TRUSTGATE
SECURE TRANSACTION. TRUSTED BUSINESS

MSC Trustgate
Certificate Policy / Certification Practice Statement

Version 6.2

8 October 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 4.6 to enhance the clarity for renewed certificate validity. • 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

#	Date	Changes	Version
14	7 October 2025	**I. Structural & Organizational Changes (Governance, Layout, and Repositories)** • **Document Scope & Compliance** (Sec. 1.1, 1.2): **Restructured the overview** (Sec. 1.1) to confirm MSC Trustgate's status as a Recognized Repository and Date/Time Stamp Service, and explicitly state compliance with national and international standards. Document identity and OID (Sec. 1.2) were refined. • **Governance Update** (Sec. 1.5): Replaced the Policy Management Authority (PMA) with the Information Security Committee (ISC) as the governing body responsible for CP/CPS administration. • **Repository Alignment** (Sec. 2): Reworked the entire section to align with the RFC 3647 structure, clarifying repository definitions, publication methods, frequency, and access controls. • **Information Consolidation**: Consolidated certificate information for clarity and auditability: ▪ **Certificate Profiles** (Sec. 7.1.2, 7.1.4): Simplified Section 7.1.2 (Extensions) and Section 7.1.4 (Name Forms) to define only general policies. ▪ **CA and OID Data** (Sec. 7.1.6): Moved and consolidated the definitive list of all Certificate Policy OIDs into the new Section 7.1.6. • **Trusted Roles** (Sec. 5.2.1): Updated responsibilities for Trusted Roles. • **Right to Audit** (**Sec. 9.17.2**): Removed the dedicated Right to Audit section to align with the default requirements of major root store programs. **II. Cryptographic & Product Updates** • **Post-Quantum Cryptography** (PQC) Support: Introduced support for the **Malaysian KAZ-Sign PQC Algorithm** and refined key generation/quality procedures for the SLH-DSA algorithm (Sec. 6.1.5.2, 6.1.6, 7.1.3). • **Product Terminology**: Updated certificate profiles and terminology for improved clarity: ▪ **TLS Server Certificates**: Redefined server-purpose certificates as TLS Server Certificates. ▪ **Device Certificates**: Grouped client-purpose device certificates under a Device Certificate category, including a specific sub-profile for mutual SSL (mTLS) client certificates (Sec. 6.1.7, 6.3.2, 7.1). • **New Service OID**: Introduced support for the Sarawakpass service, with new OID and certificate usage defined (Sec. 1.4.1, 7.1.6). **III. Policy & Semantics Updates** • **Policy Qualifier** (Sec. 7.1.8): Clarified the syntax and semantics of the userNotice policy qualifier. This change ensures clear distinction between certificates issued under the Malaysia Digital Signature Act 1997 and all other certificates.	6.2

Contents

1 INTRODUCTION

1.1 Overview

This Certificate Policy and Certification Practice Statement (CP/CPS) describes the set of rules, policies, and procedures governing the issuance and management of digital certificates and related services within the MSC Trustgate.com Sdn. Bhd. Public Key Infrastructure (MSC Trustgate PKI). This document serves as the regulatory framework for all services provided by MSC Trustgate, and all Registration Authorities (RAs), Subscribers, Relying Parties, and other PKI participants must be aware of and comply with its statements.

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 PKI. To preserve the outline specified by RFC 3647, section headings that do not apply have the statement "No stipulation".

MSC Trustgate, as a **Licensed Certification Authority**, a **Recognized Repository**, and a **Recognized Date/Time Stamp Service** in Malaysia, operates in compliance with the following:

- Malaysia Digital Signature Act 1997
- Malaysia Digital Signature Regulations 1998
- Recognition Framework for Time Stamping Authority (TSA)
- Requirements for Certification Authority (CA) to be Recognised as a Time Stamping Authority (TSA)
- WebTrust Principles and Criteria for Certification Authorities

In addition, as a member of the Adobe Approved Trust List (AATL) and other major browser Root Programs, MSC Trustgate complies with the respective policies of each program. In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document. MSC Trustgate is committed to continuously monitoring and updating this CP/CPS to ensure continued compliance.

1.2 Document Name and Identification

This document is entitled the "Certificate Policy and Certification Practice Statement of MSC Trustgate.com Sdn. Bhd. Public Key Infrastructure" and serves as the primary governance document for all certification services provided by MSC Trustgate. It will be referred to in abbreviation as the "MSC Trustgate CP/CPS".

The purpose of this document is to define and make known to all interested parties, including Registration Authorities (RAs), Subscribers, Relying Parties, and Auditors, the policies, practices, and security controls governing the issuance and management of digital certificates and related services provided by MSC Trustgate.

The structure of this document is based on the outline set forth in IETF RFC 3647, as amended by the CA/Browser Forum (CA/B Forum) Baseline Requirements and other relevant standards. MSC Trustgate complies with the current version of the following CA/B Forum documents, where applicable:

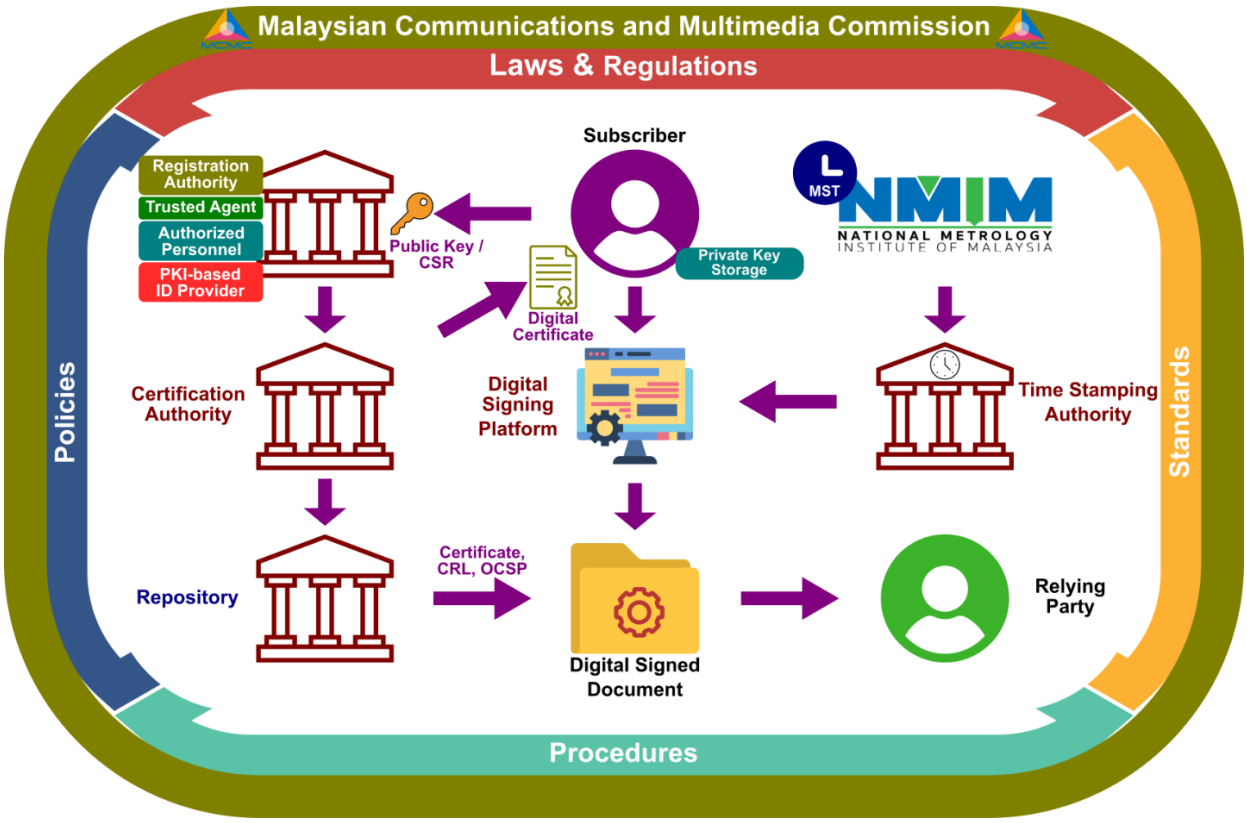
- Network and Certificate System Security Requirements
- Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates
- Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates
- Guidelines for the Issuance and Management of Extended Validation Certificates
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
- Guidelines For The Issuance And Management of Extended Validation Code Signing Certificates

The Object Identifier (OID) for this document is 1.3.6.1.4.1.49530.4.1.6.2. The OID breakdown is as follows:

- **1.3.6.1.4.1.49530**: MSC Trustgate proprietary OID root, registered with IANA.
- **4**: Documents
- **1**: Certification Practice Statement
- **6.2**: Version number of the Certification Practice Statement

1.3 PKI Participants

The diagram below illustrates the key participants in the MSC Trustgate PKI, 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 Personally 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 Authority (CA)** that issues digital certificates using its own CA system. MSC Trustgate performs all functions associated with Public Key operations, including receiving certificate requests; issuing, revoking, and renewing digital Certificates; 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 (RA)** is an entity that performs identification and authentication of certificate applicants, initiates or forwards revocation requests, and approves applications for renewal or re-keying 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 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 this 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 TLS 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 PKI operation include all end users (including entities) of certificates issued by MSC Trustgate. The Subscriber is the entity that contracts with MSC Trustgate for the issuance of credentials, while the **Subject** is the individual to whom the credential is bound. The Subscriber bears ultimate responsibility for the credential's usage, but the Subject is the individual authenticated when the credential is presented.

When "Subject" is used, it indicates a distinction from the Subscriber. When "Subscriber" is used, it may mean the Subscriber as a distinct entity but may also embrace both roles. The context of its use in this CP/CPS will provide 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 PKI operation.

1.3.5 Other Participants

1.3.5.1 Trusted Agent

A **Trusted Agent (TA)** is a government agency, financial sector participant[1], or any organization with the authority to conduct identity verification and validation processes and possesses a reliable data source, as mandated by the relevant Minister under applicable legal provisions. Applicants may request a digital certificate from the TA, who subsequently submits the validated **Personally Identifiable Information (PII)** to MSC Trustgate for certificate issuance based on the validated data. MSC Trustgate may obtain or validate additional PII data from another data source to construct a digital certificate.

The TA must enter into a contractual agreement with MSC Trustgate (**TA agreement**) before operating as a TA. The TA is required to pass the following data to MSC Trustgate for the certificate issuance process and to ensure compliance with the **Digital Signature Act 1997** and **Digital Signature Regulations 1998** (**DSA 1997** and **DSR 1998**):

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

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

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

iii. **Date and Time of Authentication**: The date and time the applicant's identity is authenticated during the certificate application process.

iv. **Verifier**: The individual, entity, or device responsible for conducting the verification process.

1.3.5.2 Authorized Personnel

Authorized Personnel (AP) are individuals granted authority by MSC Trustgate to receive certificate requests and verify the identity of 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 with MSC Trustgate (**AP agreement**) before operating as an AP. The AP is required to pass the following data to MSC Trustgate for further validation and certificate issuance, ensuring compliance with **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 of a verification process, confirming the 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 verification**: The date and time the applicant's identity is verified during the certificate application process.

iv. **Verifier**: Refers to 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 applicant's identity, which may include but is not limited to:

   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] guidelines

vi. **Evidence**: Refers to the supporting documents used to confirm the identity. The AP may also provide additional documents like a Letter of Authorization (LoA) or a membership document to associate the applicant with an organization if required for the digital certificate.

1.3.5.3 PKI-based Identity Provider

A **PKI-based Identity Provider (IDP)** is a trustworthy entity or system that manages digital identities using PKI for authentication purposes. **MyDigital ID**[3] is an example of a PKI-based IDP utilized by MSC Trustgate within its PKI ecosystem.

[2] https://www.bnm.gov.my/documents/20124/938039/pd_ekyc-apr2024.pdf
[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. It allows an entity to prove its identity to other participants in an electronic 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 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 to use a Certificate issued under this CP/CPS.

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

1. **Digital Identity Certificates**: These certificates serve as a trusted digital identity for a specific user, enabling secure authentication and the creation of legally binding digital signatures (in some cases). They provide authentication, message integrity, and non-repudiation.
    a. **MyGPKI Certificates**: Issued to Malaysian federal government officers for use in government online services.
    b. **MyDigital ID Certificates**: Used to verify the identity of users accessing various national digital services.
    c. **Sarawakpass Certificates**: Serve as a digital identity for Sarawak citizens to access various public and private sector services.
2. **Digital Signing Certificates**: These certificates are used by individuals or organizations to authenticate and digitally sign electronic documents and transactions. Their primary purpose is to provide authentication, message integrity, and non-repudiation through digital signatures. MSC Trustgate issues these certificates in accordance with the Digital Signature Act 1997 (DSA 1997) and the Digital Signature Regulations 1998 (DSR 1998), classified as Class 2 (medium) or Class 3 (high) Level of Assurance.
3. **TLS Server Certificates**: These certificates provide a secure connection between a user and a website by encrypting data transmitted between them. They also verify the ownership and identity of the website via the domain name. The level of verification varies based on the type:
    a. **Domain Validation (DV)**: Authentication of a domain.
    b. **Organization Validation (OV)**: Authenticates a domain and verifies the organization's legal status.
    c. **Extended Validation (EV)**: Authenticates a domain and a legal entity, including its operational existence and physical address.
4. **S/MIME Certificates**: These are used to secure email communications by providing digital signing and encryption, ensuring confidentiality, integrity, and authenticity.
5. **Code Signing Certificates**: These are used by software developers and publishers to digitally sign executables, scripts, and other content. This authenticates the software's origin and ensures its integrity has not been compromised since it was signed.
6. **Time-Stamping Certificates**: These are used to create a cryptographically verifiable timestamp on digital data. They provide proof of existence, integrity, and non-repudiation at a specific point in time.
7. **Device Certificates**: Also known as Device Authentication Certificates, these are used to identify and secure communication for specific hardware devices, such as HSM, network routers, IoT devices, or other online resources. **TLS Client Certificates** and **IoT Device Certificates** are specific types of Device Certificates.

8. **OCSP Responder Certificates**: A digital certificate used by an Online Certificate Status Protocol (OCSP) service to digitally sign real-time responses regarding the revocation status of other certificates.

1.4.2 Prohibited Certificate Uses

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

Certificates shall be used only to the extent that 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 rekeys 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 Information Security Committee (ISC) is responsible for the administration and oversight of this CP/CPS and all related agreements, security policies, and procedural documents. The ISC is chaired by the CEO and includes key personnel such as Executive Directors and Heads of various Divisions and Departments.

The ISC's contact information is as follows:

Information Security Committee (ISC)
MSC Trustgate.com Sdn. Bhd.
Suite 2-9, Level 2, CBD Perdana
Jalan Perdana, 63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia.
Tel: +603 8318 1800
Fax: +603 8319 1800

1.5.2 Contact person

General inquiries and correspondence concerning this CP/CPS, its policies, procedures, governance, and compliance should be directed to the CA Operation and Compliance Manager. This individual can be contacted via email at "compliance at msctrustgate dot com".

For specific issues, please use the following contact points:

- **Certificate and usage problems**: mpki-support at msctrustgate dot com
- **Revocation requests**: revoke at msctrustgate dot com
- **General inquiries and customer service**: helpdesk at msctrustgate dot com

1.5.3 Person determining CP/CPS suitability for the policy

The MSC Trustgate Information Security Committee (ISC), as the body identified in Section 1.5.1, is responsible for determining the suitability of this CP/CPS and any related documents. The ISC ensures these documents remain consistent with the established Certificate Policy.

1.5.4 CP/CPS approval procedures

This CP/CPS and all subsequent amendments are approved by the Information Security Committee (ISC). The ISC conducts a thorough review of all proposed amendments to ensure their consistency with the existing CP/CPS. The ISC may either publish an addendum or issue a fully updated version of the CP/CPS, which supersedes any conflicting provisions of the previous version. The ISC also determines whether an amendment requires a change to the Object Identifier (OID) or specific public notice. Further details on amendment procedures are outlined in Sections 9.10 and 9.12.

All approved versions and updates of this document are made publicly available at the MSC Trustgate Repository located at: https://www.msctrustgate.com/repository.

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 (Cryptographically Secure PRNG)**" A special type of PRNG (Pseudo-Random Number Generator) takes a truly random seed (from a TRNG source) and then uses a cryptographic algorithm (like a secure hash or a block cipher) to produce a long, unpredictable sequence. This extra security features make its output unpredictable and suitable for use in cryptography.

