and
4. re-verification of subscriber identity is not required by Section 3.3.1.

MSC Trustgate.com may also renew a Certificate if a CA Certificate is re-keyed or as otherwise necessary to provide services to a customer. MSC Trustgate.com may also notify Subscribers prior to a Certificate's expiration date. Certificate renewal requires payment of additional fees. MSC Trustgate.com may renew a certificate after expiration if the relevant industry permits such practices.

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to renew the expiring certificate to maintain continuity of Certificate usage.

4.6.2 Who May Request Renewal

Only the certificate subject or an authorized representative of the certificate subject may request renewal of the Subscriber's Certificates. MSC Trustgate.com may renew a Certificate without a corresponding request if the signing Certificate is re-keyed.

4.6.3 Processing Certificate Renewal Requests

Renewal procedures is to ensure that the person or organization seeking to renew an end-user Subscriber Certificate is in fact that he or she is the Subscriber (or authorized by the Subscriber) of the Certificate.

Therefore, one acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers will choose and submit with their enrollment information i.e. a Challenge Phrase (or the equivalent thereof). Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the reenrollment information (including Corporate and Technical contact information[6]) has not changed, a renewal Certificate is automatically issued.

As an alternative to using a challenge phrase (or equivalent) MSC Trustgate.com 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, MSC Trustgate.com will issue the Certificate if the enrollment information (including corporate and technical contact information[7]) has not changed.

After renewal in this fashion, and on at least alternative instances of subsequent renewal thereafter, MSC Trustgate.com or an RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in this CPS for the authentication of an original Certificate Application.

In particular, for retail Class 3 Organizational certificates MSC Trustgate.com 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.

MSC Trustgate.com 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.

Other than this procedure or another MSC Trustgate.com approved procedure, the requirements for the authentication of an original Certificate Application shall be used for renewing an end-user Subscriber Certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of certificate renewal to the Subscriber is in accordance with Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Conduct constituting Acceptance of a renewed certificate is in accordance with Section 4.4.1.

[6] If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.
[7] If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

4.6.6 Publication of the Renewal Certificate by the CA

The renewed certificate is published in MSC Trustgate.com's publicly accessible repository

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of a Certificate's renewal if the RA was involved in the issuance process.

4.7 CERTIFICATE RE-KEY

Re-keying a Certificate consists of creating a new Certificate with a new Public Key and serial number while keeping the subject information the same.

4.7.1 Circumstance for Certificate Rekey

Subscribers requesting re-key should identify and authenticate themselves as permitted by section 3.3.1.

A certificate may also be re-keyed after expiration.

4.7.2 Who May Request Certification of a New Public Key?

MSC Trustgate.com will only accept re-key requests from the subject of the Certificate, an authorized representative for an Organizational certificate, or the PKI sponsor. MSC Trustgate.com may initiate a certificate re-key at the request of the certificate subject or at MSC Trustgate.com's own discretion.

4.7.3 Processing Certificate Rekey Requests

MSC Trustgate.com will only accept re-key requests from the subject of the Certificate or the PKI sponsor. If the Private Key and any identity in a Certificate have not changed, then MSC Trustgate.com can issue a replacement Certificate using a previously issued Certificate or previously provided CSR. MSC Trustgate.com re-uses existing verification information unless re-verification and authentication is required under section 3.3.1 or if MSC Trustgate.com believes that the information has become inaccurate.

4.7.4 Notification of Certificate Rekey to Subscriber

Notification of issuance of a re-keyed certificate to the Subscriber is in accordance with Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Rekeyed Certificate

Conduct constituting Acceptance of a re-keyed certificate is in accordance with Section 4.4.1.

4.7.6 Publication of the Issued Certificate by the CA

The re-keyed certificate is published in MSC Trustgate.com's publicly accessible repository

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of a Certificate's rekey if the RA was involved in the issuance process.

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstances for Certificate Modification

Modifying a Certificate means creating a new Certificate for the same subject with authenticated information that differs slightly from the old Certificate (e.g., changes to email address or non-essential parts of names or attributes) provided that the modification otherwise complies with this CPS. The new Certificate may have the same or a different subject Public Key.

4.8.2 Who May Request Certificate Modification

MSC Trustgate.com modifies Certificates at the request of certain certificate subjects or in its own discretion. MSC Trustgate.com does not make certificate modification services available to all Subscribers.

4.8.3 Processing Certificate Modification Requests

After receiving a request for modification, MSC Trustgate.com verifies any information that will change in the modified Certificate. MSC Trustgate.com will only issue the modified Certificate after completing the verification process on all modified information. MSC Trustgate.com will not issue a modified Certificate that has a validity period that exceeds the applicable time limits found in section 3.3.1 or 6.3.2.

RAs are required to perform identification and authentication of all modified Subscriber information in terms of Section 3.2.

4.8.4 Notification of Certificate Modification to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to revoking a Certificate, MSC Trustgate.com and Issuer CAs verify that the revocation request was made by either the organization or individual that made the certificate application or by an entity with the legal jurisdiction and authority to request revocation. Issuer CAs are required to provide evidence of the revocation authorization to MSC Trustgate.com upon request.

4.9.1 Circumstances for Revocation

MSC Trustgate.com will revoke a Certificate within twenty four (24) hours after confirming one or more of the following occurred:

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

MSC Trustgate.com may revoke a certificate within twenty four (24) hours and will revoke a Certificate within five (5) days after confirming that one or more of the following occurred:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/B forum baseline requirements or any section of the Mozilla Root Store policy;
2. MSC Trustgate.com obtains evidence that the Certificate was misused and/or used outside the intended purpose as indicated by the relevant agreement;
3. The Subscriber or the cross-certified CA breached a material obligation under the CP, this CPS, or the relevant agreement;
4. MSC Trustgate.com confirms any circumstance indicating that use of a FQDN, IP address, or email 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);
5. MSC Trustgate.com confirms a material change in the information contained in the Certificate;
6. MSC Trustgate.com confirms that the Certificate was not issued in accordance with the CA/B forum requirements or relevant browser policy;
7. MSC Trustgate.com determines or confirms that any of the information appearing in the Certificate is inaccurate;
8. MSC Trustgate.com's right to issue Certificates under the CA/B forum requirements expires or is revoked or terminated, unless MSC Trustgate.com has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by the DigiCert CP and/or this CPS; or
10. MSC Trustgate.com confirms 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.

MSC Trustgate.com may revoke any Certificate in its sole discretion, including if MSC Trustgate.com believes that:

1. Either the Subscriber's or MSC Trustgate.com's obligations under the CP or this CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;
2. MSC Trustgate.com received a lawful and binding order from a government or regulatory body to revoke the Certificate;
3. MSC Trustgate.com ceased operations and did not arrange for another Certificate authority to provide revocation support for the Certificates;
4. The technical content or format of the Certificate presents an unacceptable risk to application software vendors, Relying Parties, or others;
5. The Subscriber was added as a denied party or prohibited person to a blacklist or is operating from a destination prohibited under the laws of the United States;

MSC Trustgate.com always revokes a Certificate if the binding between the subject and the subject's Public Key in the certificate is no longer valid or if an associated Private Key is compromised.

MSC Trustgate.com will revoke a Subordinate CA Certificate within seven (7) days after confirming one or more of the following occurred:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies MSC Trustgate.com that the original Certificate request was not authorized and does not retroactively grant authorization;
3. MSC Trustgate.com 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 of the CA/B forum baseline requirements or any section of the Mozilla Root Store policy;
4. MSC Trustgate.com obtains evidence that the CA Certificate was misused and/or used outside the intended purpose as indicated by the relevant agreement;
5. MSC Trustgate.com confirms that the CA Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6. MSC Trustgate.com determines that any of the information appearing in the CA Certificate is inaccurate or misleading;
7. MSC Trustgate.com or the Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the CA Certificate;
8. MSC Trustgate.com's or the Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless MSC Trustgate.com has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by DigiCert's Certificate Policy and/or Certification Practice Statement; or

10. The technical content or format of the CA Certificate presents an unacceptable risk to application software suppliers or Relying Parties.

MSC Trustgate.com will revoke a cross-Certificate if the cross-certified entity (including MSC Trustgate.com) no longer meets the stipulations of the corresponding policies, as indicated by policy OIDs listed in the policy mapping extension of the cross-Certificate.

MSC Trustgate.com may also revoke an Administrator Certificate if the Administrator's authority to act as Administrator has been terminated or otherwise has ended.

MSC Trustgate.com Subscriber Agreements require end-user Subscribers to immediately notify MSC Trustgate.com of a known or suspected compromise of its private key.

4.9.2 Who Can Request Revocation

Individual Subscribers can request the revocation of their own individual Certificates through an authorized representative of MSC Trustgate.com or an RA. In the case of organizational Certificates, a duly authorized representative of the organization shall be entitled to request the revocation of Certificates issued to the organization. A duly authorized representative of MSC Trustgate.com or a RA shall be entitled to request the revocation of an RA Administrator's Certificate. The entity that approved a Subscriber's Certificate Application shall also be entitled to revoke or request the revocation of the Subscriber's Certificate.

Only MSC Trustgate.com is entitled to request or initiate the revocation of the Certificates issued to its own CAs. RAs are entitled, through their duly authorized representatives, to request the revocation of their own Certificates, and their Superior Entities shall be entitled to request or initiate the revocation of their Certificates.

