TRUSTGATE
SECURE TRANSACTION. TRUSTED BUSINESS

MSC Trustgate
Certificate Policy/ Certification Practice Statement

Version 6.1.2

28 August 2025

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 Certificate Policy/ Certification Practice Statement

Trademark Notices

MSC Trustgate.com Sdn. Bhd.
Suite 2-9, Level 2, CBD Perdana
Jalan Perdana, 63000 Cyberjaya
Selangor Darul Ehsan, Malaysia
Attn : CA Operation & Compliance Manager Email : compliance@msctrustgate.com
Tel : +603 8318 1800 Fax : +603 8319 1800

Revision History

#	Date	Changes	Version
1	29 March 2019	This version replaces the MSC Trustgate.com CPS version 4.3.2 30 January 2019. It includes OID of MSC Trustgate.com CA.	4.3.3
2	23 August 2019	To amend Class 1 require Applicant to demonstrate control of his/her email address or mobile number. To amend the certificate validity period of DV, OV, and AATL to 825 days in Section 6.3.2	4.3.4
3	14 January 2021	This version adapts the 4.3.4 MSC Trustgate.com CPS and changes the format according to include all RFC 3647 and update with the latest CA/B Forum document (version 1.7.3 October 2020)	5.0
4	4 April 2022	This version: 1. Included validation for Onion Domain Certificate in section 3.2.2.4 2. Included the period of certificate status checking in CRL 3. Included OCSP responses period for Code Signing and Timestamp Certificate 4. Inserted Repository MUST NOT include entries that indicate certificate suspended in section 4.9.13 5. Changed the Re-Verification Required for Document Signing Certificate to At Least every six years. 6. Updated the Certificate Extension Section 7.1.2 according to CA/B Forum document 7. Added the CA issuing Timestamp Certificate and Timestamp Certificate extension in section 7.1.2 8. Inserted section 7.1.3.2, 7.1.3.2.1 and 7.1.3.2.2 to be standardized with CA/B Forum document 9. Added the Entries in the dNSName do not contain underscore characters in section 7.1.4 10. Inserted Reserved Certificate Policy Identifiers 11. Inserted section 7.1.6.1, 7.1.6.2, 7.1.6.3 and 7.1.6.4 to be standardized with CA/B Forum document	5.1
5	29 April 2022	This version: • Includes the new root, bridge, and intermediate CA certificates in section 1.2 • Amended CA representations and warranties in section 9.6.1 • Inserted RA Liability in section 9.8.2 • Amended Indemnities in section 9.9 • Amended Governing and Compliance Law in section 9.14 and 9.15	5.2
6	20 March 2023	• This version amended section 4.9.9 On-line revocation/status checking availability • Removed the OU attribute in subject DN in section 3.1.1	5.3

#	Date	Changes	Version
7	15 August 2023	This version: • Added in new policies, guidelines, and requirements in section 1.1 • Inserted new requirement for S/MIME and SSL in section 1.3.2 • Inserted High Risk Certificate Request definition in section 1.6 • Updated the version of Mozilla Root Store to Mozilla Root Store Policy v.2.8.1 • Inserted SSL/TLS Certificates websites for user agent verification in section 2.2 • Ammended Validation of Domain Authorization or Control in section 3.2.2.4 • Amended Agreed-Upon Change to Website in section 3.2.2.4.6 • Amended Validation of authority in section 3.2.5 • Amended Identification and authentication for routine re-key in section 3.3.1 • Added EV certificate authentication process in section 4.2.1 • Updated the certificate policy in section 7.1.2 • Updated Name forms in section 7.1.4	5.4
8	13 June 2024	• Added Law/Policy/Guidelines requirements in section 1.1 • Updated document name and identification table in section 1.2 • Updated the root certificate in section 1.2.1 • Updated the intermediate certificate in section 1.2.3 • Added CA high-level diagram and explanations in section 1.3 • Added PKI participants (Trusted Agent, Authorized Personnel, and PKI-Based ID Provider) in section 1.3.5 (Other Participants) • Updated an appropriate certificate usage in section 1.4.1 • Updated definitions and acronyms in section 1.6 • Updated identity and authentication in section 3. Sub-section updates: 3.1.1, 3.1.3, 3.2.5, 3.2.1, 3.2.2, and 3.2.5 • Changed section 4.1.3 "RA Certificates" to section 4.1.2.2 titled "RA/TA/AP Certificates" and added TA and AP in the explanation. • Updated key size in section 6.1.5 • Amended Cryptographic module standards and controls in section 6.2.1 • Added requirements of schedule three of DSR 1998 in section 6.8 • Updated section 7 – Certificate, CRL and OCSP Profile • Amended extKeyUsage table in section 7.1.2.7 • Amended Self-Audits in section 8.7 • Updated certificate issuance and renewal fees in section 9.1.1 • Amended Fees for other services in section 9.1.4 • Updated CA Liability in section 9.8.1 • Added Appendix A – Registration Scheme • Added High Assurance Certificates OID in section 1.2 • Added Validation of High Assurance Certificate in section 3.2.3.2	6.0
9	31 July 2024	• Changed the effective date of certificate OID for MyGPKI, AATL and MyDigital ID.	6.0.1

#	Date	Changes	Version
10	15 August 2024	• Updated the Certificates OID in section 1.2 • Updated the list of root and intermediate certificates in section 1.2 • Updated the Performing identification and authentication functions in section 4.2.1	6.0.2
11	13 March 2025	• Consolidated CP and CPS document • Updated the list of roots and intermediates of SMIME and TLS certificates in section 1.2 • Updated section 1.6.1 Definitions • Updated section 2.2 Publication of information • Updated 3.2.5 Validation of Domain Authorization or Control • Updated section 4.2 Certificate application processing • Updated section 4.3.1 CA actions during certificate issuance • Updated section 6.1.1 Key Pair Generation • Remove Section 7.1.2.7 as Extended Key Usage is now explicitly defined for each certificate type for clarity. • Add Section 7.1.2.2.1 to explicitly specify the mandatory OID for each Sub CA. • Add Section 7.1.2.2.2 to explicitly specify the EKU requirement for each Sub CA.	6.1
12	16 June 2025	• Consolidate CP and CPS to CP/CPS • Updated Section 1.2 Document ID and Identification • Update TA definition. • Update MyDigital ID link. • Updated Section 1.5 Policy administration. • Added Section 3.2.4.4 Validating control over mailbox using ACME extensions • Updated Section 3.3.1 Identification and authentication for routine re-key. • Updated Section 4.2.1 Performing identification and authentication functions • Updated Section 5.18 Off-site backup. • Updated Section 5.3.2 Background check procedures • Updated Section 6.3.2 Certificate operational periods and key pair usage periods • Updated Section 7.1.2.6 Certificate Policies • Update Appendix A	6.1.1

#	Date	Changes	Version
13	28 August 2025	• Added a new Section 1.3.2.1 **Enterprise Registration Authority**. • Updated Section 6.1.5.2 to specify supported **EdDSA**, **ML-DSA**, and **SLH-DSA** key pairs. • Updated Section 6.2.1 to clarify that all cryptographic functions, including post-quantum algorithms, use certified hardware with hybrid methods for compatibility and added security. • Updated Section 7.1.3.1 **SubjectPublicKeyInfo** to include **EdDSA**, **ML-DSA**, and **SLH-DSA** key types. • Updated Section 7.1.3.2 **Signature Algorithm Identifier** to include **EdDSA**, **ML-DSA**, and **SLH-DSA** signature algorithms. • Updated Section 7.1.3.2.1 RSA to add support for **id-RSASSA-PSS** as a signature algorithm, in addition to the existing **PKCS#1 v1.5** (shaWithRSAEncryption). • Added a new Section 7.1.4.2.2.5 **Code Signing Certificates Subject DN**. • Updated Appendix A to add **RPH** and improve the language for more clarity. • Updated Appendix B to improve the language for more clarity. • Improved language in Section 7 to reflect this document as both a **Certificate Policy (CP)** and a **Certificate Practice Statement (CPS)**.	6.1.2

Contents

1 INTRODUCTION

1.1 Overview

This Certificate Policy/ Certification Practice Statement (CP/CPS) defines the procedural in managing certification and time-stamping services. This CP/CCPS pertains to all parties utilizing MSC Trustgate certificate and time-stamping services.

MSC Trustgate's Certificate and Time-Stamp policies are controlled by the MSC Trustgate Policy Management Authority (PMA) that determines how this CPS applies to Certificate Authorities (CAs), Registration Authorities (RAs), Subscribers, Relying Parties, and other PKI entities that interoperate with or within the MSC Trustgate CA services.

Depending on the class and type of certificates, Digital Certificates may be used by Subscribers to secure websites, digitally sign documents and/or e-mails. The person who ultimately receives a signed document or communication, or accesses to a secure website is referred to as a relying party, i.e., those individuals are relying on the certificate and have to make a decision on whether to trust it. A Relying Party must rely on the certificate in terms of the relevant Relying Party Agreement included in the Certificate.

These participants and other parties are described in more detail in Section 1.3 of this CP/CPS.

Pursuant to the IETF PKIX RFC 3647 CPS framework, this CP/CPS is divided into nine parts that covers the security controls and practices and procedures for certificate and time-stamping services within the MSC Trustgate CA services. To preserve the outline specified by RFC 3647, section headings that do not apply have the statement "No stipulation".

1.2 Document Name and Identification

MSC Trustgate Certificates contain object identifier values corresponding to the applicable MSC Trustgate Class of Certificate. The OID for MSC Trustgate is an iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) MSC Trustagte.com (49530). MSC Trustgate issues certificates and time-stamp tokens containing the following OIDs arcs:

Digitally Signed Object	Object Identifier (OID)
Document Signing Certificate (Medium Assurance)	
Generic	1.3.6.1.4.1.49530.1.1.2
Government Services Certificates	1.3.6.1.4.1.49530.1.1.2.1 • 1.3.6.1.4.1.49530.1.1.2.1.1(MyGPKI, effective 2 August 2025)
Individual Certificates	1.3.6.1.4.1.49530.1.1.2.2 • 1.3.6.1.4.1.49530.1.1.2.2.1 (Basic, effective 2 August 2025) • 1.3.6.1.4.1.49530.1.1.2.2.2 (Pro, effective 2 August 2025)
Organization Certificates	• 1.3.6.1.4.1.49530.1.1.2.3 (effective 2 August 2025)
AATL Certificates	AATL certificates issued under MyTrust Class 3 ECC Enterprise CA utilized the following OID: 1.3.6.1.4.1.49530.1.1.3 AATL certificates issued under Trustgate ECC Document Signing CA utilized the following OID: • 1.3.6.1.4.1.49530.1.1.2.4.1 (AATL Individual Certificates) • 1.3.6.1.4.1.49530.1.1.2.4.2 (AATL Individual Pro Certificates) • 1.3.6.1.4.1.49530.1.1.2.4.3 (AATL Organization Certificates)
LHDN e-Invoice Organization Certificates	1.3.6.1.4.1.49530.1.1.2.5
Document Signing Certificate (High Assurance)	
High Assurance Certificates	1.3.6.1.4.1.49530.1.1.4
Code Signing Certificates	
Code Signing Certificates	1.3.6.1.4.1.49530.1.2.1
Extended Validation Code Signing Certificates	1.3.6.1.4.1.49530.1.2.2
Time Stamping Certificates	
Time Stamping Certificates (Generic)	1.3.6.1.4.1.49530.1.3.1
SSL Certificate	
Domain Validation SSL Certificates	1.3.6.1.4.1.49530.1.4.1
Organization Validation SSL Certificates	1.3.6.1.4.1.49530.1.4.2
Extended Validation SSL Certificates	1.3.6.1.4.1.49530.1.4.3
Intranet Validation SSL Certificates	1.3.6.1.4.1.49530.1.4.4

Digitally Signed Object	Object Identifier (OID)
S/MIME Certificates	
S/MIME Basic (Mailbox Validated)	1.3.6.1.4.1.49530.1.5.1
S/MIME Organization (Organization Validated)	1.3.6.1.4.1.49530.1.5.2
S/MIME Enterprise (Sponsored Validated)	1.3.6.1.4.1.49530.1.5.3
S/MIME Standard (Individual Validated)	1.3.6.1.4.1.49530.1.5.4
National ID Certificates	
MyDigital ID	1.3.6.1.4.1.49530.1.1.3 Effective 2 August 2025 MyDigital ID certificates utilize the following: • OID:1.3.6.1.4.1.49530.1.6.1

1.2.1 Root Certificate

CERT #	Subject	SHA256 Fingerprint
1	CN = Trustgate Class 2 Root Certificate Authority O = MSC Trustgate.com Sdn. Bhd. C = MY	E2026B5646F49F9671D4318E09094A23CE34C94B5410F19B39D490A761CA65D1
2	CN = Trustgate RSA Certification Authority OU = Malaysia Licensed CA No LPBP-2/2010 (1) O = MSC Trustgate.com Sdn. Bhd. C = MY	DC7ACA56E0921E3C54E7DA854A13CDE917B3EEC386B8E9D59201F812E4E9B40C
3	CN = Trustgate Time Stamping Authority CA (ECC) OU = Malaysia Licensed CA No LPBP-2/2010 (1) O = MSC Trustgate.com Sdn. Bhd. C = MY	FC794E7830873926C16824CBAC867F8EAC7CF28EFC9FF4A465B77E6FD42610B7
4	CN = Trustgate Time Stamping Authority CA OU = Malaysia Licensed CA No LPBP-2/2010 (1) O = MSC Trustgate.com Sdn. Bhd. C = MY	CF74F634C21A6AA376FD264E31EAB031845FFD048D20F9C41AC73C8ED5BC4737
5	CN = MyTrust Class 2 ECC Root CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	97351977E28FD6602FE1ADAE58E8994212CB02D995F866D2F5DC41D9E946B855
6	CN = MyTrust Class 3 ECC Root CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	BFAEC1F8E11BD4840A91472E80040F568970FD48B28F09AF018383AF9B0F9D1F
7	CN = MyTrust Class 2 RSA Root CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	A788D9F9EBE7648CFED6D8B071382A30780D9719A802731F066F59B32124A8B3
8	CN = MyTrust Digital ID Root CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd C = MY	D21BECEBF35470585672E8F5721697F71C7CC4D731C4A0FCCDB1A18FCB5691FA
9	CN = Trustgate RSA Global Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	D2BE160D6A4391630BCEE932993E48547C9CABFE21A0B052A60601C8A266C19E
10	CN = Trustgate Secure Server Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	A233FA00067C0A31EC80793F6F4623DED687E8FD71241FD560BA292D98AB3737
11	CN = Trustgate ID Root CA O = MSC Trustgate.com Sdn. Bhd	433DB9E222A1EF0AF4F4C4DFAEE76643B9039F1758A13BDFBED36C7290114162

CERT #	Subject	SHA256 Fingerprint
	C = MY	
12	CN = Trustgate MPKI Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	075CEA0ADE7133F67F3EB44815A07E6E4865534901FF1400C42A3C6D3123F95A
13	CN = Trustgate ECC Global Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	AFF58C68DFA45AF80B7D965545E8DC08221E527C8C1090E41270DD9FE7B523D6
14	CN = Trustgate ECC Time Stamping Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	BEFD8058D1CE9482799FD62275A2019A84E47F592E1B618D17E563C6540301A4
15	CN = Trustgate ECC ID Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	843C2B01DF6A1FDBAF54F7F640F41187F1818A5E429EB457EF627014AF2F5AD6
16	CN = Trustgate ECC MPKI Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	1110EAA11E493C0E9448985D207DC40B7EE2C83EAF087F10BA172E2AC262F2C5
17	CN = Trustgate SMIME RSA Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	504B5D7CD5324FB393817075F3BBDCB990EC4C930CCD35E374F97D426B1DA0EB
18	CN = Trustgate SMIME ECC Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	0E09801EB903A6F8DE6EF86799296C74B89AB8680C0AF3F2D870EAB6A095F63F
19	CN = Trustgate SMIME Enterprise RSA Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	4027859768646C2235DD86CDF7D82AC345AA7F71F742DDFACE2A2D6FD51B41AC
20	CN = Trustgate SMIME Enterprise ECC Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	E766F25782559C75324FDCCC53DDED1DE0A7BB16791CCBD0657EA873BECDACCA
21	CN = Trustgate TLS Basic RSA Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	002D96A8B5E7087B3B3CCC9ECFECF89FAA124DE61F390889C3C5FA29F16A9D6A
22	CN = Trustgate TLS RSA Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	B622543BC97CBDBC8D0890B36C4E613B105A8AF6C69B852B38B7D89B0AE0725B
23	CN = Trustgate TLS High Assurance RSA Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	455FEC3946F62073AFD03C7B701E4188BB54EEB23D438599EAFFA51CAB9F86D5
24	CN = Trustgate TLS Basic ECC Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	6D0139F87DF6A4E18005AD41E11E29748FF44A7FB7A2429E5A4441AD65225322
25	CN = Trustgate TLS ECC Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	7E3790A513679E0E21A53B7ECCC0CEC8B8B3649E15ABCD481C5ABB00CD0869AE
26	CN = Trustgate TLS High Assurance ECC Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	8FE689549B5A060DFE2C2C7052434C5013CD9BCA106A413EBA9021515BB1E5EB

1.2.2 Bridge Certificate

CERT #	Subject	SHA256 Fingerprint
1	CN = Trustgate Secure Server Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	1EA22856E474C9CF5B90F5117E17595A0FBE7E1AA3D172067676BED130C52CE6
2	CN = Trustgate ID Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	45CD58326CC8D3637C4586717072A3849AA801B69811639AAE05CD53C1E59BCE
3	CN = Trustgate MPKI Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	8E800BF38414B142440CD175398D29075C6946F0EC048A02357DCC5BEADEA32C

CERT #	Subject	SHA256 Fingerprint
4	CN = Trustgate ECC Time Stamping Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	27A491B41594F31517130E4B7EA94EB38C529358E0987E48849E3F9BC8C6D166
5	CN = Trustgate ECC ID Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	FB5EF4B679D073B4D0C4DFA469288A0C3BB949CFF7699A6141B46E2B1EDAC017
6	CN = Trustgate ECC MPKI Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	C1D86D24AAE0EF5FB7070DFBB685AAC62F0E4420907DA5C26B24BAE96A39BDCE

1.2.3 Intermediate Certificate

CERT #	Subject	SHA256 Fingerprint
1	CN = MSC Trustgate.com Class 2 MPKI CA O = MSC Trustgate.com Sdn. Bhd. C = MY	CC6ADC88D783574EA3E4F5114FF3AE4DB5B1470934242C62471B124A419C2F94
2	CN = MSC Trustgate.com Corporate ID (Token) CA OU = Malaysia Licensed CA No LPBP-2/2010(1) O = MSC Trustgate.com Sdn. Bhd. C = MY	A61D795B0EF27E96848585C2187C9476645528697ABE50BA3692F03663F08748
3	CN = Bank Negara Malaysia Class 2 CA-G3 O = MSC Trustgate.com Sdn. Bhd. C = MY	A4166F2E0125B553E84CBA1B7D240369AB2A5AB1846C0EF14E2332CEBD39E180
4	CN = INTECH-KLIS CA OU = Remote Signing System O = IDAMAN NURANI TECHNOLOGIES SDN. BHD C = MY,	D0D6BA9EA1822C1C57F96F39BEE2A47A431889B7FD4C3BA25FB2200DC1873EBF
5	CN = ABMB-MFA CA OU = Remote Signing System O = Alliance Bank Malaysia Berhad C = MY	F26EDD6166A7507C20C641D2961349E1875C2144C040D507EEA6EA7E173F43D7
6	CN = Trustgate Time Stamping Services CA (ECC) O = MSC Trustgate.com Sdn. Bhd. C = MY	67AC1B817817B9C626D6D3E8487A1C7FEC8AA27336D50148580F88BB67FFB7FF
7	CN = Trustgate Time Stamping Services CA O = MSC Trustgate.com Sdn. Bhd. C = MY	091538A9476A4F6A6956F31B133992536881C28323D19B57E2C5D91EB4770B22
8	CN = MyTrust Class 2 ECC Individual CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	F040B8C96223510A3190E0E85233159986BD26187D11C909D65AB8E0D298AA22
9	CN = Bursa Anywhere CA OU = Remote Signing System O = Bursa Malaysia Berhad C = MY	2D01696CC852C4CE5317778A9FA16BBEA14CDEE10F5FBA91A3B37D8FF52768E5
10	CN = GPKI CA ECC OU = MAMPU, O = MSC Trustgate.com Sdn. Bhd C = MY	567EF5A4C14641BC6B46452540F187B5686407DF4BDD51E5A3B1C79E678F97B8
11	CN = MyLawyer ID CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	3B89B1CED28ED8045BA39015FAEB6C7FBF7D5E6A046B2F0198B846D7BEDA0006
12	CN = MyTrust Class 3 ECC Enterprise CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	8EA69844C4A6BDA29FC13FD65A2371E9E689C22C1BF6585432406B527F86730F

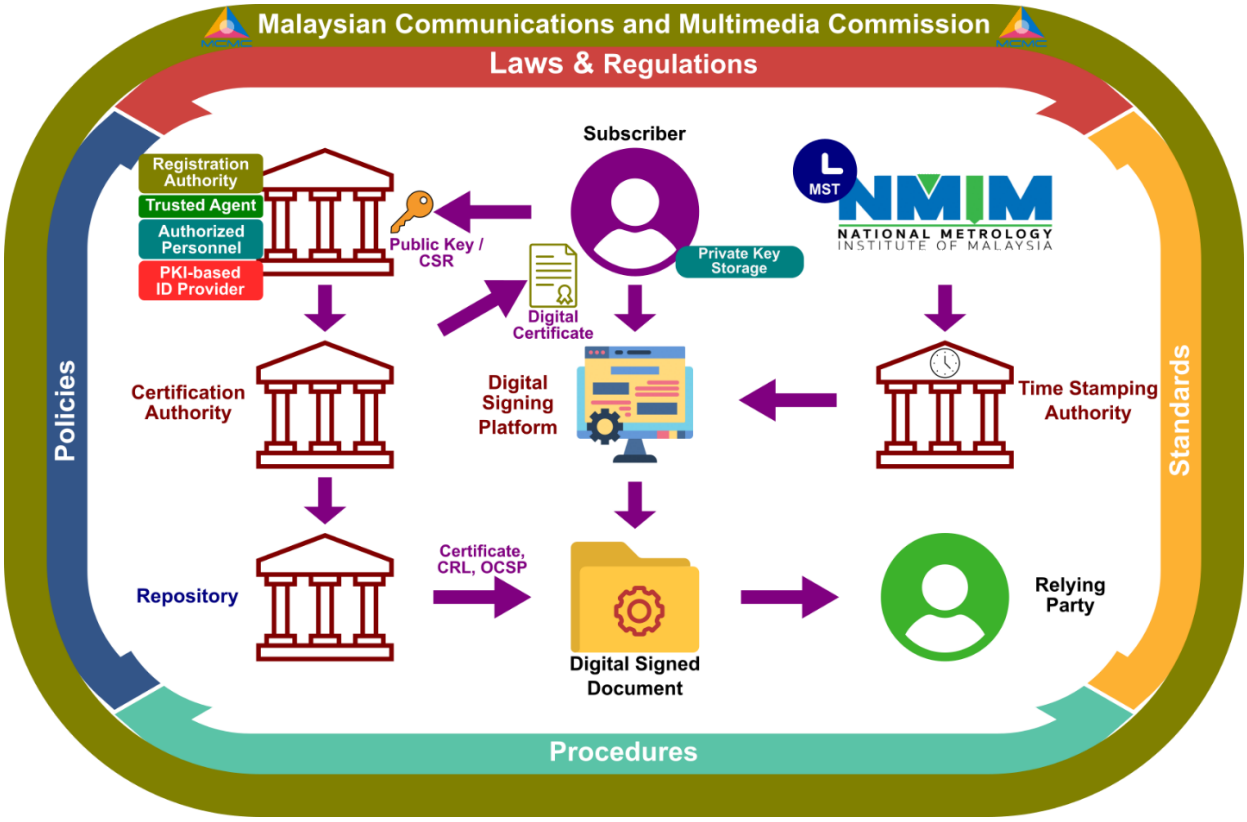
CERT #	Subject	SHA256 Fingerprint
13	CN = MyTrust Class 2 RSA Individual CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	35F1FAF93C2FAB2BF302F551525C587FD4D434BB6BB247ED75B50DB0F2FE2AB3
14	CN = MyTrust Class 2 RSA Enterprise CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	1B1EE0498319BF0A223D4917A41A454D4EA08F44C5C8BD26F65121256377CB6A
15	CN = PayNet CA O = Payments Network Malaysia Sdn Bhd C = MY	B70119C3B78800839F1A5246CB1DF54F2F148012F785371755669B278D0384AF
16	CN = MyTrust Digital ID Class 2 CA OU = MyTrust Gateway, O = MSC Trustgate.com Sdn. Bhd, C = MY	D42F0C30DD9896F8E0EDED01FC4494F317B7DC7E6530590EDDB4D84228050C99
17	CN = MyTrust Digital ID Class 3 CA OU = MyTrust Gateway, O = MSC Trustgate.com Sdn. Bhd, C = MY	94B349BC4BE13041EA9A47315CE22E0EA327873FADA258EDC99B91F56F0F8439
18	CN = Trustgate Extended Validation Server CA O = MSC Trustgate.com Sdn. Bhd. C = MY	80689FEA931C13B6399096B44989CF2DDB3BB42DBFBAC25D56D274B9FEC23968
19	CN = Trustgate Secure Server CA O = MSC Trustgate.com Sdn. Bhd. C = MY	D25E03BDBF23BF7772167268834F1FFC094CEF1D9A27C320FEB8320EF1813DBC
20	CN = Trustgate Basic Server CA O = MSC Trustgate.com Sdn. Bhd. C = MY	F6330ED89B22D8C06E46B2F733DA812374CD853B89EF1D6222B9162B0A00CAFD
21	CN = Trustgate S/MIME Individual CA O = MSC Trustgate.com Sdn. Bhd. C = MY	2CFE9402F6DDAAA69154A541D713B8B7C7F83D33FAA696F8F0D1FB87271F3AE0
22	CN = Trustgate S/MIME Organization CA O = MSC Trustgate.com Sdn. Bhd. C = MY	B4AEF17549780191EEF9E9592D40E378CE491781C0066B4D82E4F5D67B3C0134
23	CN = Trustgate Document Signing CA O = MSC Trustgate.com Sdn. Bhd. C = MY	CA3A2B1EA210207F7D7A08BBC86EFDD391B1726EC7DD5357CC7576B7092C58CF
24	CN = Trustgate MPKI Individual Subscriber CA O = MSC Trustgate.com Sdn. Bhd. C = MY	2685AD25E4393E39944F95FEACB704261DD88BFD3100A06756A563D2CAB499DA
25	CN = MyKad ID CA O = MSC Trustgate.com Sdn. Bhd. C = MY	0AE0DF704E86B6845CD0F94B0A4A51F27E8A5194D39A94BF32560F09ACEA4F88
26	CN = GPKI CA O = MSC Trustgate.com Sdn. Bhd. C = MY	962AD5D1976B0F65895788371795A1D4DEA139B82974E0E8E1EE518AEC1D6713
27	CN = eP ID CA O = MSC Trustgate.com Sdn. Bhd. C = MY	85FD130D83DBE0049818DCDB12203F6C16616289CE7EE2E6C14F03BD29FADA64
28	CN = NPRA ID CA O = MSC Trustgate.com Sdn. Bhd. C = MY	AC717550BB1446C617128B723E36D46B9CDE7AD58D89F2AE325BDD13036E95C0
29	CN = Healthcare ID CA O = MSC Trustgate.com Sdn. Bhd. C = MY	FBE9A14D3CAA3F72D0A402E5AE41581EAF1D7A79F12B4E3E722450B8372F1205
30	CN = ABMB-MFA CA - G2 O = MSC Trustgate.com Sdn. Bhd. C = MY	E623BD036F1C56E664536DE064710494816CEE48BCD5A5F36AAD744AC31CEF44
31	CN = PayNet CA - G2 O = MSC Trustgate.com Sdn. Bhd. C = MY	56B97166434D8BDE298B353F6F800A70BE185A23FF97274EE0A7765CEAEB78D0