"**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.

"**Information Security Committee**" 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 ISC evaluates non-domain policies for acceptance within the domain and oversees the overall management of PKI certificate policies. For MSC Trustgate, the ISC comprises Senior Management, Compliance personnel, CA Operations Manager, and Key Manager.

"**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.

"**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 an 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.

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
ISC	Information Security Committee
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
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 operates and maintains a public repository that serves as the official source for all public-facing PKI documentation and data. This repository is located at the following URI: https://www.msctrustgate.com/repository.

The following information is made publicly available in this repository:

- This Certificate Policy and Certification Practice Statement (CP/CPS)
- Time-Stamp Policy and Practice Statement (TSPPS)
- Audit Reports
- CA Certificates (Root, Bridge and Subordinate) and Revocation Lists (CRL)
- Agreements (Subscriber, Relying Party, Term of Access, Software License, etc)
- Privacy and Other Policies

All information within the repository is made available on a 24x7 basis. The repository is supported by systems described in Section 5 to minimize downtime and ensure high availability. For TLS Server Certificates intended to be trusted in browsers, they are also published by posting to a Certificate Transparency (CT) log.

2.2 Publication of Information

MSC Trustgate publicly discloses all information required by its selected audit schemes (see Section 8.4) and the regulatory framework it operates under. The primary method of publication is through the public repository. Additionally, MSC Trustgate communicates certification information through the following channels:

i. Web: https://www.msctrustgate.com
ii. Email: mpki-support at msctrustgate dot com
iii. Mailing Address: MSC Trustgate.com Sdn Bhd, Suite 2-9, Block 4801, CBD Perdana, 63000 Cyberjaya, Selangor, Malaysia
iv. Telephone: +603-8318 1800
v. Fax: +603-8319 1800

This CP/CPS is part of a suite of governance documents that includes registration authority agreements, subscriber agreements, relying party agreements, and privacy policies. These documents are made available to applicable users and Relying Parties.

Application Software Suppliers for TLS Server 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 publishes new and updated versions of its CRLs and OCSP responses in accordance with the schedules defined in Sections 4.9.7 and 4.9.9, respectively.

Updates to this CP/CPS are published upon approval by the Information Security Committee (ISC). A new version of the document, with an updated revision history and effective date, is published to the repository to reflect any changes.

2.4 Access Controls on Repositories

Read-only access to the public repository is unrestricted. Any attempt to modify, add, or delete information from the repository by unauthorized parties is strictly prohibited. Logical and physical access controls are implemented to prevent and detect unauthorized access to the systems and data that comprise the repository.

3 IDENTIFICATION AND AUTHENTICATION

MSC Trustgate maintains documented practices and procedures to authenticate the identity and other attributes of an Applicant prior to the inclusion of those attributes in a Certificate. MSC Trustgate also verifies all requests from parties seeking to revoke certificates.

3.1 Naming

3.1.1 Types of Names

- **For Certificates issued to an Individual**, the `subject:commonName` is a Personal Name. For S/MIME Certificates, the `subject:commonName` can be an Email Address.
- **For Certificates issued to an organization or legal entity**, the `subject:organizationName` is the organization's legal name registered with government agencies or an authority. The `subject:commonName` can be the organization's trademark or a name commonly associated with the organization.
- **For Certificates issued to a device**, the `subject:commonName` contains a MAC Address or device name.
- **For Certificates issued to a server**, the `subject:commonName` contains only one of the following: a Fully-Qualified Domain Name, a Wildcard Domain Name, or an IPv4/IPv6 address.

3.1.2 Need for Names to be Meaningful

MSC Trustgate uses 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 will be evaluated on its merits by the Information Security Committee (ISC). If allowed, the `subject:pseudonym` attribute is used if the associated Subject has been verified according to Section 3.2.3. The `subject:pseudonym` attribute is either:

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

ii. an identifier verified from one of the following:

   a. a government-issued identity document; 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 treats 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 uses the subject Distinguished Name (DN) for uniqueness, which contains specific identification attributes of the Certificate's holder.

- **For Individual Certificates**, the `subject:serialNumber` is a government-issued identity number, such as a National Registration Identity Card (NRIC) number or a passport number and is accompanied by the `subject:countryName` of the issuing country.
- **For Individual Certificates representing a regulated profession**, the `subject:serialNumber` is the membership number of the professional organization. This is accompanied by the

`subject:organizationName` of the professional organization and the `subject:countryName` of the country that regulates it.

- **For Individual Certificates representing a corporate affiliation**, the `subject:serialNumber` is optional and may specify the employee number. The `subject:Title` is optional and may specify the position held by the individual. The `subject:organizationName` is the legal name of the organization, and the `subject:countryName` is the country where the organization is registered.
- **For Organization or Legal Entity Certificates (except for LHDN e-Invoice organization certificates)** issued after April 18, 2024, the `subject:organizationIdentifier` attribute is used. It contains the Registration Reference for a Legal Entity assigned in accordance with a verified Registration Scheme (listed in Appendix A), as per Section 3.2.2. The Registration Scheme is identified using the following structure:
    i. A character Registration Scheme identifier;
    ii. A 2-character **ISO 3166** country code for the nation in which the Registration Scheme is operated, or if the scheme is global, the ISO 3166 code "XG" **SHALL** be used;
    iii. For the **NTR** Registration Scheme, where registrations are administered at the subdivision level (state or province), a plus "+" 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 "-";
    v. The 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 entities that do not have a standard identifier**:
    i. **For Government Entities**, MSC Trustgate enters the Registration Scheme identifier `GOV` followed by the 2-character ISO 3166 country code for the nation where the entity is located. If the entity is verified at a subdivision level, a plus "+" followed by an ISO 3166-2 identifier is added.
    ii. **For International Organization Entities**, MSC Trustgate enters the Registration Scheme identifier `INT` followed by the ISO 3166 code "XG." An International Organization Entity is founded by a constituent document signed by, or on behalf of, a minimum of two Sovereign State governments.
- **For Server Certificates**, the `subject:serialNumber` attribute is used in accordance with the **EV Guidelines**. MSC Trustgate EV TLS Server Certificates comply with **EV Guidelines Section 11**.

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. However, MSC Trustgate 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 a Certificate. For Server and S/MIME Certificates, 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 Applicant must demonstrate rightful possession of 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 the **PKCS #10 format**, another cryptographically equivalent demonstration, or an MSC Trustgate-approved method. This requirement does not apply where a key pair is generated by MSC Trustgate on the Applicant's behalf.

3.2.2 Authentication of Organization Identity

For a Certificate to include the `subject:organizationName` attribute, MSC Trustgate SHALL 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 Incorporation or Registration of the Legal Entity;

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

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

For LHDN e-Invoice organization certificates, the `subject:organizationIdentifier` is the LHDN Tax Identification Number (TIN)[4].

3.2.2.1 Attribute Collection of Organization Identity

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

i. A **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 **SHALL** also verify the Applicant's identity and affiliation with 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` and **SHALL NOT** use an LEI data reference if the `ValidationSources` entry is `PARTIALLY_CORROBORATED`, `PENDING`, or `ENTITY_SUPPLIED_ONLY`.

[4] 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 **SHALL** 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 MSC Trustgate SHALL verify the country associated with the Subject using one of the following:

i. The IP Address range assignment by country for either (i) the website's IP address, as indicated by the DNS record for the website, 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 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 a Certificate issued to an Individual, MSC Trustgate **SHALL** authenticate the following Individual identity attributes if included in Certificate profiles:

i. Personal name, or given name(s) and surname(s), which is the 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 **SHALL** 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 Attributes are Collected

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

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

ii. A digital certificate from a **PKI-based Identity Provider (IDP)**. The Applicant must 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 the Applicant's Certificate Request form attested by a commissioner for oath, notary, other appointed government public officer, or recognized professional bodies.

iv. **Records maintained by an Enterprise RA**.

v. **Data passed by a Trusted Agent (TA)**.

vi. **Data passed by Authorized Personnel (AP)**.

MSC Trustgate also collects company attestation for an Individual to represent an Organization for inclusion 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 3.2.2.

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

- **Changes of Name**: If the Subject presents an ID with a name that has been changed, MSC Trustgate inspects an official document such as a marriage certificate or court order documenting the change.
- **Professional/Corporate Title**: If a professional title or a corporate title is requested, MSC Trustgate verifies it against supporting documentation, a Reliable Data Source, or an Attestation.
- **Address Verification**: MSC Trustgate verifies 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 **SHALL** validate all identity attributes of the Individual to be included in the Certificate. If the evidence has an explicit validity period, MSC Trustgate **SHALL** verify that the time of the identity validation is within this validity period. The `notBefore` and `notAfter` fields of a digital signature Certificate **SHALL** be within the validity period of the document. The following are the processes for MSC Trustgate to perform individual identity validation.

i. **Validation of Government-Issued Photo ID**: MSC Trustgate **SHALL** ensure that the identity document is genuine and not counterfeit, falsified, or modified. MSC Trustgate uses manual (in-person) or online document verification. If online 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 **SHALL** 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 on existing internal records to validate an Individual's identity.

v. **Validation using Trusted Agent (TA):** MSC Trustgate trusts 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 the Notaries Public Act 1959[5].

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 Adobe Approved Trust List (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,

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

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 documents to 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 **SHALL** 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 maintains 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 in Section 4.2.1) prior to Certificate issuance.

3.2.4.1 Validating Authority Over Mailbox via Domain

MSC Trustgate **SHALL** confirm that 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 **SHALL** 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 that includes the Random Value.

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 and 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. 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 using 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 a domain. MSC Trustgate **SHALL NOT** issue Certificates for any **FQDN** containing "onion" as the rightmost label.

MSC Trustgate maintains a record of the domain validation method, including the relevant **BR** version number, used for 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 **SHALL** confirm that, prior to issuance, each FQDN listed in the Certificate has been validated using one of the following methods.

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 been used**. Prior validations using this method and validation data gathered according to this method is NOT be used 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

No Stipulation.

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

No Stipulation.

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 TLS Server 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 a re-key of a Certificate before its expiration. After receiving a re-key request, 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 **SHALL NOT** re-key a Certificate without additional authentication if doing so would allow the Subscriber to use the Certificate beyond the limits described in this CP/CPS. MSC Trustgate **SHALL** require a letter of authorization from the organization if the Certificate includes an 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, the Subscriber **SHALL** undergo the initial registration process (described in Section 3.2) prior to re-keying the Certificate.

3.4 Identification and Authentication for Revocation Requests

Before the revocation process of a Certificate, MSC Trustgate **SHALL** verify that the revocation is requested by the Certificate's Subscriber or the entity that approved the Certificate Application. The procedures for authenticating a revocation request **SHALL** include at least one of the following methods:

i. Having the Subscriber submit the Subscriber's **Challenge Phrase** (or its equivalent) and revoking the Certificate automatically if it matches the 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 that provides reasonable assurance, 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.

3.4.1 Revocation Requests by Administrators and RAs

MSC Trustgate Administrators are entitled to request the revocation of end-user Subscriber Certificates within the MSC Trustgate PKI platform. The identity of an Administrator is authenticated via access control using SSL and client authentication before they are permitted to perform revocation functions.

Registration Authorities (**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.

3.4.2 Revocation Requests for CA Certificates

Requests to revoke a CA Certificate SHALL be authenticated by 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

A Certificate Application may be submitted by any of the following:

- An individual who is the subject of the Certificate.
- An authorized representative of an Organization or entity.
- An authorized representative of a **Registration Authority (RA)**, **Trusted Agent (TA)**, or **Authorized Personnel (AP)**.

An individual or entity listed on a government denied list, list of prohibited persons, or other list that legally prohibits business with such parties under the laws of Malaysia, **SHALL NOT** submit an application for a Certificate.

4.1.2 Enrolment Process and Responsibilities

4.1.2.1 End-User Certificate Subscribers

Before issuing a Certificate, MSC Trustgate **SHALL** obtain a Certificate request along with an executed **Subscriber Agreement** and **Terms of Use**, which may be electronic and must be in line with the **CA/B Forum requirements**. The enrolment process **SHALL** consist of, but is not limited to, the following steps (which may occur in any order):

- Completing a Certificate Application and providing true and correct information.
- Generating, or arranging for the generation of, a key pair.
- Generating a **Certificate Signing Request (CSR)** using an appropriately secure tool.
- Delivering their public key directly to MSC Trustgate or through an RA/TA/AP.
- Demonstrating possession and/or exclusive control of the private key corresponding to the public key.
- Agreeing to the applicable Subscriber Agreement or Term of Use.
- Paying any applicable fees.

4.1.2.2 RA/TA/AP Certificates

Applicants for **RA**, **TA**, or **AP** Certificates **SHALL** enter into a contract with MSC Trustgate. These Applicants **SHALL** provide their credentials to demonstrate their identity and provide contact information during the contracting process.

During this contracting process, or at the latest, prior to the **Key Generation Ceremony** for the creation of their key pair, the Applicant **SHALL** cooperate with MSC Trustgate to determine the appropriate **Distinguished Name** and the content of the Certificate to be issued.

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 Applicant 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 **MUST** communicate the completion of such tasks to MSC Trustgate for Certificate issuance.

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

MSC Trustgate determines a source's reliability by considering its availability, purpose, and reputation. MSC Trustgate **SHALL NOT** consider a database, source, or form of identification to be 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**:
  - Certificates issued before March 15, 2026: **825 days**
  - Certificates issued on or after March 15, 2026: **398 days**
- **For Validation of Domain Names and IP Addresses of TLS**:
  - Certificates issued before March 15, 2026: **398 days**
  - Certificates issued on or after March 15, 2026, and before March 15, 2027: **200 days**
  - Certificates issued on or after March 15, 2027, and before March 15, 2029: **100 days**
  - Certificates issued on or after March 15, 2029: **10 days**
- **For Validation of Mailbox Authorization or Control of S/MIME**:
  - Completed validation of the control of a mail server in accordance with Section 3.2.4.1 or 3.2.4.3: **398 days**
  - 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**:
  - Formal name of the Legal Entity: **825 days**
  - A registered Assumed Name for the Legal Entity (if included in the Subject): **825 days**
  - An address of the Legal Entity (if included in the Subject): **825 days**
  - Jurisdiction of Incorporation or Registration of the Legal Entity: **825 days**
  - Organization Identifier and type of identifier for the Legal Entity: **825 days**
  - Validation of authority: **825 days** (unless a contract between the CA and the Applicant specifies a different term).
- **For Individual Validation of S/MIME and Document Signing**:
  - Given name(s) and surname(s): **825 days**
  - Pseudonym (if used): **825 days**
  - Title (if used): **825 days**
  - Address (if displayed in Subject): **825 days**
  - Further information as needed to uniquely identify the Applicant: **825 days**
- **For TLS EV Certificates**:
  - The age of all data used to support issuance of an EV Certificate (before revalidation is required) **SHALL NOT exceed 398 days**. This does not apply to reissuance of an EV Certificate under Section 11.14.2 of the EV Guidelines or when permitted otherwise in Section 11.14.1.

- **For Code Signing Certificates**:
  - All validation data **SHALL NOT be older than 398 days**. This includes legal existence and identity, assumed name, address of business, verified method of communication, operational existence, and the name, title, agency, and authority of the individual. The contract between MSC Trustgate and the Applicant MAY specify a different term.

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 such requests are properly verified under these Requirements.

4.2.1.1 CAA Checking

MSC Trustgate **SHALL** check for a **CAA record** in the DNS for each DNSName in the subjectAltName extension, excluding **Onion Domain Names**, as per **RFC 8659**, before 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 **SHALL** 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 but **MAY NOT** dispatch reports of issuance requests to the contact(s) listed in an iodef property tag.

If a 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 **SHALL** log 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;
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 **SHALL** approve an application if the following criteria are met:

i. Successful completion of the identification and authentication of all required Subscriber information as set forth in Section 3.2.
ii. Receipt of payment.

MSC Trustgate or an RA **SHALL** reject a Certificate application if:

i. The identification and authentication of all required Subscriber information as set forth in Section 3.2 cannot be completed;
ii. The Subscriber fails to furnish supporting documentation upon request;
iii. The application has been previously rejected, or a violation of the Subscriber Agreement is detected;
iv. Payment has not been received; or
v. The RA believes that issuing a Certificate to the Subscriber could damage or diminish MSC Trustgate's 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 it.