4.9.3 Procedure for Revocation Request

4.9.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate

An end-user Subscriber requesting revocation is required to communicate the request to the MSC Trustgate.com, who in turn will initiate revocation of the certificate promptly.

4.9.3.2 Procedure for Requesting the Revocation of a CA or RA Certificate

A CA or RA requesting revocation of its CA or RA Certificate is required to communicate the request to MSC Trustgate.com. MSC Trustgate.com will then revoke the Certificate. MSC Trustgate.com may also initiate CA or RA Certificate revocation.

4.9.4 Revocation Request Grace Period

The revocation request grace period is the time available to the subscriber within which the subscriber must make a revocation request after reasons for revocation have been identified.

Subscribers are required to request revocation within one (1) day after detecting the loss or compromise of the Private Key. MSC Trustgate.com may grant and extend revocation grace periods on a case-by-case basis if it does not violate this CP, the CPS, or any of the relevant requirements as listed in the sources of section 1.6.3.

MSC Trustgate.com reports the suspected compromise of its CA Private Key and requests revocation to both the policy authority and operating authority of the superior issuing CA within one hour of discovery.

4.9.5 Time within which CA Must Process the Revocation Request

MSC Trustgate.com will revoke a CA Certificate within one (1) hour after receiving clear instructions from the PMA.

Within twenty four (24) hours after receiving a Certificate problem report, MSC Trustgate.com then will investigates the facts and circumstances related to a Certificate problem report and will 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, MSC Trustgate.com works 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 MSC Trustgate.com 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. The date selected by MSC Trustgate.com will 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.

Under normal operating circumstances, MSC Trustgate.com will revoke Certificates as quickly as practical after validating the revocation request following the guidelines of this section and Section 4.9.1, generally within the following time frames:

1. Certificate revocation requests for publicly-trusted Certificates are processed within 18 hours after their receipt,
2. Revocation requests received two or more hours before CRL issuance are processed before the next CRL is published, and
3. Revocation requests received within two hours of CRL issuance are processed before the following CRL is published.

MSC Trustgate.com follows the revocation timeframes specified for malware in the Minimum Requirements for Issuance and Management of Publicly Trusted Code Signing Certificates in section 13.1.5.

4.9.6 Revocation Checking Requirement for Relying Parties

Prior to relying on information listed in a Certificate, a Relying Party must confirm the validity of each Certificate in the certificate path in accordance with IETF PKIX standards, including checking for certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each Certificate in the chain.

4.9.7 CRL Issuance Frequency

CRLs for end-user Subscriber Certificates are issued at least once per day.

CRLs for CA Certificates shall be issued at least every 6 months, but also whenever a CA Certificate is revoked.

4.9.8 Maximum Latency for CRLs

CRLs for Certificates issued to end entity subscribers are posted automatically to the online repository within a commercially reasonable time after generation, usually within minutes of generation. Irregular, interim, or emergency CRLs are posted within four hours after generation. Regularly scheduled CRLs are posted prior to the nextUpdate field in the previously issued CRL of the same scope.

4.9.9 On-line Revocation/Status Checking Availability

Online revocation and other Certificate status information are available via a web-based repository and, where offered, OCSP. Where OCSP support is required by the applicable CP, OCSP responses are provided within a commercially reasonable time and no later than ten seconds after the request is received, subject to transmission latencies over the Internet.

OCSP responses conform to RFC 6960. OCSP responses either:

1. Are signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Are signed by an OCSP Responder whose Certificate is signed by the 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 RFC 6960.

4.9.10 On-line Revocation Checking Requirements

A relying party must confirm the validity of a Certificate in accordance with section 4.9.6 prior to relying on the Certificate.

MSC Trustgate.com supports an OCSP capability using the GET method for Certificates issued in accordance with the Baseline Requirements. OCSP Responders under MSC Trustgate.com's direct control will not respond with a "good" status for a certificate that has not been issued.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Related to Key Compromise

MSC Trustgate.com uses commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects the compromise of a Private Key. MSC Trustgate.com will transition any revocation reason code in a CRL to "key compromise" upon discovery of such reason or as required by an applicable CP.

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

Certificate status information is available via CRL and OCSP responder.

The serial number of a revoked Certificate remains on the CRL until one (1) additional CRL is published after the end of the Certificate's validity period. CRLs for end-user Subscriber Certificates are issued at least once per day. The value of the nextUpdate field will not be more than ten (10) days beyond the value of the thisUpdate field.

OCSP information for subscriber Certificates is updated at least every four (4) days.

4.10.2 Service Availability

Certificate status services are available 24x7. This includes the online repository that application software can use to automatically check the current status of all unexpired Certificates issued by MSC Trustgate.com. MSC Trustgate.com operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

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

4.10.3 Optional Features

OCSP is an optional status service feature that is not available for all products and must be specifically enabled for other products

4.11 END OF SUBSCRIPTION

A Subscriber's subscription service ends if its Certificate expires or is revoked or if the applicable Subscriber Agreement expires without any renewal taken place.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy Practices

MSC Trustgate.com never escrows CA Private Keys under this CPS.

MSC Trustgate.com may escrow Subscriber key management keys to provide key recovery services. MSC Trustgate.com encrypts and protects escrowed Private Keys using the same or a higher level of security as used to generate and deliver the Private Key.

MSC Trustgate.com allows Subscribers and other authorized entities to recover escrowed (decryption) Private Keys. MSC Trustgate.com uses multi-person controls during key recovery to prevent unauthorized access to a Subscriber's escrowed Private Keys. MSC Trustgate.com accepts key recovery requests:

1. From the Subscriber or Subscriber's organization, if the Subscriber has lost or damaged the private-key token;
2. From the Subscriber's organization, if the Subscriber is not available or is no longer part of the organization that contracted with MSC Trustgate.com for Private Key escrow;
3. From an authorized investigator or auditor, if the Private Key is part of a required investigation or audit;
4. From a requester authorized by a competent legal authority to access the communication that is encrypted using the key;
5. From a requester authorized by law or governmental regulation; or
6. From an entity contracting with MSC Trustgate.com for escrow of the Private Key when key recovery is mission critical or mission essential.

Entities using MSC Trustgate.com's key escrow services are required to:

1. Notify Subscribers and get his or her consent that their Private Keys are escrowed;
2. Protect escrowed keys from unauthorized disclosure;
3. Protect any authentication mechanisms that could be used to recover escrowed Private Keys;
4. Release an escrowed key only after making or receiving (as applicable) a properly authorized request for recovery; and
5. Comply with any legal obligations to disclose or keep confidential escrowed keys, escrowed key-related information, or the facts concerning any key recovery request or process.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

Compliance with these policies is included in MSC Trustgate.com's independent audit requirements described in Section 8. The MSC Trustgate.com Physical Security Policy contains sensitive security information and is only available upon agreement with MSC Trustgate.com. An overview of the requirements are described below.

5.1.1 Site Location and Construction

MSC Trustgate.com CA and RA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems whether covert or overt.

MSC Trustgate.com also maintains disaster recovery facilities for its CA operations. MSC Trustgate.com's disaster recovery facilities are protected by multiple tiers of physical security comparable to those of MSC Trustgate.com's primary facility.

5.1.2 Physical Access

5.1.2.1 Data Centers

Systems providing online certificate issuance (e.g. Issuer CAs) are located in commercial data centers. MSC Trustgate.com protects such online equipment (including certificate status servers and CMS equipment) from unauthorized access and implements physical controls to reduce the risk of equipment tampering. Access to the data centers housing the CA requires two-factor authentication — the individual must have an authorized access card and pass biometric access control authenticators. These biometric authentication access systems log each use of the access card. MSC Trustgate.com deactivates and securely stores its CA equipment when not in use in accordance with section 5.1.2.3. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module. Activation data is never stored with the cryptographic module or removable hardware associated with equipment used to administer MSC Trustgate.com's Private Keys. Cryptographic hardware includes a mechanism to lock the hardware after a certain number of failed login attempts.

The data center is not continuously attended. MSC Trustgate.com personnel who is the last person to depart will initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 RA Operations Areas

MSC Trustgate.com's RA operations are protected against access from non-authorized individuals. Access to secure areas of buildings requires the use of an "access" or "pass" card. Access card use is logged by the building security system. The exterior and internal passageways of buildings are equipped with video cameras. Similarly, the support and vetting rooms where MSC Trustgate.com personnel perform identity vetting and other RA functions are equipped with video surveillance cameras. Access card logs and video records are reviewed on a regular basis. MSC Trustgate.com securely stores all removable media and paper containing sensitive plain-text information related to its CA or RA operations in secure containers.

5.1.2.3 Offline CA Key Storage Rooms

MSC Trustgate.com securely stores the cryptomodules used to generate and store offline CA Private Keys. Access to the rooms used for key storage is controlled and logged by the building access card system. When not in use during a key ceremony, CA cryptomodules are locked in a safe that provides two-person physical access control. Activation data is protected in accordance with section 6.4. Cryptomodule activation keys (operator cards and PED keys) are either sealed in tamper-evident bags and placed in safe deposit boxes or stored in the two-person safe when not in use. Access to the safe is manually logged. Access card logs and the manual logs of access to the safe are reviewed on a regular basis.