CERT #	Subject	SHA256 Fingerprint
32	CN = Trustgate ECC Time Stamping Services CA O = MSC Trustgate.com Sdn. Bhd. C = MY	7348112B9D8DF0042E920E202D532F6CA89A352BEDC59B8E85947C86F88B5EED
33	CN = Trustgate ECC Document Signing CA O = MSC Trustgate.com Sdn. Bhd. C = MY	6D21B608F47E08BFE8265015F25DF0ACD02B4DD6E08D20CBE56BE0DF4D69FB91
34	CN = Trustgate ECC Document Signing CA O = MSC Trustgate.com Sdn. Bhd. C = MY	3e7cdc64e3fad792a86bb130e1256c261bcd3b9049171b22f7a28439643ecf28
35	CN = Trustgate ECC MPKI Individual Subscriber CA O = MSC Trustgate.com Sdn. Bhd. C = MY	E10696EFAF72D5E0D0B62A80E687D4852227C30BAC367768F1451873A5C5BAB1
36	CN = Bursa Anywhere CA - G2 O = MSC Trustgate.com Sdn. Bhd. C = MY	9A7BC4FDC454F1B920BFF8A7E7D578CC805F2C0C09B7ADE2B68C484EAFA7DA0C
37	CN = GPKI CA ECC - G2 O = MSC Trustgate.com Sdn. Bhd. C = MY	229028210BE6A3B6176E8F5441B5EE629DA94BF28F425BA997F2E5AD5D7F8812
38	CN = MyLawyer ID CA - G2 O = MSC Trustgate.com Sdn. Bhd. C = MY	EF4C2488FA68ABAA945445254C3DEB49EF8269F736593F093493B41C7103ADF3
39	CN = Trustgate Digital ID Class 3 CA O = MSC Trustgate.com Sdn. Bhd. C = MY	7EC5C9AB617519B1655CB0587B68E668B974F8A9B098405416159ADA6D03FF3A
40	CN = MyTrust365 CA - G2 O = MSC Trustgate.com Sdn. Bhd. C = MY	F4619278085925F5703443FF2901238D422D30F975DB0E4D5DED00581EE92379
41	CN = Trustgate SMIME Basic RSA CA O = MSC Trustgate.com Sdn. Bhd. C = MY	6AABC6A71C014A2AECBE446A9C98EC05908F63B2C2D21536DABE386F719A3606
42	CN = Trustgate SMIME Standard RSA CA O = MSC Trustgate.com Sdn. Bhd. C = MY	A14A4C5C832BF6E9CE159B5245A70EFC2A2FA3560EC2191D084246BC72D8B20F
43	CN = Trustgate SMIME Enterprise RSA CA O = MSC Trustgate.com Sdn. Bhd. C = MY	98F9400AB4E27EFE6E40039AF79ED67D8F3B3827E84CAF63010CDF5515D4A223
44	CN = Trustgate SMIME Organization RSA CA O = MSC Trustgate.com Sdn. Bhd. C = MY	6BBE5F6621F8AC75B50D68B447B554E28649E105418AC298BC84F52981AFF658
45	CN = Trustgate SMIME Basic ECC CA O = MSC Trustgate.com Sdn. Bhd. C = MY	DC453E098780C277DD3780578D0001EEE614BBA885F89211E477CA3E3871EC6F
46	CN = Trustgate SMIME Standard ECC CA O = MSC Trustgate.com Sdn. Bhd. C = MY	B13AC2DA0B36F819FFFB56DAC80A9C48A4C1E83D37E9EB40F57B7E290C22EEB9
47	CN = Trustgate SMIME Enterprise ECC CA O = MSC Trustgate.com Sdn. Bhd. C = MY	6DC156503B110B7D2BA0CFB0CF91F1CEC702A1A69CDAD4EC81B68F8FBACA48E9
48	CN = Trustgate SMIME Organization ECC CA O = MSC Trustgate.com Sdn. Bhd. C = MY	DE81B6BF29E0B2FC37F9E278480201A53515AA476ABBCAB454929EA97A3740AF
49	CN = Trustgate TLS DV RSA CA O = MSC Trustgate.com Sdn. Bhd. C = MY	B900574E70C3925FA8A64CB0E0B1E349F87A5B658F84C9C2F33EE4A793A2DED9
50	CN = Trustgate TLS OV RSA CA O = MSC Trustgate.com Sdn. Bhd. C = MY	EAB6A9F072FC20161375977CF7B2469610790DAF9A277C509378E98D483794E3
51	CN = Trustgate TLS EV RSA CA O = MSC Trustgate.com Sdn. Bhd. C = MY	4E035B43435561F36F3F4DA4706268747F8263FA21778EDF1F5F29C3C09893F1
52	CN = Trustgate TLS DV ECC CA O = MSC Trustgate.com Sdn. Bhd. C = MY	F8908E9D0066F8535B6AF52FBEE7988438C421DCC13EF8CB1DC2C54888FBC273

CERT #	Subject	SHA256 Fingerprint
53	CN = Trustgate TLS OV ECC CA O = MSC Trustgate.com Sdn. Bhd. C = MY	448C5ECB1B9B2E390C05C2F1D4E9DF32F8BF3C9A10876C5BF94F6C74AE243C99
54	CN = Trustgate TLS EV ECC CA O = MSC Trustgate.com Sdn. Bhd. C = MY	A223DDCD91B2781BD46B085F3BE48AA63E21177C3B9936066EB3D7ABD4853EFC

1.3 PKI participants

The diagram below illustrates the key participants in the MSC Trustgate PKI ecosystem, focusing specifically on digital signatures.



A Subscriber may initiate a Certificate request to MSC Trustgate as a Certificate Authority (CA) through either direct engagement with the MSC Trustgate Registration Authority (RA) team or through an External RA, Trusted Agent, Authorized Personnel, or PKI-based Identity Provider. This request involves presenting a valid Certificate Signing Request (CSR) to demonstrate control over the private key, alongside Personal Identifiable Information (PII). Following a verification and validation process by the CA, a Certificate is issued to the Subscriber. This Certificate is then utilized by the Subscriber to generate digital signatures via a Digital Signature Platform, resulting in digitally signed documents. The trusted time is obtained from the National Metrology Institute of Malaysia (NMIM) to enhance the security and trustworthiness of their electronic transactions and digital signatures. Subsequently, Relying Parties validate the digital signatures on these documents using the public key of the Certificate and verify the status of the Certificate through either Certificate Revocation Lists (CRL) or Online Certificate Status Protocols (OCSP) from repositories issued by the CA.

1.3.1 Certification Authorities

MSC Trustgate is a Certification Authorities (CA) that issues digital certificates using its own CA system. MSC Trustgate 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's products and services are available at https://www.msctrustgate.com.

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 CA. MSC Trustgate may act as an RA for certificates it issues.

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

For S/MIME and SSL Certificates, MSC Trustgate does not delegate the RA function to third parties.

1.3.2.1 Enterprise Registration Authority

An Enterprise Registration Authority (Enterprise RA) is an entity operating under a project-specific agreement with MSC Trustgate and authorized to perform identification and authentication of certificate applicants within a defined scope. The defined scope may include the enterprise's internal personnel, affiliated entities, and external individuals or organizations directly related to the project, where such relationships are documented through a valid Letter of Authorization (LoA) or equivalent evidence acceptable to MSC Trustgate.

Where a certificate request contains an email address or domain name, MSC Trustgate verifies that the Enterprise RA has authorization or control of the domain, or MSC Trustgate performs the applicable validation in accordance with established domain and email control requirements. Where a certificate request contains an organization name, MSC Trustgate ensures that the name corresponds to the Enterprise RA's own organization, an Affiliate, or an organization for which the Enterprise RA acts as an authorized agent.

Enterprise RAs comply with all applicable requirements of this CP/CPS and the project-specific agreement. The agreement defines the scope of the Enterprise RA's authority, specifies that all verifications be performed using MSC Trustgate-approved methods, and requires submission of complete verification records and supporting evidence to MSC Trustgate for retention. MSC Trustgate monitors and audits Enterprise RA operations to confirm ongoing compliance.

1.3.3 Subscribers

Subscribers under the MSC Trustgate CA services includes all end users (including entities) of certificates issued by a MSC Trustgate CA services. 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 CP/CPS to distinguish between these two roles: "Subscriber", is the entity which contracts with MSC Trustgate 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" being used it may mean just the Subscriber as a distinct entity but may also use the term to embrace the two. The context of its use in this CPS will invoke the correct understanding.

1.3.4 Relying parties

Relying Parties are entities that act in reliance on a Certificate and/or digital signature issued by MSC Trustgate. 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 MSC Trustgate CA services.

1.3.5 Other participants

1.3.5.1 Trusted Agent

A Trusted Agent (TA) is a government agency or financial sector participants[1] or any organization mandated by the relevant Minister under applicable legal provisions, that holds the authority to conduct identity verification and validation processes, and possesses a reliable data source. Applicants may request a digital certificate from the Trusted Agent, who subsequently submits the validated personal identifiable information (PII) to MSC Trustgate for the issuance of a digital certificate based on the validated data. MSC Trustgate may get or validate

[1] https://www.bnm.gov.my/regulations/fsp-directory

additional PII data from another data source to construct a digital certificate. The TA must enter into a contractual agreement relationship with MSC Trustgate (TA agreement) before operation as TA for MSC Trustgate. The TA is required to pass the following data to MSC Trustgate for certificate issuance process and ensuring compliance with the Digital Signature Act 1997 and Digital Signature Regulations 1998 (DSA 1997 and DSR 1998):

i. Personally Identifiable Information (PII): Any data that can be used to identify a specific individual. Examples of PII include a person's name, address, phone number, email address, Mykad number, passport number, and any other information that can be linked directly or indirectly to a particular person.

ii. Authentication status: The outcome or result of an authentication process, confirming and establishing a linkage between the claimed identity and the real-life existence of the applicant presenting the government-issued photo ID as evidence.

iii. Date and time of authentication: To indicate date and time when applicant's identity is authenticated during the certificate application process.

iv. Verifier: To identify the individual, entity, or device responsible for conducting the verification process.

1.3.5.2 Authorized Personnel

Authorized personnel (AP) are individual who is granted the authority by MSC Trustgate to receive certificate requests and verify the identity of the certificate applicants against government-issued photo IDs such as MyKad, valid passports, driver's licenses, or other national identity documents. The AP must enter into a contractual agreement relationship with MSC Trustgate (AP agreement) before operation as AP for MSC Trustgate. The AP is required to pass the following data to MSC Trustgate for further validation and certificate issuance process, ensuring compliance with the Digital Signature Act 1997 and Digital Signature Regulations 1998 (DSA 1997 and DSR 1998):

i. **Personally Identifiable Information (PII)**: This refers to any data that can be used to identify a specific individual. Examples of PII include a person's name, address, phone number, email address, Mykad number, passport number, and any other information that can be linked directly or indirectly to a particular person.

ii. **Verification status**: Refers to the outcome or result of a verification process, confirming and establishing a linkage between the claimed identity and the real-life existence of the applicant presenting the government-issued photo ID as evidence.

iii. **Date time of verification**: To indicate date and time when applicant's identity is verified during the certificate application process.

iv. **Verifier**: Refers to identifying the individual, entity, or machine responsible for conducting the verification process.

v. **Verification Method**: Refer to the method used by the AP to confirm the identity of the applicant. It can be, and is not limited one of the following:

   a. Manual face-to-face verification
   b. Manual face-to-face verification with biometric
   c. Secure automated self-service verification with biometric
   d. e-KYC (face recognition with liveness detection) as per Bank Negara Malaysia (BNM) Electronic Know-Your-Customer (e-KYC)[2]

vi. **Evidence**: Refers to the supporting documents used to confirm and establish a linkage between the claimed identity and the real-life existence of the subject presenting the government-issued photo ID. Additionally, the Authorized Personnel (AP) may provide additional documents such as a letter of authorization (LoA) or a membership document to associate the applicant with an organization if this information is required to be included in the digital certificate.

[2] https://www.bnm.gov.my/documents/20124/938039/pd_ekyc-apr2024.pdf

1.3.5.3 PKI-based Identity Provider

PKI-based Identity Provider (IDP) is a trustworthy entity or system that manages digital identities utilizing PKI for authentication purposes. In this instance, MyDigital ID[3] is one of the PKI-based IDPs utilized by MSC Trustgate within its PKI ecosystem.

[3] Refer to https://www.digital-id.my/

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 a transaction. Digital Certificates are used in commercial environments as a digital equivalent of an identification card.

1.4.1 Appropriate certificate uses

Certificates issued by MSC Trustgate may be used for public domain transactions such as authentication, encryption, access control, and digital signature purposes. The usage of these Certificates is restricted 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 CP/CPS.

This CP/CPS covers several different types of end entity Certificates/tokens with varying levels of assurance. The following table provides a brief description of the appropriate uses of each. The descriptions are for guidance only and are not binding.

Certificates	Appropriate Use
Document Signing	Document Signing Certificates are used by individuals or organizations to authenticate and digitally sign electronic transactions, messages, and electronic documents. The primary purpose of a Client Certificate is to provide authentication, message integrity and non-repudiation (using digital signatures). MSC Trustgate issues Document Signing Certificates in accordance with DSA 1997 and DSR 1998. MSC Trustgate has classified all Document Signing Certificates as Class 2 and Class 3 Certificates[4]. Class 2 is a medium Level of Assurance. Class 3 is a high Level of Assurance.
MyDigital ID	MyDigital ID is a national digital identity authentication certificate used to verify the identity of users accessing digital services.
Domain Validation SSL/TLS Server Certificates	Authentication of a remote Domain Name and webservice and encryption of the communication channel.
Organization Validation SSL/TLS Server Certificates	Authentication of a remote Domain Name and associated organizational context and webservice and encryption of the communication channel.
Extended Validation SSL/TLS Server Certificates	Authentication of a remote Domain Name and associated organizational context and webservice and encryption of the communication channel.

[4] According to Malaysian Communications and Multimedia Commission (MCMC) Licensing Guidebook – Digital Signature ("Guidebook") dated 15 March 2024, Class 2 Certificates means a certificate that confirms that the information provided by the subscriber when applying for the certificate does not conflict with information accessible in widely recognised consumer data bases and provides a reasonable level of assurance as to the subscriber's identity, based on a automated on-line process. Class 3 certificate means a certificate that provides the higher level of confirmation and higher level of assurance as to the subscriber's identity then Class 1 and Class 2 certificate, which includes in-person and supervised remote proofing3. The application for the Class 3 certificate must be certified by a notary public duly appointed under the Notaries Public Act 1959.

Certificates	Appropriate Use
S/MIME Certificates	S/MIME Certificates are used to secure email communications. It provides a way to digitally sign and encrypt email messages, ensuring confidentiality, integrity, and authenticity.
Code Signing Certificates	Code Signing Certificates are used by content and software developers and publishers to digitally sign executables and other content.
Time Stamping Certificates	Time Stamp Certificates are used to identify the existence of data at that point in time.
Device Certificates	Device authentication Certificates can be used for specific electronic authentication transactions that support the identification of websites and other online resources, such as software objects.
OCSP Responder	An OCSP Responder Certificates is a digital certificate used to authenticate and verify the status of other digital certificates in real-time.

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 CP/CPS when the Certificate issued.

Certificates shall be used only to the extent the use is consistent with applicable law.

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 be used as CA Certificates.

MSC Trustgate 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 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 recommends the use of MSC Trustgate Roots as root certificates.

1.5 Policy administration

1.5.1 Organization administering the document

The MSC Trustgate Policy Management Authority (PMA) maintains and enforces this CP/CPS.

1.5.2 Contact person

Attn: MSC Trustgate Policy Management Authority

MSC Trustgate 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: compliance@msctrustgate.com

1.5.2.1 Revocation Reporting Contact Person

Attn: MPKI Support

MSC Trustgate 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/CPS suitability for the policy

The organization identified in Section 1.5.1 is responsible for determining whether this CP/CPS, as well as any supplemental or subordinate documents of a similar nature, are suitable under this CP/CPS.

1.5.4 CP/CPS approval procedures

The PMA approves the CP/CPS and any amendments. Amendments are made after the PMA has reviewed the amendments' consistency with the CP/CPS, by either updating the entire CP/CPS or by publishing an addendum. The PMA determines whether an amendment to this CP/CPS is consistent with the required 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 Repository located at: https://www.msctrustgate.com/repository. Updates supersede any designated or conflicting provisions of reference to the previous version of the CP/CPS.

1.6 Definitions and acronyms

1.6.1 Definitions

"Adobe Approve Trusted List" A document signing certificate authority trust store created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 9.0.

"**Applicant**" means the natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate is issued, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

"**Application Software Supplier**" A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

"Attestation Letter" A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

"Audit Period" In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in Section 8.1.

"Audit Report" A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.

"Authorization Domain Name" The FQDN used to obtain authorization for a given FQDN to be included in a Certificate. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If a Wildcard Domain Name is to be included in a Certificate, then the CA MUST remove "*." from the left-most portion of the Wildcard Domain Name to yield the corresponding FQDN. The CA may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and may use any one of the values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.

"Authorized Ports" One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).

"Base Domain Name" The portion of an applied-for FQDN that is the first Domain Name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

"CAA" From RFC 8659 (http://tools.ietf.org/html/rfc8659): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue."

"CA Key Pair" A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

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

"Certificate Data" Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

"Certificate Management Process" Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

"Certificate Policy" A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

"Certificate Problem Report" Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

"Certificate Profile" A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7, e.g. a Section in a CA's CPS or a certificate template file used by CA software.

"Certificate Revocation List" A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

"Certification Authority" An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs.

"Certification Practice Statement" One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

"Control" means "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors ; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

"Country" Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

"Cross-Certified Subordinate CA Certificate" A certificate that is used to establish a trust relationship between two CAs.

"CSPRNG" A random number generator intended for use in a cryptographic system.

"Delegated Third Party" A natural person or Legal Entity that is not the CA but is authorized by the CA, and whose activities are not within the scope of the appropriate CA audits, to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

"Enterprise RA" means an employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

"Expiry Date" means the "Not After" date in a Certificate that defines the end of a Certificate's validity period.

"Government Entity" means a government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

"High Risk Certificate Request" means a Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

"Issuing CA" In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

"Key Compromise" means a Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.

"Key Generation Script" means a documented plan of procedures for the generation of a CA Key Pair.

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

"Legal Entity" means an association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

"Linting" means a process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-be-signed object such as a tbsCertificate (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined in these Requirements.

"Multi-Perspective Issuance Corroboration" means a process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.

"**OCSP Responder**" An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

"Onion Domain Name" means a Fully Qualified Domain Name ending with the RFC 7686 ".onion" Special-Use Domain Name. For example, 2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion is an Onion Domain Name, whereas torproject.org is not an Onion Domain Name.

"Online Certificate Status Protocol" means an online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

"Policy Management Authority" means the committee responsible for managing the creation, review, and updating of Certificate Policies and Certification Practice Statements. This committee also reviews the results of audits conducted on Certification Authorities (CAs) to ensure compliance with established policies. Additionally, the PMA evaluates non-domain policies for acceptance within the domain and oversees the overall management of PKI certificate policies. For MSC Trustgate, the PMA comprises Senior Management, Compliance personnel, CA Operations Manager, and Key Manager.

"**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.

"Public Key Infrastructure" means a set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

"Publicly-Trusted Certificate" means a Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

"Qualified Auditor" means a natural person or Legal Entity that meets the requirements of Section 8.2.

"Random Value" means a value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

"Registered Domain Name" means a Domain Name that has been registered with a Domain Name Registrar.

"Registration Authority (RA)" means any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

"Reliable Data Source" means an identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

"Reliable Method of Communication" means a method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

"Relying Party" means any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

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

"**Subscriber**" means a natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

"**Subscriber's Agreement**" means an agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

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

"WHOIS" means an Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

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

1.6.2 Acronyms

AATL	Adobe Approve Trusted List
BR	Baseline Requirement
CA	Certification Authority
CAA	Certificate Authority Authorization
CAB	"CA/Browser" as in "CAB Forum"
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DBA	Doing Business As (also known as "Trading As")
FIPS	(US Government) Federal Information Processing Standard
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
IGTF	International Grid Trust Federation
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
IV	Individual Validated
LEI	Legal Entity Identifier
LHDN	Lembaga Hasil Dalam Negeri
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)
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SHA	Secure Hashing Algorithm
SSL	Secure Socket Layer
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

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

MSC Trustgate makes its CA Certificates, revocation data for issued digital Certificates, CP/CPS, Relying Party Agreements, and standard Subscriber Agreements available in public repositories. MSC Trustgate develops, implements, enforces, and annually updates this CP/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 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. If an SSL/TLS Server Certificate is intended to be trusted in Chrome, it is published by posting it in a Certificate Transparency log.

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

MSC Trustgate'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 information

MSC Trustgate publicly discloses its CP/CPS through an appropriate and readily accessible online means at https://www.msctrustgate.com , which is available on a 24x7 basis. The MSC Trustgate certificate services and the repository are accessible through several means of communication:

i. On the web: https://www.msctrustgate.com (and via URIs included in the certificates themselves)

ii. By email to mpki-support@msctrustgate.com

iii. By mail addressed to: MSC Trustgate.com Sdn Bhd, Suite 2-9, Block 4801, CBD Perdana, 63000 Cyberjaya, Selangor, Malaysia

iv. By telephone: +603-8318 1800

v. By fax: +603-8319 1800

MSC Trustgate SHALL publicly disclose its CA business practices to the extent required by the CA's selected audit scheme (see Section 8.4).

This CP/CPS is structured in accordance with RFC 3647 and includes all material required by RFC 3647.

This document specifies the policies of MSC Trustgate applies to meet the current versions of the following laws, policies, guidelines, and requirements:

Name of Law / Policy / Guideline / Requirement Standard	Location of Source Document
Malaysia Digital Signature Act 1997	https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Act-562.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
WebTrust Principles and Criteria for Certification Authorities – SSL Baseline	https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

Name of Law / Policy / Guideline / Requirement Standard	Location of Source Document
WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL	https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria
WebTrust Principles and Criteria for Certification Authorities – Network Security	https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria
WebTrust Principles and Criteria for Certification Authorities – S/MIME	https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

For Publicly Trusted Certificate, it upholds to the current and later versions of the requirements of the following scheme:

Name of Law / Policy / Guideline / Requirement Standard	Location of Source Document
Adobe Approved Trust List Members (AATL)	https://helpx.adobe.com/acrobat/kb/approved-trust-list2.html
Certification Authority / Browser Forum ("CA/B Forum") Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates	https://cabforum.org/working-groups/server/baseline-requirements/documents/
Guidelines for the Issuance and Management of Extended Validation Certificates	https://cabforum.org/working-groups/server/extended-validation/documents/
CA/B Forum Network and Certificate System Security Requirements	https://cabforum.org/network-security-requirements/
Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates	https://cabforum.org/working-groups/smime/documents/
Mozilla Root Store Policy	https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/
Microsoft Trusted Root Program	https://learn.microsoft.com/en-us/security/trusted-root/program-requirements
Apple Root Certificate Program	https://www.apple.com/certificateauthority/ca_program.html
Chrome Root Program Policy	https://googlechrome.github.io/chromerootprogram/

If any discrepancies arise between this CP/CPS and the normative directives outlined in the preceding policies, guidelines, and requirements ("Stipulated Criteria"), then the Stipulated Criteria shall hold authority over this CP/CPS. This CP/CPS is part of several documents that govern MSC Trustgate CA services. The other important documents include registration authority agreements, subscriber agreements, relying party agreements, customer agreements, and privacy policies. MSC Trustgate may publish additional certificate policies or certification practice statements as necessary to describe other products and services offered. These supplemental policies and statements are made available to applicable users or relying parties.

Application Software Suppliers for SSL/TLS Certificates may use the following websites for user agent verification:

Root CA	Status	URL
Trustgate Secure Server Root CA	Valid	https://tg-secureserver-valid.msctrustgate.com
Trustgate Secure Server Root CA	Revoked	https://tg-secureserver-revoked.msctrustgate.com
Trustgate Secure Server Root CA	Expired	https://tg-secureserver-expired.msctrustgate.com

2.3 Time or frequency of publication

MSC Trustgate develop, implement, enforce, and annually update CP/CPS that describes in detail how MSC Trustgate implements the latest version of these Requirements. MSC Trustgate indicate conformance with this requirement by incrementing the version number and adding a dated changelog entry in the revision history table, even if no other changes are made to the document.

2.4 Access controls on repositories

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

3 IDENTIFICATION AND AUTHENTICATION

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

MSC Trustgate verify the requests from parties seeking to revoke certificates.

3.1 Naming

3.1.1 Types of names

For Certificate issued to an Individual, the subject:commonName is specified as a Personal Name. For S/MIME Certificate, the subject:commonName can be an Email Address.

For Certificate issued to an organization or a legal entity, the subject:organizationName is specified the organization legal name registered with government agencies or an authority. The subject:commonName can be specified as the organization trademark or something that commonly associated with the organization.

For Certificate issued to a device, the subject:commonName contains MAC Address or device name.

For Certificate issued to a server, the subject:commonName contains only either Fully-Qualified Domain Name, Wildcard Domain Name or IPv4/IPv6 address.

MSC Trustgate EV SSL/TLS Certificates in compliance with the EV Guidelines section 11.

3.1.2 Need for names to be meaningful

MSC Trustgate use a meaningful representation of the Subject's name as verified in the identifying documentation or Enterprise RA records.

3.1.3 Anonymity or pseudonymity of subscribers

Each request for pseudonymity in an individual certificate will be evaluated on its merits by the PMA and, if allowed the subject:pseudonym attribute in the Certificate is used if the associated Subject has been verified according to Section 3.2.2. The subject:pseudonym attribute is either:

i. a unique identifier selected by the MSC Trustgate for the Subject of the Certificate; or

ii. an identifier verified from either of the following:

   a. based on government-issued identity documents; or

   b. an identifier selected by the Enterprise RA which uniquely identifies the Subject of the Certificate within the Organization included in the subject:organizationName attribute.

Pseudonym Certificates are not anonymous. MSC Trustgate treat Individual identity information relating to a Pseudonym as private in accordance with Section 9.4.2.

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

MSC Trustgate use subject Distinguished Name (DN) for uniqueness of names which contains specific identification attributes of the Certificate's holder.

For Individual Certificate, the `subject:serialNumber` is specified by government-issued identity number such as National Registration Identity Card (NRIC) number or a passport number, and this is accompanied by the `subject:countryName` in which is specified by the country that issued the identity number.

For Individual Certificate that present a regulated profession, the `subject:serialNumber` is specified by the respective membership number of the professional organization. and this is accompanied by the `subject:organizationName` in which is specified by the regulated professional organization and also by the `subject:countryName` in which is specified by the country that regulates the professional organization.

For Individual Certificate that present a corporate, the `subject:serialNumber` is optional to specify the employee number and the subject:Title is optional to specify the position held by the individual in the organization. The `subject:organizationName` is specified by the legal name of the organization and the `subject:countryName` is specified by the country that the organization registered with.