MSC Trustgate **SHALL NOT** issue Certificates containing internal names.

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 timeframe. Issuance timeframes are greatly dependent on when the Applicant provides the necessary details and documentation 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 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 for Root and Subordinate CAs

MSC Trustgate **SHALL** confirm the source of a Certificate request before issuance. Databases and CA processes occurring during Certificate issuance **SHALL** be protected from unauthorized modification. After issuance is complete, the Certificate **SHALL** be stored in a database and sent to the Subscriber.

MSC Trustgate **SHALL NOT** issue end-entity Certificates directly from its Root Certificates. CA Certificate issuance by the Root CA **SHALL** require an individual authorized by MSC Trustgate (e.g., the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command to perform a Certificate signing operation.

4.3.1.2 Linting of To-Be-Signed Certificate Content

MSC Trustgate **SHOULD** implement a Linting process 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**, MSC Trustgate **SHALL** have implemented a Linting process testing compliance with these Requirements for all certificates.

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

i. Signing 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. Specifying 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 tools that have been widely adopted by the industry (see https://cabforum.org/resources/tools/).

MSC Trustgate **MAY** contribute to open-source Linting projects 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 Certificate Issuance

MSC Trustgate **SHALL**, either directly or through an RA, notify Subscribers within a reasonable time that their Certificate has been created and provide them with access to the Certificate. 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 their computer or Hardware Security Module (HSM). A Certificate is considered accepted **thirty (30) days after its issuance**, or earlier upon use of the Certificate, if evidence exists that the Subscriber used it.

A Subscriber's failure to object to the Certificate or its content constitutes Certificate acceptance.

4.4.2 Publication of the Certificate by the CA

MSC Trustgate **SHALL** publish all CA Certificates and the Certificates in its publicly accessible repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Registration Authorities (**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 has agreed to the Subscriber Agreement and accepted the Certificate. The Certificate SHALL be used lawfully and in accordance with MSC Trustgate's Subscriber Agreement and 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 the expiration or revocation of the associated Certificate.
- Use Certificates in accordance with their intended purpose.

Parties other than the Subscriber **SHALL NOT** archive the Subscriber's 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 the risk of loss before relying on it. If 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 all of the following conditions are met:

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 its revocation status prior to use by referring to the relevant **CRLs** or **OCSP responses**.

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 a new serial number and new validity period, but without changing the Public Key or any other information in the Certificate.

4.6.1 Circumstances for Certificate Renewal

MSC Trustgate **MAY** renew a Certificate if all the following conditions are met:

i. The associated Public Key has not reached the end of its validity period.
ii. The Subscriber and their attributes are consistent with the original Certificate.
iii. The associated Private Key remains uncompromised.
iv. Re-verification of the Subscriber's 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 notify Subscribers prior to a Certificate's expiration date.

A Certificate renewal requires the payment of additional fees. MSC Trustgate **MAY** renew a Certificate after expiration if the relevant industry standards permit such practices. Prior to the expiration of an existing Subscriber's Certificate, it is the Subscriber's responsibility to renew the expiring Certificate to maintain continuity of usage.

4.6.2 Who May Request Renewal

Only the Certificate Subject or an authorized representative of the Certificate Subject **MAY** request renewal. 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 **SHALL** ensure that the person or organization seeking to renew a Certificate is, in fact, the Subscriber (or authorized by the Subscriber).

One acceptable procedure is through the use of a **Challenge Phrase** (or its equivalent), or proof of possession of the Private Key. Subscribers **SHALL** choose and submit a Challenge Phrase (or its equivalent) with their initial enrollment information. Upon renewal, if a Subscriber correctly submits the Challenge Phrase and the enrollment information (including corporate and technical contact information[6]) has not changed, a renewed Certificate is automatically issued.

Alternatively, MSC Trustgate **MAY** send an e-mail message to the e-mail address associated with the verified corporate contact for the Certificate being renewed. This email will request confirmation and authorization to issue the renewed Certificate. Upon receipt of a confirming response, MSC Trustgate WILL issue the Certificate if the enrollment information has not changed.

After renewal using this alternative procedure, and on at least every other 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.
ii. The Certificate's Distinguished Name has not been changed.
iii. The Corporate and Technical Contact information remains unchanged from that which was previously verified.

MSC Trustgate **WILL NOT** have to reconfirm via telephone, confirmatory postal mail, or a comparable procedure that the organization has authorized the Certificate Application and that the person submitting the Certificate Application is authorized to do so.

[6] 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.

When a certificate is renewed prior to its expiry, the new certificate's validity period shall commence upon issuance. The expiry date of the renewed certificate may be extended to preserve any remaining validity of the previous certificate, such that no validity period is lost due to early renewal.

4.6.4 Notification of New Certificate Issuance to Subscriber

Notification of a renewed Certificate **SHALL** be in accordance with Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Acceptance of a renewed Certificate **SHALL** be in accordance with Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

The renewed Certificate **SHALL** be 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 Circumstances for Certificate Re-key

Subscribers requesting a re-key **SHALL** 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, MSC Trustgate **CAN** issue a replacement Certificate using a previously issued Certificate or a previously provided CSR. MSC Trustgate **MAY** reuse existing verification information unless re-verification and authentication are 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 the issuance of a re-keyed Certificate to the Subscriber **SHALL** be in accordance with Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Acceptance of a re-keyed Certificate **SHALL** be in accordance with Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

The re-keyed Certificate **SHALL** be published in MSC Trustgate's publicly accessible repository.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Registration Authorities (RAs) **MAY** receive notification of a Certificate's re-key if the RA was involved in the issuance process.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Modifying a Certificate means creating a new Certificate for the same subject with authenticated information that differs slightly from the old Certificate (e.g., changes to an e-mail 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 **MAY** modify Certificates at the request of certain Certificate Subjects or in its own discretion. MSC Trustgate **SHALL NOT** make Certificate modification services available to all Subscribers.

4.8.3 Processing Certificate Modification Requests

After receiving a request for modification, MSC Trustgate **SHALL** verify any information that will change in the modified Certificate. MSC Trustgate **SHALL** only issue the modified Certificate after completing the verification process on all modified information. MSC Trustgate **SHALL NOT** issue a modified Certificate that has a validity period exceeding 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 accordance with 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 a 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 its operational period before its stated validity period expires. Prior to revoking a Certificate, MSC Trustgate and Issuer CAs SHALL verify that the revocation request was made by either the organization or individual that submitted 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.

Revocation within 24 Hours

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

i. The Subscriber requests revocation in writing without specifying a reason (`CRLReason: unspecified (0)`).
ii. The Subscriber notifies the CA that the original certificate request was not authorized (`CRLReason: privilegeWithdrawn (9)`).
iii. Evidence is obtained that the Subscriber's Private Key corresponding to the Public Key in the Certificate has been compromised (`CRLReason: keyCompromise (1)`).
iv. A demonstrated or proven method exists to easily compute the Subscriber's Private Key based on the Public Key (`CRLReason: keyCompromise (1)`).
v. Evidence is obtained that the validation of a domain or IP address in the Certificate should not be relied upon (`CRLReason: superseded (4)`).

Revocation within 5 Days

With the exception of Short-lived Subscriber Certificates, MSC Trustgate **MAY** revoke a Certificate within **twenty-four (24) hours** and **SHALL** revoke a Certificate within **five (5) days** of confirming one or more of the following:

i. The Certificate no longer complies with the requirements of Section 6.1.5 and 6.1.6 (`CRLReason: superseded (4)`).
ii. The Certificate was misused (`CRLReason: privilegeWithdrawn (9)`).
iii. The Subscriber has violated one or more material obligations under the Subscriber Agreement or Terms of Use (`CRLReason: privilegeWithdrawn (9)`).
iv. Use of a domain or IP address in the Certificate is no longer legally permitted (`CRLReason: cessationOfOperation (5)`).
v. A Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN (`CRLReason: privilegeWithdrawn (9)`).
vi. A material change in the information contained in the Certificate has occurred (`CRLReason: privilegeWithdrawn (9)`).
vii. The Certificate was not issued in accordance with CA/B Forum Requirements or the MSC Trustgate's Certification Practice Statement (`CRLReason: superseded (4)`).
viii. Any information in the Certificate is inaccurate (`CRLReason: privilegeWithdrawn (9)`).
ix. MSC Trustgate's right to issue Certificates under CA/B Forum Requirements expires or is revoked (`CRLReason: unspecified (0)`).
x. Revocation is required by the MSC Trustgate's Certificate Policy and/or Certification Practice Statement for a reason not specified elsewhere in this section (`CRLReason: unspecified (0)`).
xi. A demonstrated or proven method exposes the Subscriber's Private Key to compromise, or clear evidence exists that the key generation method was flawed (`CRLReason: keyCompromise (1)`).

Discretionary Revocation

MSC Trustgate **MAY** revoke any Certificate at its sole discretion, including if:

i. The Subscriber's or MSC Trustgate's obligations are delayed by circumstances beyond their control, threatening or compromising another entity's information.

ii. A lawful and binding order from a government or regulatory body to revoke the Certificate is received.

iii. MSC Trustgate ceases operations without arranging for another CA to provide revocation support.

iv. The technical content or format of the Certificate presents an unacceptable risk.

v. The Subscriber is added to a blacklist of denied or prohibited persons under Malaysian law.

MSC Trustgate **SHALL** always revoke a Certificate if the binding between the subject and their Public Key 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 **SHALL** revoke a Subordinate CA Certificate within **seven (7) days** after confirming one or more of the following:

i. The Subordinate CA requests revocation in writing.

ii. The Subordinate CA notifies MSC Trustgate that the original certificate request was not authorized.

iii. Evidence is obtained that the Subordinate CA's Private Key has been compromised or no longer complies with Sections 6.1.5 and 6.1.6.

iv. The Certificate was misused.

v. The Certificate was not issued in accordance with, or the Subordinate CA has not complied with, this document.

vi. Any information in the Certificate is inaccurate or misleading.

vii. MSC Trustgate or the Subordinate CA ceases operations without arranging for another CA to provide revocation support.

viii. MSC Trustgate's or the Subordinate CA's right to issue Certificates expires, is revoked, or terminated.

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

MSC Trustgate **SHALL** revoke a cross-Certificate if the cross-certified entity no longer meets the stipulations of the corresponding policies. An Administrator Certificate **MAY** also be revoked if the Administrator's authority has been terminated.

Subscribers are contractually required to immediately notify MSC Trustgate of a known or suspected compromise of their Private Key.

4.9.2 Who Can Request Revocation

i. **Individual Subscribers** can request the revocation of their own Certificates.

ii. **Organizational Certificates** can be revoked by a duly authorized representative of the organization.

iii. A duly **authorized representative of MSC Trustgate** or an **RA** can request the revocation of an RA Administrator's Certificate.

iv. The **entity that approved a Subscriber's Certificate Application** is also entitled to revoke or request the revocation of the Subscriber's Certificate.

v. Only MSC Trustgate is entitled to request or initiate the revocation of Certificates issued to its own CAs.

vi. **RAs**, through their authorized representatives, are entitled to request the revocation of their own Certificates.

4.9.3 Procedure for Revocation Request

MSC Trustgate provides a process for Subscribers to request revocation of their Certificates. The process is as follows:

i. MSC Trustgate logs the request or problem report, including the requestor's contact information and reason for revocation.

ii. MSC Trustgate verifies the revocation request from the Subscriber, where applicable, via telephone or other means.

iii. If the request is authenticated, MSC Trustgate revokes the Certificate according to the timelines in Section 4.9.1.

iv. For requests from third parties, MSC Trustgate personnel **SHALL** investigate the request within **24 hours** and decide on revocation 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 revocation is necessary, MSC Trustgate personnel will revoke the certificate and update its status. Reports **MAY** be escalated to law enforcement if deemed appropriate.

MSC Trustgate maintains a continuous **24/7** ability to respond to high-priority revocation requests and certificate problem reports via helpdesk@msctrustgate.com and other resources listed in Section 1.5.2.

For CA or RA Certificates, a request for revocation must be communicated to MSC Trustgate, which will then revoke the Certificate. MSC Trustgate **MAY** also initiate these revocations.

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 a Private Key loss or compromise. MSC Trustgate **MAY** grant and extend this grace period on a case-by-case basis if it does not violate this CP/CPS.

MSC Trustgate **SHALL** report a suspected compromise of its CA Private Key and request 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 Revocation

- A CA Certificate **SHALL** be revoked within **one (1) hour** of receiving clear instructions from the ISC.
- Within **twenty-four (24) hours** of a problem report, MSC Trustgate **SHALL** investigate and provide a preliminary report to the Subscriber and the reporting entity.
- After reviewing the report, MSC Trustgate MAY works with the Subscriber, the reporting entity 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 the receipt of a problem report to published revocation **MUST NOT** exceed the timeframe set 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 circumstances, MSC Trustgate processes publicly trusted Certificate revocation requests **within 18 hours**. Requests received at least two hours before a scheduled CRL issuance are processed before that CRL is published.

4.9.6 Revocation Checking Requirement for Relying Parties

Before relying on a Certificate, a Relying Party **MUST** confirm the validity of each Certificate in the path by checking its validity, chaining, constraints, and revocation status through CRLs or OCSP responders as defined by IETF PKIX standards.

4.9.7 CRL Issuance Frequency

- **Subscriber Certificates**: CRLs **SHALL** be updated and issued at least once every seven days. The `nextUpdate` field **SHALL NOT** be more than ten days beyond the value of the `thisUpdate` field. A new CRL **SHALL** be published within **24 hours** of revoking a certificate.
- **Subordinate CA and Timestamp Certificates**: CRLs SHALL be updated and reissued at least once every **twelve months** and within **24 hours** after revoking a Subordinate CA Certificate. The value of the `nextUpdate` field **SHALL NOT** be more than **twelve months** beyond the value of the `thisUpdate` field.

MSC Trustgate **SHALL** continue issuing CRLs until one of the following conditions is met:

i. All Subordinate CA Certificates containing the same Subject Public Key have either expired or been revoked.

ii. The corresponding Subordinate CA Private Key is destroyed.

4.9.8 Maximum Latency for CRLs

CRLs for end-entity Subscribers are posted to the repository within a commercially reasonable time, typically minutes. Irregular, interim or emergency CRLs are posted within **four hours** of generation. Regularly scheduled CRLs are posted prior to the `nextUpdate` field in the previously issued CRL of the same scope.

CRLs for Code Signing and Timestamp Certificates **MUST** contain the serial number of a revoked certificate for at least **10 years** after the certificate's expiration.

4.9.9 Online Revocation/Status Checking Availability

Online revocation status information is available via a web-based repository and, where offered, **OCSP**. 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 **SHALL** conform to **RFC 6960** and be signed by either the issuing CA or an OCSP Responder whose Certificate is signed by the issuing CA. The OCSP signing certificate SHALL contain the id-pkix-ocsp-nocheck extension, as defined in RFC 6960. The extension SHALL be non-critical and SHALL have a NULL value.

4.9.10 Online 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 **OCSP** using the GET method for Certificates issued under the Baseline Requirements. OCSP Responders under MSC Trustgate's direct control **SHALL NOT** respond with a "good" status for an unissued certificate.

- **Subscriber Certificates**: OCSP responses **MUST** have a validity interval between **8 hours** and **10 days**. Update schedules are defined based on the validity interval length:
    - If validity intervals **less than sixteen hours**, MSC Trustgate updates the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the `nextUpdate`.
    - If validity intervals **greater than or equal to sixteen hours**, 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`.
- **Subordinate CA Certificates**: OCSP information is updated at least every **twelve months** and within **24 hours** after a revocation.

MSC Trustgate **MAY** provide OCSP responses for Code Signing and Timestamp Certificates for at least 1**0 years** after their expiration.

4.9.11 Other Forms of Revocation Advertisements Available

No Stipulation.

4.9.12 Special Requirements for Key Compromise

MSC Trustgate **SHALL** use commercially reasonable efforts to inform Subscribers if their Private Keys may have been compromised. If a key compromise is confirmed, MSC Trustgate **SHALL** revoke the Certificate as set forth in Section 4.9.1 and **SHALL** transition the revocation reason code to "key compromise" in the CRL.

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 **SHALL** be available via a **Certificate Revocation List (CRL)** and an **Online Certificate Status Protocol (OCSP)** responder. The serial number of a revoked Certificate **SHALL** remain 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 **SHALL** be 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 **SHALL** operate and maintain its CRL and OCSP capability with sufficient resources 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 **SHALL** end if its Certificate expires or is revoked, or if the applicable Subscriber Agreement expires without being renewed.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

MSC Trustgate **SHALL NEVER** escrow CA Private Keys under this CP/CPS.