5.1.2.4 CA Key Generation and Signing Rooms

CA key generation and signing occurs either in the secure storage room described in section 5.1.2.3 or in a room of commensurate security in close proximity thereto. MSC Trustgate.com's Key Manager retrieve cryptographic materials necessary to perform key generation and certificate signing. At no time are cryptographic materials left unattended by fewer than two persons serving in trusted roles.

5.1.3 Power and Air Conditioning

MSC Trustgate.com's secure facilities are equipped with primary and backup:

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

5.1.4 Water Exposures

The cabinets housing MSC Trustgate.com's CA systems are located on raised flooring and the data centers are equipped with monitoring systems to detect any excess moisture.

5.1.5 Fire Prevention and Protection

The data centers are equipped with fire suppression mechanisms.

5.1.6 Media Storage

MSC Trustgate.com protects its media from accidental damage, environmental hazards, and unauthorized physical access. Backup files are created on a daily basis. MSC Trustgate.com's backup files are maintained at locations separate from MSC Trustgate.com's primary data operations facility.

5.1.7 Waste Disposal

All unnecessary copies of printed sensitive information are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal.

5.1.8 Off-site Backup

MSC Trustgate.com maintains at least one full backup and makes regular backup copies of any information necessary to recover from a system failure. Backup copies of CA Private Keys and activation data are stored for disaster recovery purposes off-site in safe deposit boxes located inside financial institutions and are accessible only by trusted personnel.

5.1.9 Certificate Status Hosting, CMS and External RA Systems

All physical control requirements under Section 5.1 applies equally to any Certificate Status Hosting, CMS, or external RA system.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

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

Trusted Persons include, but are not limited to:

DigiCert CP Trusted Role	MSC Trustgate Trusted Role Title[8]
CA Administrator	Key Manager, Master Admin (MSA)
Registration Officer	Validation roles such as MPKI Administrators and Customer Service.
System Administrator/System Engineer (Operator)	System Administrators, Data Center Operators, and/or Designated Engineers
Internal Auditor	Security Personnel
RA Administrators	Enterprise Admin (ESA)

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

5.2.2 Number of Persons Required per Task

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

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

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold “Secret Shares” and vice versa.

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

[8] Staff appointed to trusted roles will not maintain more than one trusted role identity at a time in order to maintain the separation of duties as specified in section 5.2.4 of the DigiCert CP and this CPS.

5.2.3 Identification and Authentication for each Role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing human resource or security functions and a check of well-recognized forms of identification (e.g., passports and driver's licenses). Identity is further confirmed through the background checking procedures in Section 5.3.1.

MSC Trustgate.com ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

- issued access devices and granted access to the required facilities;
- issued electronic credentials to access and perform specific functions

on MSC Trustgate.com CA, RA, or other IT systems.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties include (but are not limited to)

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

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

The PMA is responsible and accountable for MSC Trustgate.com's PKI operations and ensures compliance with this CPS and the CP. MSC Trustgate.com's personnel and management practices provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties.

There is no citizenship requirement for personnel performing trusted roles associated with the issuance of other kinds of Certificates.

The PMA ensures that all individuals assigned to trusted roles have proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, to perform their duties under this CPS, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts.

5.3.2 Background Check Procedures

MSC Trustgate verifies the identity of each employee appointed to a trusted role and performs a background check prior to allowing such person to act in a trusted role. MSC Trustgate requires each individual to appear in-person before a human resources employee whose responsibility it is to verify identity. The human resources employee verifies the individual's identity using government-issued photo identification (e.g., national identity card, passports and/or driver's licenses or comparable procedure for the jurisdiction in which the individual's identity is being verified)

Background checks may include a combination of the following as required:

- verification of the individual's identity,
- previous employment,
- professional reference,
- highest or most relevant educational degree obtained,
- criminal records (local, state or provincial, and national)
- credit/financial records
- driving records,
- Employees Provident Fund (EPF) records, and
- previous residences

These procedures shall be subject to any limitations on background checks imposed by local law. 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, MSC Trustgate.com will utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

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

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

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

The use of information revealed in a background check to take such actions is subject to the applicable Federal, State, and Local laws.

Background checks are refreshed and re-adjudication occurs at least every five (5) years.

5.3.3 Training Requirements

MSC Trustgate.com provides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. MSC Trustgate.com maintains records of such training. MSC Trustgate.com periodically reviews and enhances its training programs as necessary.

MSC Trustgate.com's training programs are tailored to the individual's responsibilities and include the following as relevant:

- Basic Public Key Infrastructure (PKI) concepts;
- MSC Trustgate.com security and operational policies and procedures;
- Use and operation of deployed hardware and software;
- Incident and Compromise reporting and handling,
- Disaster recovery and business continuity procedures;
- Authentication and verification policies and procedures;
- Common threats to the validation process, including phishing and other social engineering tactics; and
- CA/Browser Forum Guidelines and other applicable industry and government guidelines.

Training is provided via a mentoring process involving senior members of the team to which the employee belongs.

MSC Trustgate.com maintains records of who received training and what level of training was completed. Registration Officers must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges. All Registration Officers are required to pass an internal examination on the Baseline Requirements prior to validating and approving the issuance of Certificates. Where competence is demonstrated in lieu of training, MSC Trustgate.com maintains supporting documentation.

5.3.4 Retraining Frequency and Requirements

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

5.3.5 Job Rotation Frequency and Sequence

Not applicable.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of MSC Trustgate.com policies and procedures, whether through negligence or malicious intent. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

If a person who is entrusted with the role is alleged by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review. After management review and discusses the incident with the trusted personnel, management may reassign the employee to a non-trusted role or dismiss the individual from employment as appropriate.

5.3.7 Independent Contractor Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant will held the same functional and security criteria that apply to a MSC Trustgate.com employees in a comparable position.

Independent contractors and consultants who have not completed or passed the background check procedures specified in Section 5.3.2 will permitted access to MSC Trustgate.com's secure facilities only to the extent that they are escorted and directly supervised by Trusted Personnel at all times.

5.3.8 Documentation Supplied to Personnel

MSC Trustgate.com provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

MSC Trustgate.com's systems requires identification and authentication at system logon with a unique user name and password. Important system actions are logged to establish the accountability of the operators who initiate such actions.

MSC Trustgate.com enables all essential event auditing capabilities of its CA applications in order to record the events listed below. If MSC Trustgate.com's applications cannot automatically record an event, MSC Trustgate.com implements manual procedures to satisfy the requirements. For each event, MSC Trustgate.com records the relevant:

i. date and time;
ii. type of event;
iii. success or failure; and
iv. user or system that caused the event or initiated the action.

MSC Trustgate.com records 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 the CABF Requirements, the DigiCert CP, and this 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 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

As required, generally within at least once every three (3) months, MSC Trustgate.com administrator will review the logs generated by MSC Trustgate.com's systems, makes system and file integrity checks, and conducts a vulnerability assessment. The administrator may perform the checks using automated tools. During these checks, the administrator:

1. checks whether anyone has tampered with the log,
2. scans for anomalies or specific conditions, including any evidence of malicious activity, and

3. prepares a written summary of the review.

Any anomalies or irregularities found in the logs are investigated. The summaries include recommendations to MSC Trustgate.com's operations management committee and are made available to MSC Trustgate.com's auditors upon request. MSC Trustgate.com documents any actions taken as a result of a review.

5.4.3 Retention Period for Audit Log

Audit logs related to publicly trusted Certificates are retained for at least seven (7) years or in accordance with section 5.5.2. MSC Trustgate.com retains audit logs on-site until after they are reviewed. The individuals who remove audit logs from MSC Trustgate.com's CA systems are different than the individuals who control MSC Trustgate.com's signature keys.

5.4.4 Protection of Audit Log

CA audit log information is retained on equipment until after it is copied by a system administrator. MSC Trustgate.com's CA systems are configured to ensure that

i. only authorized people have read access to logs,
ii. only authorized people may archive audit logs, and
iii. audit logs are not modified.

Audit logs are protected from destruction prior to the end of the audit log retention period and are retained securely on-site until transferred to a backup site. MSC Trustgate.com's off-site storage location is a safe and secure location that is separate from the location where the data was generated.

5.4.5 Audit Log Backup Procedures

MSC Trustgate.com makes regular backup copies of audit logs and audit log summaries and saves a copy of the audit log to a secure, off-site location on at least a monthly basis.

Where required, MSC Trustgate.com creates incremental backups of audit logs daily and full backups weekly.

5.4.6 Audit Collection System (internal vs. external)

Automatic audit processes begin on system startup and end at system shutdown. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, MSC Trustgate.com's Administrators and the PMA shall be notified and the PMA will consider suspending the CA's or RA's operations until the problem is remedied.

5.4.7 Notification to Event-causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

MSC Trustgate.com performs annual risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process.

MSC Trustgate.com also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that MSC Trustgate.com has in place to control such risks. MSC Trustgate.com's Internal Auditors review the security audit data checks for continuity. MSC Trustgate.com's audit log monitoring tools alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

5.5 RECORDS ARCHIVAL

MSC Trustgate.com complies with all record retention policies that govern by law and retrieved as necessary by request of authorized parties. MSC Trustgate.com includes sufficient detail in all archived records to show that a Certificate was issued in accordance with this CPS.