Except for LHDN e-Invoice organization certificates, the organization or legal entity Certificate issued after 18 April 2024 the subject: `organizationIdentifier` attribute in the Certificate is used. It contains Registration Reference for a Legal Entity assigned in accordance with the identified Registration Scheme (listed in Appendix A) used during verification process performed in accordance with Section 3.2.3. The Registration Scheme is identified using the following structure in the presented order:

i. character Registration Scheme identifier;
ii. 2-character ISO 3166 country code for the nation in which the Registration Scheme is operated, or if the scheme is operated globally ISO 3166 code "XG" SHALL be used;
iii. For the NTR Registration Scheme identifier, where registrations are administrated at the subdivision (state or province) level, a plus "+" (0x2B (ASCII), U+002B (UTF-8)) followed by an up-to-three alphanumeric character ISO 3166-2 identifier for the subdivision of the nation in which the Registration Scheme is operated;
iv. a hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8));
v. Registration Reference allocated in accordance with the identified Registration Scheme.

For example:

i. NTRMY-12345678 (NTR Scheme, Malaysia, Unique Identifier at Country level is 12345678)
ii. NTRMY+10-12345678 (NTR Scheme, Malaysia - Selangor, Unique Identifier at State level is 12345678)

For the following types of entities that do not have an identifier from the Registration Schemes listed in Appendix A:

i. For Government Entities, MSC Trustgate enter the Registration Scheme identifier 'GOV' followed by the 2-character ISO 3166 country code for the nation in which the Government Entity is located. If the Government Entity is verified at a subdivision (state or province) level, then a plus "+" (0x2B (ASCII), U+002B (UTF-8)) followed by an ISO 3166-2 identifier for the subdivision (up to three alphanumeric characters) is added.
ii. For International Organization Entities, MSC Trustgate enter the Registration Scheme identifier 'INT' followed by the ISO 3166 code "XG". An International Organization Entity is founded by a constituent document, e.g., a charter, treaty, convention or similar document, signed by, or on behalf of, a minimum of two Sovereign State governments.

For example:

i. GOVMY (Government Entity, Malaysia)
ii. GOVMY+10 (Government Entity, Malaysia - Selangor)
iii. INTXG (International Organization)

For Server Certificate, the `subject:serialNumber` attribute in the Certificate is used in accordance with the EV Guideline.

3.1.6 Recognition, authentication, and role of trademarks

MSC Trustgate shall not approve any Certificate Application that infringes upon the Intellectual Property Rights of others. MSC Trustgate 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 reserves the right to reject any applications and to revoke any Certificate that is involved in a dispute.

3.2 Initial identity validation

MSC Trustgate may use any legal means to authenticate the identity attributes of the Subject to be included in Certificate. For Server and S/MIME Certificate, the applicant shall have control over the Domain and/or Email Address.

MSC Trustgate 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 he/she rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be PKCS #10 format, another cryptographically equivalent demonstration, or MSC Trustgate approved method. This requirement does not apply where a key pair is generated by MSC Trustgate on behalf of an Applicant.

3.2.2 Authentication of organization Identity

For Certificate to include the `subject:organizationName` attribute, MSC Trustgate authenticate the following Organization identity attributes if included in Certificate profiles:

i. Formal name of the Legal Entity;

ii. An Address of the Legal Entity

iii. Jurisdiction of Incoporation or Registration of the Legal Entity;

iv. Unique identifier and type of identifier for the Legal Entity.

v. MSC Trustgate use the `subject:serialNumber` attribute to specify the Organization Business Registration Number. However, for S/MIME certificate, MSC Trustgate use the `subject:organizationIdentifier` attribute to specify the Organization Identifier.

For LHDN e-Invoice organization certificate, `subject:organizationIdentifier` is LHDN Tax Identification Number (TIN)[5].

3.2.2.1 Attribute collection of organization identity

MSC Trustgate collects Organization identity attributes from one of following sources:

i. Reliable data source provided by or through communication with, at least one of the following:

   a. A government agency in the jurisdiction of the Legal Entity's creation, existence or recognition, such as the Companies Commission of Malaysia (Suruhanjaya Syarikat Malaysia), local authorities, or municipal council.

   b. A Legal Entity Identifier (LEI) data reference.

ii. An Attestation that includes a copy of supporting documentation used to establish the Applicant's legal existence, such as a certificate of registration, articles of incorporation, operating agreement, statute, or regulatory act.

3.2.2.2 Validation of organization identity

MSC Trustgate validates all identity attributes of the Organization to be included in the Certificate.

MSC Trustgate verify Applicant's identity and he/she affiliation to the Organization.

If an LEI data reference is used, MSC Trustgate verifies that the RegistrationStatus is ISSUED and the EntityStatus is ACTIVE. MSC Trustgate only allows the use of an LEI if the ValidationSources entry is FULLY_CORROBORATED. MSC Trustgate will not use LEI data reference if ValidationSources entry is PARTIALLY_CORROBORATED, PENDING, or ENTITY_SUPPLIED_ONLY.

[5] Refer to https://sdk.myinvois.hasil.gov.my/signature/

3.2.2.3 DBA/Tradename

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

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

ii. A Reliable Data Source;

iii. Communication with a government agency responsible for the management of such DBAs or tradenames;

iv. An Attestation Letter accompanied by documentary support; or

v. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

3.2.2.4 Verification of Country

If the subject: countryName field is present, then the MSC Trustgate verify the country associated with the Subject using one of the following:

i. 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;

ii. The ccTLD of the requested Domain Name;

iii. Information provided by the Domain Name Registrar; or

iv. A method identified in Section 3.2.2.

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

3.2.3 Authentication of individual identity

For Certificate issued to an Individual, MSC Trustgate authenticates the following Individual identity attributes if included in Certificate profiles:

i. Personal name, or given name(s) and surname(s) which is current name;

ii. National Registration Identity Card (NRIC) number, passport number or any other government-issued identity number;

iii. Pseudonym;

iv. Title;

v. Address; and

vi. Further information as needed to uniquely identify the Applicant.

MSC Trustgate comply with applicable data protection legislation in the gathering and retention of evidence relating to Individual identity supporting this Requirement in accordance with Section 9.4.

3.2.3.1 How Attribute collection of individual identity

MSC Trustgate collects Individual identity attributes from one of following sources:

i. Government-issued photo ID such as MyKad, identity cards, passports or driver license.

ii. Digital certificate from IDP. The Applicant has to digitally sign the Certificate Request using a valid personal Certificate. Identity attributes are collected from the signing Certificate only if the digital signature is valid.

iii. General attestation. MSC Trustgate accepts Individual identity attributes in Applicant's Certificate Request form attested by a commission for oath, notary, other appointed government public officer, or recognized professional bodies.

iv. Records maintained by Enterprise RA.

v. Data passes by TA.

vi. Data passes by AP.

MSC Trustgate also collects company attestation for an Individual to represent an Organization to be included in the subject:organizationName of the Certificate. MSC Trustgate still verifies the identity of the Individual in accordance with this section and the Organization in accordance with Section 3.2.3.

MSC Trustgate may additionally gather and verify supplementary evidence using authorized sources such as additional official documents, government or regulatory registers, or National Registration Department (Jabatan Pendaftaran Negara). Examples of scenarios:

i. Changes of name. If the Subject presents an ID featuring an Applicant name that has subsequently been changed MSC Trustgate inspects an official document such as a marriage certificate or court order documenting the change.

ii. Professional Title of a regulated profession in the subject:country, or a corporate Title linked to the subject:organizationName, MSC Trustgate verify against supporting documentation, a Reliable Data Source, or Attestation.

iii. MSC Trustgate verify the address (but not the identity) of the Applicant using a utility bill, bank statement, credit card statement, EPF statement, or government-issued tax document.

3.2.3.2 Validation of individual identity

MSC Trustgate validates all identity attributes of the Individual to be included in the Certificate.

If the evidence has an explicit validity period, MSC Trustgate verify that the time of the identity validation is within this validity period. The notBefore and notAfter fields of a digital signature Certificate are within the validity period of the document.

The following is the process of MSC Trustgate performing individual identity validation.

i. Validation of government-issued photo ID

MSC Trustgate is to ensure that identity document is a genuine identity document that is not counterfeit or falsified or modified. MSC Trustgate use manual (in person) or online document verification.

If the online document verification cannot automatically validate the identity document, MSC Trustgate validates it manually.

ii. Validation of digital signature with certificate

The identity attributes obtained from the signed Certificate are considered valid. The level of assurance of the digital certificate used must be lower than the level of assurance of the Certificate to be issued.

iii. Validation of a General Attestation and Other Supporting Documents

MSC Trustgate verify the reliability of the attestation before considering the validity of the identity attributes.

iv. Validation using Enterprise and External RA records

An Enterprise and External RA validate all identity attributes of an Individual to be included in the Certificate. The Enterprise and External RA may rely upon existing internal records to validate Individual identity.

v. Validation using TA

MSC Trustgate believes that the data submitted by a TA has been validated through the TA's own processes, which are governed by their respective laws, regulations, or procedures.

vi. Validation for High Assurance Certificates

The application must be certified by a notary public duly appointed under Notaries Public Act 1959[6].

vii. Validation for Document Signing Certificates

MSC Trustgate or the RA validates the information provided by the subscriber (to be included in Certificates such as commonName and serialNumber) during the certificate application process using information available from a reliable data source either manually or online. If the information can't be verified this way, MSC Trustgate will follow the validation process outlined in sections 3.2.3.2 (i) and/or 3.2.3.2 (iii).

viii. Validation for AATL Certificates

MSC Trustgate, its RA, or AP utilize biometric procedures such as face recognition with liveness detection or fingerprint scanning to verify the applicant's identity, as detailed in Section 3.2.3.2 (i). If biometric verification isn't feasible, MSC Trustgate, its RA, or AP will resort to face-to-face verification either in person or via secure video conference. Following a successful verification, a validation process outlined in Section 3.2.3.2 (vii) will be conducted.

ix. Validation for MyGPKI Certificates

For MyGPKI certificates, the GPKI AP submits the verified identity and document onto the MyGPKI portal. MSC Trustgate then validates the identity before certificate issuance.

3.2.4 Validation of Mailbox Authorization or Control

This section outlines the operational procedures for verifying the Applicant's control of Mailbox Addresses for inclusion in issued Certificates.

MSC Trustgate verify that the Applicant controls the email accounts associated with all Mailbox Fields referenced in the Certificate or has obtained authorization from the respective email account holder to act on their behalf.

MSC Trustgate SHALL NOT delegate the verification of mailbox authorization or control.

MSC Trustgate maintain a documented record specifying the validation method used, including the relevant version number from the TLS Baseline Requirements or S/MIME Baseline Requirements, for validating each domain or email address included in issued Certificates.

Once Applicant authority has been validated, it may be considered valid for the issuance of multiple Certificates over time. However, the validation process must always be initiated within the specified time period (such as Section 4.2.1) prior to Certificate issuance.

3.2.4.1 Validating Authority Over Mailbox Via Domain

MSC Trustgate confirm the Applicant, such as an Enterprise RA, has been authorized by the email account holder to act on their behalf by verifying the entity's control over the domain portion of the Mailbox Address intended for use in the Certificate.

MSC Trustgate use methods approved and specified in Section 3.2.2.4 of the TLS Baseline Requirements

to perform this verification.

For domain validation purposes, the term "Applicant" encompasses not only the Applicant itself but also its Parent Company, Subsidiary Company, or Affiliate.

3.2.4.2 Validating Control Over Mailbox Via Email

MSC Trustgate confirms the Applicant's control over each Mailbox Field to be included in a Certificate by sending a Random Value via email and then receiving a confirming response utilizing the Random Value.

[6] As per section 6(3) of DSA.

Control over each Mailbox Address is confirmed using a unique Random Value. The Random Value is sent to the email being validated and is not shared in any other manner.

The Random Value is unique in each email. It remains valid for use in a confirming response for up to 24 hours from its creation.

The Random Value is reset upon each instance of the email sent by MSC Trustgate to a Mailbox Address. However, all relevant Random Values sent to that Mailbox Address can remain valid for use in a confirming response within the specified validity period described in this Section. Additionally, the Random Value is reset upon first use by the user if intended for further use as an authentication factor following the Mailbox Address verification.

3.2.4.3 Validating Applicant as Operator of Associated Mail Server(s)

MSC Trustgate verifies the Applicant's control over each Mailbox Field intended for inclusion in the Certificate by confirming control of the SMTP Fully Qualified Domain Name (FQDN) to which messages delivered to the Mailbox Address should be directed.

The SMTP FQDN is identified using the address resolution algorithm specified in RFC 5321 Section 5.1, which determines the authoritative SMTP FQDNs for a given Mailbox Address. If multiple SMTP FQDNs are discovered, the CA will verify control of one SMTP FQDN following the selection process outlined in RFC 5321 Section 5.1. Aliases in MX record RDATA are not utilized for this validation method.

To confirm control over the SMTP FQDN, MSC Trustgate uses only the currently approved methods detailed in Section 3.2.2.4 of the TLS Baseline Requirements.

3.2.4.4 Validating control over mailbox using ACME extensions

MSC Trustgate MAY confirm the Applicant's control over each Mailbox Field to be included in a Certificate using ACME for S/MIME as defined in RFC 8823. The CA's ACME server MAY respond to a POST request by sending the Random Value token components via email and SMTP, and then receiving a confirming response utilizing the generated Random Value, in accordance with RFC 8823.

Control over each Mailbox Address SHALL be confirmed using a newly-generated Random Value. The Random Value token components SHALL only be shared in accordance with RFC 8823. As defined by RFC 8823, token-part1 SHALL contain at least 128 bits of entropy and token-part2 SHOULD contain at least 128 bits of entropy.

The Random Value SHALL NOT be reused by the MSC Trustgate for other Certificate Requests. The Random Value SHALL remain valid for use in a confirming response for no more than 24 hours from its creation. The MSC Trustgate MAY specify a shorter validity period for Random Values in its CP and/or CPS.

Implementations MAY use ACME External Account Binding as defined by RFC 8555.

3.2.5 Validation of Domain Authorization or Control

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain. MSC Trustgate does not issue certificate when the FQDN contains "onion" as the rightmost label.

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

FQDNs may be listed in Subscriber Certificates using dNSNames in the subjectAltName extension or in Subordinate CA Certificates via dNSNames in permittedSubtrees within the Name Constraints extension.

MSC Trustgate confirm that prior to issuance, each Fully-Qualified Domain Name (FQDN) listed in the Certificate is validated as follows:

3.2.5.1 Validating the Applicant as a Domain Contact

This method (BR Section 3.2.2.4.1) has been retired and not be used. Prior validations using this method and validation data gathered according to this method is not use to issue certificates.

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

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

Each email, fax, SMS, or postal mail MAY confirm control of multiple Authorization Domain Names. MSC Trustgate may send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email, fax, SMS, or postal mail.

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

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

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

Effective January 15, 2025: - When issuing Subscriber Certificates, the CA MUST NOT rely on Domain Contact information obtained using an HTTPS website, regardless of whether previously obtained information is within the allowed reuse period. - When obtaining Domain Contact information for a requested Domain Name the CA: - if using the WHOIS protocol (RFC 3912), MUST query IANA' s WHOIS server and follow referrals to the appropriate WHOIS server. - if using the Registry Data Access Protocol (RFC 7482), MUST utilize IAN's bootstrap file to identify and query the correct RDAP server for the domain. - MUST NOT rely on cached 1) WHOIS server informationthat is more than 48 hours old, or 2) RDAP bootstrap data from IANA that is more than 48 hour sold, to ensure that it relies upon up-to-date and accurate information.

Effective July 15, 2025: - MSC Trustgate MUST NOT rely on this method. - Prior validations using this method and validation data gathered according to this method MUST NOT be used to issue Subscriber Certificates.

3.2.5.3 Phone Contact with Domain Contact

This method has been retired and NOT being used. Prior validations using this method and validation data gathered according to this method will NOT be used to issue certificates.

3.2.5.4 Constructed Email to Domain Contact

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.

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

Random Value is unique in each email. MSC Trustgate may re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient remain unchanged.

The Random Value remains valid for use in a confirming response for no more than 30 daysfrom its creation.

3.2.5.5 Domain Authorization Document

This method has been retired and NOT being used. Prior validations using this method and validation data gathered according to this method will NOT be used to issue certificates.

3.2.5.6 Agreed-Upon Change to Website

This method has been retired and NOT being used. Prior validations using this method and validation data gathered according to this method will NOT be used to issue certificates.

3.2.5.7 DNS Change

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.

MSC Trustgate provide a Random Value unique to the Certificate request and not use the Random Value after

i. 30 days or

ii. if the Applicant submitted the Certificate request, the time frame permitted for reuse of validated information relevant to the Certificate (such as in Section 4.2.1 of these CP/CPS or Section 11.14.3 of the EV Guidelines).

MSC Trustgate performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.10. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective.

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

3.2.5.8 IP Address

Confirming the Applicant's control over the FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with Section 3.2.6.

MSC Trustgate performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.10. To count as corroborating, a Network Perspective MUST observe the same IP address as the Primary Network Perspective.

Note: Once the FQDN has been validated using this method, the MSC Trustgate MUST NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the CA performs separate validations for each of those other FQDNs using authorized methods. This method is NOT suitable for validating Wildcard Domain Names.

3.2.5.9 Test Certificate

This method has been retired and NOT being used. Prior validations using this method and validation data gathered according to this method will NOT be used to issue certificates.

3.2.5.10 TLS Using a Random Value

This method has been retired and NOT being used. Prior validations using this method and validation data gathered according to this method will NOT be used to issue certificates.

3.2.5.11 Any Other Method

This method has been retired and is not used.

3.2.5.12 Validating Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact. This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

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

Effective January 15, 2025: - When issuing Subscriber Certificates, MSC Trustgate NOT rely on Domain Contact information obtained using an HTTPS website, regardless of whether previously obtained information is within the allowed reuse period. - When obtaining Domain Contact information for a requested Domain Name the CA: - if using the WHOIS protocol (RFC 3912), MUST query IANA's WHOIS server and follow referrals to the appropriate WHOIS server. - if using the Registry Data Access Protocol (RFC 7482), MUST utilize IANA's bootstrap file to identify and query the correct RDAP server for the domain. - MUST NOT rely on cached 1) WHOIS server information that is more than 48 hours old, or 2) RDAP bootstrap data from IANA that is more than 48 hours old, to ensure that it relies upon up-to-date and accurate information.

3.2.5.13 Email to DNS CAA Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659, Section 3.

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

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

MSC Trustgates performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.10. To count as corroborating, a Network Perspective MUST observe the same selected contact address used for domain validation as the Primary Network Perspective.

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

3.2.5.14 Email to DNS TXT Contact

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

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

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

MSC Trustgate performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.10. To count as corroborating, a Network Perspective MUST observe the same selected contact address used for domain validation as the Primary Network Perspective.

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

3.2.5.15 Phone Contact with Domain Contact

Confirm the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtain a confirming response to validate the authorized Domain Name (AND). Each phone call MAY confirm control

of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

In the event that someone other than a Domain Contact is reached, MSC Trustgate request to be transferred to the Domain Contact. In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. Random Value MUST be returned to MSC Trustgate to approve the request.

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

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

Effective January 15, 2025: - When issuing Subscriber Certificates, MSC Trustgate NOT rely on Domain Contact information obtained using an HTTPS website, regardless of whether previously obtained information is within the allowed reuse period. - When obtaining Domain Contact information for a requested Domain Name the CA: - if using the WHOIS protocol (RFC 3912), MUST query IANA's WHOIS server and follow referrals to the appropriate WHOIS server. - if using the Registry Data Access Protocol (RFC 7482), MUST utilize IANA's bootstrap file to identify and query the correct RDAP server for the domain. - MUST NOT rely on cached 1) WHOIS server information that is more than 48 hours old, or 2) RDAP bootstrap data from IANA that is more than 48 hours old, to ensure that it relies upon up-to-date and accurate information.

Effective July 15, 2025: - MSC Trustgate NOT rely on this method. Prior validations using this method and validation data gathered according to this method MUST NOT be used to issue Subscriber Certificates.

3.2.5.16 Phone Contact with DNS TXT Record Phone Contact

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

MSC Trustgate MUST NOT knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation. In the event of reaching voicemail, MSC Trustgate may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to MSC Trustgate to approve the request.

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

CAs performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.10. To count as corroborating, a Network Perspective MUST observe the same selected contact address used for domain validation as the Primary Network Perspective.

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

3.2.5.17 Phone Contact with DNS CAA Phone Contact

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

CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659 Section 3. MSC Trustgate MUST NOT be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation.

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

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

MSC Trustgate performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.10. To count as corroborating, a Network Perspective MUST observe the same selected contact address used for domain validation as the Primary Network Perspective.

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

3.2.5.18 Agreed-Upon Change to Website v2

Confirming the Applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file.

i. The entire Request Token or Random Value MUST NOT appear in the request used to retrieve the file, and

ii. MSC Trustgate receives a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Value:

i. MUST be located on the Authorization Domain Name, and

ii. MUST be located under the "/.well-known/pki-validation" directory, and

iii. MUST be retrieved via either the "http" or "https" scheme, and

iv. MUST be accessed over an Authorized Port.

If MSC Trustgate follows redirects, the following apply:

i. Redirects MUST be initiated at the HTTP protocol layer.

   a) For validations performed on or after July 1, 2021, redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.

   b) For validations performed prior to July 1, 2021, redirects MUST be the result of an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4. MSC Trustgate SHOULD limit the accepted status codes and resource URLs to those defined within i.a.

ii. Redirects MUST be to resource URLs with either the "http" or "https" scheme.

iii. Redirects MUST be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:

i. MSC Trustgate provides a Random Value unique to the certificate request.

ii. The Random Value MUST remain valid for use in a confirming response for no more than 30

days from its creation.

Except for Onion Domain Names, MSC Trustagte performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.10. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective.

Note: MSC Trustgate does NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless MSC Trustgate performs separate validations for each of those other FQDNs using authorized methods. This method is NOT suitable for validating Wildcard Domain Names.

3.2.5.19 Agreed-Upon Change to Website - ACME

Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555. The following are additive requirements to RFC 8555.

MSC Trustgate MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The token (as defined in RFC 8555, Section 8.3) MUST NOT be used for more than 30 days from its creation.

If the MSC Trustgate follows redirects, the following apply:

i. Redirects MUST be initiated at the HTTP protocol layer.

   a) For validations performed on or after July 1, 2021, redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.

   b) For validations performed prior to July 1, 2021, redirects MUST be the result of an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4. CAs SHOULD limit the accepted status codes and resource URLs to those defined within i.a.

ii. Redirects MUST be to resource URLs with either the "http" or "https" scheme.

iii. Redirects MUST be to resource URLs accessed via Authorized Ports.

Except for Onion Domain Names, MSC Trustgate performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.10. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. token) as the Primary Network Perspective.

Note: MSC Trustgate does NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the CA performs separate validations for each of those other FQDNs using authorized methods. This method is NOT suitable for validating Wildcard Domain Name

3.2.5.20 TLS Using ALPN

Confirming the Applicant's control over a FQDN by validating domain control of the FQDN by negotiating a new application layer protocol using the TLS Application-Layer Protocol Negotiation (ALPN) Extension [RFC7301] as defined in RFC 8737. The following are additive requirements to RFC 8737.

The token (as defined in RFC 8737, Section 3) MUST NOT be used for more than 30 days from its creation.

Except for Onion Domain Names, MSC Trustgate performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.10. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. token) as the Primary Network Perspective.

Note: Once the FQDN has been validated using this method, MSC Trustgate does NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the CA performs separate validations for each of those other FQDNs using authorized methods. This method is NOT suitable for validating Wildcard Domain Names.

3.2.6 Authentication for an IP Address

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of an IP Address listed in a Certificate.

MSC Trustgate confirm that, prior to issuance, each IP Address listed in the Certificate has been validated using at least one of the methods specified in this section.

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 of this CP/CPS) prior to Certificate issuance. For purposes of IP Address validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

After July 31, 2019, MSC Trustgate SHALL maintain a record of which IP validation method, including the relevant BR version number, was used to validate every IP Address.

3.2.6.1 Agreed-Upon Change to Website

Confirming the Applicant's control over the requested IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of validating control of IP Addresses, on the IP Address that is accessible by MSC Trustgate via HTTP/HTTPS over an Authorized Port. The Request Token or Random Value MUST NOT appear in the request.

If a Random Value is used, MSC Trustgate provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of

i. 30 days or

ii. if the Applicant submitted the certificate request, the time frame permitted for reuse of validated information relevant to the certificate (such as in Section 4.2.1 of this document).

MSC Trustgate MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.10 when performing validations using this method. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective.

3.2.6.2 Email, Fax, SMS, or Postal Mail to IP Address Contact

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

Each email, fax, SMS, or postal mail MAY confirm control of multiple IP Addresses.

MSC Trustgate send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the IP Address Registration Authority as representing the IP Address Contact for every IP Address being verified using the email, fax, SMS, or postal mail.

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

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

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

3.2.6.3 Reverse Address Lookup

Confirming the Applicant's control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under Section 3.2.5.

MSC Trustgate performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.10. To count as corroborating, a Network Perspective MUST observe the same FQDN as the Primary Network Perspective.

3.2.6.4 Any Other Method

Using any other method of confirmation, including variations of the methods defined in Section 3.2.6, provided that the CA maintains documented evidence that the method of confirmation establishes that the Applicant has control over the IP Address to at least the same level of assurance as the methods previously described in version 1.6.2 of these CA/ Browser Forum Baseline Requirements.

MSC Trustgate SHALL NOT perform validations using this method after July 31, 2019. Completed validations using this method SHALL NOT be re-used for certificate issuance after July 31, 2019. Any certificate issued prior to August 1, 2019 containing an IP Address that was validated using any method that was permitted under

the prior version of this Section 3.2.6 MAY continue to be used without revalidation until such certificate naturally expires.

3.2.6.5 Phone Contact with IP Address Contact

Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number and obtaining a response confirming the Applicant's request for validation of the IP Address. MSC Trustgate place the call to a phone number identified by the IP Address Registration Authority as the IP Address Contact. Each phone call SHALL be made to a single number.

In the event that someone other than an IP Address Contact is reached, MSC Trustgate MAY request to be transferred to the IP Address Contact.

In the event of reaching voicemail, MSC Trustgate may leave the Random Value and the IP Address(es) being validated. The Random Value SHALL be returned to MSC Trustgate to approve the request.

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

3.2.6.6 ACME "http-01" method for IP Addresses

Reserved.

3.2.6.7 ACME "tls-alpn-01" method for IP Addresses

Reserved.

3.2.7 Wildcard Domain Validation

Before issuing a Wildcard Certificate, MSC Trustgate establish and follow a documented procedure that determines if the FQDN portion of any Wildcard Domain Name in the Certificate is"registry-controlled" or is a "public suffix" (e.g. "*.com", "*.co.uk", see RFC 6454 Section 8.2 for further explanation).

If the FQDN portion of any Wildcard Domain Name is "registry-controlled" or is a "public suffix", MSC Trustgate MUST refuse issuance unless the Applicant proves its rightful control of the entire Domain Namespace. (e.g. MSC Trustgate MUST NOT issue "*.co.uk" or "*.local", but MAY issue "*.example.com" to Example Co.).

Determination of what is "registry-controlled" versus the registerable portion of a Country Code Top-Level Domain Namespace is not standardized at the time of writing and is not a property of the DNS itself. Current best practice is to consult a "public suffix list" such as the Public Suffix List (PSL), and to retrieve a fresh copy regularly.