MSC Trustgate **MAY** escrow Subscriber key management keys to provide key recovery services. MSC Trustgate SHALL encrypt and protect escrowed Private Keys using the same or a higher level of security as that used to generate and deliver the Private Key.

MSC Trustgate **SHALL** allow Subscribers and other authorized entities to recover escrowed (decryption) Private Keys. MSC Trustgate SHALL use multi-person controls during key recovery to prevent unauthorized access to a Subscriber's escrowed Private Keys. MSC Trustgate SHALL accept key recovery requests from the following:

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

ii. 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. An authorized investigator or auditor, if the Private Key is part of a required investigation or audit.

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

v. A requester authorized by law or governmental regulation.

vi. 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 obtain their consent that their Private Keys will be 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 receiving a properly authorized request for recovery.

v. Comply with any legal obligations to disclose or keep confidential escrowed keys, 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

5.1 Physical Security Controls

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

5.1.1 Site Location and Construction

MSC Trustgate's CA and RA operations **SHALL** be conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems. MSC Trustgate **SHALL** also maintain disaster recovery facilities for its CA operations that are protected by multiple tiers of physical security comparable to those of the primary facility.

5.1.2 Physical Access

5.1.2.1 Data Centers

Systems providing online certificate issuance (e.g., Issuer CAs) **SHALL** be located in commercial data centers. MSC Trustgate **SHALL** protect such online equipment from unauthorized access and implement physical controls to reduce the risk of equipment tampering.

Access to the data centers housing the CA **SHALL** require two-factor authentication, including a valid access card and biometric authentication. These biometric systems SHALL log each use of the access card. When not in use, MSC Trustgate **SHALL** deactivate and securely store its CA equipment in accordance with Section 5.1.2.3.

Activation data **SHALL** either be memorized or recorded and stored in a manner commensurate with the security afforded to the cryptographic module. Activation data **SHALL** NEVER be stored with the cryptographic module or any removable hardware used to administer MSC Trustgate's Private Keys. The cryptographic hardware **SHALL** include a mechanism to lock the hardware after a specific number of failed login attempts.

The data center is not continuously attended. The last person to depart **SHALL** initial a sign-out sheet indicating the date and time, and assert that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 RA Operations Areas

MSC Trustgate's RA operations **SHALL** be protected against access from unauthorized individuals. Access to secure areas of buildings **SHALL** require an access card. Access card use **SHALL** be logged by the building security system. The exterior and internal passageways of buildings, as well as support and vetting rooms where MSC Trustgate personnel perform identity vetting and other RA functions, **SHALL** be equipped with video cameras. Access card logs and video records **SHALL** be reviewed on a regular basis. MSC Trustgate **SHALL** securely store 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 **SHALL** securely store the cryptomodules used to generate and store offline CA Private Keys. Access to these rooms **SHALL** be controlled and logged by the building access card system. When not in use, CA cryptomodules **SHALL** be locked in a safe that provides two-person physical access control. Activation data **SHALL** be protected in accordance with Section 6.4. Cryptomodule activation keys (operator cards and PED keys) **SHALL** be 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 **SHALL** be manually logged. Access card logs and the manual logs of safe access **SHALL** be reviewed on a regular basis.

5.1.3 Power and Air Conditioning

MSC Trustgate's secure facilities **SHALL** be equipped with primary and backup:

- Power systems to ensure continuous, uninterrupted access to electric power.
- Heating, Ventilation, and Air Conditioning (HVAC) systems to control temperature and relative humidity.

5.1.4 Water Exposure

The cabinets housing MSC Trustgate's CA systems **SHALL** be located on raised flooring, and the data centers **SHALL** be equipped with monitoring systems to detect excess moisture.

5.1.5 Fire Prevention and Protection

The data centers **SHALL** be equipped with fire suppression mechanisms.

5.1.6 Media Storage

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

5.1.7 Waste Disposal

All unnecessary copies of printed sensitive information **SHALL** be shredded before disposal. Media used to collect or transmit sensitive information **SHALL** be rendered unreadable before disposal. Cryptographic devices **SHALL** be physically destroyed or zeroized in accordance with the manufacturer's guidance prior to disposal.

5.1.8 Off-site Backup

MSC Trustgate **SHALL** maintain at least one full backup and make regular backup copies of any information necessary to recover from a system failure. These backups, including copies of CA Private Keys and activation data, **SHALL** be stored at off-site facilities equipped with physical and procedural safeguards appropriate to their operational environment.

5.2 Procedural Controls

5.2.1 Trusted Roles

A Trusted Person is any employee, contractor, or consultant who holds a Trusted Position and has access to, or control over, authentication or cryptographic operations that may materially affect:

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

Trusted Roles[7] include, but are not limited to:

- **CA Operations & Compliance Manager**: The person with ultimate responsibility for the CA's security practices, operations, and policy enforcement. This role is also responsible for overseeing compliance and security audits.
- **ICT Operations Manager**: The person responsible for overseeing the day-to-day operations of the CA and supporting systems, including the physical security of all CA and RA facilities, data centers, key storage rooms, and access controls. This role has no access to cryptographic devices.
- **PKI Engineer**: A person authorized to manage the CA Key and Certificate Lifecycle. This role creates certificate profiles for Subscriber Certificates and ensures all certificates are issued according to the policies defined in the CP/CPS. This role works in conjunction with the Key Custodian(s) for cryptographic device and key activation.
- **System Engineer**: The person responsible for the installation and maintenance of the CA and supporting systems, and for assisting the ICT Operations Manager with day-to-day operations. This role also has no access to cryptographic devices.
- **RA Operator**: The person who performs identity vetting and authentication of subscribers and their information before submitting a request to the CA.
- **Internal Auditor**: The person responsible for reviewing all CA operations, procedures, and logs to ensure compliance with the CP/CPS and other external requirements. This is a highly trusted, non-operational role.
- **Key Custodian(s)**: The group of persons responsible for the physical security of the CA's cryptographic devices and the safekeeping of the secret shares of the CA's private keys' activation data. They operate under a split knowledge M-of-N control, where a minimum of M custodians must be present to reconstruct the secret. They are required to be present during any key activation ceremony to enforce two-person control and/or M-of-N control.

MSC Trustgate considers the categories of personnel identified in this section as Trusted Persons holding a Trusted Position. Individuals seeking to become Trusted Persons MUST successfully complete the screening requirements outlined in this CP/CPS.

[7] 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.

5.2.2 Number of Persons Required Per Task

MSC Trustgate **SHALL** establish, maintain, and enforce rigorous control procedures to ensure the segregation of duties based on job responsibility. **Multiple Trusted Persons** are required to perform sensitive tasks to minimize the risk of a single point of failure or malicious activity.

The most sensitive tasks, such as access to and management of **CA cryptographic hardware (cryptographic signing unit or CSU)** and associated key material, **SHALL** require the participation of multiple Trusted Persons. These internal control procedures are designed to ensure that a minimum of **two Trusted Persons** 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 **SHALL** be invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules **SHALL 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 system, **SHALL** require the participation of at least two 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.

5.2.3 Identification and Authentication for Each Role

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

MSC Trustgate **SHALL** ensure that personnel have achieved **Trusted Status** and received departmental approval before they are:

- Issued access devices and granted access to required facilities.
- 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

The principle of Separation of Duties SHALL apply to the following roles and responsibilities (this list is not exhaustive):

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.

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

iv. The handling of Subscriber information or requests.

v. The generation, issuance, or destruction of a CA certificate.

vi. The loading of a CA to a Production environment.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The **Information Security Committee (ISC)** is responsible and accountable for MSC Trustgate's PKI operations and **SHALL** ensure compliance with this **CP/CPS**. MSC Trustgate's personnel and management practices **SHALL** provide reasonable assurance of the trustworthiness and competence of its employees and 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 ISC **SHALL** ensure that all individuals assigned to trusted roles have proof of the requisite background, qualifications, and experience to perform their prospective job responsibilities competently and satisfactorily. This includes proof of any government clearances, if applicable, necessary for performing certification services under government contracts.

5.3.2 Background Check Procedures

MSC Trustgate **SHALL** verify the identity of each employee appointed to a trusted role and perform a background check prior to allowing such person to act in that role. MSC Trustgate **SHALL** require each individual to appear in person before a human resources employee whose responsibility is to verify identity. The human resources employee **SHALL** verify the individual's identity using government-issued photo identification (e.g., national identity card, passport, and/or driver's license) or a comparable procedure for the applicable jurisdiction.

Background checks MAY include a combination of the following:

- Verification of the individual's identity.
- Previous employment.
- Professional references.
- Highest or most relevant educational degree obtained.
- Bankruptcy records.
- Driving records.

These procedures are subject to any limitations on background checks imposed by local law. To the extent that any of these requirements cannot be met due to legal prohibitions, MSC Trustgate **SHALL** utilize a substitute investigative technique that provides substantially similar information, including but not limited to a background check performed by the applicable governmental agency.

The factors revealed in a background check that **MAY** be considered grounds for rejecting candidates or taking action against an existing Trusted Person include, but are not limited to:

- Misrepresentations made by the candidate or Trusted Person.
- Highly unfavorable or unreliable professional references.
- Indications of a lack of financial responsibility.

Reports containing such information **SHALL** be evaluated by human resources personnel, with the assistance of legal counsel when necessary, to determine the appropriate course of action. Such actions **MAY** include the cancellation of employment offers or the termination of existing Trusted Persons. The use of information from a background check for these actions **SHALL** be subject to applicable local laws.

Background checks **SHALL** be refreshed, and re-adjudication **SHALL** occur at least every **five (5) years**.

5.3.3 Training Requirements

MSC Trustgate **SHALL** provide its personnel with training upon hire, as well as the requisite on-the-job training, to perform their job responsibilities competently and satisfactorily. MSC Trustgate **SHALL** maintain records of such training. MSC Trustgate **SHALL** periodically review and enhance its training programs as necessary.

MSC Trustgate's training programs **SHALL** be tailored to the individual's responsibilities and include the following:

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

Training **SHALL** be provided via a mentoring process involving senior members of the relevant team. MSC Trustgate **SHALL** maintain records of who received training and the level of training completed. **RA Operators MUST** have the minimum skills to satisfactorily perform validation duties before being granted validation privileges. All RA Operators are required to pass an internal examination provided by MSC Trustgate on the **Baseline Requirements** prior to validating and approving Certificates. Where competence is demonstrated in lieu of training, MSC Trustgate **SHALL** maintain supporting documentation.

5.3.4 Retraining Frequency and Requirements

MSC Trustgate **SHALL** provide refresher training and updates to its personnel to the extent and frequency required to ensure they maintain the necessary 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 **SHALL** be taken for unauthorized actions or other violations of MSC Trustgate policies, whether through negligence or malicious intent. Disciplinary actions **MAY** include measures up to and including termination and **SHALL** be commensurate with the frequency and severity of the unauthorized actions.

If a person in a trusted role is alleged by management to have performed unauthorized or inappropriate actions, the person **SHALL** be immediately removed from the trusted role pending management review. After the review, 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 **SHALL** meet the same functional and security criteria that apply to 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 only be permitted access to MSC Trustgate's secure facilities if they are escorted and directly supervised by **Trusted Person** at all times.

5.3.8 Documentation Supplied to Personnel

MSC Trustgate **SHALL** provide its employees with 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 **SHALL** require identification and authentication at system logon with a unique username and password. Important system actions **SHALL** be logged to establish the accountability of the operators who initiate such actions.

MSC Trustgate **SHALL** enable all essential event auditing capabilities of its **CA** applications to record the events listed below. If an event cannot be automatically recorded, MSC Trustgate **SHALL** implement manual procedures to satisfy the requirements. For each event, MSC Trustgate **SHALL** record the following:

i. Date and time.
ii. Type of event.
iii. Success or failure.
iv. User or system that caused the event or initiated the action.

MSC Trustgate **SHALL** record at least the following events:

i. **CA key lifecycle management events**:
   a. Key generation, backup, storage, recovery, archival, and destruction.
   b. Cryptographic device lifecycle management events.

ii. **CA and Subscriber Certificate lifecycle management events**:
   a. Certificate requests, renewal, re-key requests, and revocation.
   b. All verification activities stipulated in the CA/B Forum Baseline Requirements and 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.
   f. Generation of Certificate Revocation Lists and OCSP entries.

iii. **Security events**:
   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.
   f. Entries to and exits from the CA facility.

Log entries **SHALL** include the following elements:

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

5.4.2 Frequency of Processing Log

At least once every **three (3) months**, a designated MSC Trustgate administrator **SHALL** review the logs generated by the systems, perform system and file integrity checks, and conduct a vulnerability assessment. The administrator **MAY** perform these checks using automated tools. During these checks, the administrator **SHALL** perform the following tasks:

i. Check for any tampering with the log.
ii. Scan for anomalies or specific conditions, including evidence of malicious activity.
iii. Prepare a written summary of the review.

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

5.4.3 Retention Period for Audit Log

Audit logs related to publicly trusted Certificates **SHALL** be retained for at least **ten (10) years** or in accordance with Section 5.5.2. MSC Trustgate **SHALL** retain audit logs on-site until after they are reviewed. The individuals who remove audit logs from MSC Trustgate's CA systems **SHALL** be different from the individuals who control MSC Trustgate's signature keys.

5.4.4 Protection of Audit Log

CA audit log information **SHALL** be retained on equipment until it is copied by a system administrator. MSC Trustgate's CA systems **SHALL** be configured to ensure that:

i. Only authorized people have read access to logs.
ii. Only authorized people **MAY** archive audit logs.
iii. Audit logs are not modified.

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

5.4.5 Audit Log Backup Procedures

MSC Trustgate **SHALL** make regular backup copies of audit logs and audit log summaries. A copy of the audit log **SHALL** be saved to a secure, off-site location at least on a monthly basis. Where required, MSC Trustgate **SHALL** create incremental backups of audit logs daily and full backups weekly.

5.4.6 Audit Collection System

Automatic audit processes **SHALL** 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 it is at risk, MSC Trustgate's Administrators and the **ISC SHALL** be notified. The ISC 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 **SHALL** perform annual risk assessments that identify and evaluate 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 **SHALL** also routinely assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements in place to control such risks. MSC Trustgate's Internal Auditors **SHALL** review the security audit data checks for continuity. MSC Trustgate's audit log monitoring tools **SHALL** 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 **SHALL** conduct regular vulnerability assessments and penetration testing covering all MSC Trustgate assets related to Certificate issuance, products, and services. Assessments **SHALL** 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 **SHALL** comply with all record retention policies governed by law. Archived records **SHALL** be retrieved as necessary upon request of authorized parties. All archived records **SHALL** include sufficient detail to demonstrate that a Certificate was issued in accordance with this **CP/CPS**.

5.5.1 Types of Records Archived

MSC Trustgate **SHALL** retains the following information in its archives, as it pertains to MSC Trustgate's PKI operations:

i. Accreditations of MSC Trustgate.
ii. CP/CPS versions.
iii. Contractual obligations and other agreements.
iv. System and equipment configurations, modifications, and updates.
v. The acceptance or rejection of a certificate request.
vi. Certificate issuance, rekey, renewal, and revocation requests.
vii. Sufficient identity authentication data to satisfy the requirements of Section 3.2, including details of telephone verification calls.
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. The approval or rejection of a revocation request.
xxii. The appointment of an individual to a trusted role.
xxiii. The destruction of a cryptographic module.
xxiv. Certificate compromise notifications.
xxv. Remedial action taken as a result of physical security violations.
xxvi. Violations of the CP/CPS.
xxvii. Books of account.

5.5.2 Retention Period for Archive

MSC Trustgate and the RA **SHALL** retain archived data associated with Certificates for at least **ten (10) years**.

5.5.3 Protection of Archive

Archive records **SHALL** be stored in a secure location and maintained in a manner that prevents unauthorized modification, substitution, or destruction. Archives **SHALL NOT** be released except as permitted by the **ISC** or as required by law. MSC Trustgate **SHALL** maintain 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, both archived locations and/or pieces of equipment **SHALL** be maintained until the transfer is complete. All transfers to new archives **SHALL** occur in a secure manner.