5.5.1 Types of Records Archived

MSC Trustgate.com retains the following information in its archives (as such information pertains to MSC Trustgate.com's CA operations):

1. Accreditations of MSC Trustgate.com,
2. CP and CPS versions,
3. Contractual obligations and other agreements concerning the operation of the CA,
4. System and equipment configurations, modifications, and updates,
5. Rejection or acceptance of a certificate request,
6. Certificate issuance, rekey, renewal, and revocation requests,
7. Sufficient identity authentication data to satisfy the identification requirements of Section 3.2, including information about telephone calls made for verification purposes,
8. Any documentation related to the receipt or acceptance of a Certificate or token,
9. Subscriber Agreements,
10. Issued Certificates,
11. A record of certificate re-keys,
12. CRLs for CAs cross-certified with the Federal Bridge CA,
13. Data or applications necessary to verify an archive's contents,
14. Compliance auditor reports,
15. Changes to MSC Trustgate.com's audit parameters,
16. Any attempt to delete or modify audit logs,
17. CA Key generation and destruction,
18. Access to Private Keys for key recovery purposes,
19. Changes to trusted Public Keys,
20. Export of Private Keys,
21. Approval or rejection of a revocation request,
22. Appointment of an individual to a trusted role,
23. Destruction of a cryptographic module,
24. Certificate compromise notifications,
25. Remedial action taken as a result of violations of physical security, and
26. Violations of the CP or CPS.

5.5.2 Retention Period for Archive

MSC Trustgate.com and the RA retains archived data associated Certificates for at least ten (10) years.

5.5.3 Protection of Archive

Archive records are stored at a secure location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction. Archives are not released except as allowed by the PMA or as required by law. MSC Trustgate.com maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If MSC Trustgate.com needs to transfer any media to a different archive site or equipment, MSC Trustgate.com will maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives will occur in a secure manner.

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for Time-stamping of Records

MSC Trustgate.com automatically time-stamps archived records with system time (non-cryptographic method) as they are created. MSC Trustgate.com synchronizes its system time at least every eight hours using a real time value distributed by a recognized UTC(k) laboratory or National Metrology Institute of Malaysia (NMIM).

5.5.6 Archive Collection System (internal or external)

Archive information is collected internally by MSC Trustgate.com.

5.5.7 Procedures to Obtain and Verify Archive Information

Details concerning the creation and storage of archive information are found in section 5.5.4. After receiving a request made for a proper purpose by a Customer, its agent, or a party involved in a dispute over a transaction involving the DigiCert PKI, MSC Trustgate.com may elect to retrieve the information from archival. The integrity of archive information is verified by comparing a hash of the archive disk with the hash originally stored for that disk, as described in Section 5.5.4. MSC Trustgate.com may elect to transmit the relevant information via a secure electronic method or courier, or it may also refuse to provide the information in its discretion and may require prior payment of all costs associated with the data.

5.6 KEY CHANGEOVER

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of a CA Private Key's lifetime, MSC Trustgate.com ceases using the expiring CA Private Key to sign Certificates and that uses the old Private Key only to sign CRLs and OCSP responder Certificates. A new CA signing Key Pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. This key changeover process helps to minimize any adverse effects from CA certificate expiration. The corresponding new CA Public Key Certificate is provided to subscribers and relying parties through the delivery methods detailed in Section 6.1.4.

Where MSC Trustgate.com cross-certified with DigiCert PKI that is in the process of a key rollover, MSC Trustgate.com submit a new CA Public Key (PKCS#10) to DigiCert and obtain new CA Certificate from DigiCert and distributes a new CA cross Certificate following the procedures described above.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

MSC Trustgate.com maintains incident response procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. MSC Trustgate.com reviews, tests, and updates its incident response plans and procedures on at least an annual basis.

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

MSC Trustgate.com will makes regular system backups on weekly basis and maintains backup copies of its CA Private Keys, which are stored in a secure separate location. If MSC Trustgate.com discovers that any of its computing resources, software, or data operations have been compromised, MSC Trustgate.com assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If MSC Trustgate.com determines that a continued operation could pose a significant risk to Relying Parties or Subscribers, MSC Trustgate.com suspends such operation until it determines that the risk is mitigated.

5.7.3 Entity Private Key Compromise Procedures

If MSC Trustgate.com suspects that one of its CA Private Keys or DigiCert Infrastructure has been comprised or lost then MSC Trustgate.com's Key Compromise Response procedures are enacted by the MSC Trustgate.com Security Incident Response Team (VSIRT). This team, which includes Security Manager, Cryptographic Business Operations, Production Services personnel, and other Digicert management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from MSC Trustgate.com executive management. This incident must be reported. The report must detail the cause of the compromise or loss and the measures should be taken to prevent a reoccurrence.

If CA Certificate revocation is required, the following procedures are performed:

- The Certificate's revoked status is communicated to Relying Parties through the MSC Trustgate.com Repository in accordance with Section 4.9.7
- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected DigiCert PKI Participants, and
- The CA will generate a new key pair in accordance with Section 5.6, except where the CA is being terminated in accordance with Section 5.8.

5.7.4 Business Continuity Capabilities after a Disaster

To maintain the integrity of its services, MSC Trustgate.com implements data backup and recovery procedures as part of its Business Continuity Management Plan (BCMP). Stated goals of the BCMP are to ensure that the certificate status services will be only minimally affected by any disaster involving MSC Trustgate.com's primary facility and that MSC Trustgate.com will be capable of maintaining other services or resuming them as quickly as possible following a disaster. MSC Trustgate.com reviews, tests, and updates the BCMP and supporting procedures at least annually.

MSC Trustgate.com's systems are redundantly configured at its primary facility and are mirrored at a separate, geographically diverse location for failover in the event of a disaster. If a disaster causes MSC Trustgate.com's primary CA operations to become inoperative, MSC Trustgate.com will re-initiate its operations at its secondary location giving priority to the provision of certificate status information and time stamping capabilities, if affected.

5.8 CA OR RA TERMINATION

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

1. Provision of notice to parties affected by the termination, such as Subscribers and Relying Parties, informing them of the status of the CA,
2. Handling the cost of such notice,
3. Transfer all responsibilities to a qualified successor entity

If a qualified successor entity does not exist, MSC Trustgate.com will:

1. transfer all relevant records to a government supervisory or legal body;
2. revoke all Certificates that are still un-revoked or un-expired on a date as specified in the notice and publish final CRLs;
3. destroy all Private Keys; and
4. make other necessary arrangements that are in accordance with this CPS.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

All keys must be generated using a FIPS-approved method or equivalent international standard.

MSC Trustgate.com's CA Key Pairs generation is performed by multiple pre-selected, trained and trusted individuals using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys. The cryptographic modules used for key generation meet the requirements of FIPS 140-2 Level 3. Activation of the hardware requires the use of two-factor authentication tokens. MSC Trustgate.com creates auditable evidence during the key generation process to prove that the CPS was followed and role separation was enforced during the key generation process.

The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. For CA keys to be used as publicly trusted Certificates, MSC Trustgate.com requires that an external auditor to witness the generation of or review a recording of the CA keys. For other CA key pair generation ceremonies, an Internal Auditor, external auditor, or independent third party will attends the ceremony, or an external auditor examines the signed and documented record of the key generation ceremony, as allowed by applicable policy.

Generation of RA key pairs is generally performed by the RA using a minimum of FIPS 140-2 Level 2 certified cryptographic module.

Generation of end-user Subscriber key pairs is generally performed by the Subscriber in a manner that is appropriate for the certificate type. The Class 3 Certificates (Hardware-based) must be generated in a medium that prevents exportation or duplication and that meets or exceeds FIPS 140-2 Level 2 certification standards.

6.1.2 Private Key Delivery to Subscriber

If MSC Trustgate.com or an RA generates a key for a Subscriber, then it must deliver the Private Key securely to the Subscriber. Keys may be delivered electronically (such as through secure email or stored in a cloud-based system) or on a hardware cryptographic module. In all cases:

1. Except where escrow/backup services are authorized and permitted, the key generator must not retain access to the Subscriber's Private Key after delivery,
2. The key generator must protect the Private Key from activation, compromise, or modification during the delivery process,
3. The Subscriber must acknowledge receipt of the Private Key(s), typically by having the Subscriber use the related Certificate, and
4. The key generator must deliver the Private Key in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers, including:
    a. For hardware modules, the key generator maintaining accountability for the location and state of the module until the Subscriber accepts possession of it, and
    b. For electronic delivery of Private Keys, the key generator encrypting key material using a cryptographic algorithm and key size at least as strong as the Private Key. The key generator shall deliver activation data using a separate secure channel.

The entity assisting the Subscriber with key generation shall maintain a record of the Subscriber's acknowledgement of receipt of the device containing the Subscriber's Key Pair. A RA providing key delivery services is required to provide a copy of this record to MSC Trustgate.com.

S/MIME email signature certificates shall not be distributed as PKCS#12 packages. S/MIME encryption certificates can be distributed as PKCS#12 packages using secure channels and sufficiently secure passwords sent out of band from the package.

6.1.3 Public Key Delivery to Certificate Issuer

End-user Subscribers and RAs generate Key Pairs and submit the Public Key to MSC Trustgate.com for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Secure Sockets Layer (SSL). Where CA, RA, or end-user Subscriber key pairs are generated by MSC Trustgate.com, this requirement is not applicable.

6.1.4 CA Public Key Delivery to Relying Parties

MSC Trustgate.com's Public Keys are provided to Relying Parties as

- specified in a certificate validation or path discovery policy file;
- trust anchors in commercial browsers and operating system root store; and/or
- roots signed by other CAs.