If using the PSL, MSC Trustgate SHOULD consult the "ICANN DOMAINS" section only, not the "PRIVATE DOMAINS" section. The PSL is updated regularly to contain new gTLDs delegated by ICANN, which are listed in the "ICANN DOMAINS" section. A CA is not prohibited from issuing a Wildcard Certificate to the Registrant of an entire gTLD, provided that control of the entire namespace is demonstrated in an appropriate way.

3.2.8 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, MSC Trustgate evaluate the source for its reliability, accuracy and resistance to alteration or falsification. MSC Trustgate considers the following criteria for its decision whether or not to accept data from a Data Source:

i. The age of the information provided,

ii. The frequency of updates to the information source,

iii. The data provider and purpose of the data collection,

iv. The public accessibility of the data availability, and

v. The relative difficulty in falsifying or altering the data.

Databases maintained by MSC Trustgate do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under this Section 3.2.

3.2.9 CAA Records

As part of the Certificate issuance process, MSC Trustgate MUST retrieve and process CAA records in accordance with RFC 8659 for each dNSName in the subjectAltName extension that does not contain an Onion Domain Name. These practices MUST be described in Section 4.2 of the CA's Certificate Policy and/or Certification Practice Statement, including specifying the set of Issuer Domain Names that the CA recognizes in CAA "issue" or "issuewild" records as permitting it to issue.

Some methods relied upon for validating the Applicant's ownership or control of the subject domain(s) (see Section 3.2.5) or IP address(es) (see Section 3.2.6) to be listed in a certificate require CAA records to be retrieved and processed from additional remote Network Perspectives before Certificate issuance (see Section 3.2.2.9). To corroborate the Primary Network Perspective, a remote Network Perspective's CAA check response MUST be interpreted as permission to issue, regardless of whether the responses from both Perspectives are byte-for-byte identical. Additionally, MSC Trustgate MAY consider the response from a remote Network Perspective as corroborating if one or both of the Perspectives experience an acceptable CAA record lookup failure, as defined in this section.

MSC Trustgate MAY check CAA records at any other time.

When processing CAA records, MSC Trustgate MUST process the issue, issuewild, and iodef property tags as specified in RFC 8659, although they are not required to act on the contents of the iodef property tag. Additional property tags MAY be supported, but MUST NOT conflict with or supersede the mandatory property tags set out in this document. MSC Trustgate MUST respect the critical flag and not issue a certificate if they encounter an unrecognized property tag with this flag set.

If MSC Trustgate issues a certificate after processing a CAA record, it MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater.

RFC 8659 requires that CAs "MUST NOT issue a certificate unless the CA determines that either (1) the certificate request is consistent with the applicable CAA RRset or (2) an exception specified in the relevant CP or CPS applies." For issuances conforming to these Baseline Requirements, MSC Trustgate MUST NOT rely on any exceptions specified in their CP/CPS unless they are one of the following:

i. CAA checking is optional for certificates for which a Certificate Transparency Precertificate (see Section 7.1.2.9 of CAB/F Baseline Requirement) was created and logged in at least two public logs, and for which CAA was checked at time of Precertificate issuance.

ii. CAA checking is optional for certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Section 7.1.2.3 of CAB/F Baseline Requirement or Section 7.1.2.5 of CAB/F Baseline Requirement, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.

MSC Trustgate are permitted to treat a record lookup failure as permission to issue if:

i. the failure is outside the CA's infrastructure; and

ii. the lookup has been retried at least once; and

iii. the domain's zone does not have a DNSSEC validation chain to the ICANN root.

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

3.2.10 Multi-Perspective Issuance Corroboration

Multi-Perspective Issuance Corroboration attempts to corroborate the determinations (i.e., domain validation pass/fail, CAA permission/prohibition) made by the Primary Network Perspective from multiple remote Network Perspectives before Certificate issuance.

MSC Trustgate uses either the same set, or different sets of Network Perspectives when performing MultiPerspective Issuance Corroboration for the required:

i. Domain Authorization or Control and
ii. CAA Record checks

The set of responses from the relied upon Network Perspectives provides MSC Trustgate with the necessary information to allow it to affirmatively assess:

i. The presence of the expected:
   a) Request Token;
   b) IP Address; or
   c) Contact Address, as required by the relied upon validation method specified in Sections 3.2.5 and 3.2.9 of this CP/CPS; and
   d) Contact address
ii. MSC Trustgate authority to issue to the requested domain(s), as specified in Section 4.2.1.1.

Results or information obtained from one Network Perspective will not be reused or cached when performing validation through subsequent Network Perspectives (e.g., different Network Perspectives cannot rely on a shared DNS cache to prevent an adversary with control of traffic from one Network Perspective from poisoning the DNS cache used by other Network Perspectives). The network infrastructure providing Internet connectivity to a Network Perspective MAY be administered by the same organization providing the computational services required to operate the Network Perspective. All communications between a remote Network Perspective and MSC Trustgate will take place over an authenticated and encrypted channel relying on modern protocols (e.g., over HTTPS). A Network Perspective can use a recursive DNS resolver that is not co-located with the Network Perspective. However, the DNS resolver used by the Network Perspective will fall within the same Regional Internet Registry service region as the Network Perspective relying upon it. Furthermore, for any pair of DNS resolvers used on a Multi-Perspective Issuance Corroboration attempt, the straight-line distance between the two DNS resolvers will be at least 500 km. The location of a DNS resolver is determined by the point where unencapsulated outbound DNS queries are typically first handed off to the network infrastructure providing Internet connectivity to that DNS resolver.

MSC Trustgate may immediately retry Multi-Perspective Issuance Corroboration using the same validation method or an alternative method (e.g., MSC Trustgate can immediately retry validation using “Email to DNS TXT Contact” if “Agreed-Upon Change to Website - ACME” does not corroborate the outcome of Multi-Perspective Issuance Corroboration). When retrying Multi-Perspective Issuance Corroboration, MSC Trustgate must not rely on corroborations from previous attempts. There is no stipulation regarding the maximum number of validation attempts that may be performed in any period of time.

The "Quorum Requirements" Table describes quorum requirements related to Multi-Perspective Issuance Corroboration. If MSC Trustgate does not rely on the same set of Network Perspectives for both Domain Authorization or Control and CAA Record checks, the quorum requirements will be met for both sets of Network Perspectives (i.e.,the Domain Authorization or Control set and the CAA record check set). Network Perspectives are considered distinct when the straight-line distance between them is at least 500 km. Network Perspectives are considered "remote" when they are distinct from the Primary Network Perspective and the other Network Perspectives represented in a quorum.

MSC Trustgate may reuse corroborating evidence for CAA record quorum compliance for a maximum of 398 days. After issuing a Certificate to a domain, remote Network Perspectives may omit retrieving and processing CAA records for the same domain or its subdomains in subsequent Certificate requests from the same Applicant for up to a maximum of 398 days.

Quorum Requirements Table

# of Distinct Remote Network Perspectives Used	# of Allowed non-Corroborations
2-5	1
6+	2

Remote Network Perspectives performing Multi-Perspective Issuance Corroboration must rely upon networks (e.g., Internet Service Providers or Cloud Provider Networks) implementing measures to mitigate BGP routing incidents in the global Internet routing system for providing internet connectivity to the Network Perspective.

For TLS Certificates issued on or after March 15th, 2025, MSC Trustgate will require Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. MSC Trustgate may proceed with certificate issuance if the number of remote Network Perspectives that do not corroborate the determinations made by the Primary Network Perspective ("non-corroborations") is greater than allowed in the Quorum Requirements table.

3.2.11 Non-verified subscriber information

MSC Trustgate does not include Subscriber information that has not been verified in accordance with this CP/CPS.

3.2.12 Validation of authority

MSC Trustgate has implemented a procedure to determine the authorized individuals that can request certificates on behalf of an organization. Each organization may limit authorized certificate requestors.

Registration Authorities have procedures per which the Applicant's status and relationship with the organization are being verified. This is possible either with electronic lists assembled by each RA from the qualified source (such as human resources department), or by presenting official id where the relationship of the Applicant with the organization is certified.

MSC Trustgate uses information from data sources per section 3.2.3 to establish a reliable method of communication.

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

For Extended Validation Certificate requests (either EV SSL/TLS or EV Code Signing), MSC Trustgate shall follow procedures described in section 11.8 of the Guidelines For The Issuance and Management of Extended Validation Certificates to verify the authority of the request.

3.2.13 Criteria for interoperation

No Stipulation.

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 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 may perform some revalidation of the Applicant but may also rely on information previously provided or obtained.

MSC Trustgate 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.

MSC Trustgate do require letter of authorization of the organization if the certificate have organization in the subjectDN.

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

Before the revocation process of a Certificate, MSC Trustgate verifies that the revocation is requested by the Certificate's Subscriber, the entity that approved the Certificate Application, for procedure to authenticating the revocation request of a Subscriber include:

i. 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.)

ii. Receiving a message from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked,

iii. 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 Administrators are entitled to request the revocation of end-user Subscriber Certificates within MSC Trustgate's PKI platform and authenticate the identity of Administrator via access control using SSL and client authentication before permitting them to perform revocation functions.

RAs using an Automated Administration Software Module may submit bulk revocation requests to MSC Trustgate. 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 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:

i. Any individual who is the subject of the certificate,

ii. Any authorized representative of an Organization or entity,

iii. Any authorized representative of an RA/TA/AP.

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 Enrolment process and responsibilities

4.1.2.1 End-User Certificate Subscribers

Before issuing a certificate, MSC Trustgate obtains a certificate request along with an executed Subscriber Agreement and Terms of Use, which may be electronic and in line with the CA/B Forum requirements. Undergo an enrolment process (in no particular order) consisting of:

i. Completing a Certificate Application and providing true and correct information;

ii. Generating, or arranging to have generated, a key pair;

iii. Generating a Certificate Signing Request(CSR) using an appropriately secure tool;

iv. Delivering his, her, or its public key, directly to MSC Trustgate or through an RA/TA/AP;

v. Demonstrating possession and/or exclusive control of the private key corresponding to the public key delivered to MSC Trustgate;

vi. Agreeing to the applicable Subscriber Agreement or Term of Access; and

vii. Paying any applicable fees.

4.1.2.2 RA/TA/AP Certificates

RA/TA/AP Certificates enter into a contract with MSC Trustgate. RA/TA/AP applicant 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 RA/TA/AP key pair, the applicant shall cooperate with MSC Trustgate to determine the appropriate distinguished name and the content of the Certificate to be issued by the applicant.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

MSC Trustgate or an RA shall perform identification and authentication of all Applicants' information to be included in the Certificate as set forth in Section 3.2. If an RA assists in the verification, the RA must create and maintain records sufficient to establish that it has performed the required verification tasks and communicate the completion of such task to MSC Trustgate for issuance of certificates.

In cases where the certificate request does not contain all the necessary information about the Applicant, MSC Trustgate SHALL obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant.

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

Section 6.3.2 limits the validity period of Subscriber Certificates.

MSC Trustgate MAY reuse completed validations and/or supporting evidence performed in accordance with Section 3.2 within the following limits:

For Organization and Individual Validation of TLS:

i. Certificate issued before March 15, 2026 – 825 days
ii. Certificate issued on or after March 15, 2026 – 398 days

For validation of Domain Names and IP Addresses of TLS:

i. Certificate issued before March 15, 2026 - 398 day
ii. Certificate issued on or after March 15, 2026, and before March 15, 2027 - 200 days
iii. Certificate issued on or after March 15, 2027, and before March 15, 2029 - 100 days
iv. Certificate issued on or after March 15, 2029 – 10 days

For Validation of mailbox authorization or control of S/MIME:

i. Completed validation of the control of a mail server in accordance with Section 3.2.4.1 or Section 3.2.4.3 – 398 days
ii. Completed validation of control of a mailbox in accordance with Section 3.2.4.2 SHALL be obtained no more than 30 days prior to issuing the Certificate.

For Organization Validation of S/MIME and Document Signing:

i. Formal name of the Legal Entity – 825 days
ii. A registered Assumed Name for the Legal Entity (if included in the Subject) – 825 days
iii. An address of the Legal Entity (if included in the Subject) – 825 days
iv. Jurisdiction of Incorporation or Registration of the Legal Entity – 825 days
v. Organization Identifier and type of identifier for the Legal Entity – 825 days
vi. Validation of authority – 825 days (unless a contract between the CA and the Applicant specifies a different term. For example, the contract MAY include the perpetual assignment of roles until revoked by the Applicant or CA, or until the contract expires or is terminated).

For Individual Validation of S/MIME and Document Signing:

i. Given name(s) and surname(s)– 825 days
ii. Pseudonym (if used – 825 days
iii. Title (if used) – 825 days
iv. Address (if displayed in Subject) – 825 days
v. Further information as needed to uniquely identify the Applicant – 825 days

For TLS EV Certificates, except for reissuance of an EV Certificate under section 11.14.2 of the EV Guidelines and except when permitted otherwise in section 11.14.1 of the EV Guidelines, the age of all data used to support issuance of an EV Certificate (before revalidation is required) SHALL NOT exceed the following limits:

i. Legal existence and identity – 398 days;
ii. Assumed name – 398 days;
iii. Address of Place of Business – 398 days;
iv. Verified Method of Communication – 398 days;
v. Operational existence – 398 days;
vi. Domain Name – 397 days;

For Code Signing:

i. Legal existence and identity – 398 days;
ii. Assumed name – 398 days;
iii. Address of Place of Business – 398 days;
iv. Verified Method of Communication – 398 days;
v. Operational existence – 398 days;
vi. Name, Title, Agency, and Authority – 398 days, unless a contract between MSC Trustgate and the Applicant specifies a different term, in which case, the term specified in such contract controls. For example, the contract MAY include the perpetual assignment of EV roles until revoked by the Applicant or CA, or until the contract expires or is terminated.

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

4.2.1.1 CAA Checking

MSC Trustgate check for a CAA record in the DNS for each DNSName in the subjectAltName extension, excluding Onion Domain Names as per RFC8659, prior to issuing a TLS certificate. MSC Trustgate processes the "issue" and "issuewild" property tags.

Prior to issuing an S/MIME certificate on or after March 15, 2025, MSC Trustgate check the DNS for the existence of a CAA record in accordance with RFC 9495 for each Mailbox Address in the subjectAltName extension of the S/MIME certificate to be issued. MSC Trustgate processes the "issuemail" property tag and may not dispatch reports of issuance requests to the contact(s) listed in an "iodef" property tag.

If the Certificate is issued, it will be issued within the Time to Live (TTL) of the CAA record, or 8 hours, whichever is greater. MSC Trustgate logs actions taken based on CAA records, and documents issuance

prevented by CAA. CAA checking is optional for certificates issued by a Technically Constrained Subordinate CA Certificate. MSC Trustgate's CAA issuer domain is "msctrustgate.com".

MSC Trustgate may treat a record lookup failure as permission to issue if:

i. The failure is outside the MSC Trustgate's infrastructure; and
ii. The lookup has been retried at least once; and
iii. The domain's zone does not have a DNSSEC validation chain to the ICANN root.

After verification, the Issuer CA assesses the information and determines whether to issue the certificate.

4.2.2 Approval or rejection of certificate applications

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

i. Successfully completed the identification and authentication of all required Subscriber information as set forth in Section 3.2.
ii. Payment has been received.

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

i. Identification and authentication of all required Subscriber information as set forth in Section 3.2 cannot be completed, or
ii. The Subscriber fails to furnish supporting documentation upon request, or
iii. The application has previously been rejected or violation of subscriber agreement, or
iv. Payment has not been received, or
v. The RA believes that issuing a certificate to the Subscriber could damage or diminish MSC Trustgate reputation or business.

MSC Trustgate 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.

MSC Trustgate shall not issue certificates containing internal name.

4.2.3 Time to process certificate applications

Under normal circumstances, MSC Trustgate 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 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 can delay the issuance process.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

4.3.1.1 Manual authorization of certificate issuance for Root CAs

MSC Trustgate 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 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 (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.

4.3.1.2 Linting of to-be-signed Certificate content

MSC Trustgate consider Linting process is best practice to implement to test the technical conformity of each to-be-signed artifact prior to signing it. Effective March 15, 2025, MSC Trustgate SHOULD implement a Linting process testing compliance with these Requirements for S/MIME Certificates. Effective September 15, 2025 the MSC Trustgate SHALL implemented a Linting process testing compliance with these Requirements.

Methods used to produce a Certificate containing the to-be-signed Certificate content include, but are not limited to:

i. Sign the tbsCertificate with a "dummy" Private Key whose Public Key component is not certified by a Certificate that chains to a publicly-trusted CA Certificate; or
ii. Specify a static value for the signature field of the Certificate ASN.1 SEQUENCE.

MSC Trustgate MAY implement its own Certificate Linting tools, but SHOULD use the Linting tools that have been widely adopted by the industry (see https://cabforum.org/resources/tools/).

MSC Trustgate contribute to open-source Linting projects, such as by:

i. Creating new or improving existing lints;
ii. Reporting potentially inaccurate linting results as bugs;
iii. Notifying maintainers of Linting software of checks that are not covered by existing lints;
iv. Updating documentation of existing lints; and
v. Generating test Certificates for positive/negative tests of specific lints.

4.3.1.3 Linting of issued Certificates

MSC Trustgate MAY use a Linting process to test each issued Certificate.

4.3.2 Notification to subscriber by the CA of issuance of certificate

MSC Trustgate 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 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's Subscriber Agreement, the terms of this CP/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 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 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 repository.

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

i. The digital signature was created during the operational period of a valid Certificate and can be verified by referencing a valid Certificate,

ii. 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

iii. The Certificate is being used for its intended purpose and in accordance with this CP/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 may renew a Certificate if:

i. The associated Public Key has not reached the end of its validity period,

ii. The Subscriber and attributes are consistent,

iii. The associated Private Key remains uncompromised, and

iv. Re-verification of subscriber identity is not required by Section 3.3.1.

MSC Trustgate may also renew a Certificate if a CA Certificate is re-keyed or as otherwise necessary to provide services to a customer. MSC Trustgate may also notify Subscribers prior to a Certificate's expiration date. Certificate renewal requires payment of additional fees. MSC Trustgate 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 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 enrolment 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 re-enrolment information, and the re-enrolment information (including Corporate and Technical contact information[7]) has not changed, a renewal Certificate is automatically issued.

Alternative to a Challenge Phrase (or equivalent) MSC Trustgate 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 will issue the Certificate if the enrolment information (including corporate and technical contact information) has not changed.

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

For AATL certificates MSC Trustgate re-authenticates the Organization name and domain name included in the certificate at intervals described in Section 6.3.2. In circumstances where:

i. The challenge phrase is correctly used for the subsequent renewal certificate and;

ii. The certificate Distinguished Name has not been changed, and

iii. The Corporate and Technical Contact information remains unchanged from that, which was previously verified.

MSC Trustgate 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.

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

Other than this procedure or another MSC Trustgate 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

Conduct constituting Notification of a renewed certificate 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.

4.6.6 Publication of the renewal certificate by the CA

The renewed certificate is published in MSC Trustgate'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 re-key

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 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 may initiate a certificate re-key at the request of the certificate subject or at MSC Trustgate's own discretion.

4.7.3 Processing certificate re-keying requests

MSC Trustgate 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 can issue a replacement Certificate using a previously issued Certificate or previously provided CSR. MSC Trustgate re-uses existing verification information unless re-verification and authentication is required under section 3.3.1 or if MSC Trustgate believes that the information has become inaccurate.

4.7.4 Notification of new certificate issuance 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 re-keyed certificate

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

4.7.6 Publication of the re-keyed certificate by the CA

The re-keyed certificate is published in MSC Trustgate'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 Circumstance 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 CP/CPS. The new Certificate may have the same or a different subject Public Key.

4.8.2 Who may request certificate modification

MSC Trustgate modifies Certificates at the request of certain certificate subjects or in its own discretion. MSC Trustgate 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 verifies any information that will change in the modified Certificate. MSC Trustgate will only issue the modified Certificate after completing the verification process on all modified information. MSC Trustgate 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 new certificate issuance 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 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 upon request.

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

MSC Trustgate MAY support revocation of Short-lived Subscriber Certificates.

With the exception of Short-lived Subscriber Certificates, MSC Trustgate will revoke a Certificate within twenty-four (24) hours and use the corresponding CRLReason after confirming one or more of the following occurred:

i. The Subscriber requests in writing, without specifying a CRLreason, that the CA revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);

ii. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);

iii. MSC Trustgate obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);

iv. MSC Trustgate is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate, including but not limited to those identified in Section 6.1.1.3(5) (CRLReason #1, keyCompromise)

v. The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded).

With the exception of Short-lived Subscriber Certificates, MSC Trustgate 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:

i. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 (CRLReason #4, superseded);

ii. MSC Trustgate obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);

iii. MSC Trustgate is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use (CRLReason #9, privilegeWithdrawn);

iv. MSC Trustgate is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator; has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation);

v. MSC Trustgate is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);

vi. MSC Trustgate is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);

vii. MSC Trustgate is made aware that the Certificate was not issued in accordance with CA/B forum Requirements or the MSC Trustgate's Certification Practice Statement (CRLReason #4, superseded);

viii. MSC Trustgate's determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);

ix. MSC Trustgate's right to issue Certificates under CA/B forum Requirements expires or is revoked or terminated, unless MSC Trustgate has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);

x. Revocation is required by the MSC Trustgate's Certificate Policy and/or Certification Practice Statement for a reason that is not otherwise required to be specified by this section 4.9.1.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL); or

xi. MSC Trustgate is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise).

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

i. Either the Subscriber's or MSC Trustgate's obligations under the CP/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;

ii. MSC Trustgate received a lawful and binding order from a government or regulatory body to revoke the Certificate;

iii. MSC Trustgate ceased operations and did not arrange for another Certificate authority to provide revocation support for the Certificates;

iv. The technical content or format of the Certificate presents an unacceptable risk to application software vendors, Relying Parties, or others;

v. 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 Malaysia;

MSC Trustgate 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.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

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

i. The Subordinate CA requests revocation in writing;

ii. The Subordinate CA notifies the MSC Trustgate that the original certificate request was not authorized and does not retroactively grant authorization;

iii. MSC Trustgate 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 Section 6.1.5 and Section 6.1.6;

iv. MSC Trustgate obtains evidence that the Certificate was misused;

v. MSC Trustgate is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;

vi. MSC Trustgate determines that any of the information appearing in the Certificate is inaccurate or misleading;

vii. MSC Trustgate or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;

viii. MSC Trustgate or Subordinate CAs right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or

ix. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.

MSC Trustgate will revoke a cross-Certificate if the cross-certified entity (including MSC Trustgate) 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 may also revoke an Administrator Certificate if the Administrator's authority to act as Administrator has been terminated or otherwise has ended.

MSC Trustgate Subscriber Agreements require end-user Subscribers to immediately notify MSC Trustgate 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 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 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 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

MSC Trustgate provides a process for subscribers to request revocation of their own certificates as described in this CP/CPS.

MSC Trustgate processes a revocation request as follows:

i. MSC Trustgate logs the request or problem report, including the requestor's contact information through the revocation form, and includes reasons for revocation in the log.
ii. MSC Trustgate verifies the revocation request from the subscriber, where applicable, via telephone communication and others.
iii. If the request is authenticated, MSC Trustgate revokes the Certificate according to the timelines listed in 4.9.1.
iv. For requests from third parties, MSC Trustgate's personnel investigate the request within 24 hours after receiving the request and decide whether revocation is appropriate based on the following criteria:
    a) the nature of the reported problem;
    b) the identity of the complainants;
    c) relevant legislation;
    d) the potential impact on stakeholders;
    e) the credibility and authenticity of the evidence provided; or
    f) compliance with internal policies and industry best practices.
v. If MSC Trustgate determines that revocation is necessary, MSC Trustgate personnel will revoke the certificate and update the certificate status accordingly. Additionally, if deemed appropriate, MSC Trustgate may escalate the revocation reports to law enforcement authorities.

MSC Trustgate maintains a continuous 24/7 ability to internally respond to any high priority revocation requests and certificate problem reports via helpdesk@msctrustgate.com and other resources as indicated in Section 1.5.2 of this CP/CPS.

For CA or RA requesting revocation of its CA or RA Certificate is required to communicate the request to MSC Trustgate. MSC Trustgate will then revoke the Certificate. MSC Trustgate 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 may grant and extend revocation grace periods on a case-by-case basis if it does not violate this CP/CPS, or any of the relevant requirements as listed in the sources of section 1.6.3.

MSC Trustgate 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 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 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 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 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 will consider the following criteria:

i. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
ii. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
iii. The number of Certificate problem reports received about a particular Certificate or Subscriber;
iv. 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
v. Relevant legislation.

Under normal operating circumstances, MSC Trustgate 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:

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

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

i. Subscriber certificates

MSC Trustgate updates CRLs are issued at least once every seven days, and the value of the nextUpdate field is not more than ten days beyond the value of the thisUpdate field. A new CRL is published within 24 hours of revoking a certificate.

ii. Subordinate CA and Timestamp

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

MSC Trustgate continue issuing CRLs until one of the following is true:

i. all Subordinate CA;

ii. Certificates containing the same Subject Public Key are expired or revoked; or

iii. the corresponding Subordinate CA Private Key is destroyed.

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.

CRLs, and the serial number of a revoked certificate MUST remain on the CRL for at least 10 years after the expiration of the certificate for Code Signing Certificates and Timestamp Certificates.

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:

i. Are signed by the CA that issued the Certificates whose revocation status is being checked, or

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

For the status of Subscriber Certificates:

i. OCSP responses have a validity interval greater than or equal to eight hours;

ii. OCSP responses MUST have a validity interval less than or equal to ten days;

iii. For OCSP responses with validity intervals less than sixteen hours, then MSC Trustgate updates the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.

iv. For OCSP responses with validity intervals greater than or equal to sixteen hours, then the MSC Trustgate updates the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For the status of Subordinate CA Certificates, MSC Trustgate updates information provided via an Online Certificate Status Protocol (i) at least every twelve months; and (ii) within 24 hours after revoking a Subordinate CA Certificate.

OCSP Responders under MSC Trustgate's direct control will not respond with a "good" status for a certificate that has not been issued.

MSC Trustgate MAY provide OCSP responses for Code Signing Certificates and Timestamp Certificates for the time period specified in this CP/CPS, which MAY be at least 10 years after the expiration of the certificate.

4.9.11 Other forms of revocation advertisements available

No Stipulation.

4.9.12 Special requirements re key compromise

MSC Trustgate uses commercially reasonable efforts to inform the subscribers if it discovers or suspects their Private Keys may have been compromised. If the key compromised had been ascertained, MSC Trustgate shall revoke the certificate using the procedure as set forth in Section 4.9.1. MSC Trustgate will transition any revocation reason code in a CRL to "key compromise" upon discovery of such reason or as required by an applicable Certificate Profile.

4.9.13 Circumstances for suspension

The Repository MUST NOT include entries that indicate that a Certificate is suspended.

4.9.14 Who can request suspension

No Stipulation.

4.9.15 Procedure for suspension request

No Stipulation.

4.9.16 Limits on suspension period

No Stipulation.

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.

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. MSC Trustgate 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.

4.10.3 Operational features

No Stipulation.

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 and practices

MSC Trustgate never escrows CA Private Keys under this CP/CPS.

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

i. From the Subscriber or Subscriber's organization if the Subscriber has lost or damaged the private-key token;

ii. From the Subscriber's organization, if the Subscriber is not available or is no longer part of the organization that contracted with MSC Trustgate for Private Key escrow;

iii. From an authorized investigator or auditor, if the Private Key is part of a required investigation or audit;

iv. From a requester authorized by a competent legal authority to access the communication that is encrypted using the key;

v. From a requester authorized by law or governmental regulation; or

vi. From an entity contracting with MSC Trustgate for escrow of the Private Key when key recovery is mission critical or mission essential.