5.5.4 Archive Backup Procedures

MSC Trustgate **SHALL** incrementally back up electronic archives of its issued Certificate information on a daily basis and perform 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 **SHALL** automatically time-stamp archived records with system time (a non-cryptographic method) as they are created. MSC Trustgate **SHALL** synchronize its system time at least every **eight hours** using a real-time value distributed by a recognized **UTC(k)** laboratory or the **National Metrology Institute of Malaysia (NMIM)**.

5.5.6 Archive Collection System

The archive collection system **SHALL** comply with the security requirements detailed 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. Upon receiving a request made for a proper purpose by a Customer, its agent, or a party involved in a dispute over a transaction, MSC Trustgate **MAY** retrieve the information from the archive. The integrity of archive information **SHALL** be 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. MSC Trustgate **MAY** also refuse to provide the information at its discretion and **MAY** require prior payment of all costs associated with the data.

5.6 Key Changeover

Key changeover procedures **SHALL** enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of a CA Private Key's lifetime, MSC Trustgate **SHALL** cease using the expiring CA Private Key to sign new Certificates. The old Private Key **SHALL** only be used to sign CRLs and OCSP responder Certificates. A new CA signing Key Pair **SHALL** be commissioned, and all subsequently issued Certificates and CRLs **SHALL** be signed with the new private signing key.

Both the old and 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 **SHALL** be 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 **SHALL** have a Security Incident Response Plan, Business Continuity Management, and Disaster Recovery Plan. These plans **SHALL** be 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 **SHALL NOT** disclose its business continuity plans to Subscribers, Relying Parties, or Application Software Suppliers, but **SHALL** provide these plans to MSC Trustgate's CA auditors upon request. MSC Trustgate **SHALL** annually test, review, and update these procedures.

The business continuity plan **SHALL** include:

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 individuals.
viii. A Recovery Time Objective (RTO).
ix. Regular testing of contingency plans.
x. The plan to maintain or restore business operations in a timely manner following an interruption or failure of critical business processes.
xi. A requirement to store critical cryptographic materials (i.e., a secure cryptographic device and activation materials) at an alternate location.
xii. A definition of an acceptable system outage and recovery time.
xiii. The frequency of backup copies of essential business information and software.
xiv. The distance of recovery facilities from the primary site.
xv. Procedures for securing the facility following a disaster and prior to restoring a secure environment at either the original or a remote site.

Additionally, serious vulnerabilities and security incidents **MUST** be reported to **Bugzilla**.

5.7.2 Corrupted Computing Resources, Software, and/or Data

MSC Trustgate **SHALL** make regular system backups on a weekly basis and maintain backup copies of its CA Private Keys in a secure, separate location.

If MSC Trustgate discovers that any of its computing resources, software, or data operations have been compromised, it **SHALL** assess the threats and risks posed to the integrity or security of its operations or those of affected parties. If MSC Trustgate determines that continued operation poses a significant risk to Relying Parties or Subscribers, it **SHALL** suspend such operation until the risk is mitigated.

5.7.3 Entity Private Key Compromise Procedures

If MSC Trustgate suspects that one of its CA Private Keys has been compromised or lost, the MSC Trustgate **Security Incident Response Plan SHALL** be enacted by the MSC Trustgate **Incident Response Team (IRT)**. This team **SHALL** assess the situation, develop an action plan, and implement it with approval from MSC Trustgate ISC.

The incident **MUST** be reported. The report **MUST** detail the cause of the compromise or loss and the measures taken to prevent a reoccurrence.

If **CA Certificate revocation** is required, the following procedures **SHALL** be performed:

i. The Certificate's revoked status **SHALL** be 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 PKI participants.
iii. The **CA WILL** generate a new key pair in accordance with Section 5.6, unless 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 **SHALL** implement data backup and recovery procedures as part of its **Business Continuity Plan (BCP)**. The stated goals of the BCP **ARE** to ensure that certificate status services will be minimally affected by any disaster and that MSC Trustgate will be capable of maintaining or resuming other services as quickly as possible. MSC Trustgate SHALL review, test, and update the BCP and supporting procedures at least annually.

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

5.8 CA or RA Termination

In the event that it is necessary for a MSC Trustgate CA to cease operation, MSC Trustgate **SHALL** make a commercially reasonable effort to notify its Subscribers, Relying Parties, and other affected entities in advance.

Where CA termination is required, MSC Trustgate **WILL** develop a termination plan to minimize disruption. The plan **MAY** address the following:

i. Provision of notice to affected parties, such as Subscribers and Relying Parties.
ii. Handling the cost of such notice.
iii. Transferring all responsibilities to a qualified successor entity.

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

i. Transfer all relevant records to a government supervisory or legal body.
ii. Revoke all Certificates that are still unrevoked or unexpired on a date specified in the notice and publish final CRLs.
iii. Destroy all Private Keys.
iv. Make other necessary arrangements in accordance with this CP/CPS.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

All keys **MUST** be generated using a **FIPS-approved** method, an equivalent international standard, or an authoritative national standard.

6.1.1.1 CA Key Pair Generation

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

For **CA keys** intended for use as **publicly trusted Certificates**, the CA key pair generation SHALL require the following process:

i. A **Key Generation Script SHALL** be prepared and followed.

ii. A **Qualified Auditor SHALL** witness the CA Key Pair generation process or a video of the entire process SHALL be recorded.

iii. A Qualified Auditor **SHALL** issue a report confirming that the CA followed its key ceremony during the key and certificate generation process and that the controls used to ensure the integrity and confidentiality of the key pair were effective.

iv. The report **SHALL** be dated and signed by all individuals involved.

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

i. A Key Pair Generation Script **SHALL** be prepared and followed.

ii. An Internal Auditor, external auditor, or independent third party **SHALL** attend the ceremony, or an external auditor **SHALL** examine the signed and documented record of the key generation ceremony, as allowed by applicable policy.

In all cases, MSC Trustgate **SHALL** adhere to the following procedures:

i. The CA Key Pair **SHALL** be generated in a physically secured environment, as described in the CA's CP/CPS.

ii. The CA Key Pair **SHALL** be generated by personnel in Trusted Roles under the principles of multiple person control and split knowledge.

iii. The CA Key Pair **SHALL** be generated within cryptographic modules meeting the applicable technical and business requirements disclosed in the CA's CP/CPS.

iv. All CA Key Pair generation activities **SHALL** be logged.

v. Effective controls **SHALL** be maintained to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in this CP/CPS and (if applicable) its Key Generation Script.

6.1.1.2 RA Key Pair Generation

The generation of RA Key Pairs **SHALL** be performed by the RA using a minimum of a FIPS 140-2 Level 2 certified cryptographic module.

6.1.1.3 Subscriber Key Pair Generation

MSC Trustgate **SHALL** reject 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 requests 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. **Debian weak keys vulnerability**: The Issuer CA **SHALL** reject all keys listed at https://github.com/cabforum/Debian-weak-keys/ for each key type (e.g., RSA, ECDSA) and size. 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. **ROCA vulnerability**: The Issuer CA **SHALL** reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.

   c. **Close Primes vulnerability**: 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].

The generation of end-user **Subscriber Key Pairs SHALL** be performed by the Subscriber in a manner appropriate for the certificate type. **AATL Certificates 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, it **MUST** deliver the Private Key securely to the Subscriber. Keys **MAY** be delivered electronically (e.g., via secure email or stored in a cloud-based system) or on a hardware cryptographic module.

In all cases:

i. The key generator **MUST NOT** retain access to the Subscriber's Private Key after delivery, except where escrow/backup services are authorized.

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 using the related Certificate.

iv. The key generator **MUST** deliver the Private Key in a way that ensures 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.

   b. For electronic delivery, the key generator encrypting the 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 acknowledgment of receipt. 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. The Private Key **MUST** be encrypted 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 an unauthorized person or organization, 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 **SHALL** generate Key Pairs and submit the Public Key to MSC Trustgate for certification electronically through a **PKCS#10** Certificate Signing Request (CSR) or another digitally signed package in a session secured by TLS. 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 **SHALL** be 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 stores.

iii. Roots signed by other CAs.

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

MSC Trustgate generally provides the full certificate 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 rollover Certificate. Relying Parties **MAY** obtain MSC Trustgate's CA Certificates via MSC Trustgate's website or by email.

6.1.5 Key Sizes

MSC Trustgate **SHALL** strictly adhere to the key sizes specified within this section and **SHALL NOT** utilize any other sizes.

6.1.5.1 Related to Code Signing and Timestamping Certificates

For keys corresponding to **Root and Subordinate CAs**:

- **RSA**: The modulus **MUST** be at least **4096** bits in length.
- **ECDSA**: The curve **MUST** be one of **NIST P-256**, **P-384**, or P-**521**.

For keys corresponding to **subscriber certificates**:

- **RSA**: The modulus **MUST** be at least **3072** bits in length.
- **ECDSA**: The curve **MUST** be one of **NIST P-256**, **P-384**, or **P-521**.

6.1.5.2 Other types of Certificates

- **RSA**: The modulus **MUST** be at least **2048** bits in length and evenly divisible by 8.
- **ECDSA**: Keys **MUST** represent a valid point on one of the **NIST P-256**, **P-384**, or **P-521** elliptic curves.
- **EdDSA**: Keys **MUST** represent a valid point on the **Curve25519** (256-bit private keys) or **Curve448** (456-bit private keys) elliptic curves.

In addition to the classical schemes above, MSC Trustgate also supports the following **ML-DSA**, **SLH-DSA**, and **KAZ-Sign**[8] post-quantum digital signature parameter sets:

- **ML-DSA**: ML-DSA-44, ML-DSA-65, ML-DSA-87.
- **SLH-DSA**: SLH-DSA-SHA2-128s, SLH-DSA-SHA2-128f, SLH-DSA-SHA2-192s, SLH-DSA-SHA2-192f, SLH-DSA-SHA2-256s, SLH-DSA-SHA2-256f.
- **KAZ-Sign**: KAZ458, KAZ738, KAZ970.

No other algorithms or key sizes are permitted.

[8] KAZ-Sign is an Asymmetric Key Based Algorithm (AKBA) developed and approved by the Malaysian government under the MySeal program, a recognized national standard for cryptographic algorithms. More information can be found at https://mykripto.cybersecurity.my/index.php/services/myseal/myseal-category/akba-myseal/akba-myseal-2-1

6.1.6 Public Key Parameters Generation and Quality Checking

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

For ECDSA key pairs: MSC Trustgate **SHALL** confirm 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 **SHALL** confirm 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 **SHALL** generate and validate post-quantum ML-DSA key pairs (**Dilithium**) in accordance with **FIPS 204**.

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.

For SLH-DSA key pairs: MSC Trustgate **SHALL** generate and validate post-quantum SLH-DSA key pairs (**SPHINCS+**) in accordance with **FIPS 205**.

i. Key pairs **SHALL** be generated for one of the approved parameter sets—SLH-DSA-SHA2-128s, SLH-DSA-SHA2-128f, SLH-DSA-SHA2-192s, SLH-DSA-SHA2-192f, SLH-DSA-SHA2-256s, SLH-DSA-SHA2-256f—using a **NIST-compliant CSPRNG**.

ii. Public keys **SHALL** be validated to ensure they are the correct length and are properly derived from the private key.

iii. Key validation **SHALL** include:

   a. Recomputing the public key from the private key and verifying byte-for-byte equality.

   b. Performing a test signature and verification process using the generated key pair to confirm it operates correctly.

For KAZ-Sign key pairs: MSC Trustgate **SHALL** generate and validate post-quantum KAZ-Sign key pairs in accordance with the Malaysian government's MySeal standard.

i. Private keys **MUST** be generated using a cryptographically secure random number generator with the bit-length required by the parameter set.

ii. Public keys **MUST** be a valid point on the curve used for the key generation and must correspond to the private key.

iii. Key validation **SHALL** include:

   a. Recomputing the public key from the private key to verify byte-for-byte equality.

   b. Performing a test signature and verification process to ensure proper functionality of the generated key pair.

6.1.7 Key Usage Purposes

MSC Trustgate's Certificates **SHALL** include **key usage extension fields** that specify the intended use of the Certificate and technically limit its functionality in **X.509v3-compliant software**. The use of a specific key is determined by the **key usage extension**.

Private Keys corresponding to **Root CA** Certificates **SHALL NOT** be used to sign Certificates except for the following cases:

i. Self-signed Certificates for the Root CA.

ii. Certificates for Subordinate CAs and Cross Certificates.

iii. Certificates for infrastructure purposes.

iv. Certificates for OCSP Response verification.

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

i. **CA Certificate**: `keyCertSign`, `cRLSign`.

ii. **OCSP Responder Certificate**: `digitalSignature`.

iii. **Subscriber Certificate**: assert key usages based on the intended application and CANNOT include `anyExtendedKeyUsage`.

MSC Trustgate **SHALL NOT** issue Certificates with key usage for both signing and encryption. Instead, MSC Trustgate **SHALL** issue Subscribers two Key Pairs—one for key management and one for digital signature and authentication.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

MSC Trustgate **SHALL** implement a combination of physical, logical, and procedural controls to ensure the security of MSC Trustgate Private Keys. Subscribers **SHALL** be required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of their 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** standard. MSC Trustgate's third party **RA SHALL** utilize **FIPS 140-2 Level 2** cryptographic devices to generate, store, and use Key Pairs for accessing the Registration Authority system.

AATL Certificates SHALL be 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 an equivalent certification. Additionally, key activation **MUST** rely on a minimum **2-factor authentication (2FA)** process if the device is managed by a third party on behalf of the signer.

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

MSC Trustgate **SHALL** ensure 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, MSC Trustgate **SHALL** employ hybrid cryptography to maintain compatibility and layered security. These operations **SHALL** be 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 (M out of N) Multi-Person Control

MSC Trustgate **SHALL** implement technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. MSC Trustgate **SHALL** use a "Secret Sharing" scheme to split the activation data needed to use 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 (**N**) created and distributed for a particular hardware cryptographic module is required to activate a CA private key.

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 **SHALL** be protected in accordance with this **CP/CPS**.

6.2.3 Private Key Escrow

MSC Trustgate **SHALL 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 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, they **SHALL** be 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 a 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 backed-up Certificates **SHALL** be protected in a manner that only the Subscriber can control the Private Key. Backed-up keys **SHALL NEVER** be stored in a plaintext form outside of the cryptographic module.

6.2.5 Private Key Archival

MSC Trustgate **SHALL NOT** archive Private Keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

All keys **MUST** be generated by and within a cryptographic module. Private Keys **SHALL** be exported from the cryptographic module into backup tokens only for **HSM** transfer, offline storage, and backup purposes. The Private Keys **SHALL** be encrypted when transferred out of the module and **SHALL NEVER** exist in a plaintext form. When transported between cryptographic modules, MSC Trustgate **SHALL** encrypt the Private Key and protect the keys used for encryption from disclosure. Private Keys used to encrypt backups **SHALL** be 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 **SHALL** 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 **SHALL** be generated and stored inside MSC Trustgate's cryptographic module, which has been evaluated to at least **FIPS 140-2 Level 3**. **Root Private Keys SHALL** be stored offline in cryptographic modules or backup tokens as described 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 **SHALL** be activated according to the specifications of the cryptographic module manufacturer. Activation data entry **SHALL** be 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 its use and its associated private key without the Subscriber's authorization. When deactivated, private keys **SHALL** be kept in an 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 **SHALL** be deactivated via logout procedures on the applicable HSM device when not in use. MSC Trustgate **SHALL** 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, **SHALL** destroy CA, RA, and status server Private Keys when they are 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 **SHALL** also zeroize the HSM device and associated backup tokens according to the specifications of the hardware manufacturer. This procedure reinitializes the device and overwrites the data with binary zeros. If the zeroization or re-initialization procedure fails, MSC Trustgate **SHALL** destroy CA private keys in a manner that reasonably ensures there are no residuals of the key that could lead to its reconstruction.

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 SHALL issue Certificates with operational periods and key pair usage periods that do not exceed the maximum validity periods listed in the following table. All periods are subject to applicable industry standards, such as those from the CA/Browser Forum and other regulatory bodies.

Type	Private Key Term[9]	Certificate Term
Publicly Trusted Root CAs	No stipulation	25 years
Publicly Trusted Sub CAs / Issuer CAs	No stipulation	15 years
Domain Validation TLS Server 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 TLS Server 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 TLS Server 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
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 the Certificate's expiration.