All accreditation authorities supporting MSC Trustgate.com Certificates and all application software providers are permitted to redistribute MSC Trustgate.com's root anchors.

MSC Trustgate.com generally provides the full certificate chain (including the issuing CA and any CAs in the chain) to the end-user Subscriber upon Certificate issuance. MSC Trustgate.com may also distribute Public Keys that are part of an updated signature Key Pair as a self-signed Certificate, as a new CA Certificate, or in a key roll-over Certificate. Relying Parties may obtain MSC Trustgate.com's CA Certificates via MSC Trustgate.com's web site or by email.

6.1.5 Key Sizes

MSC Trustgate.com generally follows the NIST timelines in using and retiring signature algorithms and key sizes. Accordingly, MSC Trustgate.com had phased out its use of the SHA-1 hash algorithm. Currently, MSC Trustgate.com generates and uses at least the following minimum key sizes, signature algorithms, and hash algorithms for signing Certificates, CRLs, and certificate status server responses:

Key Type	Key Size (bit)	OID	Algorithm hex-encoded bytes
RSA	> 2048	1.2.840.113549.1.1.1 with a NULL parameter	300d06092a864886f70d0101010500
ECDSA	256	1.2.840.10045.2.1	301306072a8648ce3d020106082a8648ce3d030107
ECDSA	384	1.2.840.10045.2.1	301006072a8648ce3d020106052b81040022

MSC Trustgate.com requires end-entity Certificates to contain a key size that is at least 2048 bits for RSA, or 256 bits for elliptic curve algorithms.

MSC Trustgate.com may require higher bit keys in its sole discretion if it is compliant with references in section 1.1 and 1.6.3.

MSC Trustgate.com and Subscribers may fulfill the transmission security requirements under the CP and this CPS using TLS or another protocol that provides similar security, provided the protocol requires at least AES 128 bits or equivalent for the symmetric key and at least 2048-bit RSA or equivalent for the asymmetric keys.

MSC Trustgate.com CAs shall reject a certificate request if the requested Public Key does meet the minimum algorithm key sizes set forth in this section.

6.1.6 Key Usage Purposes (as per X.509 v3 key usage field)

MSC Trustgate.com's Certificates includes key usage extension fields that specify the intended use of the Certificate and technically limit the Certificate's functionality in X.509v3-compliant software.

The use of a specific key is determined by the key usage extension in the X.509 Certificate.

Private Keys corresponding to Root CA Certificates are not 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
4. Certificates for OCSP Response verification

The following is permitted Key Usage for each type of certificate:

Entity	Permitted Key Usage
CA Certificate	keyCertSign, cRLSign
OCSP Responder Certificate	digitalSignature
Subscriber Certificate	assert key usages based on the intended application of the Key Pair and cannot include anyExtendedKeyUsage

MSC Trustgate.com does not issue Certificates with key usage for both signing and encryption. Instead, DigiCert issues Subscribers two Key Pairs—one for key management and one for digital signature and authentication.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

MSC Trustgate.com has implemented a combination of physical, logical, and procedural controls to ensure the security of MSC Trustgate.com private keys. Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Cryptographic Module Standards and Controls

MSC Trustgate.com's cryptographic modules for all of its CA and OCSP responder Key Pairs are validated to the FIPS 140-2 Level 3.

Cryptographic module requirements for subscribers and registration authorities are shown in the table below:

Assurance Level	Subscriber	Registration Authorities
Class 1 Certificates	N/A	FIPS 140-2 Level 2 (Hardware)
Class 2 Certificates	FIPS 140-2 Level 1 (Software or Hardware)	FIPS 140-2 Level 2 (Hardware)
Class 3 Certificates	FIPS 140-2 Level 1 (Software) FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (Hardware)

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

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

The threshold number of shares needed to sign a CA certificate is 3. It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with this CPS.

6.2.3 Private Key Escrow

MSC Trustgate.com does not escrow its CA private keys. Subscribers may not escrow their private signature keys. MSC Trustgate.com may provide escrow services for other types of Certificates in order to provide key recovery as described in section 4.12.1.

6.2.4 Private Key Backup

MSC Trustgate.com's Private Keys are generated and operated inside MSC Trustgate.com’s cryptographic module, which has been evaluated to at least FIPS 140-2 Level 3. When keys are transferred to other media for backup and disaster recovery purposes, the keys are transferred and stored in an encrypted form. MSC Trustgate.com's CA Key Pairs are backed up by multiple trusted individuals using a cryptographic hardware device as part of scripted and video-recorded key backup process.

MSC Trustgate.com may provide backup services for Private Keys that are not required to be kept on a hardware device. Access to back up Certificates is protected in a manner that only the

Subscriber can control the Private Key. Backed up keys are never stored in a plain text form outside of the cryptographic module.

6.2.5 Private Key Archival

MSC Trustgate.com does not archive Private Keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

All keys must be generated by and in a cryptographic module. Private Keys are exported from the cryptographic module into backup tokens only for HSM transfer, offline storage, and backup purposes. The Private Keys are encrypted when transferred out of the module and never exist in plaintext form. When transported between cryptographic modules, MSC Trustgate.com encrypts the Private Key and protects the keys used for encryption from disclosure. Private Keys used to encrypt backups are securely stored and require two-person access. If MSC Trustgate.com 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 MSC Trustgate.com will revoke all certificates that include the Public Key corresponding to the communicated Private Key.

If MSC Trustgate.com pre-generates private keys and transfers them into a hardware token, for example transferring generated end-user Subscriber private keys into a smart card, it will securely transfer such private keys into the token to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.2.7 Private Key Storage on Cryptographic Module

MSC Trustgate.com's Private Keys are generated and stored inside MSC Trustgate.com's cryptographic module, which has been evaluated to at least FIPS 140-2 Level 3. Root Private Keys are stored offline in cryptographic modules or backup tokens as described above in Sections 6.2.2, 6.2.4, and 6.2.6.

6.2.8 Method of Activating Private Keys

MSC Trustgate.com's Private Keys are activated according to the specifications of the cryptographic module manufacturer. Activation data entry is protected from disclosure.

Subscribers are solely responsible for protecting their Private Keys in a manner commensurate with the Certificate type. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key. Subscribers should also take commercially reasonable measures for the physical protection of their workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization. When deactivated, private keys shall be kept in encrypted form only and secured. At a minimum, Subscribers are required to authenticate themselves to the cryptographic module before activating their Private Keys. See also Section 6.4.

6.2.9 Method of Deactivating Private Keys

MSC Trustgate.com's Private Keys are deactivated via logout procedures on the applicable HSM device when not in use. MSC Trustgate.com prevent unauthorized access to any activated cryptographic modules.

Subscribers should deactivate their Private Keys via logout and removal procedures when not in use.

6.2.10 Method of Destroying Private Keys

MSC Trustgate.com personnel, acting in trusted roles, destroy CA, RA, and status server Private Keys when no longer needed. Subscribers shall destroy their Private Keys when the corresponding Certificate is revoked or expired or if the Private Key is no longer needed.

MSC Trustgate.com may destroy a Private Key by deleting it from all known storage partitions. MSC Trustgate.com also zeroizes the HSM device and associated backup tokens according to the specifications of the hardware manufacturer. This reinitializes the device and overwrites the data with binary zeros. If the zeroization or re-initialization procedure fails, MSC Trustgate.com destroy CA private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

MSC Trustgate.com archives copies of Public Keys in accordance with Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

MSC Trustgate.com Certificates have maximum validity periods of:

Type	Private Key Use[9]	Certificate Term
Publicly Trusted Root CAs	No stipulation	25 years
Publicly Trusted Sub CAs / Issuer CAs	No stipulation	15 years
CRL and OCSP responder signing	3 years	31 days
Time Stamping Authority	15 months	135 months
All Subscriber Certificates	36 months	36 months

Participants shall cease all use of their key pairs after their usage periods have expired. Relying parties may still validate signatures generated with these keys after expiration of the Certificate.

MSC Trustgate.com may voluntarily retire its CA Private Keys before the periods listed above to accommodate key changeover processes. MSC Trustgate.com does not issue Subscriber Certificates with an expiration date that exceeds the Issuer CA's public key term stated in the table above or that exceeds the routine re-key identification requirements specified in Section 3.1.1.

[9] CA Private Keys may continue to be used to sign CRLs and OCSP responses

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

MSC Trustgate.com activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. This method has been evaluated as meeting the requirements of FIPS 140-2 Level 3. The cryptographic hardware is held under two-person control as explained in Section 5.2.2 and elsewhere in this CPS. MSC Trustgate.com will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

All MSC Trustgate.com personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords that meet the requirements specified by the CAB Forums Network Security Requirements. If MSC Trustgate.com uses passwords as activation data for a signing key, MSC Trustgate.com will change the activation data change upon rekey of the CA Certificate.

6.4.2 Activation Data Protection

MSC Trustgate.com protects data that used to unlock Private Keys from disclosure using a combination of cryptographic and physical access control mechanisms. Protection mechanisms include keeping activation mechanisms secure using role-based physical control. All MSC Trustgate.com personnel are instructed to memorize and not to write down their password or share it with any another individual. MSC Trustgate.com locks accounts used to access secure CA processes if a certain number of failed password attempts occur as specified in the internal security policies, procedures, and relevant requirements in references listed in Section 1.6.3.