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

i. Notify Subscribers and get his or her consent that their Private Keys are escrowed;

ii. Protect escrowed keys from unauthorized disclosure;

iii. Protect any authentication mechanisms that could be used to recover escrowed Private Keys;

iv. Release an escrowed key only after making or receiving (as applicable) a properly authorized request for recovery; and

v. 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

No Stipulation

5 MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

The CA/Browser Forum's Network and Certificate System Security Requirements are incorporated by reference as if fully set forth herein.

5.1 Physical security controls

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

5.1.1 Site location and construction

MSC Trustgate 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 also maintains disaster recovery facilities for its CA operations. MSC Trustgate's disaster recovery facilities are protected by multiple tiers of physical security comparable to those of MSC Trustgate'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 protects such online 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 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'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 personnel who are 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'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 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 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 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.

5.1.3 Power and air conditioning

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

i. Power systems to ensure continuous, uninterrupted access to electric power and

ii. Heating/ ventilation/ air conditioning systems to control temperature and relative humidity.

5.1.4 Water exposures

The cabinets housing MSC Trustgate'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 protects its media from accidental damage, environmental hazards, and unauthorized physical access. Backup files are created on a daily basis. MSC Trustgate's backup files are maintained at locations separate from MSC Trustgate'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 with the manufacturers' guidance prior to disposal.

5.1.8 Off-site backup

MSC Trustgate maintains at least one full backup and makes regular backup copies of any information necessary to recover from a system failure. These backups including copies of CA Private Keys and activation data are stored at offsite facilities equipped with physical and procedural safeguards appropriate to their operational environment.

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:

i. The validation of information in Certificate Applications;

ii. The acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrolment information;

iii. The issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository;

iv. The handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

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 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 CP/CPS.

5.2.2 Number of persons required per task

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

i. Issued access devices and granted access to the required facilities;

ii. Issued electronic credentials to access and perform specific functions on MSC Trustgate 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):

i. The validation of information in Certificate Applications;

ii. The acceptance, rejection, or other processing of Certificate Applications, revocation requests, recovery requests or renewal requests, or enrolment information;

iii. The issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository;

iv. The handling of Subscriber information or requests;

v. The generation, issuing or destruction of a CA certificate; and

vi. 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's PKI operations and ensures compliance with this CP/CPS. MSC Trustgate'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 CP/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 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:

i. Verification of the individual's identity,

ii. Previous employment,

iii. Professional reference,

iv. Highest or most relevant educational degree obtained,

v. Bankruptcy records,
vi. Driving records.

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 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:

i. Misrepresentations made by the candidate or Trusted Person;
ii. Highly unfavourable or unreliable professional references; and
iii. 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 behaviour uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

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

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

5.3.3 Training requirements

MSC Trustgate 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 maintains records of such training. MSC Trustgate periodically reviews and enhances its training programs, as necessary.

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

i. Basic Public Key Infrastructure (PKI) concepts;
ii. MSC Trustgate security and operational policies and procedures;
iii. Use and operation of deployed hardware and software;
iv. Incident and Compromise reporting and handling,
v. Disaster recovery and business continuity procedures;
vi. Authentication and verification policies and procedures;
vii. Common threats to the validation process, including phishing and other social engineering tactics; and
viii. 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 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 maintains supporting documentation.

5.3.4 Retraining frequency and requirements

MSC Trustgate 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

No Stipulation.

5.3.6 Sanctions for unauthorized actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of MSC Trustgate 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 hold the same functional and security criteria that apply to a MSC Trustgate 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'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 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's systems require identification and authentication at system logon with a unique username and password. Important system actions are logged to establish the accountability of the operators who initiate such actions.

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

i. CA key lifecycle management events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction; and
    b. Cryptographic device lifecycle management events.
ii. 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 MSC Trustgate in this CP/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.

iii. 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:

i. Date and time of entry;
ii. Identity of the person making the journal entry; and
iii. Description of the entry.

5.4.2 Frequency of processing log

As required, generally within at least once every three (3) months, MSC Trustgate administrator will review the logs generated by MSC Trustgate'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:

i. Checks whether anyone has tampered with the log;
ii. Scans for anomalies or specific conditions, including any evidence of malicious activity; and
iii. Prepares a written summary of the review.

Any anomalies or irregularities found in the logs are investigated. The summaries include recommendations to MSC Trustgate's operations management committee and are made available to MSC Trustgate's auditors upon request. MSC Trustgate 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 ten (10) years or in accordance with section 5.5.2. MSC Trustgate retains audit logs on-site until after they are reviewed. The individuals who remove audit logs from MSC Trustgate's CA systems are different than the individuals who control MSC Trustgate'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'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'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 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 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'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 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 also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that MSC Trustgate has in place to control such risks. MSC Trustgate's Internal Auditors review the security audit data checks for continuity. MSC Trustgate'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.

MSC Trustgate conducts regular vulnerability assessment and penetration testing covering all MSC Trustgate assets related to Certificate issuance, products, and services. Assessments focus on internal and external threats that could result in unauthorized access, tampering, modification, alteration, or destruction of the Certificate issuance process.

5.5 Records archival

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

5.5.1 Types of records archived

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

i. Accreditations of MSC Trustgate;
ii. CP/CPS versions;
iii. Contractual obligations and other agreements concerning the operation of the CA;
iv. System and equipment configurations, modifications, and updates;
v. Rejection or acceptance of a certificate request;
vi. Certificate issuance, rekey, renewal, and revocation requests;
vii. Sufficient identity authentication data to satisfy the identification requirements of Section 3.2, including information about telephone calls made for verification purposes;

viii. Any documentation related to the receipt or acceptance of a Certificate or token;
ix. Subscriber Agreements;
x. Issued Certificates;
xi. A record of certificate re-keys;
xii. CRLs for CAs cross-certified with the Federal Bridge CA;
xiii. Data or applications necessary to verify an archive's contents;
xiv. Compliance auditor reports;
xv. Changes to MSC Trustgate's audit parameters;
xvi. Any attempt to delete or modify audit logs;
xvii. CA Key generation and destruction;
xviii. Access to Private Keys for key recovery purposes;
xix. Changes to trusted Public Keys;
xx. Export of Private Keys;
xxi. Approval or rejection of a revocation request;
xxii. Appointment of an individual to a trusted role;
xxiii. Destruction of a cryptographic module;
xxiv. Certificate compromise notifications;
xxv. Remedial action taken as a result of violations of physical security
xxvi. Violations of the CP/CPS; and
xxvii. Books of account.

5.5.2 Retention period for archive

MSC Trustgate 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 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 needs to transfer any media to a different archive site or equipment, MSC Trustgate 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 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 automatically time-stamps archived records with system time (non-cryptographic method) as they are created. MSC Trustgate 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)

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

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 MSC Trustgate CA services, MSC Trustgate 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 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 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.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

MSC Trustgate has a Security Incident Response Plan, Business Continuity Management and Disaster Recovery Plan. MSC Trustgate documents business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers and Relying Parties in the event of a disaster, security compromise, or business failure.

MSC Trustgate does not disclose business continuity plans to Subscribers, Relying Parties, or to Application Software Suppliers, but will provide business continuity plan and security plans to the MSC Trustgate's CA auditors upon request.

MSC Trustgate annually tests, reviews, and updates these procedures. The business continuity plan includes:

i. The conditions for activating the plan;
ii. Emergency Procedures;
iii. Fall- back procedures;
iv. Resumption procedures;
v. A maintenance schedule for the plan;
vi. Awareness and education requirements;
vii. The responsibilities of the individuals;
viii. Recovery time objective (RTO);
ix. Regular testing of contingency plans;
x. The MSC Trustgate's plan to maintain or restore the MSC Trustgate's business operations in a timely manner following interruption to or failure of critical business processes;
xi. A requirement to store critical cryptographic materials (i.e: secure cryptographic device and activation materials) at an alternate location;
xii. What constitutes an acceptable system outrage and recovery time;

xiii. How frequently backup copies of essential business information and software are taken;

xiv. The distance of recovery facilities to the MSC Trustgate's main site; and

xv. Procedure for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

Additionally, MSC Trustgate must be reported in Bugzilla for serious vulnerabilities and security incidents.

5.7.2 Computing resources, software, and/or data are corrupted

MSC Trustgate 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 discovers that any of its computing resources, software, or data operations have been compromised, MSC Trustgate 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 determines that a continued operation could pose a significant risk to Relying Parties or Subscribers, MSC Trustgate suspends such operation until it determines that the risk is mitigated.

5.7.3 Entity private key compromise procedures

If MSC Trustgate suspects that one of its CA Private Keys Infrastructure has been comprised or lost then MSC Trustgate's Key Compromise Response procedures are enacted by the MSC Trustgate Security Incident Response Team (SIRT). This team, which includes Security Manager, Cryptographic Business Operations, Production Services personnel, and other management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from MSC Trustgate 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:

i. The Certificate's revoked status is communicated to Relying Parties through the MSC Trustgate Repository in accordance with Section 4.9.7;

ii. Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected MSC Trustgate CA services Participants; and

iii. 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 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's primary facility and that MSC Trustgate will be capable of maintaining other services or resuming them as quickly as possible following a disaster. MSC Trustgate reviews, tests, and updates the BCMP and supporting procedures at least annually.

MSC Trustgate'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's primary CA operations to become inoperative, MSC Trustgate 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 CA to cease operation, MSC Trustgate 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 will develop a termination plan to minimize disruption to Subscribers and Relying Parties. Such termination plans may address the following, as applicable:

i. Provision of notice to parties affected by the termination, such as Subscribers and Relying Parties, informing them of the status of the CA;

ii. Handling the cost of such notice;

iii. Transfer all responsibilities to a qualified successor entity

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

i. Transfer all relevant records to a government supervisory or legal body;

ii. Revoke all Certificates that are still un-revoked or un-expired on a date as specified in the notice and publish final CRLs;

iii. Destroy all Private Keys; and

iv. Make other necessary arrangements that are in accordance with this CP/CPS.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA Key Pair Generation

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

MSC Trustgate'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 creates auditable evidence during the key generation process to prove that the CP/CPS was followed, and role separation was enforced during the key generation process.

For CA keys to be used as publicly trusted Certificates, the CA key pair generation require the following process:

i. prepare and follow a Key Generation Script,

ii. have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process,

iii. have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

iv. dated and signed by all individuals involved.

For other CA key pair generation ceremonies, the following process is required.

i. Prepare and follow a Key Pair generation script;

ii. an Internal Auditor, external auditor, or

iii. independent third party will attend the ceremony, or

iv. an external auditor examines the signed and documented record of the key generation ceremony, as allowed by applicable policy.

In all cases, MSC Trustgate SHALL maintain the followings procedures:

i. generate the CA Key Pair in a physically secured environment as described in the CA's Certificate Policy and/or Certification Practice Statement

ii. generate the CA Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge;

iii. generate the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's Certificate Policy and/or Certification Practice Statement;

iv. log its CA Key Pair generation activities; and

v. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

6.1.1.2 RA key pair generation

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

6.1.1.3 Subscriber key pair generation

MSC Trustgate rejects a certificate request if one or more of the following conditions are met:

i. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6;

ii. There is clear evidence that the specific method used to generate the Private Key was flawed;

iii. The Issuer CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise

iv. The Issuer CA has previously been notified that the applicant's Private Key has suffered a Key Compromise using the Issuer CA's procedure for revocation request as described in Section 4.9.3 and Section 4.9.12;

v. The Public Key corresponds to an industry-demonstrated weak Private Key. For requests submitted on or after November 15, 2024, at least the following precautions SHALL be implemented:

a) In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), the Issuer CA shall reject all keys found at https://github.com/cabforum/Debian-weak-keys/ for each key type (e.g. RSA, ECDSA) and size listed in the repository. For all other keys meeting the requirements of Section 6.1.5, with the exception of RSA key sizes greater than 8192 bits, the Issuer CA shall reject Debian weak keys.

b) In the case of ROCA vulnerability, the Issuer CA shall reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.

c) In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), the Issuer CA shall reject weak keys which can be factored within 100 rounds using Fermat's factorization method.

MSC Trustgate SHALL not generate the key pair on behalf of a subscriber if the certificate request has an extendedKeyUsage extension containing either the values id-kp-serverAuth [RFC5280] or anyExtendedKeyUsage [RFC5280].

Generation of end-user Subscriber key pairs is generally performed by the Subscriber in a manner that is appropriate for the certificate type. The AATL 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 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:

i. Except where escrow/backup services are authorized and permitted, the key generator must not retain access to the Subscriber's Private Key after delivery;

ii. The key generator must protect the Private Key from activation, compromise, or modification during the delivery process;

iii. The Subscriber must acknowledge receipt of the Private Key(s), typically by having the Subscriber use the related Certificate, and

iv. 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. An RA providing key delivery services is required to provide a copy of this record to MSC Trustgate.

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. Encrypt the Private Key with at least 112 bits of encryption strength.

If MSC Trustgate or an Enterprise RA becomes aware that a subscriber's Private Key has been communicated to a person or organization not authorized by the subscriber, then MSC Trustgate must revoke all certificates associated with that Private Key.

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 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, this requirement is No Stipulation.

6.1.4 CA public key delivery to relying parties

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

i. Specified in a certificate validation or path discovery policy file;

ii. Trust anchors in commercial browsers and operating system root store; and/or

iii. Roots signed by other CAs.

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

MSC Trustgate 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 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's CA Certificates via MSC Trustgate's web site or by email.

6.1.5 Key sizes

MSC Trustgate strictly adheres to the key sizes specified within this section and does not utilize any other sizes.

6.1.5.1 Related to Code Signing and Timestamping Certificates

For keys corresponding to Root and Subordinate CAs:

i. For RSA keys, the modulus must be at least 4096 bits in length.

ii. For ECDSA keys, the curve must be one of NIST P-256 (providing ~128-bit security), P-384 (providing ~192-bit security), or P-521 (providing ~256-bit security).

For keys corresponding to subscriber certificates:

i. For RSA keys, the modulus must be at least 3072 bits in length.

ii. For ECDSA keys, the curve must be one of NIST P-256 (providing ~128-bit security), P-384 (providing ~192-bit security), or P-521 (providing ~256-bit security).

6.1.5.2 Other type of Certificates

For **RSA** key pairs:

i. The modulus must be at least 2048 bits in length.

ii. The size must be evenly divisible by 8 when measured in bits.

For **ECDSA** key pairs:

i. Keys must represent a valid point on one of the following elliptic curves: **NIST P-256** (providing ~128-bit security), **P-384** (providing ~192-bit security), or **P-521** (providing ~256-bit security).

For EdDSA key pairs:

i. Keys must represent a valid point on the **Curve25519** (using 256-bit private keys) or **Curve448** (using 456-bit private keys) elliptic curves.

In addition to the classical schemes above, MSC Trustgate also supports the following **ML-DSA** and **SLH-DSA** post-quantum digital-signature parameter sets:

Parameter Set	NIST Security Level	Public Key Size (bytes)	Private Key Size (bytes)	Signature Size (bytes)
ML-DSA-44	2 (≈128-bit)	1 312	2 560	2 420
ML-DSA-65	3 (≈192-bit)	1 952	4 032	3 309
ML-DSA-87	5 (≈256-bit)	2 592	4 896	4 627
SLH-DSA-SHA2-128s	1 (≈128-bit)	32	64	7,856
SLH-DSA-SHA2-128f	1 (≈128-bit)	32	64	17,088
SLH-DSA-SHA2-192s	3 (≈192-bit)	48	96	16,224
SLH-DSA-SHA2-192f	3 (≈192-bit)	48	96	35,664
SLH-DSA-SHA2-256s	5 (≈256-bit)	64	128	29,792
SLH-DSA-SHA2-256f	5 (≈256-bit)	64	128	49,856

No other algorithms or key sizes are permitted.

6.1.6 Public key parameters generation and quality checking

For RSA key pairs: MSC Trustgate confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between 2^16 + 1 and 2^256 - 1. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. (See NIST SP 800-89, Section 5.3.3.)

For ECDSA key pairs: MSC Trustgate confirms the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. (See NIST SP 800-56A: Revision 2, Sections 5.6.2.3.2 and 5.6.2.3.3.)

For EdDSA key pairs: MSC Trustgate confirms that EdDSA key pairs are generated and validated in accordance with RFC 8032.

i. Private keys MUST be generated using a NIST-approved cryptographically secure random number generator and have the bit-length required by the curve (256 bits for Ed25519; 456 bits for Ed448).

ii. Public keys MUST correspond to a valid point on the Twisted Edwards curve (Ed25519 or Ed448).

iii. Key validation shall include:

   a. Checking that the public-key coordinates lie on the curve equation.

   b. Verifying that the public key has the correct order (i.e. multiplying by the cofactor yields the identity).

   c. Confirming private-public key consistency by recomputing the public key from the private key and matching it.

For ML-DSA key pairs: MSC Trustgate generates and validates post-quantum ML-DSA key pairs (Dilithium) in accordance with FIPS 204 as follows:

i. Key pairs shall be generated for one of the approved parameter sets—ML-DSA-44, ML-DSA-65, or ML-DSA-87—using a NIST-compliant CSPRNG.

ii. Public keys consist of the Dilithium public vector components; validation SHALL include:

   a. Ensuring each coefficient in the public vector lies within the bounds specified by the parameter set.

   b. Verifying that the public vector satisfies the lattice equation $A \cdot s_1 + s_2 = t$ (i.e. recomputing and matching the "t" component).

iii. Quality checks shall include:

   a. Confirming the seed and randomness inputs conform exactly to the required lengths for the chosen parameter set.

   b. Regenerating the public key from the private key and verifying byte-for-byte equality.

   c. Ensuring no public-key component is all-zero or otherwise trivially invalid.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

MSC Trustgate'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:

i. Self-signed Certificates to represent the Root CA itself;

ii. Certificates for Subordinate CAs and Cross Certificates;

iii. Certificates for infrastructure purposes (e.g., administrative role certificates, internal CA operational device certificates; and

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

6.2 Private Key Protection and Cryptographic

MSC Trustgate has implemented a combination of physical, logical, and procedural controls to ensure the security of MSC Trustgate 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's cryptographic modules for all of its CA and OCSP responder Key Pairs are validated to the FIPS 140-2 Level 3. MSC Trustgate's Validation Team (Internal RA) utilizes FIPS 140-2 Level 2 cryptographic devices to generate, store, and utilize Key Pairs that is used accessing Registration Authority system.

AATL Certificates are issued only when MSC Trustgate confirms that the Key Pairs are generated and stored using a trustworthy system employing cryptographic hardware devices certified to either FIPS 140-2 Level 2 or Level 3, or Common Criteria (ISO 15408 & ISO 18045) - Protection Profiles CEN prEN 14169 (all applicable parts) or equivalent certification. Additionally, key activation must rely on a minimum 2-factor authentication (2FA) process if the device is managed by third party on behalf of the signer (example roaming/remote Certificates).

For other types of certificates, subscribers have the option to use either a hardware-based cryptographic device, software, or a file for their Key Pairs.

MSC Trustgate ensures that all cryptographic operations, including those involving emerging post-quantum algorithms, are performed using cryptographic hardware certified to FIPS 140-2 Level 3 or Common Criteria (ISO/IEC 15408). Where possible, we employ hybrid cryptography to maintain compatibility and layered security. These operations are governed by established security policies, subjected to regular compliance audits, and designed with crypto-agility to accommodate evolving cryptographic standards, thereby maintaining trust and regulatory alignment.

6.2.2 Private key (n out of m) multi-person control

MSC Trustgate has implemented technical and procedural mechanisms that requires the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. MSC Trustgate 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 CP/CPS.

6.2.3 Private key escrow

MSC Trustgate does not escrow its CA private keys. Subscribers may not escrow their private signature keys. MSC Trustgate 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's Private Keys are generated and operated inside MSC Trustgate'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'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 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 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 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 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 will revoke all certificates that include the Public Key corresponding to the communicated Private Key.

If MSC Trustgate pre-generates private keys and transfers them into a hardware token, for example transferring generated end-user Subscriber private keys into a token, 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's Private Keys are generated and stored inside MSC Trustgate'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 key

MSC Trustgate'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 key

MSC Trustgate's Private Keys are deactivated via logout procedures on the applicable HSM device when not in use. MSC Trustgate 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 key

MSC Trustgate 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 may destroy a Private Key by deleting it from all known storage partitions. MSC Trustgate 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 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 archives copies of Public Keys in accordance with Section 5.5.

6.3.2 Certificate operational periods and key pair usage periods

MSC Trustgate 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
Domain Validation SSL/TLS Certificates	No Stipulation	• 398 days* (Issued before March 15, 2026) • 200 days* (Issued on or after March 15, 2026, and before March 15, 2027) • 100 days (Issued on or after March 15, 2027, and before March 15, 2029) • 47 days (Issued on or after March 15, 2029)
Organization Validation SSL/TLS Certificates	No Stipulation	• 398 days* (Issued before March 15, 2026) • 200 days* (Issued on or after March 15, 2026, and before March 15, 2027) • 100 days* (Issued on or after March 15, 2027, and before March 15, 2029) • 47 days* (Issued on or after March 15, 2029)
Extended validation SSL/TLS Certificates	No Stipulation	• 398 days* (Issued before March 15, 2026) • 200 days* (Issued on or after March 15, 2026, and before March 15, 2027) • 100 days* (Issued on or after March 15, 2027, and before March 15, 2029) • 47 days* (Issued on or after March 15, 2029)
S/MIME strict and multipurpose Certificates	No Stipulation	825 days
S/MIME legacy Certificates	No Stipulation	1185 days
AATL Certificate	No Stipulation	825 days
CRL and OCSP responder signing	3 years	31 days
Time Stamping Authority	15 months	135 months

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

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 may voluntarily retire its CA Private Keys before the periods listed above to accommodate key changeover processes. MSC Trustgate 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.

6.4 Activation data

6.4.1 Activation data generation and installation

MSC Trustgate 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 CP/CPS. MSC Trustgate 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 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 uses passwords as activation data for a signing key, MSC Trustgate will change the activation data change upon rekey of the CA Certificate.

6.4.2 Activation data protection

MSC Trustgate 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 personnel are instructed to memorize and not to write down their password or share it with any another individual. MSC Trustgate 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

No Stipulation

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

MSC Trustgate secures its CA systems and authenticates and protects communications between its systems and trusted roles. MSC Trustgate'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's CA systems are configured to:

i. Authenticate the identity of users before permitting access to the system or applications;
ii. Manage the privileges of users and limit users to their assigned roles;
iii. Generate and archive audit records for all transactions;
iv. Enforce domain integrity boundaries for security critical processes; and
v. Support recovery from key or system failure.

All Certificate Status Servers:

i. Authenticate the identity of users before permitting access to the system or applications;
ii. Manage privileges to limit users to their assigned roles;
iii. Enforce domain integrity boundaries for security critical processes; and
iv. Support recovery from key or system failure.

MSC Trustgate 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 security controls

6.6.1 System development controls

MSC Trustgate uses only:

i. CA systems software that is provided by MSC Trustgate. MSC Trustgate 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/CPS;
ii. 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; and
iii. 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's operations are scanned for malicious code on first use and periodically thereafter. MSC Trustgate does not install software that are not part of the CA's operation

6.6.2 Security management controls

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

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

All CA and RA systems must be protected in accordance with the CA/Browser Forum's Network and Certificate System Security Requirements. MSC Trustgate and RA functions are performed using networks secured in accordance with all standards documented in this CP/CPS to prevent unauthorized access,

tampering, and denial-of-service attacks. Communications of sensitive information shall be protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

The Issuer MSC Trustgate document and control the configurations of its systems, including any upgrades or modifications made. The Issuer MSC Trustgate implement a process for detecting unauthorized modifications to its hardware or software and for installing and maintaining its systems.

The Issuer CA and its RAs shall implement appropriate network security controls, including turning off any unused network ports and services and only using network software that is necessary for the proper functioning of the CA systems. The Issuer MSC Trustgate implement the same network security controls to protect a CMS as used to protect its other CA equipment.

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

6.8 Timestamping

MSC Trustgate Date/Time Stamp service utilized a trusted time source by National Metrology Institute of Malaysia (NMIM).

If a timestamp is needed under any written law or if a specific time is important for using digitally signed data, the subscriber should subscribe to a service from a recognized date/time stamp provider such as MSC Trustgate.

If a digital signature on a document lacks a timestamp, it is advisable for the subscriber to re-sign the document with a new digital certificate before the current certificate expires.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Policy

1. The CA SHALL generate Certificates that meet the technical requirements set forth in Section 2.2 (Publication of certification information), Section 6.1.5 (Key Sizes), and Section 6.1.6 (Public Key Parameters Generation and Quality Checking).
2. The CA SHALL generate non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG).

Practice

1. MSC Trustgate exclusively issues Certificates that meet the technical requirements set forth in Section 2.2, Section 6.1.5, and Section 6.1.6.
2. MSC Trustgate's system is configured to generate **non-sequential Certificate serial numbers** that are greater than zero and contain at least **64 bits** of output from a **CSPRNG**.
3. Prior to **18 April 2024**, MSC Trustgate **issued** certificates following either the profile outlined in this **CP/CPS**, or the profile specified in **CP/CPS version 5.4**. Effective **18 April 2024**, MSC Trustgate issues certificates according to the profile outlined in this **CP/CPS**.
4. MSC Trustgate generates Certificates in adherence to **RFC 5280** standards, incorporating updates outlined in **RFC 6818**. The following section describes in detail the certificate profile that MSC Trustgate uses to generate certificates.

7.1.1 Version number(s)

Policy: Certificates SHALL conform to the X.509 version 3 standard.

Practice: MSC Trustgate generates only X.509 Version 3 Certificates.

7.1.2 Certificate content and extensions

This section specifies the additional requirements for Certificate content and extensions for Certificates issued by MSC Trustgate.

7.1.2.1 Root CA Certificate Extensions

MSC Trustgate utilizes the following extension for all its Root CA Certificates:

Field	Criticality	Value or Value Constraint
basicConstraints	TRUE	MUST be present, cA MUST be TRUE, pathLenConstraint MUST NOT be present
keyUsage	TRUE	MUST be present, Bit positions for keyCertSign and cRLSign MUST be SET, Other bits MUST NOT be SET
subjectKeyIdentifier	FALSE	MUST be present. Composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
authorityKeyIdentifier	FALSE	MAY be present. keyIdentifier identical to the subjectKeyIdentifier field. authorityCertIssuer and authorityCertSerialNumber MUST NOT be present.

Field	Criticality	Value or Value Constraint
Any other extension		MUST NOT be present.

7.1.2.2 Subordinate CA Certificate Extensions

MSC Trustgate does not utilize its Subordinate CA Certificate to sign OCSP Responders. Additionally, MSC Trustgate employs the following extension for all of its Subordinate CA Certificates:

Certificate Extension	Criticality	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, Other bit positions MUST NOT be SET
subjectKeyIdentifier	FALSE	MUST be present. Composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
authorityKeyIdentifier	FALSE	MUST be present. Contain keyIdentifier that identical to the subjectKeyIdentifier field of the Issuing CA. MUST not contain authorityCertIssuer and authorityCertSerialNumber.
certificatePolicies	FALSE	MUST be present for Document Signing, SSL/TLS, S/MIME, Code Signing and Timestamping Certificates. Additionally, it MUST contain at least one PolicyInformation. See Section 7.1.2.2.1. MAY be present for other type of Certificates. If present, see Section 7.1.2.6.
cRLDistributionPoints	FALSE	MUST be present, contains HTTP URL of the CA's CRL service
extKeyUsage	FALSE	MUST be present for SSL/TLS, S/MIME, Code Signing and Timestamping Certificates. MAY be present for other types of Certificats. See Section 7.1.2.2.2.
authorityInfoAccess	FALSE	SHOULD be present, contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). MAY contains HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).
nameConstraints	TRUE	MAY be present if id-kp-emailProtection KeyPurposeIds is included. See Section 7.1.5

7.1.2.2.1 Policy Object Identifiers (OIDs)

MSC Trustgate assigns Subordinate CA a specific Policy Object Identifier (OID) to define its intended usage and ensure compliance with relevant certification policies. These OIDs clearly distinguish between certificate types and their respective trust levels. The table below lists the mandatory Policy OIDs for each Subordinate CA.