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

[9] CA Private Keys may continue to be used to sign CRLs and OCSP responses after its certificate expired.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

MSC Trustgate **SHALL** activate 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 **SHALL** 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 **SHALL** be instructed to use strong passwords and to protect **PINs** and passwords that meet the requirements specified by the **CA/B Forum Network Security Requirements**. If MSC Trustgate uses passwords as activation data for a signing key, MSC Trustgate **SHALL** change the activation data upon rekey of the CA Certificate.

6.4.2 Activation Data Protection

MSC Trustgate **SHALL** protect data used to unlock Private Keys from disclosure using a combination of cryptographic and physical access control mechanisms. Protection mechanisms include securing activation mechanisms 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 other individual. MSC Trustgate **SHALL** lock 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 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 **SHALL** secure its CA systems and authenticate and protect communications between its systems and Trusted Roles. MSC Trustgate's CA servers and support-and-vetting workstations **SHALL** run on trustworthy systems that are configured and hardened using industry best practices. All CA systems **SHALL** be 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 **SHALL** prevent 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 **SHALL** be 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.
v. Support recovery from key or system failure.

All Certificate Status Servers **SHALL**:

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.
iv. Support recovery from key or system failure.

MSC Trustgate **SHALL** enforce multi-factor authentication on any account capable of directly causing Certificate issuance.

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

MSC Trustgate **SHALL** only use CA system software that is provided by MSC Trustgate. MSC Trustgate **SHALL** have its own mechanisms in place to control and monitor the acquisition and development of the CA systems and **SHALL** comply with this CP/CPS.

All hardware and software **SHALL** be 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. Hardware and software **SHALL** be dedicated only to performing the CA functions for CA operation purposes.

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

6.6.2 Security Management Controls

MSC Trustgate **SHALL** have mechanisms and/or policies in place to control and monitor the configuration of its CA systems. MSC Trustgate **SHALL** create a hash of all software packages and MSC Trustgate software updates. This hash **SHALL** be used to manually verify the integrity of such software. Upon installation and periodically thereafter, MSC Trustgate **SHALL** validate 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 **SHALL** be 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 **SHALL** document and control the configurations of its systems, including any upgrades or modifications. The Issuer MSC Trustgate **SHALL** 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 SHALL 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 (NAT)** 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 Time-stamping

MSC Trustgate's Date/Time Stamp service **SHALL** utilize a trusted time source provided by the **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

This section defines the content and format of all certificates issued by MSC Trustgate. All certificates issued under this CP/CPS **SHALL** conform to the profile defined in **RFC 5280**, with the specific constraints and values detailed herein.

The full certificate structure **SHALL** adhere to the following components:

Field	Presence	Description
tbsCertificate	**SHALL**	The section of the certificate that is signed by the issuer. Its contents and structure are detailed below
signatureAlgorithm	**SHALL**	An OID that identifies the cryptographic algorithm used to sign the tbsCertificate field. The encoded value MUST be byte-for-byte identical to the `tbsCertificate.signature` field.
signature	**SHALL**	The digital signature computed upon the ASN.1 DER-encoded `tbsCertificate`.

The **tbsCertificate** structure **SHALL** adhere to the following:

Field	Presence	Description
version	**SHALL**	As specified in Section 7.1.1.
serialNumber	**SHALL**	MUST be a non-sequential positive integer greater than zero (0) and less than 2^{159}, containing at least 64 bits of output from a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG).
signatureAlgorithm	**SHALL**	Identifies the cryptographic algorithm used by the issuing CA to sign the certificate. As specified in Section 7.1.3.2.
issuer	**SHALL**	Identifies the entity that has signed and issued the certificate. As specified in Section 7.1.4.
validity	**SHALL**	The time period during which the certificate is valid. As specified in Section 7.1.10.1.
subject	**SHALL**	Identifies the entity associated with the public key. As specified in Section 7.1.4.
subjectPublicKeyInfo	**SHALL**	The public key and its algorithm. As specified in Section 7.1.3.1.
issuerUniqueID	**MUST NOT**	
subjectUniqueID	**MUST NOT**	
extensions	**SHALL**	Additional fields for certificate metadata, constraints, and key usage. As specified in Section 7.1.2.

7.1.1 Version Number(s)

All certificates generated by MSC Trustgate **SHALL** conform to the X.509 version 3 standard (certificate version field set to 2).

7.1.2 eCertificate Extensions

This section details the certificate extensions that **SHALL** be included in all certificates issued by MSC Trustgate, as well as their criticality and value constraints. The profiles for each certificate type are provided in the following subsections.

7.1.2.1 Root CA Certificates

MSC Trustgate **SHALL** contain the following extensions for all its Root CA Certificates:

Extension Name	Critical	Value/Constraints
`basicConstraints`	TRUE	`cA` **MUST** be `TRUE`, `pathLenConstraint` **MUST NOT** be present.
`keyUsage`	TRUE	The `keyCertSign` and `cRLSign` bit **MUST** be set. All other bits **MUST NOT** be set.
`subjectKeyIdentifier`	FALSE	**MUST** be present. The value is the SHA-1 hash of the `subjectPublicKey` (excluding tag, length, and unused bits).
`authorityKeyIdentifier`	FALSE	**MAY** be present. The `keyIdentifier` MUST be identical to the `subjectKeyIdentifier`. `authorityCertIssuer` and `authorityCertSerialNumber` **MUST NOT** be present.
Any other extension		**MUST NOT** be present.

7.1.2.2 Subordinate CA Certificates

Subordinate CA Certificates issued by MSC Trustgate **SHALL** contain the following extensions, subject to the constraints specified below:

Extension	Critical	Value or Value Constraint
`basicConstraints`	TRUE	`cA` **MUST** be `TRUE`, `pathLenConstraint` **MUST NOT** be present.
`keyUsage`	TRUE	The `keyCertSign` and `cRLSign` bit **MUST** be set. All other bits **MUST NOT** be set.
`subjectKeyIdentifier`	FALSE	**MUST** be present. The value is the SHA-1 hash of the `subjectPublicKey` (excluding tag, length, and unused bits).
`authorityKeyIdentifier`	FALSE	**MUST** be present. The `keyIdentifier` **MUST** be identical to the `subjectKeyIdentifier` of the Issuing CA. `authorityCertIssuer` and `authorityCertSerialNumber` **MUST NOT** be present.
`cRLDistributionPoints`	FALSE	**MUST** be present. This extension **MUST** contain a `URI` to the CRL for this Subordinate CA.
`authorityInfoAccess`	FALSE	**MUST** be present. This extension **MAY** contain one or more `accessMethod` values of type `id-ad-ocsp` (`1.3.6.1.5.5.7.48.1`) that specify the URI of the Issuing CA's OCSP responder. This extension **SHOULD** contain at least one `accessMethod` value of type `id-ad- caIssuers` (`1.3.6.1.5.5.7.48.2`) that specifies the URI of the Issuing CA's Certificate.
`extKeyUsage`	Varies	**MAY** be present. The specific constraints for this extension vary based on the certificate type and are detailed in Section 7.1.2.2.1.
`certificatePolicies`	FALSE	**MAY** be present. The specific constraints for this extension vary based on the certificate type and are detailed in Section 7.1.2.2.2.
`nameConstraints`	TRUE	**MAY** be present. If present, **SHALL** specify the naming restrictions imposed on subordinate CAs below this certificate. See Section 7.1.5.
Any other extension		NOT RECOMMENDED.

7.1.2.2.1 Extended Key Usage (EKU)

Subordinate CA Certificates issued by MSC Trustgate **SHALL** contain the `extendedKeyUsage` extension to technically constrain the types of certificates they are permitted to issue. The table below outlines the specific EKU values for each dedicated Subordinate CA.

Certificate Type	Criticality	Value
TLS Server	FALSE	**MUST** contain `id-kp-serverAuth` (`1.3.6.1.5.5.7.3.1`). All other EKU values MUST NOT be present.
TLS Client	FALSE	**MUST** contain id-kp-clientAuth (1.3.6.1.5.5.7.3.2). All other EKU MUST NOT be present.
S/MIME	FALSE	**SHALL** contain `id-kp-emailProtection` (`1.3.6.1.5.5.7.3.4`). 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`) All other EKU values **MAY** be present.
Code Signing	FALSE	**MUST** contain `id-kp-codeSigning` (`1.3.6.1.5.5.7.3.3`). The following EKU values **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`) All other EKU values **SHOULD NOT** be present.
Timestamping	TRUE	**MUST** contain `id-kp-timeStamping` (`1.3.6.1.5.5.7.3.8`). All other EKU values **MUST NOT** be present.
Digital Signing	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-documentSigning (1.3.6.1.5.5.7.3.36) • id-kp-clientAuth (1.3.6.1.5.5.7.3.2) 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) All other EKU **MAY** be present.

7.1.2.2.2 Certificate Policies

The certificatePolicies extension **SHALL** be included in all Subordinate CA Certificates issued by MSC Trustgate. The policy identifiers and qualifiers included in this extension **SHALL** reflect the policies under which the Subordinate CA is authorized to issue Subscriber Certificates.

7.1.2.2.2.1 For Publicly Trusted Certificates

(TLS Server, S/MIME, Code Signing, and Timestamping)

The `certificatePolicies` extension **MUST** contain at least two `PolicyInformation` values:

i. The first `PolicyInformation` value **SHALL** contain a `policyIdentifier` that corresponds to the applicable **CA/Browser Forum** reserved certificate policy OID (See Section 7.1.6). This `policyIdentifier` **SHALL NOT** include `policyQualifiers`.

ii. The second `PolicyInformation` value **SHALL** contain a policy identifier that corresponds to the applicable MSC Trustgate certificate policy OID (See Section 7.1.6). This `policyIdentifier` **MUST** include `policyQualifiers` as specified in Section 7.1.8.

7.1.2.2.2.2 For non-Publicly Trusted Certificates

The `certificatePolicies` extension **MUST** contain a policy identifier that corresponds to the applicable MSC Trustgate certificate policy OID (See Section 7.1.6). This `policyIdentifier` **MUST** include `policyQualifiers` as specified in Section 7.1.8.

7.1.2.3 Subscriber (End-user) Certificates

This section specifies the certificate extensions that **SHALL** be included in Subscriber Certificates issued by MSC Trustgate. These extensions are categorized into common extensions, which apply to all or most certificates, and specific extensions, which are applicable only to certain certificate types

7.1.2.3.1 Common Extensions

The following extensions **MUST** be included in all Subscriber Certificates unless a specific certificate type profile states otherwise.

Extension	Critical	Value or Value Constraint
`basicConstraints`	TRUE	`cA` **MUST** be `FALSE`, `pathLenConstraint` **MUST NOT** be present.
`keyUsage`	TRUE	**SHALL** be present. The specific bits for this extension vary based on the certificate type, as detailed in Section 7.1.2.3.3.
`subjectKeyIdentifier`	FALSE	**SHALL** be present. The value **SHALL** be the SHA-1 hash of the subject public key (excluding tag, length, and unused bits).
`authorityKeyIdentifier`	FALSE	**MUST** be present. The `keyIdentifier` **MUST** be identical to the `subjectKeyIdentifier` of the Issuing CA. `authorityCertIssuer` and `authorityCertSerialNumber` **MUST NOT** be present.
`cRLDistributionPoints`	FALSE	**MUST** be present. This extension **MUST** contain a `URI` to the CRL for this Certificate.
`authorityInfoAccess`	FALSE	**MUST** be present. This extension **MAY** contain one or more `accessMethod` values of type `id-ad-ocsp` (`1.3.6.1.5.5.7.48.1`) that specify the URI of the Issuing CA's OCSP responder. This extension **SHOULD** contain at least one `accessMethod` value of type `id-ad- caIssuers` (`1.3.6.1.5.5.7.48.2`) that specifies the URI of the Issuing CA's Certificate.

7.1.2.3.2 Other Extensions

The following extensions **MAY** be included in Subscriber Certificates, subject to the constraints specified for each certificate type.

Extension	Certificate Type	Critical	Value or Value Constraint
`extKeyUsage`	All	Varies	**MAY** be present. The specific constraints for this extension vary based on the certificate type and are detailed in Section 7.1.2.3.4.
`certificatePolicies`	All	FALSE	**MAY** be present. The specific constraints for this extension vary based on the certificate type and are detailed in Section 7.1.2.3.5.
`subjectAltName`	TLS Server	FALSE	**MUST** be present and contain at least one entry. • The `dNSName` entry SHALL contain either a Fully-Qualified Domain Name or Wildcard Domain Name validated in accordance with Section 3.2.4. • The `iPAddress` entry SHALL contain a validated IPv4 or IPv6 address.

Extension	Certificate Type	Critical	Value or Value Constraint
`subjectAltName`	S/MIME	FALSE	**MUST** be present and contain at least one `GeneralName` entry of of the following type: • `rfc822Name` and/or • `otherName` of type `id-on-SmtpUTF8Mailbox`. The email address **SHALL** be validated in accordance with Section 3.2.3. All Mailbox Addresses in the `subject` field or `dirName` entries **SHALL** be repeated here.

7.1.2.3.3 Key Usage

The `keyUsage` extension **MUST** be present and marked Critical (`TRUE`) in all Subscriber Certificates. MSC Trustgate **SHALL** set the following bits based on the intended certificate purpose. All bits not listed as **MUST** or **MAY** for a specific Certificate Type **MUST NOT** be set.

Certificate Type	digitalSignature (0)	nonRepudiation (1)	keyEncipherment (2)	keyAgreement (4)
TLS Server (RSA)	MUST	MUST NOT	MUST	MUST NOT
TLS Server (ECC)	MUST	MUST NOT	MUST NOT	MUST
S/MIME Signing	MUST	MAY	MUST NOT	MUST NOT
S/MIME Encryption (RSA)	MUST NOT	MUST NOT	MUST	MUST NOT
S/MIME Encryption (ECC)	MUST NOT	MUST NOT	MUST NOT	MUST
S/MIME Signing & Encryption (RSA)	MUST	MAY	MUST	MUST NOT
S/MIME Signing & Encryption (ECC)	MUST	MAY	MUST NOT	MUST
Code Signing	MUST	MAY	MUST NOT	MUST NOT
Timestamping	MUST	MUST NOT	MUST NOT	MUST NOT
Digital Signing	MUST	MUST	MUST NOT	MUST NOT
OCSP Responder	MUST	MUST NOT	MUST NOT	MUST NOT

Note: *The* `encipherOnly (7)` *and* `decipherOnly (8)` *bits are only used in conjunction with* `keyAgreement`. *If* `keyAgreement` *is set, the* `encipherOnly` *and/or* `decipherOnly` *bits* ***MUST BE SET*** *if the key is used only for enciphering or deciphering, respectively, during key agreement. Otherwise, they* ***MUST NOT BE SET****.*

7.1.2.3.4 Extended Key Usage (EKU)

The `extKeyUsage` extension **MUST** be present in all Subscriber Certificates. The specific Extended Key Usage OIDs are defined by the intended purpose of the certificate and **SHALL** be a subset of the EKU values present in the issuing Subordinate CA Certificate (as detailed in Section 7.1.2.2.1).

Certificate Type	Criticality	Required EKU OID(s)	Prohibited EKU OID(s)
TLS Server	FALSE	**MUST** contain `id-kp-serverAuth` (`1.3.6.1.5.5.7.3.1`).	All other EKU values **MUST NOT** be present.
TLS Client	FALSE	**MUST** contain id-kp-clientAuth (1.3.6.1.5.5.7.3.2).	All other EKU **MUST NOT** be present.

Certificate Type	Criticality	Required EKU OID(s)	Prohibited EKU OID(s)
S/MIME	FALSE	**SHALL** contain `id-kp-emailProtection` (`1.3.6.1.5.5.7.3.4`). All other EKU values **MAY** 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`)
Code Signing	FALSE	**MUST** contain `id-kp-codeSigning` (`1.3.6.1.5.5.7.3.3`). The following EKU values **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`)	All other EKU values **SHOULD NOT** be present.
Timestamping	TRUE	**MUST** contain `id-kp-timeStamping` (`1.3.6.1.5.5.7.3.8`).	All other EKU values **MUST NOT** be present.
Digital Signing		**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-documentSigning (1.3.6.1.5.5.7.3.36) • id-kp-clientAuth (1.3.6.1.5.5.7.3.2)	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)

7.1.2.3.5 Certificate Policies

The certificatePolicies extension MUST be present in all Subscriber Certificates. The policy identifiers included SHALL be consistent with the issuing Subordinate CA Certificate (as defined in Section 7.1.2.2.2).