End-user Subscribers shall protect the activation data for their private keys, if any, to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.4.3 Other Aspects of Activation Data

Not applicable.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

MSC Trustgate.com secures its CA systems and authenticates and protects communications between its systems and trusted roles. MSC Trustgate.com's CA servers and support-and-vetting workstations run on trustworthy systems that are configured and hardened using industry best practices. All CA systems are scanned for malicious code and protected against spyware and viruses.

RAs must ensure that the systems maintaining RA software and data files are trustworthy systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under Section 5.4.1.

RAs must logically separate access to these systems and this information from other components. This separation prevents access except through defined processes. RAs must use firewalls to protect the network from internal and external intrusion and limit the nature and source of activities that may access such systems and information. RAs must require the use of passwords with a minimum character length and a combination of alphanumeric and special characters.

MSC Trustgate.com's CA systems are configured to:

1. authenticate the identity of users before permitting access to the system or applications,
2. manage the privileges of users and limit users to their assigned roles,
3. generate and archive audit records for all transactions,
4. enforce domain integrity boundaries for security critical processes, and
5. support recovery from key or system failure.

All Certificate Status Servers:

1. authenticate the identity of users before permitting access to the system or applications,
2. manage privileges to limit users to their assigned roles,
3. enforce domain integrity boundaries for security critical processes, and
4. support recovery from key or system failure.

MSC Trustgate.com enforces multi-factor authentication on any account capable of directly causing Certificate issuance.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

MSC Trustgate.com uses only:

1. CA systems software that is provided by DigiCert. DigiCert shall has its own mechanisms in place to control and monitor the acquisition and development of the CA systems and shall be complied with the CP.
2. All hardware and software are shipped under standard conditions to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering
3. Hardware and software that is dedicated only to performing the CA functions for CA operation purposes.

Updates of equipment and software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel. All hardware and software essential to MSC Trustgate.com's operations is scanned for malicious code on first use and periodically thereafter. MSC Trustgate.com does not install software that are not part of the CA's operation

6.6.2 Security Management Controls

MSC Trustgate.com has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. MSC Trustgate.com creates a hash of all software packages and MSC Trustgate.com software updates. This hash is used to verify the integrity of such software manually. Upon installation and periodically thereafter, MSC Trustgate.com validates the integrity of its CA systems.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 NETWORK SECURITY CONTROLS

MSC Trustgate.com performs all its CA and RA functions using networks secured in accordance with the standards documented in the DigiCert CP to prevent unauthorized access and other malicious activity. MSC Trustgate.com protects its communications of sensitive information through the use of point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

MSC Trustgate.com documents and controls the configuration of its systems, including any upgrades or modifications made.

MSC Trustgate.com's CA system is connected to one internal network and is protected by firewalls and Network Address Translation for all internal IP addresses (e.g., 192.168.x.x). MSC Trustgate.com's customer support and vetting workstations are also protected by firewall(s) and only use internal IP addresses. Root Keys are kept offline and brought online only when necessary to sign Certificate-issuing subordinate CAs, OCSP Responder Certificates, or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems.

MSC Trustgate.com's security policy is to block all ports and protocols and open only ports necessary to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. MSC Trustgate.com's network

configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.

6.8 TIME-STAMPING

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

The system time on DigiCert's computers is updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every eight hours. All times are traceable to a real time value distributed by a UTC(k) laboratory or National Metrology Institute of Malaysia (NMIM) and are updated when a leap second occurs as notified by the appropriate body.

7 CERTIFICATE, CRL, AND OCSP PROFILES

MSC Trustgate.com uses the ITU X.509, version 3 standard to construct digital Certificates for use within the DigiCert PKI. MSC Trustgate.com adds certain certificate extensions to the basic certificate structure for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. DigiCert generates.

At a minimum, X.509 Certificates shall contain the basic fields and indicated prescribed values or value constraints in table below as well as certificate extension described in Section 7.1.2:

Field	Value or Value Constraint
Serial Number	Non-sequential Certificate serial numbers (positive numbers greater than zero) that contain at least 64 bits of output from a CSPRNG
Signature Algorithm	Object Identifier of the algorithm used to sign the certificate
Issuer DN	See Section 7.1.4
Valid From	Universal Coordinate Time base. Synchronized with National Metrology Institute of Malaysia (NMIM). Encoded in accordance with RFC5280.
Valid To	Universal Coordinate Time base. Synchronized with National Metrology Institute of Malaysia (NMIM). Encoded in accordance with RFC5280.
Subject DN	See Section 7.1.4
Subject Public Key	Encoded in accordance with RFC 5280
Signature	Generated and encoded in accordance with RFC 5280

7.1 CERTIFICATE PROFILE

7.1.1 Version Number(s)

All Certificates are X.509 version 3 Certificates.

7.1.2 Certificate Extensions

MSC Trustgate.com populates X.509 Version 3 DigiCert PKI Certificates with the extensions required by Table below. Private extensions are permissible, but the use of private extensions is not warranted under this CP and the applicable CPS unless specifically included by reference. Effective 1 April 2020, the following certificate extension will be used:

7.1.2.1 Root CA Certificate

Certificate Extension	Criticallity	Value or Value Constraint
basicConstraints	TRUE	MUST be present , cA MUST be TRUE, pathLenConstraint SHOULD not be present
keyUsage	TRUE	MUST be present, Bit positions for keyCertSign and cRLSign MUST be SET, Bit positions for digitalSignature MUST be SET if it is used for signing OCSP Responder
certificatePolicies	FALSE	SHOULD NOT be present
extKeyUsage	FALSE	SHOULD NOT be present
subjectKeyIdentifier	FALSE	MAY be present. Composed of the 160-bit SHA-1 hash of the public key of the Certificate.

7.1.2.2 Subordinate/Intermediate/Issuer CA Certificate

Certificate Extension	Criticallity	Value or Value Constraint
basicConstraints	TRUE	MUST be present , cA MUST be TRUE, pathLenConstraint MAY be present
keyUsage	TRUE	MUST be present, Bit positions for keyCertSign and cRLSign MUST be SET, Bit positions for digitalSignature MUST be SET if it is used for signing OCSP Responder
certificatePolicies	FALSE	MUST be present, policyIdentifier (required), policyQualifiers:policyQualifierId (optional) policyQualifiers:qualifier:cPSuri (optional)
cRLDistributionPoints	FALSE	MUST be present, contains HTTP URL of the CA's CRL service
authorityInfoAccess	FALSE	MAY be present, contains HTTP URL of the Issuing CA's OCSP responder, SHOULD also contain the HTTP URL of the Issuing CA's certificate

Certificate Extension	Criticallity	Value or Value Constraint
extKeyUsage	FALSE	MAY be present. If set: • aligning to Application Software Supplier granted trust bits and private PKI use cases • must not contain the anyExtendedKeyUsage KeyPurposeId • MUST not include both the id-kp-serverAuth and id-kp-emailProtection KeyPurposeIds in the same certificate
nameConstraints	TRUE	MUST be present if id-kp-emailProtection KeyPurposeIds is included. Contains verified domain to be used for S/MIME certificate
subjectKeyIdentifier	FALSE	MAY be present. Composed of the 160-bit SHA-1 hash of the public key of the Certificate.
authorityKeyIdentifier	FALSE	MAY be present. When the certificate issuer contains the Subject Key Identifier extension, the Authority Key Identifier is composed of the 160-bit SHA-1 hash of the public key of the CA issuing the Certificate. Otherwise the Authority Key Identifier extension includes the issuing CA's subject distinguished name and serial number.

7.1.2.3 Subscriber Certificate

Certificate Extension	Criticallity	Value or Value Constraint
basicConstraints	TRUE	MAY be present. cA MUST NOT be TRUE
keyUsage	TRUE[10]	MAY be present. Bit positions for keyCertSign and cRLSign MUST NOT be set.
certificatePolicies	FALSE	MUST be present, policyIdentifier (required), policyQualifiers:policyQualifierId (optional) policyQualifiers:qualifier:cPSuri (optional)
cRLDistributionPoints	FALSE	MAY be present, contains HTTP URL of the CA's CRL service
authorityInfoAccess	FALSE	MAY be present, contains HTTP URL of the Issuing CA's OCSP responder, SHOULD also contain the HTTP URL of the Issuing CA's certificate

[10] MAY also set to FALSE

Certificate Extension	Criticallity	Value or Value Constraint
extKeyUsage	FALSE	MUST be present. • aligning to Application Software Supplier granted trust bits and private PKI use cases • must not contain the anyExtendedKeyUsage KeyPurposeId • MUST NOT include both the id-kp-serverAuth and id-kp-emailProtection KeyPurposeIds in the same certificate
subjectAltName	FALSE	MUST be present if id-kp-emailProtection KeyPurposeIds is included. Populated in accordance with RFC 5280 with the authenticated value in the Email field of the subject DN (domain name). The SubjectAltName extension may contain additional authenticated domain names.
subjectKeyIdentifier	FALSE	Composed of the 160-bit SHA-1 hash of the public key of the Certificate.
authorityKeyIdentifier	FALSE	When the certificate issuer contains the Subject Key Identifier extension, the Authority Key Identifier is composed of the 160-bit SHA-1 hash of the public key of the CA issuing the Certificate. Otherwise the Authority Key Identifier extension includes the issuing CA's subject distinguished name and serial number.