Certificate Types	Policy Identifier
Domain Validation SSL Certificates	• 2.23.140.1.2.1 • 1.3.6.1.4.1.49530.1.4.1
Organization Validation SSL Certificates	• 2.23.140.1.2.2 • 1.3.6.1.4.1.49530.1.4.2
Extended Validation SSL Certificates	• 2.23.140.1.1 • 1.3.6.1.4.1.49530.1.4.3
Intranet Validation SSL Certificates	• 1.3.6.1.4.1.49530.1.4.4
S/MIME Basic (Mailbox-validated)	• 2.23.140.1.5.1.3 • 1.3.6.1.4.1.49530.1.5.1
S/MIME Organization (Organization-validated)	• 2.23.140.1.5.2.3 • 1.3.6.1.4.1.49530.1.5.2
S/MIME Enterprise (Sponsored-validated)	• 2.23.140.1.5.3.3 • 1.3.6.1.4.1.49530.1.5.3
S/MIME Standard (Individual-validated)	• 2.23.140.1.5.4.3 • 1.3.6.1.4.1.49530.1.5.4
Code Signing Certificates	• 2.23.140.1.4.1 • 1.3.6.1.4.1.49530.1.2.1
Extended Validation Code Signing Certificates	• 2.23.140.1.3 • 1.3.6.1.4.1.49530.1.2.2
Timestamp Certificates	• 2.23.140.1.4.2 • 1.3.6.1.4.1.49530.1.3.1

7.1.2.2.2 Extended Key Usage (EKU) extensions

MSC Trustgate technically constrains Subordinate CA certificates through specific Extended Key Usage (EKU) extensions, restricting their cryptographic functions to intended purposes. These constraints ensure that Subordinate CAs cannot issue certificates for unauthorized uses, enforcing compliance with security and trust requirements.

The table below outlines the mandatory EKU extensions for each Subordinate CA, specifying whether a certificate is permitted for server authentication, client authentication, code signing, or email protection.

Certificate Type	Criticality	Value
SSL/TLS	FALSE	id-kp-serverAuth (1.3.6.1.5.5.7.3.1) MUST be present. id-kp-clientAuth (1.3.6.1.5.5.7.3.2) MAY be present. Other values MUST NOT be present.
S/MIME	FALSE	id-kp-emailProtection (1.3.6.1.5.5.7.3.4) SHALL be present. The following value SHALL NOT be present: • id-kp-serverAuth (1.3.6.1.5.5.7.3.1) • id-kp-codeSigning (1.3.6.1.5.5.7.3.3) • id-kp-timeStamping (1.3.6.1.5.5.7.3.8) • anyExtendedKeyUsage (2.5.29.37.0) Other values MAY be present.
Code Signing	FALSE	id-kp-codeSigning (1.3.6.1.5.5.7.3.3) MUST be present. Additionally, the following EKUs MAY be present: • szOID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12) • szOID_KP_LIFETIME_SIGNING (1.3.6.1.4.1.311.10.3.13) Other values SHOULD NOT be present.
Timestamping	TRUE	id-kp-timeStamping (1.3.6.1.5.5.7.3.8) MUST be present. Other values MUST NOT be present.

7.1.2.3 Subscriber (End-user) Certificate

7.1.2.3.1 Document Signing Certificates

MSC Trustgate utilizes the following extension for all of its Document Signing Certificates:

Certificate Extension	Criticality	Value or Value Constraint
basicConstraints	TRUE	MAY be present, cA MUST NOT be TRUE, pathLenConstraint MUST NOT be present.
keyUsage	TRUE	MUST be present, For RSA Public Key, bit positions for digitalSignature MUST be SET. Bit position of nonrepudiation and keyEncipherment MAY be SET. For ECC Public Key, bit positions for digitalSignature MUST be SET. Bit position of nonrepudiation, keyAgreement, encipherOnly, decipherOnly MAY be SET. Other bit positions SHALL NOT be SET
subjectKeyIdentifier	FALSE	MUST be present. Composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
authorityKeyIdentifier	FALSE	MUST be present. Contain keyIdentifier that identical to the subjectKeyIdentifier field of the Issuing CA. MUST not contains authorityCertIssuer and authorityCertSerialNumber.
certificatePolicies	FALSE	MUST be present. See Section 7.1.2.6.2
cRLDistributionPoints	FALSE	MUST be present, contains HTTP URL of the CA's CRL service
extKeyUsage	FALSE	MUST be present and contain any of the following: • Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) • szOID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12) • id-kp-clientAuth (1.3.6.1.5.5.7.3.2) • id-kp-documentSigning (1.3.6.1.5.5.7.3.36) The following value SHALL NOT be present: • id-kp-serverAuth (1.3.6.1.5.5.7.3.1) • id-kp-timeStamping (1.3.6.1.5.5.7.3.8) • anyExtendedKeyUsage (2.5.29.37.0) Other values MAY be present.
authorityInfoAccess	FALSE	SHOULD be present, contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2 value of type id-ad-caIssuers). MAY contains HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1 values of type id-ad-ocsp).

7.1.2.3.1.1 LHDN e-Invoice Organization Certificates

For LHDN e-Invoice Organization Certificates, MSC Trustgate employs the following certification extensions:

Certificate Extension	Criticality	Value or Value Constraint
basicConstraints	TRUE	cA = FALSE, pathLenConstraint NOT present.
keyUsage	TRUE	Only the following bits is SET: • digitalSignature • nonRepudiation
subjectKeyIdentifier	FALSE	Composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
authorityKeyIdentifier	FALSE	keyIdentifier = 780ddbeb312dc28d25bf5f3c1da5bb33f84ad495 (identical to the subjectKeyIdentifier field of the Issuing CA)

certificatePolicies	FALSE	MUST be present.
		PolicyInformation = {
		policyIdentifier = 1.3.6.1.4.1.49530.1.1.2.5,
		poliycyQualifiers = {
		policyQualifierId = id-qt-cps (OID: 1.3.6.1.5.5.7.2.1),
		qualifier = {
		cPSuri = https://www.msctrustgate.com/tgcps
		}
		}, {
		policyQualifierId = id-qt-unotice (OID: 1.3.6.1.5.5.7.2.2),
		qualifier = {
		userNotice = {
		explicitText = https://www.msctrustgate.com/tgrpa
		}
		}
		}
		}

cRLDistributionPoints	FALSE	DistributionPoint = {
		distributionPoint = fullName,
		URI=
		https://pki.msctrustgate.com/crl/cdp/repo/tgmpkirca.crl
		}

extKeyUsage	FALSE	MUST be present and contain only szOID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12)

authorityInfoAccess	FALSE	AuthorityInfoAccess = {
		accessMethod = id-ad-caIssuers (OID: 1.3.6.1.5.5.7.48.2)
		accessLocation = URI:
		https://www.msctrustgate.com/cacerts/Trustgate_MPKI_IS_CA.cer
		}

7.1.2.3.2 MyDigital ID Certificates

MSC Trustgate generate MyDigital ID Certificates with the following extension:

Certificate Extension	Criticality	Value
basicConstraints	TRUE	cA = FALSE, pathLenConstraint NOT present.
keyUsage	TRUE	Only the following bits is SET: • digitalSignature • keyAgreement
subjectKeyIdentifier	FALSE	Composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
authorityKeyIdentifier	FALSE	keyIdentifier = 38:A2:9B:DC:0E:9B:49:AE:4D:8B:53:07:78:92:EA:62 :61:A6:3B:82 (identical to the subjectKeyIdentifier field of the Issuing CA)

certificatePolicies	FALSE	PolicyInformation = {
		policyIdentifier = 1.3.6.1.4.1.49530.1.1.5.1,
		poliycyQualifiers = {
		policyQualifierId = id-qt-cps (OID: 1.3.6.1.5.5.7.2.1),
		qualifier = {
		cPSuri = https://www.msctrustgate.com/tgcps
		}
		}, {
		policyQualifierId = id-qt-unotice (OID: 1.3.6.1.5.5.7.2.2),
		qualifier = {
		userNotice = {
		explicitText = https://www.msctrustgate.com/tgrpa
		}
		}
		}
		}

cRLDistributionPoints	FALSE	DistributionPoint = {
		distributionPoint = fullName,
		URI=http://pki.msctrustgate.com/crl/cdp/MyTrust_ Digital_ID_Class_3_CA.crl
		}

extKeyUsage	FALSE	• MUST be present and contain only id-kp-clientAuth (1.3.6.1.5.5.7.3.2)

Certificate Extension	Criticality	Value

authorityInfoAccess	FALSE	AuthorityInfoAccess = {
		accessMethod = id-ad-caIssuers (OID: 1.3.6.1.5.5.7.48.2)
		accessLocation =
		URI:http://pki.msctrustgate.com/repo/ca/MyTrust_
		Digital_ID_Class_3_CA.cer
		}, {
		accessMethod = id-ad-ocsp (OID: 1.3.6.1.5.5.7.48.1)
		accessLocation =
		URI:http://pki.msctrustgate.com/ocsp
		}

7.1.2.3.3 SSL/TLS Certificates

MSC Trustgate utilizes the following extension for all of its SSL/TLS Certificates:

Certificate Extension	Criticality	Value or Value Constraint
basicConstraints	TRUE	MAY be present, cA MUST NOT be TRUE, pathLenConstraint MUST NOT be present.
keyUsage	TRUE	SHOULD be present, For RSA Public Key, bit positions for digitalSignature and keyEncipherment MUST be SET. For ECC Public Key, bit positions for digitalSignature MUST be SET. Other bit positions MUST NOT be SET
subjectKeyIdentifier	FALSE	NOT RECOMMENDED.
authorityKeyIdentifier	FALSE	MUST be present. Contain keyIdentifier that identical to the subjectKeyIdentifier field of the Issuing CA. MUST not contain authorityCertIssuer and authorityCertSerialNumber.
certificatePolicies	FALSE	MUST be present. See Section 7.1.2.6.1.
cRLDistributionPoints	FALSE	SHALL be present, contains HTTP URL of the CA's CRL service
extKeyUsage	FALSE	id-kp-serverAuth (1.3.6.1.5.5.7.3.1) MUST be present. id-kp-clientAuth (1.3.6.1.5.5.7.3.2) MAY be present. Other values MUST NOT be present.
authorityInfoAccess	FALSE	MUST be present, contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). MAY contains HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).
subjectAltName	TRUE if subject field is empty, otherwise FALSE	See Section 7.1.4.2.1
nameConstraints	TRUE	MUST NOT be PRESENT.

7.1.2.3.4 S/MIME Certificates

MSC Trustgate utilizes the following extension for all of its S/MIME Certificates:

Certificate Extension	Criticality	Value or Value Constraint
basicConstraints	TRUE	MAY be present, cA MUST NOT be TRUE, pathLenConstraint MUST NOT be present.
keyUsage	TRUE	SHALL be present, For RSA Public Key, bit positions for digitalSignature and keyEncipherment SHALL be SET. Bit position of nonrepudiation MAY also be SET. For ECC Public Key, bit positions for digitalSignature and keyAgreement SHALL be SET. Bit position of nonrepudiation, encipherOnly, decipherOnly MAY also be SET. Other bit positions SHALL NOT be SET
subjectKeyIdentifier	FALSE	SHOULD be present. Composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
authorityKeyIdentifier	FALSE	SHALL be present. Contain keyIdentifier that identical to the subjectKeyIdentifier field of the Issuing CA. MUST not contains authorityCertIssuer and authorityCertSerialNumber.
certificatePolicies	FALSE	SHALL be present. See Section 7.1.2.6.1.
cRLDistributionPoints	FALSE	SHALL be present, contains HTTP URL of the CA's CRL service
extKeyUsage	FALSE	id-kp-emailProtection (1.3.6.1.5.5.7.3.4) SHALL be present. The following value SHALL NOT be present: • id-kp-serverAuth (1.3.6.1.5.5.7.3.1) • id-kp-codeSigning (1.3.6.1.5.5.7.3.3) • id-kp-timeStamping (1.3.6.1.5.5.7.3.8) • anyExtendedKeyUsage (2.5.29.37.0) Other values MAY be present.
authorityInfoAccess	FALSE	SHOULD be present, contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2 value of type id-ad-caIssuers). MAY contains HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1 values of type id-ad-ocsp).
subjectAltName	TRUE if subject field is empty, otherwise FALSE	See Section 7.1.4.2.1

7.1.2.3.5 Code Signing Certificates

MSC Trustgate utilizes the following extension for all of its Code Signing Certificates:

Certificate Extension	Criticality	Value or Value Constraint
basicConstraints	TRUE	MAY be present, cA MUST NOT be TRUE, pathLenConstraint MUST NOT be present.
keyUsage	TRUE	MUST be present, Bit positions for digitalSignature MUST be SET. Other bit positions MUST NOT be SET
subjectKeyIdentifier	FALSE	MAY be present. Composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
authorityKeyIdentifier	FALSE	MUST be present. Contain keyIdentifier that identical to the subjectKeyIdentifier field of the Issuing CA. MUST not contains authorityCertIssuer and authorityCertSerialNumber.
certificatePolicies	FALSE	MUST be present. See Section 7.1.2.6.1.
cRLDistributionPoints	FALSE	MUST be present, contains HTTP URL of the CA's CRL service
extKeyUsage	FALSE	id-kp-codeSigning (1.3.6.1.5.5.7.3.3) MUST be present. Additionally, the following EKUs MAY be present: • szOID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12) • szOID_KP_LIFETIME_SIGNING (1.3.6.1.4.1.311.10.3.13) Other values SHOULD NOT be present.
authorityInfoAccess	FALSE	MUST be present, contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2 value of type id-ad-caIssuers). MAY contains HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1 values of type id-ad-ocsp).

7.1.2.3.6 Timestamping Certificates

MSC Trustgate utilizes the following extension for its Timestamping Certificates:

Certificate Extension	Criticality	Value or Value Constraint
basicConstraints	TRUE	MAY be present, cA MUST NOT be TRUE, pathLenConstraint MUST NOT be present.
keyUsage	TRUE	MUST be present, Bit positions for digitalSignature MUST be SET. Other bit positions MUST NOT be SET
subjectKeyIdentifier	FALSE	MAY be present. Composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
authorityKeyIdentifier	FALSE	MUST be present. Contain keyIdentifier that identical to the subjectKeyIdentifier field of the Issuing CA. MUST not contain authorityCertIssuer and authorityCertSerialNumber.
certificatePolicies	FALSE	MUST be present. See Section 7.1.2.6.1.
cRLDistributionPoints	FALSE	MUST be present, contains HTTP URL of the CA's CRL service
extKeyUsage	TRUE	MUST be present and can only contain id-kp-timeStamping (1.3.6.1.5.5.7.3.8).
authorityInfoAccess	FALSE	MUST be present, contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2 value of type id-ad-caIssuers). MAY contains HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1 values of type id-ad-ocsp).

7.1.2.3.7 Device Certificates

MSC Trustgate utilizes the following extension for all of its Device Certificates:

Certificate Extension	Criticality	Value or Value Constraint
basicConstraints	TRUE	MAY be present, cA MUST NOT be TRUE, pathLenConstraint MUST NOT be present.
keyUsage	TRUE	MUST be present, For RSA Public Key, bit positions for digitalSignature and keyEncipherment MUST be SET. For ECC Public Key, bit positions for digitalSignature MUST be SET. Bit position of keyAgreement, encipherOnly, decipherOnly MAY be SET. Other bit positions SHALL NOT be SET
subjectKeyIdentifier	FALSE	MUST be present. Composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
authorityKeyIdentifier	FALSE	MUST be present. Contain keyIdentifier that identical to the subjectKeyIdentifier field of the Issuing CA. MUST not contain authorityCertIssuer and authorityCertSerialNumber.
certificatePolicies	FALSE	MAY be present. See Section 7.1.2.6.2.
cRLDistributionPoints	FALSE	MUST be present, contains HTTP URL of the CA's CRL service
extKeyUsage	FALSE	MUST be present and contain any of the following: • id-kp-serverAuth (1.3.6.1.5.5.7.3.1) • id-kp-clientAuth (1.3.6.1.5.5.7.3.2) Additionally, the following EKUs MAY be present: • Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)
authorityInfoAccess	FALSE	SHOULD be present, contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2 value of type id-ad-caIssuers). MAY contains HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1 values of type id-ad-ocsp).

7.1.2.4 OCSP Responder Certificates

Extension	Presence	Criticality	Value or Value Constraint
basicConstraints	MAY	TRUE	cA MUST NOT be TRUE, pathLenConstraint MUST NOT be present.
keyUsage	MUST	TRUE	Bit positions for digitalSignature MUST be SET. Other bit positions MUST NOT be SET
subjectKeyIdentifier	SHOULD	FALSE	Composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
authorityKeyIdentifier	MUST	FALSE	Contain keyIdentifier that identical to the subjectKeyIdentifier field of the Issuing CA. MUST not contains authorityCertIssuer and authorityCertSerialNumber.
certificatePolicies	MUST NOT	-	-
cRLDistributionPoints	MUST NOT	-	-
extKeyUsage	MUST	FALSE	Can only contain id-kp-ocspSigning (1.3.6.1.5.5.7.3.).
authorityInfoAccess	NOT RECOMMENDED	-	-
nameConstraints	MUST NOT	-	-
subjectAltName	MUST NOT	-	-
id-pkix-ocsp-nocheck	MUST NOT	-	-

7.1.2.5 All Certificates

MSC Trustgate issues certificates with all fields and extensions set in accordance with RFC 5280. Furthermore, MSC Trustgate does not issue certificates containing keyUsage flags, extKeyUsage values, Certificate extensions, or other data not specified in Section 7.1.2.1, Section 7.1.2.2, or Section 7.1.2.3.

7.1.2.5.1 tbsCertificate Fields

All Certificates utilize the following fields within the tbsCertificate section:

Field	Description
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG
signature	See Section 7.1.3.2
issuer	Encoded value that is byte-for-byte identical to the encoded subject
validity	See Section 7.1.2.5.2
subject	For Root and Subordinate CA, see Section 7.1.4.3 For subscriber (end-user), see Section 7.1.4.2
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present

7.1.2.5.2 Certificate Validity

notBefore is the date of signing, with the time set to midnight (00:00) Greenwich Mean Time (GMT).

notAfter is the date that is calculated by adding a specific number of days to the date of signing. The time is set to one second before midnight (23:59:59) Greenwich Mean Time (GMT). Furthermore, this date must not surpass the 'notAfter' date of its issuer. The exact number of days varies depending on the certificate type:

Certificate Type	Number of days
Root CA Certificates	Between 2,922 (approx. 8 years) and 9,132 days (approx. 25 years)
Subordinate CA Certificates	Less than 6,477 days (approx. 15 years)
Subscriber (End-user) Certificates	SSL/TLS Certificates: Less than 397 days. S/MIME Certificats.: Less than 825 days. Code Signing Certificate: Less than 1187 days (approx. 39 months). Document Signing Certificates: Less than 1095 days (approx. 3 years). Timestamp Certificates: Less than 4,105 days (approx. 135 months) BUT is subject to a maximum key pair usage period of 455 days (approx. 15 months). Other type of Certificates: Unspecified.

The validity period of a certificate may also be contingent upon the validity period of any associated evidence. For instance, in the case of a registered professional required to periodically renew their membership, the notBefore and notAfter fields of a certificate must fall within the membership's validity period.

7.1.2.6 Certificate Policies

7.1.2.6.1 For SSL/TLS, S/MIME, Code Signing, and Timestamping Certificates

MSC Trustgate uses the Certificate Policies extension adhering to the following guidelines:

i. The first PolicyInformation value MUST contain exactly one Reserved Certificate Policy Identifier (refer to section 7.1.5.1). The policyQualifiers SHOULD NOT be present.

ii. The second PolicyInformation value SHALL contain the MSC Trustgate Certificate Policy Identifier (refer to section 7.1.6.2). This policyIdentifier MUST include only policyQualifiers with the id-qt-cps OID (1.3.6.1.5.5.7.2.1), with a value of the MSC Trustgate repository (https://www.msctrustgate.com/repository). The repository host MSC Trustgate Certificate Policies, Certification Practice Statement, and Relying Party Agreement. Other qualifier types SHOULD NOT be present.

7.1.2.6.2 For Document Signing Certificates and Other Type of Certificates

The PolicyInformation value MUST contain the MSC Trustgate Certificate Policy Identifier (refer to section 1.2). This policyIdentifier MUST include only policyQualifiers with the id-qt-cps OID (1.3.6.1.5.5.7.2.1), with a value of the MSC Trustgate repository (https://www.msctrustgate.com/repository). The repository host MSC Trustgate Certificate Policies, Certification Practice Statement, and Relying Party Agreement. Other qualifier types SHOULD NOT be present.

7.1.3 Algorithm object identifiers

7.1.3.1 SubjectPublicKeyInfo

Policy

The subjectPublicKeyInfo field in X.509 certificates SHALL contain a public key and an AlgorithmIdentifier that specifies the associated cryptographic algorithm. The subjectPublicKeyInfo field within a Certificate SHALL adhere to specific requirements, and no other encodings are permitted.

Practice

MSC Trustgate's practice is to issue certificates with the subjectPublicKeyInfo field using only a limited set of algorithms, each with precisely defined OIDs and ASN.1 DER encodings to ensure strict adherence to standards and maximize interoperability. These specific algorithms are described in the following subsections.

7.1.3.1.1 RSA

Policy

1. **For S/MIME and TLS Certificates**: When indicating an RSA public key in the subjectPublicKeyInfo field, the CA SHALL use the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters MUST be present and MUST be an explicit NULL. The AlgorithmIdentifier for RSA keys MUST be byte-for-byte identical with the following hex-encoded bytes: 300d06092a864886f70d0101010500.
2. **For other Certificates** (e.g., **Code Signing**, **Document Signing**): The subjectPublicKeyInfo field SHALL use the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters MUST be present and MUST be an explicit NULL. This policy allows for the use of the id-RSASSA-PSS signature algorithm, as described in Section 7.1.3.2.1.

Practice

When issuing a certificate with an RSA public key, MSC Trustgate's practice is to adhere to the above policies.

1. **For S/MIME and TLS** certificates, MSC Trustgate indicates the usage of an RSA key using the rsaEncryption algorithm identifier with NULL parameter and ensures the encoded AlgorithmIdentifier is byte-for-byte identical with the specified hex bytes.
2. For **Code Signing**, **Document Signing**, **and other** certificate types, MSC Trustgate uses the rsaEncryption algorithm identifier and ensures its parameters are set to NULL. This practice allows for the use of id-RSASSA-PSS as the signature algorithm, which is defined in a separate section.

7.1.3.1.2 ECDSA

Policy

1. The CA SHALL indicate the usage of an ECDSA key using the id-ecPublicKey algorithm identifier (OID: 1.2.840.10045.2.1).
2. The algorithm parameters for ECDSA keys are specified using one of the following named curves:
    i. For P-256 keys, secp256r1 (OID: 1.2.840.10045.3.1.7).
    ii. For P-384 keys, secp384r1 (OID: 1.3.132.0.34).
    iii. For P-521 keys, secp521r1 (OID: 1.3.132.0.35).
3. When encoded, the AlgorithmIdentifier for ECDSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes:
    i. For P-256 keys, 301306072a8648ce3d020106082a8648ce3d030107.
    ii. For P-384 keys, 301006072a8648ce3d020106052b81040022.
    iii. For P-521 keys, 301006072a8648ce3d020106052b81040023.

Practice

When issuing a certificate with an ECDSA public key, MSC Trustgate's practice is to adhere to the above policies. MSC Trustgate indicates the usage of an ECDSA key using the id-ecPublicKey algorithm identifier with the specified parameters and ensures the encoded AlgorithmIdentifier is byte-for-byte identical with the specified hex bytes.

7.1.3.1.3 EdDSA

Policy

1. The CA **SHALL** indicate the use of an EdDSA key by using one of the following algorithm identifiers:
    i. For Curve25519 keys, id-Ed25519 (OID: 1.3.101.112).
    ii. For Curve448 keys, id-Ed448 (OID: 1.3.101.113).
2. The parameters for EdDSA keys **SHALL be absent**.
3. When encoded, the AlgorithmIdentifier for EdDSA keys **SHALL** be byte-for-byte identical with the following hex-encoded bytes:
    i. For Curve25519 keys, 300506032b6570.
    ii. For Curve448 keys, 300506032b6571.

Practice

When issuing a certificate with an EdDSA public key, MSC Trustgate's practice is to adhere to the above policies. MSC Trustgate indicates the usage of an EdDSA key using the specified algorithm identifier **without including any parameters** and ensures the encoded AlgorithmIdentifier is byte-for-byte identical with the specified hex bytes.

7.1.3.1.4 ML-DSA

Policy

1. The CA **SHALL** indicate the use of an ML-DSA key by using one of the following algorithm identifiers:
   i. ML-DSA-44 (OID: 2.16.840.1.101.3.4.3.17)
   ii. ML-DSA-65 (OID: 2.16.840.1.101.3.4.3.18)
   iii. ML-DSA-87 (OID: 2.16.840.1.101.3.4.3.19)
2. The parameters for ML-DSA keys **SHALL be absent**. The CA MUST NOT use HashML-DSA; only "pure" ML-DSA is permitted.
3. When encoded, the AlgorithmIdentifier for ML-DSA keys **SHALL** be byte-for-byte identical with the following hex-encoded bytes:
   i. For ML-DSA-44: 300b0609608648016503040311
   ii. For ML-DSA-65: 300b0609608648016503040312
   iii. For ML-DSA-87: 300b0609608648016503040313

Practice

When issuing a certificate with an ML-DSA public key, MSC Trustgate's practice is to adhere to the above policies. MSC Trustgate uses the specified algorithm identifier, omits the parameters as required, and ensures the encoded AlgorithmIdentifier is byte-for-byte identical with the specified hex bytes.

ML-DSA is currently restricted to S/MIME and Document Signing certificates, limited to approved variants (ML-DSA-44, ML-DSA-65, ML-DSA-87). MSC Trustgate may also use ML-DSA in non-production environments for **testing and compatibility purposes**. It is not used for TLS, Code Signing, or other certificate types in production environments.

7.1.3.1.5 SLH-DSA

Policy

1. The CA **SHALL** indicate the use of an SLH-DSA key by using one of the following algorithm identifiers:
   i. SLH-DSA-SHA2-128s (OID: 2.16.840.1.101.3.4.3.20)
   ii. SLH-DSA-SHA2-128f (OID: 2.16.840.1.101.3.4.3.21)
   iii. SLH-DSA-SHA2-192s (OID: 2.16.840.1.101.3.4.3.22)
   iv. SLH-DSA-SHA2-192f (OID: 2.16.840.1.101.3.4.3.23)
   v. SLH-DSA-SHA2-256s (OID: 2.16.840.1.101.3.4.3.24)
   vi. SLH-DSA-SHA2-256f (OID: 2.16.840.1.101.3.4.3.25)
2. The parameters for SLH-DSA keys **SHALL be absent**.
3. When encoded, the AlgorithmIdentifier for SLH-DSA keys **SHALL** be byte-for-byte identical with the following hex-encoded bytes:
   i. SLH-DSA-SHA2-128s: 300b0609608648016503040314
   ii. SLH-DSA-SHA2-128f: 300b0609608648016503040315
   iii. SLH-DSA-SHA2-192s: 300b0609608648016503040316
   iv. SLH-DSA-SHA2-192f: 300b0609608648016503040317
   v. SLH-DSA-SHA2-256s: 300b0609608648016503040318
   vi. SLH-DSA-SHA2-256f: 300b0609608648016503040319

Practice

When issuing a certificate with an SLH-DSA public key, MSC Trustgate's practice is to adhere to the above policies. MSC Trustgate uses the specified algorithm identifier, omits the parameters as required, and ensures the encoded AlgorithmIdentifier is byte-for-byte identical with the specified hex bytes.