7.1.2.3.6 Certificate Policies

The `certificatePolicies` extension **SHALL** be included in all Subordinate CA Certificates issued by MSC Trustgate. The policy identifiers and qualifiers included in this extension **SHALL** reflect the policies under which the Subordinate CA is authorized to issue Subscriber Certificates.

7.1.2.3.6.1 For Publicly Trusted Certificates

(TLS Server, S/MIME, Code Signing, and Timestamping)

The `certificatePolicies` extension **MUST** contain at least two `PolicyInformation` values:

iii. The first `PolicyInformation` value **SHALL** contain a `policyIdentifier` that corresponds to the applicable **CA/Browser Forum** reserved certificate policy OID (See Section 7.1.6). This `policyIdentifier` **SHALL NOT** include `policyQualifiers`.

iv. The second `PolicyInformation` value **SHALL** contain a policy identifier that corresponds to the applicable MSC Trustgate certificate policy OID (See Section 7.1.6). This `policyIdentifier` **MUST** include `policyQualifiers` as specified in Section 7.1.8.

7.1.2.3.6.2 For non-Publicly Trusted Certificates

The `certificatePolicies` extension **MUST** contain a policy identifier that corresponds to the applicable MSC Trustgate certificate policy OID (See Section 7.1.6). This `policyIdentifier` **MUST** include `policyQualifiers` as specified in Section 7.1.8.

7.1.2.4 OCSP Responder Certificates

OCSP Responder Certificates are a specialized form of Subscriber Certificate used solely for digitally signing OCSP responses. They MUST comply with the following constraints:

Extension	Critical	Value or Value Constraint
`basicConstraints`	TRUE	`cA` **MUST** be `FALSE`, `pathLenConstraint` **MUST NOT** be present.
`keyUsage`	TRUE	**MUST** be set to `digitalSignature` (0) and MUST NOT include any other bit.. The specific bits for this extension vary based on the certificate type, as detailed in Section 7.1.2.3.3.
`subjectKeyIdentifier`	FALSE	**MUST** be present. The value **SHALL** be the SHA-1 hash of the subject public key (excluding tag, length, and unused bits).
`authorityKeyIdentifier`	FALSE	**MUST** be present. The `keyIdentifier` **MUST** be identical to the `subjectKeyIdentifier` of the Issuing CA. `authorityCertIssuer` and `authorityCertSerialNumber` **MUST NOT** be present.
`cRLDistributionPoints`	FALSE	**MUST** be present. This extension **MUST** contain a `URI` to the CRL for this Certificate.
`authorityInfoAccess`	FALSE	**MUST** be present. This extension **SHOULD NOT** contain `id-ad-ocsp` (`1.3.6.1.5.5.7.48.1`) `accessMethod` if the `id-pkix-ocsp-nocheck` extension is present. This extension **SHOULD** contain at least one `accessMethod` value of type `id-ad-caIssuers` (`1.3.6.1.5.5.7.48.2`) that specifies the URI of the Issuing CA's Certificate.
`extKeyUsage`	FALSE	**MUST** contain `id-kp-OCSPSigning` (`1.3.6.1.5.5.7.3.9`) and **MUST NOT** contain any other EKU OID, including `anyExtendedKeyUsage`.
`certificatePolicies`	FALSE	**MUST** contain the applicable MSC Trustgate Policy OID (as detailed in Section 7.1.6).
`id-pkix-ocsp-nocheck`	FALSE	**SHOULD** be present. This extension asserts that no revocation checking is required for this specific certificate.

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: 300b06096086480165030403 11
   ii. For ML-DSA-65: 300b06096086480165030403 12
   iii. For ML-DSA-87: 300b06096086480165030403 13

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: 300b06096086480165030403 14
   ii. SLH-DSA-SHA2-128f: 300b06096086480165030403 15
   iii. SLH-DSA-SHA2-192s: 300b06096086480165030403 16
   iv. SLH-DSA-SHA2-192f: 300b06096086480165030403 17
   v. SLH-DSA-SHA2-256s: 300b06096086480165030403 18
   vi. SLH-DSA-SHA2-256f: 300b06096086480165030403 19

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.

7.1.3.1.6 KAZ-Sign

The KAZ-Sign algorithm is a Post-Quantum Cryptography (PQC) digital signature algorithm developed under the MySEAL initiative. Its use is constrained as follows:

1. **Algorithm Identifiers**: The CA **SHALL** indicate the use of a KAZ-Sign key by using one of the following algorithm identifiers:
    a. KAZ-SIGN 128 (OID: **1.3.6.1.4.1.62395.1.2.1**)
    b. KAZ-SIGN 192 (OID: **1.3.6.1.4.1.62395.1.2.2**)
    c. KAZ-SIGN 256 (OID: **1.3.6.1.4.1.62395.1.2.3**)
2. **Parameters Constraint**: The **parameters** field within the SubjectPublicKeyInfo's `AlgorithmIdentifier` for KAZ-Sign keys **SHALL** be either **absent** or an **explicitly encoded NULL** value, as defined by the KAZ-Sign cryptographic specification.
3. **Key Usage Restriction**: KAZ-Sign **MUST** be used only for National Digital Identity, Document Signing. KAZ-Sign **MUST NOT** be used for publicly trusted TLS Server, S/MIME, Code Signing or Time-Stamping certificates.
4. **Practice**: MSC Trustgate's practice is to ensure compliance with the specified OIDs and usage restrictions for KAZ-Sign.

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: 300b060960864801650304031 1.
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: 300b060960864801650304031 2.
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: 300b060960864801650304031 3.

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 300b060960864801650304031 4.
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 300b060960864801650304031 5.
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 300b060960864801650304031 6.
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 300b060960864801650304031 7.
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 300b060960864801650304031 8.
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 300b060960864801650304031 9.

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.

7.1.3.2.6 KAZ-Sign Signatures

This section defines the signature algorithm identifiers used when signing certificates and CRLs with the KAZ-Sign algorithm.

1. **Algorithm Identifiers**: The CA **SHALL** use the following algorithm identifiers to indicate the KAZ-Sign signature scheme. These OIDs implicitly define the hash function used for the signature (e.g., KAZ-SIGN 256 uses the KAZ signature scheme with a 256-bit security level).
    a. KAZ-SIGN 128 (OID: **1.3.6.1.4.1.62395.1.2.1**)
    b. KAZ-SIGN 192 (OID: **1.3.6.1.4.1.62395.1.2.2**)
    c. KAZ-SIGN 256 (OID: **1.3.6.1.4.1.62395.1.2.3**)
2. **Parameters Constraint**: The parameters field within the `SignatureAlgorithmIdentifier` **SHALL** be either **absent** or an **explicitly encoded NULL** value, as defined by the KAZ-Sign cryptographic specification.
3. **Usage**: The KAZ-Sign signature algorithms **SHALL** be used for issuing National Digital Identity, Document Signing using the KAZ-Sign key type. They **MUST NOT** be used for certificates or CRLs signed by RSA or ECC key types.

7.1.4 Name Forms

This section defines the encoding rules and the required or prohibited components within the **Subject and Issuer Distinguished Names (DNs)** of all certificates issued by MSC Trustgate. All name fields within the DNs **SHALL** be encoded in accordance with **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 Root and Subordinate CA Certificates

MSC Trustgate's policy is to adhere to the following Subject Distinguished Name requirements when issuing Root and Subordinate CA Certificates. When issuing any CA Certificate, MSC Trustgate **SHALL** ensure all Subject Information is accurate and verified in accordance with the procedures outlined in Section 3.2.2.

Field	OID	Encoding	Content & Constraint
`commonName (CN)`	2.5.4.3	`UTF8String`	**MUST** be present. This field **SHALL** contain an identifier such that the Certificate's **Name is unique** across all Certificates issued by the Issuing CA. For Root CAs, the name **SHALL** clearly identify MSC Trustgate.
`organizationName (O)`	2.5.4.10	`UTF8String`	**MUST** be present. This field SHALL contain the Subject CA's legal name or DBA, as verified under Section 3.2.2.
`countryName (C)`	2.5.4.6	`PrintableString`	**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 legally located.
`organizationIdentifier`	2.5.4.97	`UTF8String`	**MAY** be present. If present, this field **SHALL** contain a unique legal entity identifier (See Appendix A.1) and **MUST** be verified in accordance with Section 3.2.2.
`Organizational Unit (OU)`	2.5.4.11	`UTF8String`	**MUST NOT** be present in publicly trusted CA certificates. If required for specific national or closed-system profiles, it **MAY** be present, but the information **MUST** be verified in accordance with Section 3.2.2.
`Locality (L)`	2.5.4.7	`UTF8String`	**MAY** be present. If present, the information **MUST** be verified in accordance with Section 3.2.2.
`State/Province (ST)`	2.5.4.8	`UTF8String`	**MAY** be present. If present, the information **MUST** be verified in accordance with Section 3.2.2.
Other Subject Attributes	Varies	Varies	**MUST NOT** be present unless explicitly permitted by the relevant Certificate Profile or a superior policy document. If present, verification **MUST** be performed.

7.1.4.3 Subscriber (End-user) Certificates

MSC Trustgate's policy governs the issuance of Subscriber Certificates as follows:

1. **Verification Assurance**: When issuing a Certificate, MSC Trustgate **SHALL** affirm that all Subject Information was accurate and verified in accordance with the procedures outlined in Section 3.2 as of the certificate's issuance date.
2. **Attribute Content Constraint**: Subject attributes **SHALL NOT** consist solely of metadata, such as '.', '-', and ' ' (space) characters, or any other value suggesting the absence, incompleteness, or inapplicability of the field.
3. **Distinguished Name Fields**: MSC Trustgate utilizes the following Subject Distinguished Name fields for its Subscriber Certificates.

Field	OID	Encoding	Content & Constraint
`commonName (CN)`	2.5.4.3	`UTF8String`	The content **SHALL** consist of a Personal Name, Pseudonym, Email Address, Fully Qualified Domain Name (FQDN), or the value of the subject:organizationName field. The content **MUST** be verified in accordance with Section 3.2.
`serialNumber`	2.5.4.5	`PrintableString`	The content **SHALL** consist of: • a Natural Person Identifier assigned by the country such as MyKad Number, Passport Number, • a Business Registration Number for a Legal Entity assigned by an authority. • a membership number of Professional Organization (such medical, architect) • an identifier assigned by the CA or RA to identify and/or to disambiguate the Subscriber. The content **MUST** be verified in accordance with Section 3.2.
`countryName (C)`	2.5.4.6	`PrintableString`	This field **SHALL** 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).
`localityName (L)`	2.5.4.7	`UTF8String`	The content **SHALL** consist of the Subject's locality information as verified under Section 3.2.2 (for an organization) or Section 3.2.3 (for an individual).
`stateOrProvinceName (ST)`	2.5.4.8	`UTF8String`	The content **SHALL** consist of 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).
`organizationName (O)`	2.5.4.10	`UTF8String`	The content **SHALL** consist of the Subject's full legal organization name and/or an Assumed Name as verified under Section 3.2.2.

Field	OID	Encoding	Content & Constraint
`Organizational Unit (OU)`	2.5.4.11	`UTF8String`	**MUST NOT** be present in publicly trusted CA certificates. If required for specific national or closed-system profiles, it **MAY** be present, but the information **MUST** be verified in accordance with Section 3.2.2.
`Title (T)`	2.5.4.12	`UTF8String`	The content **SHALL** consist of an organizational role/title or a regulated professional designation verified according to Section 3.2.2.
`pseudonym`	2.5.4.65	`UTF8String`	The content **SHALL** consist of a unique identifier linked to an Individual in a **pseudonymized manner** when specific privacy conditions are required. The field **SHALL** be verified according to Section 3.1.3. The field **SHALL NOT** be present if the `subject:givenName` and/or `subject:surname` are present.
`organizationIdentifier`	2.5.4.97	`UTF8String`	This field **SHALL** contain a unique legal entity identifier (See Appendix A.1) and **MUST** be verified in accordance with Section 3.2.2.
`emailAddress (E)`	1.2.840.113549.1.9.1	`IA5String`	**MUST NOT** be present in TLS/SSL certificates. **MAY** be present in S/MIME or Document Signing certificates. The content **SHALL** consist of single Mailbox Address as verified under Section 3.2.4.
Other Subject Attributes	Varies	Varies	**MUST NOT** be present unless explicitly permitted by the relevant Certificate Profile or a superior policy document. If present, verification **MUST** be performed.

7.1.5 Name Constraints

This section defines the mandatory constraints applied to Subordinate CA Certificates to ensure they are **Technically Constrained** in accordance with this CP/CPS.

7.1.5.1 Technically Constrained Subordinate CA Certificates

1. **Extended Key Usage (EKU) Constraint**: For a Subordinate CA Certificate to be considered Technically Constrained, the Certificate **SHALL** include an EKU extension that specifies all extended key usages for which the Subordinate CA Certificate is authorized to issue Certificates.
2. **Wildcard Exclusion**: The `anyExtendedKeyUsage KeyPurposeId` **SHALL NOT** appear within the EKU extension. MSC Trustgate **MUST** explicitly populate the EKU extension with only the authorized key usages.

7.1.5.2 Constraints for Email Protection

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:

Constraint Type	Rule & Enforcement
`rfc822Name` (Format)	For each rfc822Name in permittedSubtrees, it **SHALL** contain either a fully qualified domain name (FQDN) or a U+002E FULL STOP (".") character followed by a FQDN. The rfc822Name SHALL NOT contain an email address.
`rfc822Name` (Verification)	MSC Trustgate **SHALL** confirm that the Applicant has registered the FQDN or has been authorized by the domain registrant to act on their behalf (in line with Section 3.2.5).
`directoryName`	For each `directoryName` in `permittedSubtrees`, the MSC Trustgate **SHALL** confirm the Applicant's and/or Subsidiary's Organizational name and location to ensure end-entity Certificates issued from this CA are compliant with the requirements of this CP/CPS.

7.1.6 Certificate Policy Object Identifier

Subordinate CA Certificates and Subscriber Certificates **SHALL** use a Policy Object Identifier (OID) within the `certificatePolicies` extension to indicate the policy under which the certificate was issued.

For Publicly Trusted Certificates, the certificate SHALL contain the CA/Browser Forum Baseline Requirements OID and the corresponding MSC Trustgate proprietary OID.

Certificate Types	Policy Identifier
Digital Signing Certificates (Generic)	• 1.3.6.1.4.1.49530.1.1.2
Digital Signing Certificates (Government)	• 1.3.6.1.4.1.49530.1.1.2.1
Digital Signing Certificates (MyGPKI)	• 1.3.6.1.4.1.49530.1.1.2.1.1
Digital Signing Certificates (Sarawakpass)	• 1.3.6.1.4.1.49530.1.1.2.1.2
Digital Signing Certificates (Basic)	• 1.3.6.1.4.1.49530.1.1.2.2.1 #
Digital Signing Certificates (Pro)	• 1.3.6.1.4.1.49530.1.1.2.2.2 #
Digital Signing Certificates (Organization)	• 1.3.6.1.4.1.49530.1.1.2.3 #
AATL Certificates (Individual Basic)	• 1.3.6.1.4.1.49530.1.1.2.4.1
AATL Certificates (Individual Pro)	• 1.3.6.1.4.1.49530.1.1.2.4.2
AATL Certificates (Organization)	• 1.3.6.1.4.1.49530.1.1.2.4.3
LHDN e-Invoice Organization Certificates	• 1.3.6.1.4.1.49530.1.1.2.5
AATL Certificates	• 1.3.6.1.4.1.49530.1.1.3 ^
Digital Signing Certificate (High Assurance)	• 1.3.6.1.4.1.49530.1.1.4
Code Signing Certificates	• 2.23.140.1.4.1 * • 1.3.6.1.4.1.49530.1.2.1
EV 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
DV TLS Server Certificates	• 2.23.140.1.2.1 * • 1.3.6.1.4.1.49530.1.4.1
EV TLS Server Certificates	• 2.23.140.1.2.2 * • 1.3.6.1.4.1.49530.1.4.2
Extended Validation TLS Server Certificates	• 2.23.140.1.1 * • 1.3.6.1.4.1.49530.1.4.3
Intranet Validation TLS Server 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
MyDigital ID	• 1.3.6.1.4.1.49530.1.1.3 • 1.3.6.1.4.1.49530.1.6.1 α
Sarawakpass Digital Identity	• 1.3.6.1.4.1.49530.1.6.2
Device Certificates (Generic)	• 1.3.6.1.4.1.49530.1.7.1
Device Certificates (TLS Client)	• 1.3.6.1.4.1.49530.1.7.2
Device Certificates (Sarawakpass Service Provider)	• 1.3.6.1.4.1.49530.1.7.3

* *CA/Browser Forum reserved policy OIDs*, α *For MyDigital ID Certificates Issued by MyDigital ID CA*

\# *Effective 2 August 2025*, ^ *For AATL Certificates Issued by MyTrust Class 3 ECC Enterprise CA*

For Certificates **NOT** intended for public trust, the CA/Browser Forum reserved policy OIDs **SHALL NOT** be used.