7.1.3 Algorithm Object Identifiers

MSC Trustgate.com Certificates are signed using one of the following algorithms:

Algorithm	OID
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-sha256	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 2}
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 3}

Certificate signatures produced using these algorithms shall comply with RFC 3279.

MSC Trustgate.com does not currently sign Certificates using RSA with PSS padding.

MSC Trustgate.com and Subscribers may generate Key Pairs using the following:

Algorithm	OID
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
ecdsa-with-sha256	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) id-publicKeyType(2) 1}

Elliptic curve Public Keys submitted to MSC Trustgate.com for inclusion in end entity Certificates should all be based on NIST "Suite B" curves.

7.1.4 Name Forms

Each Certificate includes a unique serial number that is never reused. MSC Trustgate.com has a process that limits information in OU fields that has not been verified in accordance with Section 3.

For CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.

The content of the Certificate Issuer Distinguished Name field matches the Subject DN of the Issuer CA to support name chaining as specified in RFC 5280, section 4.1.2.4. Certificates are populated with the Issuer Name and Subject Distinguished Name required under Section 3.1.1.

In addition, MSC Trustgate.com may include within end-user Subscriber Certificates an additional Organizational Unit field that contains a notice stating that the terms of use of the Certificate are set forth in a URL which is a pointer to the applicable Relying Party Agreement. Exceptions to the foregoing requirement are permitted only when space, formatting, or interoperability limitations within Certificates make such an Organizational Unit impossible to use in conjunction with the application for which the Certificates are intended, or if a pointer to the applicable Relying Party Agreement is included in the policy extension of the certificate.

7.1.5 Name Constraints

MSC Trustgate.com may include name constraints in the nameConstraints field when appropriate.

7.1.5.1 Name-Constrained serverAuth CAs

Not applicable.

7.1.5.2 Name-Constrained emailProtection CAs

If the technically constrained Subordinate CA certificate includes the id-kp-emailProtection extended key usage, it also includes the Name Constraints X.509v3 extension with constraints on rfc822Name, with at least one name in permittedSubtrees, each such name having its ownership validated according to section 3.2.2.4 of the Baseline Requirements.

7.1.6 Certificate Policy Object Identifier

An object identifier (OID) is a unique number that identifies an object or policy. The OIDs used by MSC Trustgate.com are listed in Section 1.2.

7.1.7 Usage of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

MSC Trustgate.com generally populates X.509 Version 3 Digicert PKI Certificates with a policy qualifier within the Certificate Policies extension. Generally, such Certificates contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the MSC Trustgate.com CPS. In addition, some Certificates contain a User Notice Qualifier which points to the applicable Relying Party Agreement.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL PROFILE

7.2.1 Version number(s)

MSC Trustgate.com issues version 2 CRLs that contain the following fields:

Field	Value
Version	2
Signature Algorithm	Algorithm used to sign the CRL in accordance with RFC 3279.
Issuer	Issuer Entity who has signed and issued the CRL.
Effective Date	Issue date of the CRL. CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued. CRL issuance frequency is in accordance with Section 4.9.7.
Revoked Certificates	Revoked Certificates Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.
Issuer's Signature	[Signature]

7.2.2 CRL and CRL Entry Extensions

CRLs have the following extensions:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the Certificate
Invalidity Date	Optional. Date in UTC format
Reason Code	Optional. Reason for revocation

7.3 OCSP PROFILE

MSC Trustgate.com's operate an OCSP in accordance with RFC 6960.

7.3.1 Version Number(s)

MSC Trustgate.com's OCSP responders conform to version 1 of RFC 6960.

7.3.2 OCSP Extensions

Not applicable.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest versions of the WebTrust Programs for Certification Authorities as required by the Mozilla Root Store policy and other programs listed in section 1.1 and 1.6.3.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

MSC Trustgate.com receives an annual period in time audit by an independent external auditor to assess MSC Trustgate.com's compliance with this CPS, referenced requirements, any applicable CPs, and the WebTrust for CA programs criteria. The audit covers MSC Trustgate.com's RA systems, Sub CAs, and OCSP Responders.

Audits are conducted over unbroken sequences of audit periods with each period no longer than one year duration.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

WebTrust auditors must meet the requirements of Section 8.2 of the CA/Browser Baseline Requirements. The auditors must also been accredited as qualified auditor by the Malaysian Communications & Multimedia Commission (MCMC). The list of qualified auditors can be found here: https://www.mcmc.gov.my/en/sectors/digital-signature/list-of-qualified-auditors.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

WebTrust audits of MSC Trustgate.com are performed by a public accounting firm that is independent of MSC Trustgate.com.

8.4 TOPICS COVERED BY ASSESSMENT

The audit covers MSC Trustgate.com's business practices disclosure, the integrity of MSC Trustgate.com's PKI operations, and MSC Trustgate.com's compliance with this CPS and referenced requirements. The audit verifies that MSC Trustgate.com is compliant with the CP, this CPS, and any MOA between it and any other PKI.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports a material non-compliance with the applicable law, this CPS, the CP, or any other contractual obligations related to MSC Trustgate.com's services, then:

1. the auditor will document the discrepancy,
2. the auditor will promptly notify MSC Trustgate.com, and
3. MSC Trustgate.com will develop a plan to cure the noncompliance.

MSC Trustgate.com will submit the plan to the Management for approval and to any third party that MSC Trustgate.com is legally obligated to satisfy. The MSC Trustgate.com Management may require additional action if necessary to rectify any significant issues created by the non-compliance, including requiring revocation of affected Certificates. MSC Trustgate.com is entitled to suspend and/or terminate of services through revocation or other actions as deemed by the MSC Trustgate.com Management to address the non-compliant Issuer CA.

8.6 COMMUNICATION OF RESULTS

The results of each audit are reported to the Management and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results. Copies of MSC Trustgate.com's WebTrust for CAs audit reports can be found at: https://www.msctrustgate.com. On an annual basis and within three months of completion, MSC Trustgate.com submits copies of relevant audit compliance reports to various parties, such as Malaysian Communications and Multimedia Commission (MCMC), DigiCert, etc. In the event of a delay greater than three (3) months, MSC Trustgate.com shall provide an explanatory letter signed by the Qualified Auditor.

8.7 SELF-AUDITS

On at least a quarterly basis, MSC Trustgate.com performs regular internal audits against a randomly selected sample of Certificates issued since the last internal audit. Internal audit will be at the discretion of MSC Trustgate.com to gain reasonable assurance of compliance to applicable root program requirements.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

MSC Trustgate.com is entitled to charge end-user Subscribers for the issuance, management, and renewal of Certificates.

9.1.2 Certificate Access Fees

MSC Trustgate.com does not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

MSC Trustgate.com does not charge a fee as a condition of making the CRLs required by this CP available in a repository or otherwise available to Relying Parties. MSC Trustgate.com is, however, entitled to charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services.

MSC Trustgate.com does not permit access to revocation information, Certificate status information, or time stamping in their repositories by third parties that provide products or services that utilize such Certificate status information without MSC Trustgate.com's prior express written consent.

9.1.4 Fees for Other Services

MSC Trustgate.com does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with the entity holding the copyright to the document.

9.1.5 Refund Policy

Within MSC Trustgate.com's Sub-domain, the following refund policy is in effect:

MSC Trustgate.com adheres to, and stands behind, rigorous practices and policies in undertaking certification operations and in issuing certificates. Nevertheless, if for any reason a subscriber is not completely satisfied with the certificate issued to him, her, or it, the subscriber may request that MSC Trustgate.com revoke the certificate within thirty (30) days of issuance and provide the subscriber with a refund. Following the initial thirty (30) day period, a subscriber may request that MSC Trustgate.com revoke the certificate and provide a refund if MSC Trustgate.com has breached a warranty or other material obligation under this CPS relating to the subscriber or the subscriber's certificate.

After MSC Trustgate.com revokes the subscriber's certificate, MSC Trustgate.com will promptly credit the subscriber's credit card account (if the certificate was paid for via credit card) or otherwise reimburse the subscriber via cheque or any other agreed method, for the full amount of the applicable fees paid for the certificate. To request a refund, please call customer service at +603 8318 1800. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to subscribers.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

MSC Trustgate.com maintains Professional Indemnity Insurance with a policy limit of at least 2 million Malaysia Ringgit (RM2,000,000.00) in coverage.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

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

- CA application records, whether approved or disapproved,
- Certificate Application records,
- Transactional records (both full records and the audit trail of transactions),
- Audit trail records created or retained by Digicert or a Customer,
- Audit reports created by MSC Trustgate.com or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public),
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of MSC Trustgate.com hardware and software and the administration of Certificate services and designated enrollment services.

9.3.2 Information Not Within the Scope of Confidential Information

Certificates, Certificate revocation and other status information, MSC Trustgate.com repositories and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under Section 9.3.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

MSC Trustgate.com secures private information from compromise and disclosure to the third parties.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

MSC Trustgate.com has implemented a privacy policy, which is sited at: https://www.msctrustgate.com/privacy-notice

9.4.2 Information Treated as Private

Any information about the Subscribers that is not publicly available through the content of the issued certificate, certificate directory and online CRLs is treated as private.

9.4.3 Information Not Deemed Private

Subject to the local laws, all information made public in a certificate is deemed not private.