SLH-DSA is currently restricted to Document Signing certificates only. MSC Trustgate may also use SLH-DSA in non-production environments for testing and compatibility purposes. It is not used for S/MIME, TLS, Code Signing, or other certificate types in production environments.

7.1.3.2 Signature AlgorithmIdentifier

Policy

1. All objects signed by an MSC Trustgate CA Private Key MUST conform to these requirements for the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.
2. This policy applies to the following fields:
   - The signatureAlgorithm field of a Certificate or Precertificate.
   - The signature field of a TBSCertificate (for example, as used by either a Certificate or Precertificate).
   - The signatureAlgorithm field of a CertificateList.
   - The signature field of a TBSCertList.
   - The signatureAlgorithm field of a BasicOCSPResponse.
3. No other encodings are used for these fields.

Practice

MSC Trustgate's practice is to ensure that all objects signed by its CA Private Key adhere to the above policies. The CA signing software is configured to use only the specific signature algorithms and encodings detailed in the following subsections, and automated checks are performed during issuance to confirm compliance.

7.1.3.2.1 RSA Signatures

Policy

1. The CA SHALL use one of the following algorithm identifiers to specify RSA-based signatures:
   i. For **sha256WithRSAEncryption** (OID: 1.2.840.113549.1.1.11), the AlgorithmIdentifier SHALL be byte-for-byte identical with 300d06092a864886f70d01010b0500.
   ii. For **sha384WithRSAEncryption** (OID: 1.2.840.113549.1.1.12), the AlgorithmIdentifier SHALL be byte-for-byte identical with 300d06092a864886f70d01010c0500.
   iii. For **sha512WithRSAEncryption** (OID: 1.2.840.113549.1.1.13), the AlgorithmIdentifier SHALL be byte-for-byte identical with 300d06092a864886f70d01010d0500.
2. The CA SHALL also use the id-RSASSA-PSS (OID: 1.2.840.113549.1.1.10) algorithm identifier, with the following parameters:
   - The Mask Generation Function (MGF) **SHALL** be mgf1 (OID: 1.2.840.113549.1.1.8).
   - The hash algorithm for the signature and MGF **SHALL** match one of the following:
     i. **SHA-256** (OID: 2.16.840.1.101.3.4.2.1), with a salt length of 32 bytes. The AlgorithmIdentifier **SHALL** be byte-for-byte identical with 3031300d06092a864886f70d01010a3020a009300706052b0e03021a010420a109300706052b0e03021a020120a203020101.
     ii. **SHA-384** (OID: 2.16.840.1.101.3.4.2.2), with a salt length of 48 bytes. The AlgorithmIdentifier **SHALL** be byte-for-byte identical with 3031300d06092a864886f70d01010a3020a009300706052b0e03021a010420a109300706052b0e03021a020130a203020101.
     iii. **SHA-512** (OID: 2.16.840.1.101.3.4.2.3), with a salt length of 64 bytes. The AlgorithmIdentifier **SHALL** be byte-for-byte identical with 3031300d06092a864886f70d01010a3020a009300706052b0e03021a010420a109300706052b0e03021a020140a203020101.

Practice

MSC Trustgate's practice is to ensure adherence to the above policies. The CA signing software is configured to use only the specific sha256WithRSAEncryption, sha384WithRSAEncryption, sha512WithRSAEncryption, and id-RSASSA-PSS signature algorithms. Automated checks are performed during issuance to confirm compliance with the specified OIDs, parameters, and encodings for each algorithm.

7.1.3.2.2 ECDSA Signatures

Policy

The CA **SHALL** use the appropriate signature algorithm and encoding based on the signing key. For the specified named curves, the following rules **SHALL** apply:

1. **For a P-256 signing key**: The signature **SHALL** use ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2). The encoded AlgorithmIdentifier **SHALL** be byte-for-byte identical with 300a06082a8648ce3d040302.
2. **For a P-384 signing key**: The signature **SHALL** use ecdsa-with-SHA384 (OID: 1.2.840.10045.4.3.3). The encoded AlgorithmIdentifier **SHALL** be byte-for-byte identical with 300a06082a8648ce3d040303.
3. **For a P-521 signing key**: The signature **SHALL** use ecdsa-with-SHA512 (OID: 1.2.840.10045.4.3.4). The encoded AlgorithmIdentifier **SHALL** be byte-for-byte identical with 300a06082a8648ce3d040304.

Practice

MSC Trustgate's practice is to ensure that all objects signed by its CA Private Key adhere to the above policies. The CA signing software is configured to automatically select the correct hash algorithm and encoding based on the signing key's curve and ensures the encoded AlgorithmIdentifier is byte-for-byte identical to the specified values.

7.1.3.2.3 EdDSA Signatures

Policy

The CA **SHALL** use the appropriate signature algorithm and encoding based on the signing key used. For the specified named curves, the following rules **SHALL** apply:

1. **For a Curve25519 signing key**: The signature algorithm **SHALL** be id-Ed25519 (OID: 1.3.101.112). The encoded AlgorithmIdentifier **SHALL** be byte-for-byte identical with 300506032b6570.
2. **For a Curve448 signing key**: The signature algorithm **SHALL** be id-Ed448 (OID: 1.3.101.113). The encoded AlgorithmIdentifier SHALL be byte-for-byte identical with 300506032b6571.

Practice

MSC Trustgate's practice is to ensure that all objects signed by its CA Private Key adhere to the above policies. The CA signing software is configured to automatically select the correct EdDSA algorithm based on the signing key's curve and ensures the encoded AlgorithmIdentifier is byte-for-byte identical to the specified values.

7.1.3.2.4 ML-DSA Signatures

Policy

The CA **SHALL** use the appropriate signature algorithm and encoding based on the signing key used. For the specified ML-DSA signing keys, the following rules **SHALL** apply:

1. **For an ML-DSA-44 signing key**: The signature algorithm **SHALL** be id-ml-dsa-44 (OID: 2.16.840.1.101.3.4.3.17). When encoded, the AlgorithmIdentifier **SHALL** be byte-for-byte identical with the hex-encoded bytes: 300b0609608648016503040311.
2. **For an ML-DSA-65 signing key**: The signature algorithm **SHALL** be id-ml-dsa-65 (OID: 2.16.840.1.101.3.4.3.18). When encoded, the AlgorithmIdentifier **SHALL** be byte-for-byte identical with the hex-encoded bytes: 300b0609608648016503040312.
3. **For an ML-DSA-87 signing key**: The signature algorithm **SHALL** be id-ml-dsa-87 (OID: 2.16.840.1.101.3.4.3.19). When encoded, the AlgorithmIdentifier **SHALL** be byte-for-byte identical with the hex-encoded bytes: 300b0609608648016503040313.

Practice

MSC Trustgate's practice is to ensure that all objects signed by its CA Private Key adhere to the above policies by configuring the CA signing software to automatically select the correct ML-DSA algorithm based on the signing key and ensuring the encoded AlgorithmIdentifier is byte-for-byte identical to the specified values.

7.1.3.2.5 SLH-DSA Signatures

Policy

The CA **SHALL** use the appropriate signature algorithm and encoding based on the signing key used. For the specified SLH-DSA signing keys, the following rules **SHALL** apply:

1. For an SLH-DSA-SHA2-128s signing key: The signature algorithm **SHALL** be id-slh-dsa-sha2-128s (OID: 2.16.840.1.101.3.4.3.20). When encoded, the AlgorithmIdentifier **SHALL** be byte-for-byte identical with 300b0609608648016503040314.
2. For an SLH-DSA-SHA2-128f signing key: The signature algorithm **SHALL** be id-slh-dsa-sha2-128f (OID: 2.16.840.1.101.3.4.3.21). When encoded, the AlgorithmIdentifier **SHALL** be byte-for-byte identical with 300b0609608648016503040315.
3. For an SLH-DSA-SHA2-192s signing key: The signature algorithm **SHALL** be id-slh-dsa-sha2-192s (OID: 2.16.840.1.101.3.4.3.22). When encoded, the AlgorithmIdentifier **SHALL** be byte-for-byte identical with 300b0609608648016503040316.
4. For an SLH-DSA-SHA2-192f signing key: The signature algorithm **SHALL** be id-slh-dsa-sha2-192f (OID: 2.16.840.1.101.3.4.3.23). When encoded, the AlgorithmIdentifier **SHALL** be byte-for-byte identical with 300b0609608648016503040317.
5. For an SLH-DSA-SHA2-256s signing key: The signature algorithm **SHALL** be id-slh-dsa-sha2-256s (OID: 2.16.840.1.101.3.4.3.24). When encoded, the AlgorithmIdentifier **SHALL** be byte-for-byte identical with 300b0609608648016503040318.
6. For an SLH-DSA-SHA2-256f signing key: The signature algorithm **SHALL** be id-slh-dsa-sha2-256f (OID: 2.16.840.1.101.3.4.3.25). When encoded, the AlgorithmIdentifier **SHALL** be byte-for-byte identical with 300b0609608648016503040319.

Practice

MSC Trustgate's practice is to ensure that all objects signed by its CA Private Key adhere to the above policies by configuring the CA signing software to automatically select the correct SLH-DSA algorithm based on the signing key and ensuring the encoded AlgorithmIdentifier is byte-for-byte identical to the specified DER encoding for the selected variant.

7.1.4 Name forms

MSC Trustgate encodes attribute values in accordance with the specifications defined in RFC 5280.

7.1.4.1 Name encoding

For every valid Certification Path (as defined by RFC 5280, Section 6):

i. For each certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field SHALL be byte-for-byte identical to the encoded form of the Subject Distinguished Name field of the issuing CA certificate.

ii. For each CA certificate in the Certification Path, the encoded content of the Subject Distinguished Name field SHALL be byte-for-byte identical among all certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, including expired and revoked certificates.

7.1.4.2 Subject information - subscriber certificates

When issuing a Certificate, MSC Trustgate affirms that all subject information was accurate and verified in accordance with the procedures outlined in this CP/CPS as of the certificate's issuance date.

MSC Trustgate does not issue certificates with subject attributes that solely consist of metadata, such as '.', '-', and ' ' (space) characters, or any other indication suggesting absence, incompleteness, or inapplicability of the value.

7.1.4.2.1 Subject alternative name extension

7.1.4.2.1.1 SSL/TLS Certificates

The Subject Alternative Name MUST contain at least one entry of the following types:

i. dNSName - MUST contain either a FQDN or Wildcard Domain Name. MUST NOT contain an Internal Name, and/or

ii. iPAddress - MUST contain the IPv4 or IPv6 address. MUST NOT contain a Reserved IP Address

7.1.4.2.1.2 S/MIME Certificates

The Subject Alternative Name SHALL contain at least one GeneralName entry of the following types:

i. rfc822Name, and/or

ii. otherName of type id-on-SmtpUTF8Mailbox, encoded in accordance with RFC 8398

All Mailbox Addresses in the subject field or entries of type dirName of this extension SHALL be repeated as rfc822Name or otherName values of type id-on-SmtpUTF8Mailbox in this extension.

7.1.4.2.2 Subject distinguished name fields

MSC Trustgate utilizes the following Subject distinguished name fields for its subscriber certificates:

Field	OID	Contents
commonName	2.5.4.3	Personal Name, Pseudonym, Email Address, FQDN, or subject:organizationName
surname	2.5.4.4	Natural Person subject's names, as verified under Section 3.2.2, used the following guidelines: • Subjects with a single legal name are required to provide the name in the subject:surname field. • For societies that do not practice given and surname conventions, subjects may also provide their full name in the subject:surname field. The subject:surname and subject:givenName fields SHALL NOT be present if the subject:pseudonym is present.
givenName	2.5.4.42	
pseudonym	2.5.4.65	The subject:pseudonym field SHALL be verified according to Section 3.1.3. The subject:pseudonym field SHALL NOT be present if the subject:givenName and/or subject:surname are present.
serialNumber	2.5.4.5	Contain a Natural Person Identifier assigned by the country such as MyKad Number, Passport Number. It may also contain a Business Registration Number for a Legal Entity assigned by an authority. It may also contain an identifier assigned by the CA or RA to identify and/or to disambiguate the Subscriber.
emailAddress	1.2.840.113549.1.9.1	Contain a single Mailbox Address as verified under Section 3.2.4
title	2.5.4.12	Contain only an organizational role/title or a regulated professional designation verified according to Section 3.2.2
organizationName	2.5.4.10	Subject's full legal organization name and/or an Assumed Name as verified under Section 3.2.2
organizationIdentifier	2.5.4.97	Contain a Registration Reference for a Legal Entity assigned in accordance with the identified Registration Scheme. It SHALL be encoded as a PrintableString or UTF8String. See Appendix A.
localityName	2.5.4.7	Contain the Subject's locality information as verified under Section 3.2.2 (for an organization) or Section 3.2.3 (for an individual).
stateOrProvinceName	2.5.4.8	Contain the Subject's state or province information as verified under Section 3.2.2 (for an organization) or Section 3.2.3 (for an individual).

Field	OID	Contents
countryName	2.5.4.6	Contain the two-letter ISO 3166-1 country code associated with the location of the Subject as verified under Section 3.2.2 (for an organization) or Section 3.2.3 (for an individual).

7.1.4.2.2.1 Document Signing Certificates

MSC Trustgate issues various types of Document Signing Certificates, each with its own distinct set of subject DN attributes, outlined in this section.

7.1.4.2.2.1.1 LHDN e-Invoice Organization Certificates

MSC Trustgate issues Organization Certificates for e-Invoice, facilitating companies, tax agents, or aggregators to digitally sign and submit e-Invoice to LHDN.

Here are the subject DN attributes for the Organization Certificates:

Attributes	Value or Value Constraint
commonName	MUST be present.
serialNumber	MUST be present. The Business Registration Number (BRN) of the subject:organizationName, registered with Suruhanjaya Syarikat Malaysia or any other country or state government agency. This BRN must be linked with subject:organizationIdentifier.
organizationName	MUST be present.
organizationIdentifier	MUST be present. The Tax Identification Number of the subject:organizationName, registered with Malaysia Inland Revenue Board (Lembaga Hasil Dalam Negeri).
countryName	MUST be present. Country that regulate or register the subject:organizationName.
Other Attributes	NOT RECOMMENDED.

7.1.4.2.2.1.2 MyGPKI

MSC Trustgate collaborates with Jabatan Digital Negara (formerly known as MAMPU) to issue MyGPKI Certificates to Malaysian government officers, facilitating secure online transactions and communications with government entities nationwide. These certificates play a vital role in authenticating users' identities, encrypting data, and digitally signing documents and transactions, thereby ensuring their confidentiality, integrity, and authenticity.

Below are the subject DN attributes for the MyGPKI Certificates:

Attributes	Value or Value Constraint
commonName	MUST be present. Name as appear on MyKad.
serialNumber	MUST be present. It represents MyKad number.
surname	MUST be present. It represents the MyKad number for backward compatibility with some applications.
countryName	MUST be present and set to MY. It indicates that the subject is a Malaysian citizen and an officer of the Malaysian government.

Attributes	Value or Value Constraint
Other Attributes	NOT RECOMMENDED.

7.1.4.2.2.1.3 Other Certificates

MSC Trustgate issues other Document Signing Certificates, including AATL Certificates. There are various types of Certificates:

7.1.4.2.2.1.3.1 Individual Basic Certificates

Individual Basic Certificates are distinguished only with Natural Person attributes in the Subject.

Attributes	Value or Value Constraint
commonName	MUST be present. Name as appear on MyKad or Passport.
serialNumber	MUST be present. MyKad or Passport Number.
countryName	MUST be present. Country that issue the subject:serialNumber.
Other Attributes	NOT RECOMMENDED.

7.1.4.2.2.1.3.2 Individual Pro Certificates

Individual Pro Certificates are uniquely identified through a blend of Natural Person attributes, complemented by the subject's organizationName attribute within the Subject field. For instance, such a certificate might be issued to an employee of an organization or a member of a regulated professional body.

Attributes	Value or Value Constraint
commonName	MUST be present. Name as appear on MyKad or Passport.
serialNumber	MAY be present. Contain a registration number of a regulated professional organization
title	MAY be present. Contain only an organizational role/title or a regulated professional designation.
organizationName	MUST be present.
organizationIdentifier	MAY be present. Contain a registration number of the subject:organizationName
localityName	MAY be present.
stateOrProvinceName	MAY be present.
countryName	MUST be present. Country that regulate or register the subject:organizationName.
Other Attributes	NOT RECOMMENDED.

See Appendix A.2 on how to construct serialNumber attributes.

Organization Certificates

Organization Certificates are distinguished by their registration number with a recognized authority, ensuring their legitimacy and credibility.

Attributes	Value or Value Constraint
commonName	MUST be present.
organizationName	MUST be present.
organizationIdentifier	MUST be present. Contain a registration number of the subject:organizationName
localityName	MAY be present.
stateOrProvinceName	MAY be present.
countryName	MUST be present. Country that regulate or register the subject:organizationName.
Other Attributes	NOT RECOMMENDED.

See Appendix A.1 on contructing organizationIdentifier attributes.

7.1.4.2.2.2 MyDigital ID Certificates

MSC Trustgate issues MyDigital ID Certificates, empowering subscribers to authenticate themselves across a range of Malaysian online services. Below are the subject DN attributes for the MyDigital ID Certificates:

Attributes	Value or Value Constraint
commonName	MUST be present. Name as appear on MyKad.
serialNumber	MUST be present. MyKad Number.
Other Attributes	MUST NOT be present.

7.1.4.2.2.3 SSL/TLS Certificates

7.1.4.2.2.3.1 Domain Validation (DV) Certificates

Here is subject DN for DV SSL/TLS Certificates:

Attributes	Value or Value Constraint
countryName	MAY be present. The two-letter ISO 3166-1 country code for the country associated with the Subject.
commonName	NOT RECOMMENDED. If present, MUST contain a value derived from the subjectAltName extension according to Section 7.1.4.2.1.1.
Other Attributes	NOT RECOMMENDED.

7.1.4.2.2.3.2 Organization Validation (OV) Certificates

Here is subject DN for OV SSL/TLS Certificates:

Attributes	Value or Value Constraint
countryName	MUST be present. The two-letter ISO 3166-1 country code for the country associated with the Subject.
stateOrProvinceName	MUST be present if localityName is absent, MAY be present otherwise. If present, MUST contain the Subject's state or province information.
localityName	MUST be present if stateOrProvinceName is absent, MAY be present otherwise. If present, MUST contain the Subject's locality information.
organizationName	The Subject's name or DBA. MSC Trustgate MAY include information in this field that differs slightly from the verified name, such as common variations or Abbreviations. MSC Trustgate documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows "Company Name Berhad", MSC Trustgate MAY use "Company Name Bhd." or "Company Name".
commonName	NOT RECOMMENDED. If present, MUST contain a value derived from the subjectAltName extension according to Section 7.1.4.2.1.1.
Other Attributes	NOT RECOMMENDED.

7.1.4.2.2.4 S/MIME Certificates

7.1.4.2.2.4.1 Mailbox Validated Certificates

Attributes	Value or Value Constraint
commonName	MAY be present.
serialNumber	MAY be present.
emailAddress	MAY be present.
Other Attributes	SHALL NOT be present.

7.1.4.2.2.4.2 Organization Validated Certificates

Attributes	Value or Value Constraint
commonName	MAY be present.
serialNumber	MAY be present.
emailAddress	MAY be present.
organizationName	SHALL be present.
organizationIdentifier	SHALL be present.
localityName	MAY be present
stateOrProvinceName	MAY be present
countryName	MAY be present
Other Attributes	SHALL NOT be present.

7.1.4.2.2.4.3 Sponsor Validated Certificates

Attributes	Value or Value Constraint
commonName	MAY be present.
givenName	MAY be present.
surname	MAY be present.
pseudonym	MAY be present.
serialNumber	MAY be present.
emailAddress	MAY be present.
organizationName	SHALL be present.
organizationIdentifier	SHALL be present.
title	MAY be present.
localityName	MAY be present
stateOrProvinceName	MAY be present
countryName	MAY be present

Attributes	Value or Value Constraint
Other Attributes	SHALL NOT be present.

7.1.4.2.2.4.4 Individual Validated Certificates

Attributes	Value or Value Constraint
commonName	MAY be present.
givenName	MAY be present.
surname	MAY be present.
pseudonym	MAY be present.
serialNumber	MAY be present.
emailAddress	MAY be present.
title	MAY be present.
localityName	MAY be present
stateOrProvinceName	MAY be present
countryName	MAY be present
Other Attributes	SHALL NOT be present.

7.1.4.2.2.5 Code Signing Certificates

7.1.4.2.2.5.1 Code Signing Certificates

Attributes	Value or Value Constraint
commonName	MUST be present. MUST contain the Subject's legal name as verified under Section 3.2.2 or 3.2.3.
organizationName	MUST be present. Must contain the Subject's name or DBA. MSC Trustgate MAY include information in this field that differs slightly from the verified name, such as common variations or Abbreviations. MSC Trustgate documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows "Company Name Berhad", MSC Trustgate MAY use "Company Name Bhd." or "Company Name".
localityName	MUST be present if stateOrProvinceName is absent, MAY be present otherwise. If present, MUST contain the Subject's locality information.
stateOrProvinceName	MUST be present if localityName is absent, MAY be present otherwise. If present, MUST contain the Subject's state or province information.
countryName	MUST be present. The two-letter ISO 3166-1 country code for the country associated with the Subject.
Other Attributes	SHALL NOT be present.

7.1.4.2.2.5.2 Extended Validation Code Signing Certificates

Attributes	Value or Value Constraint
commonName	MUST be present. MUST contain the Subject's legal name as verified under Section 3.2.2 or 3.2.3.
serialNumber	MUST be present. For Private Organizations. MUST contain the Registration Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. For Government Entities, MUST enter appropriate language to indicate that the Subject is a Government Entity. For Business Entities, If the business has such a registration number, that number must be entered into the field. Otherwise, the date of registration should be entered into the field.
organizationName	MUST be present. Must contain the Subject's name or DBA. MSC Trustgate MAY include information in this field that differs slightly from the verified name, such as common variations or Abbreviations. MSC Trustgate documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows "Company Name Berhad", MSC Trustgate MAY use "Company Name Bhd." or "Company Name".
businessCategory	MUST be present. MUST contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" .
Address	MAY be present. MUST contain the address of the physical location of the Subject's Place of Business.
localityName	Must be present. MUST contain the Subject's locality information.
stateOrProvinceName	MUST be present. , MUST contain the Subject's state or province information.
countryName	MUST be present. The two-letter ISO 3166-1 country code for the country associated with the Subject.
Other Attributes	SHALL NOT be present.

7.1.4.3 Subject information - root and subordinate CA certificates

When issuing a Subordinate CA Certificate, MSC Trustgate affirms that all subject information was accurate and verified in accordance with the procedures outlined in this CP/CPS as of the certificate's issuance date.

7.1.4.3.1 Subject distinguished name fields

MSC Trustgate utilizes the following Subject distinguished name fields for its subscriber certificates:

Field	OID	Contents
commonName	2.5.4.3	MUST be present. This field SHOULD contain an identifier for the Certificate such that the Certificate's Name is unique across all Certificates issued by the Issuing CA
organizationName	2.5.4.10	MUST be present. This field SHALL contain either the Subject CA's name or DBA as verified under Section 3.2.3.3.
countryName	2.5.4.6	MUST be present. This field SHALL contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.
Other Subject Attributes		MAY be present. If present, MSC Trustgate verifies the information contained in other attributes.

7.1.5 Name constraints

Policy

1. For a Subordinate CA Certificate to be considered Technically Constrained, the Certificate SHALL include an Extended Key Usage (EKU) extension that specifies all extended key usages for which the Subordinate CA Certificate is authorized to issue Certificates.
2. The anyExtendedKeyUsage KeyPurposeId SHALL NOT appear within this extension.
3. If the Subordinate CA Certificate includes the id-kp-emailProtection extended key usage, it SHALL also include the nameConstraints X.509v3 extension with constraints on rfc822Name and directoryName as follows:
    - For each rfc822Name in permittedSubtrees, it SHALL contain either a FQDN or a U+002E FULL STOP (“.”) character followed by a FQDN.
    - The rfc822Name SHALL NOT contain an email address.
    - The CA SHALL confirm that the Applicant has registered the FQDN or has been authorized by the domain registrant to act on their behalf.
    - For each directoryName in permittedSubtrees, the CA SHALL confirm the Applicant’s and/or Subsidiary’s Organizational name and location to ensure compliance with the requirements of this document.

Practice

To meet the policies set forth above, MSC Trustgate's practice is to:

1. Populate the EKU extension for Technically Constrained Subordinate CA Certificates with the authorized key usages and omit the anyExtendedKeyUsage KeyPurposeId.
2. When a Technically Constrained Subordinate CA Certificate is issued with the id-kp-emailProtection extended key usage, MSC Trustgate populates the nameConstraints extension with the required constraints on rfc822Name and directoryName.
    - For each rfc822Name in permittedSubtrees, MSC Trustgate ensures it contains a FQDN or a . character followed by a FQDN and confirms the Applicant has registration or authorization for the domain in line with Section 3.2.5.
    - For each directoryName in permittedSubtrees, MSC Trustgate confirms the Applicant’s and/or Subsidiary’s Organizational name and location to ensure end-entity Certificates issued from this CA are in compliance with Section 7.1.2.5.

7.1.6 Certificate policy object identifier

This section sets forth the minimum requirements for the content and management of the certificatePolicies extension in Root CA, Subordinate CA, and Subscriber Certificates, as implemented by MSC Trustgate.

7.1.6.1 Reserved Certificate Policy Identifiers

The following Certificate Policy identifiers, as defined by the CA/Browser Forum, are used by MSC Trustgate to assert that a Certificate has been issued and managed in accordance with the respective Baseline Requirements:

- SSL/TLS Domain-validated: 2.23.140.1.2.1
- SSL/TLS Organization-validated: 2.23.140.1.2.2
- SSL/TLS Individual-validated: 2.23.140.1.2.3
- SSL/TLS Extended-validated: 2.23.140.1.1
- S/MIME Mailbox-validated: 2.23.140.1.5.1.3
- S/MIME Organization-validated: 2.23.140.1.5.2.3
- S/MIME Sponsor-validated: 2.23.140.1.5.3.3
- S/MIME Individual-validated: 2.23.140.1.5.4.3
- Non-EV Code Signing Certificates: 2.23.140.1.4.1
- EV Code Signing Certificates: 2.23.140.1.3
- Timestamp Certificates: 2.23.140.1.4.2

7.1.6.2 Root CA Certificates

A Root CA Certificate SHALL NOT contain the certificatePolicies extension.

MSC Trustgate's practice is to not include the certificatePolicies extension in its Root CA Certificates.

7.1.6.3 Subordinate CA Certificates

Policy

1. SSL/TLS, S/MIME, Code Signing, and Timestamping Certificates issued to a Subordinate CA MUST include one or more explicit policy identifiers from Section 7.1.6.1.
2. These certificates MUST NOT contain the anyPolicy identifier (2.5.29.32.0).
3. Other Certificates issued to a Subordinate CA MAY contain the anyPolicy identifier.

Practice

1. For Subordinate CA Certificates designated for SSL/TLS, S/MIME, Code Signing, or Timestamping, MSC Trustgate includes one or more explicit policy identifiers from Section 7.1.6.1. This practice indicates the Subordinate CA's compliance with the respective CA/B Forum Baseline Requirements. These certificates may also contain one identifier from Section 1.2, but the anyPolicy identifier is not included.
2. For all other types of Subordinate CA Certificates, MSC Trustgate may include one policy identifier from Section 1.2. The anyPolicy identifier may also be included in place of an explicit policy identifier.

7.1.6.4 Subscriber Certificates

Policy

1. SSL/TLS, S/MIME, Code Signing, and Timestamping Certificates issued to a Subscriber MUST include one or more explicit policy identifiers from Section 7.1.6.1.
2. These certificates MUST NOT contain the anyPolicy identifier (2.5.29.32.0).
3. Other Certificates issued to a Subscriber MAY contain the anyPolicy identifier.

Practice

1. For Subscriber Certificates designated for SSL/TLS, S/MIME, Code Signing, or Timestamping, MSC Trustgate includes one or more explicit policy identifiers from Section 7.1.6.1. This practice indicates the Subscriber's compliance with the respective CA/B Forum Baseline Requirements. These certificates may also contain one identifier from Section 1.2, but the anyPolicy identifier is not included.
2. For all other types of Subscriber Certificates, MSC Trustgate may include one policy identifier from Section 1.2. The anyPolicy identifier may also be included in place of an explicit policy identifier.

7.1.7 Usage of Policy Constraints extension

Reserved.

7.1.8 Policy qualifiers syntax and semantics

Certificates SHALL contain policy qualifiers within the certificatePolicies extension. The policy qualifier SHOULD include a CP/CPS pointer qualifier. The policy qualifier MAY also include a User Notice Qualifier. These qualifiers SHALL point to the applicable Relying Party Agreement or CP/CPS.

MSC Trustgate generally populates Certificates with a policy qualifier within the certificatePolicies extension. Its practice is to include a CP/CPS pointer qualifier that points to the applicable Relying Party Agreement or the MSC Trustgate CP/CPS. Additionally, 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

Reserved.

7.2 CRL profile

MSC Trustgate SHALL issue CRLs in accordance with the profile specified in this section, which is derived from RFC 5280. The CRLReason for a revoked issuing CA MUST NOT be unspecified (0) or certificateHold (6). If a reasonCode CRL entry extension is present, the CRLReason MUST indicate the most appropriate reason for revocation.

To meet this policy, when MSC Trustgate generates a CRL for a revoked issuing CA, its practice is to ensure that the CRLReason is not unspecified (0) or certificateHold (6). If the reason for revocation is determined to be unspecified, MSC Trustgate omits the reasonCode entry extension. When a reasonCode CRL entry extension is present, MSC Trustgate populates it with the most appropriate reason for the certificate's revocation. The full list of reason codes that MSC Trustgate uses is specified in Section 7.2.2.

7.2.1 Version number(s)

MSC Trustgate issues version 2 CRLs that conform to RFC 5280.

7.2.2 CRL and CRL entry extensions

MSC Trustgate issues CRLs with the following extensions:

i. CRL Number
ii. Authority Key Identifier
iii. Invalidity Date
iv. Reason Code

MSC Trustgate specifies the following CRLReason codes from RFC 5280, section 5.3.1, as appropriate for use in the Reason Code entry extension:

- keyCompromise (1)
- cACompromise (2)
- affiliationChanged (3)
- superseded (4)
- cessationOfOperation (5)
- privilegeWithdrawn (9)

7.3 OCSP profile

MSC Trustgate's OCSP services are operated in accordance with RFC 6960, including the profile for high-volume environments as defined in RFC 5019. The revocationReason field in the RevokedInfo of the CertStatus SHALL be present for all revoked certificates, including Root CA, Subordinate CA, Cross, and end-user certificates. The value of this field SHALL conform to the CRLReason codes defined in Section 7.2.2. To meet this policy, MSC Trustgate populates the revocationReason field with the conforming CRLReason code for any certificate it revokes.

7.3.1 Version number(s)

OCSP responses are generated with a version field value of v1.

7.3.2 OCSP extensions

The OCSP response uses the crlReason field within the RevokedInfo structure to indicate the reason for revocation, and this information is not represented as a separate extension within the singleExtensions list.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices in this CP/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.

8.1 Frequency or circumstances of assessment

MSC Trustgate receives an annual period audit by an independent external auditor to assess MSC Trustgate's compliance with this CP/CPS and the WebTrust for CA programs criteria. The audit covers MSC Trustgate's RA systems, and OCSP Responders.

Audits are conducted over unbroken sequences of audit periods with each period no longer than one (1) year duration.

If MSC Trustgate has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 8.4, then no pre-issuance readiness assessment is necessary.

If MSC Trustgate does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in Section 8.4, then, before issuing Publicly-Trusted Certificates, MSC Trustgate SHALL successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in Section 8.4. The point-in-time readiness assessment SHALL be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.

8.2 Identity/qualifications of assessor

WebTrust auditors must meet the requirements of Section 8.2 of the CA/Browser Baseline Requirements. The auditors must also be 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 are performed by a public accounting firm that is independent of MSC Trustgate.

8.4 Topics covered by assessment

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

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

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

8.5 Actions taken as a result of deficiency

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

i. The auditor will document the discrepancy;

ii. The auditor will promptly notify MSC Trustgate; and

iii. MSC Trustgate will develop a plan to cure the noncompliance.

MSC Trustgate will submit the plan to the Management for approval and to any third party that MSC Trustgate is legally obligated to satisfy. The MSC Trustgate 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 is entitled to suspend and/or terminate of services through revocation or other actions as deemed by the MSC Trustgate 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'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 submits copies of relevant audit compliance reports to various parties, such as Malaysian Communications and Multimedia Commission (MCMC), Mozilla, Adobe, and other relying body. In the event of a delay greater than three (3) months, MSC Trustgate shall provide an explanatory letter signed by the Qualified Auditor.

For Audit Reports in which the Audit Period includes a date later than 2020-08-01, then the requirements set forth in the remainder of this Section 8.6 SHALL be met. Audit Reports for Audit Periods that conclude prior to 2020-08-01 SHOULD meet these requirements.

The Audit Report MUST contain at least the following clearly labelled information:

i. Name of the organization being audited;

ii. Name and address of the organization performing the audit;

iii. The SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross Certificates, that were in-scope of the audit;

iv. Audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);

v. A list of the CA policy documents, with version numbers, referenced during the audit;

vi. Whether the audit assessed a period of time or a point in time;

vii. The start date and end date of the Audit Period, for those that cover a period of time;

viii. The point in time date, for those that are for a point in time;

ix. The date the report was issued, which will necessarily be after the end date or point in time date;

x. All incidents disclosed by the CA, discovered by the auditor, or reported by a third party, that, at any time during the audit period, occurred or were open in Mozilla's Bugzilla reporting system.

An authoritative English language version of the publicly available audit information MUST be provided by the Qualified Auditor and the MSC Trustgate ensure it is publicly available.

The Audit Report MUST be available as a PDF and SHALL be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report MUST be uppercase letters and MUST NOT contain colons, spaces, or line feeds.

8.7 Self-Audits

MSC Trustgate ensures compliance with the Certificate Policy, Certification Practice Statement, and other external requirements specified in section 1.1 through regular self-audits. These audits involve monitoring service quality through quarterly assessments, which include randomly selecting samples representing at least 3% (6% for EV SSL Certificates and EV Code Signing Certificates) of the issued Certificates. This process supports maintaining strict control over service quality.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

MSC Trustgate is entitled to charge end-user Subscribers for the issuance, management, and renewal of Certificates. For Document Signing Certificates, the fee is not more than Ringgit Malaysia One Hundred Twenty (RM 120) for Medium Assurance certificates. For High Assurance certificates the fee is Ringgit Malaysia One Thousand Five Hundred (RM 1500). However, the fee does not include government tax, postage, public notary fee, storage, signing services, date/time stamping services, and others.

9.1.2 Certificate access fees

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

MSC Trustgate 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's prior express written consent.

9.1.4 Fees for other services

MSC Trustgate does not charge a fee for access to this CP/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.

MSC Trustgate reserves the right to charge for additional services, including digital signing services, key management services for roaming/remote certificates, and date/time stamping services.

9.1.5 Refund policy

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

MSC Trustgate 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 to 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 revoke the certificate and provide a refund if MSC Trustgate has breached a warranty or other material obligation under this CP/CPS relating to the subscriber or the subscriber's certificate.

After MSC Trustgate revokes the subscriber's certificate, MSC Trustgate 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 only be liable for the issuance certificates not exceeding the amount as per section 9.8.

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"):

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

9.3.2 Information not within the scope of confidential information

Certificates, Certificate revocation and other status information, MSC Trustgate 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 secures private information from compromise and disclosure to third parties.

9.4 Privacy of personal information

9.4.1 Privacy plan

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

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

MSC Trustgate CA services 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 otherwise stated in this CP/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 shall be entitled to disclose Confidential/ Private Information if, in good faith, MSC Trustgate believes that:

i. Disclosure is necessary in response to subpoenas and search warrants; and

ii. 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 Sub-domain Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such MSC Trustgate Sub-domain Participants.

9.6 Representations and warranties

9.6.1 CA representations and warranties

CA warrant that:

i. The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate;

ii. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier;

iii. All Relying Parties who reasonably rely on a Valid Certificate. The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with these Requirements and its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate.

iv. 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;

v. Their private key is protected, and that no unauthorized person has ever had access to the Subscriber's private key;

vi. All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true;

vii. All information supplied by the Subscriber and contained in the Certificate is true;

viii. The Certificate is being used exclusively for authorized and legal purposes, consistent with this CP/CPS; and

ix. 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.

x. Subscriber Agreements may include additional representations and warranties.

xi. MSC Trustgate represents and warrants to Certificate Beneficiaries that when the Certificate is valid, the Issuing CA has complied with its CP/CPS in issuing and managing the Certificate.

9.6.2 RA Representations and Warranties

RAs warrant that:

i. 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;

ii. 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;

iii. Their Certificates meet all material requirements of this CP/CPS; and

iv. Revocation services (when applicable) and use of a repository conform to the applicable CP/CPS in all material aspects;

v. Subscriber Agreements may include additional representations and warranties.

9.6.3 Subscriber representations and warranties

Before being issued and receiving a certificate, subscribers are fully responsible for any misrepresentations they make to third parties and for all transactions conducted using their Private Key, regardless of whether such use was authorized. Subscribers must notify MSC Trustgate and any relevant Registration Authority (RA) of any changes that could impact the certificate's status.

As part of the Subscriber Agreement or Terms of Use, MSC Trustgate requires the Applicant to make the commitments and warranties outlined in this section for the benefit of MSC Trustgate and the Certificate Beneficiaries.

Before issuing a certificate, MSC Trustgate will obtain, for the explicit benefit of DigiCert and the Certificate Beneficiaries, either:

i. The Applicant's agreement to the Subscriber Agreement with MSC Trustgate, or

ii. The Applicant's acknowledgment of the Terms of Use.

Subscribers warrant that:

i. 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;

ii. Their private key is protected, and that no unauthorized person has ever had access to the Subscriber's private key;

iii. All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true;

iv. All information supplied by the Subscriber and contained in the Certificate is true,

v. The Certificate is being used exclusively for authorized and legal purposes, consistent with this CP/CPS; and

vi. 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 CP/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's possible warranties, including any warranty of merchantability or fitness for a particular purpose.

9.8 Limitations of liability

9.8.1 CA Liability

To the extent MSC Trustgate has issued and managed the Certificate(s) at issue in compliance with the MSC Trustgate Certificate Policy and the MSC Trustgate Certification Practice Statement, MSC Trustgate 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's liability. Limitations of liability shall include an exclusion of indirect, special, incidental, and consequential damages.

Liability is limited solely to actual and legally provable damages. MSC Trustgate is not liable for:

i. Any indirect, consequential, special, or punitive damages, including loss of profit, revenue, data, or opportunities, even if MSC Trustgate has been informed of the potential for such damages.

ii. Any liability arising from fraud or intentional misconduct by the Applicant.

iii. Any liability resulting from the use of a Certificate beyond the intended purpose, specified limitations on usage, value, or transactions, as outlined in the Certificate or this CP/CPS.

iv. Any liability concerning the security, usability, or integrity of products not provided by MSC Trustgate, including hardware used by the subscriber or Relying Party.

v. Any liability related to the compromise of a subscriber's Private Key.

They shall also include the following liability caps limiting MSC Trustgate's damages concerning a specific Certificate:

Certificate Type	Liability Caps
AATL Individual Basic	Ringgit Malaysia Thirty Thousand (RM30,000)
AATL Individual Pro	Ringgit Malaysia Forty Thousand (RM40,000)
AATL Organization	Ringgit Malaysia Eighty Thousand (RM80,000)

Document Signing (Medium Assurance)	Ringgit Malaysia Twenty-Five Thousand (RM25,000)
Document Signing for Organization (Medium Assurance)	Ringgit Malaysia Fifty Thousand (RM50,000)
Document Signing (High Assurance)	Ringgit Malaysia Four Hundred Thousand (RM400,000)
MyDigital ID	Ringgit Malaysia Four Hundred Thousand (RM400,000)
SSL Domain Validation (non-public trusted)	Ringgit Malaysia Five Hundred (RM500)
SSL Organization Validation (non-public trusted)	Ringgit Malaysia Fifty Thousand (RM50,000)
S/MIME Mailbox	Ringgit Malaysia Five Hundred (RM500)
S/MIME Individual	Ringgit Malaysia Ten Thousand (RM10,000)
S/MIME Sponsored	Ringgit Malaysia Twenty-Five Thousand (RM25,000)
S/MIME Organization	Ringgit Malaysia Fifty Thousand (RM50,000)

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 MSC Trustgate 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.

9.8.2 RA Liability

RAs shall subject to the same liabilities as applicable to MSC Trustgate, as listed in CP/CPS Part 9.8.1 should there be any violation of provision in the CP/CPS that may cause damage to the subscribers.

9.9 Indemnities

9.9.1 Indemnification by MSC Trustgate

MSC Trustgate assumes no financial responsibility for improperly used certificates, CRLs, etc.

9.9.2 Indemnification by Subscribers

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

i. Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application;

ii. 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;

iii. 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

iv. 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 for:

i. The Relying Party's failure to perform the obligations of a Relying Party;

ii. The Relying Party's reliance on a Certificate that is not reasonable under the circumstances; or

iii. 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 CP/CPS becomes effective upon publication in the MSC Trustgate repository. Amendments to this CP/CPS become effective upon publication in the MSC Trustgate repository.

9.10.2 Termination

This CP/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 CP/CPS, MSC Trustgate sub-domain participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual notices and communications with participants

MSC Trustgate accepts notices related to this CP/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. 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 may allow other forms of notice in its Subscriber Agreements.

MSC Trustgate will notify Adobe a month in advance of any updates or changes with the potential to affect compliance with the AATL program, including:

i. Additions of Root CAs and Subordinate CAs;

ii. Additional CP/CPS at the Root CA level;

iii. Changes in Certificate issuance procedures; or

iv. Terminations or transition of ownership of Root CAs or Subordinate CAs.

MSC Trustgate will notify Mozilla if:

i. Ownership or control of the CA certificates changes;

ii. 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 MSC Trustgate included certificate(s);

iii. Ownership or control of MSC Trustgate's operations changes; or

iv. There is a material change in MSC Trustgate's operations (e.g., when the cryptographic hardware related to a certificate in Mozilla's root store is consequently moved from one place to another)

9.12 Amendments

9.12.1 Procedure for amendment

This CP/CPS is reviewed annually. Amendments to this CP/CPS may be made by the MSC Trustgate Policy Management Authority (PMA). Amendments shall either be in the form of a document containing an amended form of the CP/CPS or an update. Amended versions or updates shall be linked to the Practices Updates and Notices section of the MSC Trustgate Repository located at: https://www.msctrustgate.com/repository. 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 CP/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 and the PMA reserve the right to amend the CP/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 CP/CPS shall appear in the Practices Updates and Notices section of the MSC Trustgate Repository, which is located at: https://www.msctrustgate.com/repository.

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

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. Disputes involving MSC Trustgate 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.

Parties are required to notify MSC Trustgate and attempt to resolve disputes directly with MSC Trustgate before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

9.14 Governing law

This CPS complies with Malaysian law, i.e., the Digital Signature Act 1997 (Act 562) and the Digital Regulations 1998, and compliance with other applicable laws.

9.15 Compliance with applicable law

MSC Trustgate is obliged to adhere to the applicable legislation as stated under 9.14.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No Stipulation

9.16.2 Assignment

No Stipulation

9.16.3 Severability

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No Stipulation

9.16.5 Force Majeure

In no event shall the MSC Trustgate be deemed in default or liable for any loss or damage resulting from the failure or delay in the performance of its obligations under the CP/CPS, any Subscription Agreement, or any Relying Party Agreement, arising out of or caused by, directly or indirectly, any event or circumstance beyond MSC Trustgate's reasonable control, including but not limited to, floods, fires, hurricanes, earthquakes, tornados, epidemics, pandemics, other acts of God or nature, strikes and other labor disputes, failure of utility, transportation or communications infrastructures, riots or other acts of civil disorder, acts of war, terrorism (including cyber terrorism), malicious damage, judicial action, lack of or inability to obtain export permits or approvals, acts of government such as expropriation, condemnation, embargo, changes in applicable laws or regulations, and shelter-in-place or similar orders, and acts or defaults of third party suppliers or service providers.

9.17 Other provisions

9.17.1 Personal Data

MSC Trustgate are subjected to the PDPA Act 2010 (Act 709) and registered and party with the Jabatan Perlindungan Data Peribadi (JPDP). All the obligation stipulated in the act is deemed to be accepted by all parties as final and will not be subjected to any other obligations. The personal data involved shall be protected under the law.

9.17.2 Right to audit

MSC Trustgate has been deemed been audit by its independent external auditor appointed by MCMC and shall not be subjected to any other audit requirements as stipulated by any other written law as it will conflicting the jurisdiction among government agencies i.e., MCMC and any other Commissions and legislations.

APPENDIX A: REGISTRATION SCHEME

A.1: organizationIdentifier

The following Registration Schemes are recognized as valid under these Requirements for use in the `subject:organizationIdentifier` attribute described in Section 7.1.4.2.2.

Registration Scheme Identifier	Description
GOV	For government entities named in the `subject:organizationName`.
NTR	For an identifier allocated by a national or state trade register to the Legal Entity named in the `subject:organizationName`.
VAT	For an identifier allocated by the national tax authorities to the Legal Entity named in the `subject:organizationName`.
OTH	For an identifier allocated by other national authorities to the Legal Entity named in the `subject:organizationName`.
LEI	For a Legal Entity Identifier as specified in ISO 17442 for the entity named in the `subject:organizationName`. The 3-character Registration Scheme identifier be set to INT and the 2 characters ISO 3166 country code SHALL be set to 'XG'.

The `subject:organizationIdentifier` field SHALL contains a Registration Reference for a Legal Entity assigned in accordance to the identified Registration Scheme. The Registration Reference SHOULD be unique where the Registration Scheme and jurisdiction provide unique identifiers.

The `subject:organizationIdentifier` SHALL be encoded as a PrintableString or UTF8String.

The Registration Scheme identified in the Certificate SHALL be the result of the verification performed in accordance with Section 3.2.2.

If the Registration Reference is assigned at the country level, the Registration Scheme SHALL be identified using the following structure in the presented order:

- 3 characters Registration Scheme identifier; and
- 2 characters ISO 3166-1 country code for the nation in which the Registration Scheme is operated, or as described in Note 1; and
- a hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and
- Registration Reference allocated in accordance with the identified Registration Scheme.

If the Registration Reference is assigned at the subdivision (state or province) level and is not unique at the national level, the Registration Scheme SHALL be identified using the following structure in the presented order:

- 3 characters Registration Scheme identifier; and
- 2 characters ISO 3166-1 country code for the nation in which the Registration Scheme is operated, or as described in Note 1; and
- plus "+" (0x2B (ASCII), U+002B (UTF-8)); and
- up-to-3 character ISO 3166-2 identifier for the subdivision; and
- a hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and
- Registration Reference allocated in accordance with the identified Registration Scheme.

Registration References MAY contain hyphens but Registration Schemes, ISO 3166-1 country codes, and ISO 3166-2 identifiers SHALL NOT contain hyphens. Therefore, if more than one hyphen appears in the structure, the leftmost hyphen is a separator, and the remaining hyphens are part of the Registration Reference.

Illustrative examples of Registration References are as follows:

- NTRMY-478231-X (representing the **NTR scheme** for Malaysia, where the unique identifier at the **national level** is 478231-X).
- NTRMY+13-1128178-A (representing the **NTR scheme** for Malaysia, with **13** denoting the **state of Sarawak**, and the unique identifier at **the state level** is 1128178-A)
- VATMY+IRB-C2584563202 (representing the **VAT scheme** for Malaysia, where **IRB** refers to the **Inland Revenue Board**, and the **Tax Identification Number (TIN)** is C2584563202)

Registration Schemes listed in Appendix A are recognized as valid under these Requirements. The CA SHALL:

1. Confirm that the organization represented by the Registration Reference is the same as the organization named in the `organizationName` field as specified in Section 7.1.4.2.2; and
2. Further verify the Registration Reference matches other information verified in accordance with Section 3.2.3.

Note 1: With the exception of the LEI in INT Registration Schemes, if a `subject:countryName` is present in the Certificate, the country code used in the Registration Scheme identifier SHALL match that of the `subject:countryName` in the Certificate. For the LEI Registration Scheme, the ISO 3166-1 code "XG" SHALL be used.

In Malaysia, the national trade register (NTR) shall refer to Suruhanjaya Syarikat Malaysia (SSM) under Registration of Businesses Act 1956 [Act 197], Companies Act 2016 [Act 777] and Limited Liability Partnerships Act 2012 [Act 743].

In Sabah, the trade register is the administrative officer or his assistant in charge of the district in which the premises are situated, or the person usually resides as mentioned in Section 4(1) of Trades Licensing Ordinance 1948 (Sabah Cap. 144).

In Sarawak, the state trade register is the District Officers in districts other than Kuching as mentioned in Section 3 of Business Names Ordinance 1958 (Chapter 64) and Section 5 of Businesses, Professions and Trades Licensing Ordinance 1958 (Sarawak Chapter 33). The name can be verified via Electronic Resident & District Office (https://erndo2.sarawak.gov.my/).

For VAT registration scheme in Malaysia, there are two (2) recognized tax authorities in Malaysia, using the following 3 characters:

- IRB - Inland Revenue Board (Lembaga Hasil Dalam Negeri) collects income tax, real property gain taxes, stamp duties, petroleum income tax.
- RMC - Royal Malaysia Customs Department (Jabatan Kastam Di Raja Malaysia) collects import duties, export duties, excise duties, sales tax, service tax, and tourism tax.

For OTH registration scheme in Malaysia, the following are recognized other authorities in Malaysia:

- CIDB - Construction Industry Development Board is a government agency under the Ministry of Works, established by the Malaysia Construction Industry Development Act (Act 520). Among its key responsibilities is the registration and accreditation of contractors and personnel within the construction sector
- BAM - Board of Architects Malaysia is a statutory authority under the Ministry of Works, responsible for the enforcement of the Malaysia Architects Act 1967. Among its key responsibilities is the registration of Architects, Graduate Architects, Interior Designers, Graduate Interior Designers, Building Draughtsmen, Inspector of Works and Architectural Technologists; and registration of Architectural Consultancy Practices and Interior Design Consultancy Practices

A.2: Natural Person Identifier

The following Registration Schemes are recognized as valid for use in the subject:serialNumber attribute described in Section 7.1.4.2.2.

Registration Scheme Identifier	Description
PAS	For an identifier based on a passport number issued to the Subject Individual.
IDC	For an identifier based on a national identity card issued to the Subject Individual.
TAX	For an identifier based on a personal tax reference number issued by a national tax authority.
MMC	For an identifier issued by Malaysian Medical Council (MMC).
RPH	For an identifier issued by Pharmacy Board of Malaysia (PBM)
BAM	For an identifier issued by Board of Architects Malaysia.
BEM	For an identifier issued by Board of Engineers Malaysia.
MBOT	For an identifier issued by Malaysia Board of Technologist.
RISM	For an identifier issued by Royal Institute of Surveyor Malaysia.
ILAM	For an identifier issued by Institute of Landscape Architects Malaysia.
MIP	For an identifier issued by Malaysian Institute of Planners.
MIA	For an identifier issued by Malaysian Institute of Accountants.

An illustrative example of a Subject Distinguished Name (DN) for Individual Pro Certificates might be as follows:

Use case	Example of Subject DN
Ali Ahmad is a Director of Trust Services at MSC Trustgate.com Sdn. Bhd.	CN=Ali Ahmad, T=Director, Trust Services, O=MSC Trustgate.com Sdn. Bhd., organizationIdentifier=NTRMY-478231-X, C=MY
Dr Mazlina Alias is a Pegawai Perubatan UD48 at Hospital Putrajaya (Government Hospital)	CN=Dr Mazlina Alias, serialnumber=MMC-12345, T=Pegawai Perubatan UD48, O=Hospital Putrajaya, organizationIdentifier=GOVMY, C=MY
Dr Faiz Othman is a General Paediatrics at Kajang Specialist Hospital Sdn Bhd (Private Hospital)	CN=Dr Faiz Othman, serialnumber=MMC-13579, T=General Paediatrics, O=Kajang Specialist Hospital Sdn Bhd, organizationIdentifier=NTRMY-211797-T, L=Kajang, ST=Selangor, C=MY
Hafiz Ahmad is a registered Engineer working as Mechatronics Engineer at Robotic Manufacturing Sdn Bhd	CN=Hafiz Ahmad, serialnumber=BEM-G24680A, T=Mechatronics Engineer, O=Robotic Manufacturing Sdn Bhd, organizationIdentifier=NTRMY-431697-M, C=MY
David Law is a registered architect working as Architect at ABC Professional Service Sdn Bhd which also a registered Architecture with Board of Architect	CN=David Law, serialnumber=BAM-384/2024, T=Architect, O=ABC Professional Service Sdn Bhd, organizationIdentifier=OTHMY+BAM-MDP/IC, C=MY
Fahmy Ahmad is a construction worker working at ABC Enterprise. He and his company registered with CIDB	CN=Fahmy Ahmad, serialNumber=880808181357, T=Construction Personnel, O=ABC Enterprise, organizationIdentifier=OTHMY+CIDB-20214342-432455, C=MY

APPENDIX B. RECLASSIFICATION OF CERTIFICATE CLASSES

In the effort to improve the overall validation process, MSC Trustgate has reclassified certain certificate classes. The most significant change involves the Class 3 certificates.

Certificates issued under Object Identifier (OID) 1.3.6.1.4.1.49530.1.1.4 are now categorized as Class 3 (High Assurance). These certificates are subject to an enhanced validation process, which includes mandatory identity verification through a Public Notary, as detailed in Section 3.2 of this CP/CPS.

Certificates issued under OID 1.3.6.1.4.1.49530.1.1.3 are classified as Medium Assurance. These certificates will gradually transition to a new OID and will follow the procedures outlined in Section 3.2 of this CP/CPS.