9.4.4 Responsibility to Protect Private Information

DigiCert PKI participants receiving private information shall secure it from being compromise and disclosure to third parties and shall comply with all local privacy laws in their jurisdiction.

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

MSC Trustgate.com shall be entitled to disclose Confidential/Private Information if, in good faith, MSC Trustgate.com believes that:

- disclosure is necessary in response to subpoenas and search warrants.
- disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

This section is subject to applicable privacy laws.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 INTELLECTUAL PROPERTY RIGHTS

The allocation of Intellectual Property Rights among MSC Trustgate.com Sub-domain Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such MSC Trustgate.com Sub-domain Participants. The following subsections of Section 9.5 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

9.5.1 Property Rights in Certificates and Revocation Information

CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue. MSC Trustgate.com and Customers grant permission to reproduce and distribute Certificates on a non-exclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate. MSC Trustgate.com and Customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL Usage Agreement, Relying Party Agreement, or any other applicable agreements.

9.5.2 Property Rights in the CPS

DigiCert PKI Participants acknowledge that MSC Trustgate.com retains all Intellectual Property Rights in and to this CPS.

9.5.3 Property Rights in Names

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

9.5.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CAs and end-user Subscribers are the property of the CAs and end-user Subscribers that are the respective Subjects of these Certificates, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs.

Without limiting the generality of the foregoing, Digicert's Root public keys and the Root Certificates containing them, including all PCA public keys and self-signed Certificates, are the property of Digicert. Digicert licenses software and hardware manufacturers to reproduce such root Certificates to place copies in trustworthy hardware devices or software. Finally, Secret Shares of a CA's private key is the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares even though they cannot obtain physical possession of the those shares or the CA from Digicert.

9.5.5 Violation of Property Rights

MSC Trustgate.com shall not knowingly violate the intellectual property rights of any third party.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

MSC Trustgate.com warrants that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services and use of a repository conform to the applicable CPS in all material aspects.

Subscriber Agreements may include additional representations and warranties.

9.6.2 RA Representations and Warranties

RAs warrant that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services (when applicable) and use of a repository conform to the applicable CPS in all material aspects.

Subscriber Agreements may include additional representations and warranties.

9.6.3 Subscriber Representations and Warranties

Subscribers warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- Their private key is protected and that no unauthorized person has ever had access to the Subscriber's private key,
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
- All information supplied by the Subscriber and contained in the Certificate is true,
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS, and
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

Subscriber Agreements may include additional representations and warranties.

9.6.4 Relying Party Representations and Warranties

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

Relying Party Agreements may include additional representations and warranties.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall disclaim MSC Trustgate.com's possible warranties, including any warranty of merchantability or fitness for a particular purpose.

9.8 LIMITATIONS OF LIABILITY

To the extent MSC Trustgate.com has issued and managed the Certificate(s) at issue in compliance with the DigiCert Certificate Policy and the MSC Trustgate.com Certification Practice Statement, MSC Trustgate.com shall have no liability to the Subscriber, any Relying Party, or any other third parties for any damages or losses suffered as a result of the use or reliance on such Certificate(s). To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall limit MSC Trustgate.com's liability. Limitations of liability shall include an exclusion of indirect, special, incidental, and consequential damages. They shall also include the following liability caps limiting MSC Trustgate.com's damages concerning a specific Certificate:

Class	Liability Caps
Class 1	Ringgit Malaysia Five Hundred (RM500.00)
Class 2	Ringgit Malaysia Twenty-Five Thousand (RM25,000.00)
Class 3	Ringgit Malaysia Four Hundred Thousand (RM400,000)

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber agreements.

The liability (and/or limitation thereof) of enterprise RAs and the applicable CA shall be set out in the agreement(s) between them.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.9 INDEMNITIES

9.9.1 Indemnification by MSC Trustgate.com

To the extent permitted by applicable law, MSC Trustgate.com are required to indemnify DigiCert for any violation of this CP. MSC Trustgate.com may 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 MSC Trustgate.com, depending on the cause of action or legal theory involved which will be access by Legal Team appointed by MSC Trustgate.

This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the MSC Trustgate.com 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 revocation status is currently available from MSC Trustgate.com online, and the application software failed to check such status or ignored an indication of revoked status).

9.9.2 Indemnification by Subscribers

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

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

The applicable Subscriber Agreement may include additional indemnity obligations.

9.9.3 Indemnification by Relying Parties

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

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

The applicable Relying Party Agreement shall include additional indemnity obligations.

9.10 TERM AND TERMINATION

9.10.1 Term

The CPS becomes effective upon publication in the MSC Trustgate.com repository. Amendments to this CPS become effective upon publication in the MSC Trustgate.com repository.

9.10.2 Termination

This CPS will be amended from time to time and shall remain in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

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

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

MSC Trustgate.com accepts notices related to this CPS at the locations specified in Section 2.2. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from MSC Trustgate.com . If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 2.2 using either a courier service that confirms delivery or via registered mail with postage prepaid and return receipt requested. MSC Trustgate.com may allow other forms of notice in its Subscriber Agreements.

MSC Trustgate.com will notify DigiCert and Mozilla if:

1. Ownership or control of the CA certificates changes;
2. An organization other than the CA obtains control of an unconstrained intermediate certificate (as defined in section 5.3.2 of the Mozilla Root Store policy) that directly or transitively chains to DigiCert's included certificate(s);
3. Ownership or control of MSC Trustgate.com's operations changes; or
4. There is a material change in MSC Trustgate.com's operations (e.g., when the cryptographic hardware related to a certificate in Mozilla's root store is consequently moved from one secure location to another).

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

This CPS is reviewed annually. Amendments to this CPS may be made by the MSC Trustgate.com Policy Management Authority (PMA). Amendments shall either be in the form of a document containing an amended form of the CPS or an update. Amended versions or updates shall be linked to the Practices Updates and Notices section of the MSC Trustgate.com Repository located at: https://www.msctrustgate.com/repository.htm. The updates will supersede any designated or conflicting provisions of the referenced version of the CPS. The PMA shall determine whether the changes to the CPS require a change in the Certificate policy object identifiers of the Certificate policies corresponding to each Class of Certificate.

9.12.2 Notification Mechanism and Period

MSC Trustgate.com and the PMA reserve the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The PMA's decision to designate amendments as material or non-material shall be within the PMA's sole discretion Proposed amendments to the CPS shall appear in the Practices Updates and Notices section of the MSC Trustgate.com Repository, which is located at: https://www.msctrustgate.com/repository.htm.

Notwithstanding anything in the CPS to the contrary, if the PMA believes that the material amendments to the CPS are necessary immediately to stop or prevent a breach of the security of the Digicert or any portion of it, MSC Trustgate.com and the PMA shall be entitled to make such amendments by publication in the MSC Trustgate.com Repository. Such amendments will be effective immediately upon publication. Within a reasonable time after publication, MSC Trustgate.com shall provide notice to of such amendments to MSC Trustgate.com sub-domain participants.

9.12.3 Circumstances under which OID Must Be Changed

If the PMA determines that a change is necessary in the object identifier corresponding to a Certificate policy, the amendment shall contain new object identifiers for the Certificate policies corresponding to each Class of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.

9.13 DISPUTE RESOLUTION PROVISIONS

9.13.1 Disputes among DigiCert, Affiliates, and Customers

Disputes among MSC Trustgate.com sub-domain participants shall be resolved pursuant to provisions in the applicable agreements among the parties or if it is silence on it to the extent permitted by law, before you may invoke any dispute resolution mechanism with respect to a dispute involving any aspect of this CPS, you shall notify MSC Trustgate.com, and any other party to the dispute for the purpose of seeking dispute resolution. If the dispute is not resolved within sixty (60) days after the initial notice, then a party may proceed by referring such dispute to arbitration in Kuala Lumpur, Malaysia in accordance with the Rules of Asian International Arbitration Centre (AIAC) for the time being in force. The Tribunal shall consist one (1) arbitrator to be appointed by the Chairman of AIAC. The decision of the arbitration shall be final and binding on all parties. Nothing in this Subscriber Agreement will be deemed as preventing either party from seeking injunctive relief (or any other provisional remedy) from any court having jurisdiction over the parties and the subject matter of this dispute as is necessary to protect either party's name, proprietary information, trade secret, know-how, or, or any other intellectual property rights. The arbitration shall be held at the AIAC using the arbitration rules of the center and utilizing the facilities and system available at that center. The arbitration proceedings shall be conducted in the Bahasa Malaysia and/or English language. Each party shall bear its own costs of the arbitration proceedings.

9.13.2 Disputes with End-User Subscribers or Relying Parties

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. Disputes involving MSC Trustgate.com require an initial negotiation period of sixty (60) days followed by litigation in court of Malaysia, in the case of claimants who are Malaysia residents or, in the case of all other claimants, arbitration administered by the Asian International Arbitration Centre (AIAC) in Kuala Lumpur as per Rules of AIAC.

9.14 GOVERNING LAW

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

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

9.15 COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to applicable National, State, Local and Foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. MSC Trustgate.com licenses its CAs in each jurisdiction that it operates where licensing is required by the law of such jurisdiction for the issuance of Certificates.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

Not applicable.

9.16.2 Assignment

Not applicable.

9.16.3 Severability

In the event that a clause or provision of this CPS is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CPS shall remain valid.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force Majeure

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting Digicert.

9.17 OTHER PROVISIONS

No stipulation.