7.1.7 Usage of Policy Constraints Extension

No Stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

This section specifies the use of policy qualifiers within the `certificatePolicies` extension.

The `policyQualifiers` sequence **MAY** be included in a `PolicyInformation` value to provide additional information about the policy. When included, the following qualifiers **SHALL** be used:

- `cPSuri`: If present, this qualifier **SHALL** contain a URI pointing to the published MSC Trustgate CP/CPS document located at https://www.msctrustgate.com/tgcps.
- `userNotice`: If present, this qualifier **SHALL** contain a `userNotice` field that includes a `explicitText` containing the following descriptive text, based on the certificate type:
    - **For Certificates governed by the Malaysia Digital Signature Act 199**7:

        "This Certificate has been issued by a Licensed Certification Authority in Malaysia, MSC Trustgate.com Sdn. Bhd., under the Digital Signature Act 1997."

    - **For all other Certificates**:

        "This Certificate has been issued by a Licensed Certification Authority in Malaysia, MSC Trustgate.com Sdn. Bhd."

7.1.9 Processing Semantics for the Critical Certificate Policies

No Stipulation.

7.1.10 Other Certificate Profiles

7.1.10.1 Certificate Validity

`notBefore` **SHALL** be the date of signing, with the time set to `00:00:00` Greenwich Mean Time (**GMT**).

`notAfter` **SHALL** be a date calculated by adding a specific number of days to the date of signing, with the time set to `23:59:59` **GMT**. Furthermore, this date **MUST NOT** surpass the `notAfter` date of its issuer. The exact number of days varies depending on the certificate type, as specified in the table in Section 6.3.2.

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	• TLS Server Certificates: Less than 398 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, for 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.

7.2 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 that conform to RFC 6960.

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 undergoes an annual period audit by an independent external auditor to assess compliance with this CP/CPS and one of the audit schemes defined in Section 8.4. The audit **SHALL** cover the full scope of MSC Trustgate's **PKI** operations, including the **CA**, **RA**, and processes related to **Subscribers**.

Audits **SHALL** be conducted over unbroken sequences of audit periods with each period no longer than one (1) year.

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 a qualified auditor by the Malaysian Communications & Multimedia Commission (MCMC). The list of qualified auditors can be found at: 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 **SHALL** cover 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 **SHALL** undergo an audit in accordance with one of the following schemes:

1. WebTrust for Certification Authorities (latest version); including criteria for:
    a. WebTrust for CA – Network Security
    b. WebTrust for CA – S/MIME
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.
iii. MSC Trustgate will develop a plan to cure the noncompliance.

MSC Trustgate will submit the plan to the **ISC** for approval and to any third party that MSC Trustgate is legally obligated to satisfy. The **ISC 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 services through revocation or other actions as deemed by the **ISC** to address the non-compliant **Issuer CA**.

8.6 Communication of Results

The results of each audit are reported to the ISC 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/repository. On an annual basis and within three months of completion, MSC Trustgate submits copies of relevant audit compliance reports to various parties, such as the Malaysian Communications and Multimedia Commission (**MCMC**), Mozilla, Adobe, and other relying bodies. 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 labeled 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 MSC Trustgate **SHALL** 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 **SHALL** ensure 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 for Medium Assurance certificates **SHALL NOT** exceed Ringgit Malaysia One Hundred Twenty (RM 120). For High Assurance certificates, the fee **SHALL NOT** exceed Ringgit Malaysia One Thousand Five Hundred (RM 1500). Fees **SHALL NOT** include government tax, postage, public notary fees, storage, signing services, date/time stamping services, or other additional services.

9.1.2 Certificate Access Fees

MSC Trustgate **SHALL 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 **SHALL 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 **SHALL NOT** permit access to revocation information, Certificate status information, or time stamping in its repositories by third parties that provide products or services which utilize such Certificate status information without MSC Trustgate's prior express written consent.

9.1.4 Fees for Other Services

MSC Trustgate **SHALL 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

The following refund policy is in effect for MSC Trustgate's Certification Domain:

If a subscriber is not completely satisfied with the certificate issued, the subscriber **MAY** request that MSC Trustgate 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.

Upon revocation of the subscriber's certificate, MSC Trustgate **SHALL** promptly credit the subscriber's credit card account (if payment was made via credit card) or otherwise reimburse the subscriber via cheque or another agreed method for the full amount of the applicable fees paid for the certificate. To request a refund, please contact customer service via the contact methods specified on the MSC Trustgate website. 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's liability for issued certificates is limited and **SHALL NOT** exceed the amount specified in 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 treated as confidential and private ("Confidential 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 the information contained within them are not considered Confidential Information. Information not expressly deemed Confidential 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 SHALL secure confidential 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 located 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 local laws, all information made public in a certificate is deemed not private.

9.4.4 Responsibility to Protect Private Information

MSC Trustgate PKI participants receiving private information **SHALL** secure it from being compromised and disclosed 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 processes 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 participants.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The CA warrants that:

i. The Subscriber 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. 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.
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 **SHALL** obtain, for the explicit benefit of MSC Trustgate 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.
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

MSC Trustgate's liability for issued Certificates is explicitly limited. To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements SHALL limit MSC Trustgate's liability.

In no event SHALL MSC Trustgate be liable to any Subscriber, Relying Party, or any other third party for any indirect, incidental, special, or consequential damages, including loss of profit, revenue, data, or business opportunities, regardless of the cause of action and even if MSC Trustgate has been advised of the possibility of such damages.

Furthermore, MSC Trustgate SHALL NOT be liable for any damages or losses arising from:

i. Fraud or intentional misconduct by an Applicant or Subscriber.
ii. The use of a Certificate beyond its intended purpose, specified usage limitations, value, or transaction limits, as outlined in the Certificate or this CP/CPS.
iii. The security, usability, or integrity of any products or hardware not provided by MSC Trustgate.
iv. The compromise or misuse of a Subscriber's Private Key.

Liability is limited to actual and direct damages, subject to the caps outlined below:

- 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 of Subscribers, RAs, and Relying Parties SHALL be as set forth in their respective agreements with MSC Trustgate.

9.8.2 RA Liability

RAs SHALL be subject to the same liabilities as applicable to MSC Trustgate, as listed in Section 9.8.1, in the event of a violation of this CP/CPS that causes damage. The specific liabilities and their limitations for each RA SHALL be further defined in the separate agreement between MSC Trustgate and the respective RA.

9.9 Indemnities

MSC Trustgate **SHALL NOT** indemnify any other party. Instead, other parties **SHALL** indemnify MSC Trustgate as described in this Section.

9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, **Subscriber Agreements SHALL** require Subscribers to indemnify MSC Trustgate for any claims, damages, or losses arising from:

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 their 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.

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.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, **Relying Party Agreements SHALL** require Relying Parties to indemnify MSC Trustgate for any claims, damages, or losses arising from:

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.
iii. The Relying Party's failure to check the status of a Certificate to determine if it is expired or revoked.

The applicable **Relying Party Agreement** may include additional indemnity obligations.

9.10 Term and Termination

9.10.1 Term

This CP/CPS **SHALL** be effective upon its publication in the MSC Trustgate repository and **SHALL** remain in effect until it is formally terminated or superseded by a new version. All amendments **SHALL** become effective upon their publication in the same repository.

9.10.2 Termination

This CP/CPS **MAY** be terminated or superseded by a new version published in the MSC Trustgate repository. In the event of a full termination of the CP/CPS without a replacement, MSC Trustgate **SHALL** issue a formal notice of termination, which will be published in the repository.

9.10.3 Effect of Termination and Survival

Upon termination of this CP/CPS, the terms contained herein **SHALL** nevertheless remain binding on MSC Trustgate and all PKI participants for all certificates issued for the remainder of their validity periods. This ensures that the original terms under which the certificates were issued continue to apply even if the policy document is no longer in effect.

9.11 Individual Notices and Communications with Participants

MSC Trustgate **SHALL** accept notices related to this CP/CPS at the locations specified in Section 2.2. A notice is deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from MSC Trustgate. If an acknowledgment of receipt is not received within five (5) business days, the sender **SHALL** resend the notice in paper form to the street address specified in Section 2.2 using a courier service that confirms delivery or via registered mail with postage prepaid and return receipt requested. MSC Trustgate **MAY** permit alternative forms of notice in its **Subscriber Agreements**.

9.11.1 Root Store Program Notifications

MSC Trustgate SHALL provide advance notice to various root store programs regarding material changes.

1. **Adobe AATL Program**: MSC Trustgate **SHALL** notify Adobe at least 30 days in advance of any updates or changes with the potential to affect compliance with the AATL program, including:
    a. Additions of Root CAs and Subordinate CAs.
    b. Additional CP/CPS at the Root CA level.
    c. Changes in Certificate issuance procedures.
    d. Terminations or transition of ownership of Root CAs or Subordinate CAs.
2. **Mozilla Root Store Program**: MSC Trustgate **SHALL** notify Mozilla if:
    a. Ownership or control of the CA certificates changes.
    b. 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's included certificate(s).
    c. Ownership or control of MSC Trustgate's operations changes.
    d. 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 **SHALL** be reviewed annually. Amendments to this CP/CPS **SHALL** be made by the MSC Trustgate **Information Security Committee (ISC)**. Amendments **SHALL** be published in the form of a new, amended version of the CP/CPS document, which will be linked to the Certificate Policy (CP) and Certification Practice Statement (CPS) section of the MSC Trustgate Repository located at: https://www.msctrustgate.com/repository. A new version of the CP/CPS **SHALL** supersede all designated or conflicting provisions of any prior version. The ISC **SHALL** determine whether changes to this CP/CPS require a change in the Certificate Policy Object Identifiers (OIDs) for each Certificate Type.

9.12.2 Notification Mechanism and Period

MSC Trustgate and the **ISC** reserve the right to amend this CP/CPS without notification for amendments that are not material, including corrections of typographical errors, changes to URLs, and updates to contact information. The **ISC's** decision to designate amendments as material or non-material **SHALL** be within its sole discretion. Proposed material amendments **SHALL** be communicated to PKI participants by their publication in the Certificate Policy (CP) and Certification Practice Statement (CPS) section of the MSC Trustgate Repository.

9.12.3 Emergency Amendments

Notwithstanding anything in this CP/CPS to the contrary, if the **ISC** believes that a material amendment to this CP/CPS is necessary immediately to stop or prevent a breach of the security of MSC Trustgate or any portion of its **PKI**, MSC Trustgate and the **ISC SHALL** be entitled to make such amendments by immediate publication in the MSC Trustgate Repository. Such amendments **SHALL** be effective immediately upon publication. Within a reasonable time after publication, MSC Trustgate **SHALL** provide notice of such amendments to all participants in the Certification Domain.

9.12.4 Circumstances under which OID must be changed

If the **ISC** determines that a change is necessary in the OID corresponding to a Certificate Policy, the amendment **SHALL** contain new OIDs for the Certificate Policies corresponding to each Certificate Type. Otherwise, amendments **SHALL NOT** require a change in the Certificate Policy OID.

9.13 Dispute Resolution Provisions

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements SHALL contain a dispute resolution clause.

Prior to pursuing any formal legal or dispute resolution mechanism, all parties SHALL provide written notice of a dispute to MSC Trustgate and attempt to resolve the matter directly through good faith negotiations for a period of at least sixty (60) days from the date of the notice.

If a dispute is not resolved through negotiation:

- For claimants who are residents of Malaysia, the dispute SHALL be submitted to the courts of Malaysia.
- For all other claimants, the dispute SHALL be resolved by arbitration administered by the Asian International Arbitration Centre (AIAC) in Kuala Lumpur, in accordance with the Rules of AIAC.

9.14 Governing Law

This CP/CPS and its application **SHALL** be governed by and construed in accordance with the laws of Malaysia.

9.15 Compliance with Applicable Law

All participants in the Certification Domain **SHALL** comply with applicable law in their respective jurisdictions. MSC Trustgate is obliged to adhere to applicable Malaysian legislation, including but not limited to the **Digital Signature Act 1997** (**Act 562**) and the **Digital Signature Regulations 1998**.

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 is subject to the **Personal Data Protection Act 2010** (**Act 709**) and is a registered party with the **Jabatan Perlindungan Data Peribadi** (**JPDP**). All participants in the **Certification Domain SHALL** comply with the obligations stipulated in this act regarding the protection of personal data.

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.

APPENDIX C: CA CERTIFICATES

C.1: Root CA Certificates

#	Subject DN	SHA256 Thumbprint	Serial Number	Subject Key Identifier	Key Size	Signature Algorithm	Validity
1.	CN = Trustgate Class 2 Root Certificate Authority O = MSC Trustgate.com Sdn. Bhd. C = MY	E2026B5646F49F9671D4318E09094A23CE34C94B5410F19B39D490A761CA65D1	0A8BC4060F5A6CD34D07805DA007ABF5	2a3d3b9f9d04906ae10124c53951d15b95705166	RSA (2048 Bits)	sha256RSA	30 Years
2.	CN = Trustgate RSA Certification Authority OU = Malaysia Licensed CA No LPBP-2/2010 (1) O = MSC Trustgate.com Sdn. Bhd. C = MY	DC7ACA56E0921E3C54E7DA854A13CDE917B3EEC386B8E9D59201F812E4E9B40C	703B113DCDB38E30F4E57DAC18A5310F	682d2c5f3ee2d6832a4156e3492cb822199a34f4	RSA (4096 Bits)	sha256RSA	25 Years
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	51e80251ad3e7ff755cac506ddb64bde	53fcea6b6f9221160a1f7243dde349fec433e0e8	ECC (384 Bits)	sha384ECDSA	25 Years
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	4139bac7f7f45005dcd7f76adebf17b1	48dc4e36de951aab57394f5335eb341aae9aca09	RSA (4096 Bits)	sha256RSA	25 Years
5.	CN = MyTrust Class 2 ECC Root CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	97351977E28FD6602FE1ADAE58E8994212CB02D995F866D2F5DC41D9E946B855	601d50352ffca3c4abd91c3f32522933	9173b201a3d2b94012c6630ddff5d58e7319b196	ECC (384 Bits)	sha384ECDSA	25 Years

#	Subject DN	SHA256 Thumbprint	Serial Number	Subject Key Identifier	Key Size	Signature Algorithm	Validity
6.	CN = MyTrust Class 3 ECC Root CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	BFAEC1F8E11BD4840A91472E80040F568970FD48B28F09AF018383AF9B0F9D1F	3f9289237e806a1da7326edc082052d3	130885330660934c9bd33695a6c3d775fd8ad9de	ECC (384 Bits)	sha384ECDSA	25 Years
7.	CN = MyTrust Class 2 RSA Root CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	A788D9F9EBE7648CFED6D8B071382A30780D9719A802731F066F59B32124A8B3	01f6e41a6cecc7338dc6fb31ad68a10b	5ce3bd7f944d92ca1b5a7b424353a60308c50cc2	RSA (2048 Bits)	sha256RSA	25 Years
8.	CN = MyTrust Digital ID Root CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd C = MY	D21BECEBF35470585672E8F5721697F71C7CC4D731C4A0FCCDB1A18FCB5691FA	68a309b10ae497b9a91eaf8b35a5e87b	fc06aac4b0f749c206b54a2c646dfd5260c4d937	ECC (384 Bits)	sha384ECDSA	25 Years
9.	CN = Trustgate RSA Global Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	D2BE160D6A4391630BCEE932993E48547C9CABFE21A0B052A60601C8A266C19E	00c17fdf24740cbdd3e69d2dd055962c85	b1e02f97018674843166cabebfcfed4bb8120084	RSA (3072 Bits)	sha384RSA	25 Years
10.	CN = Trustgate Secure Server Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	A233FA00067C0A31EC80793F6F4623DED687E8FD71241FD560BA292D98AB3737	3336f4583b923409818fcf3577b40ece	ab604e47e04232b9794441f682ab37efb9fcb059	RSA (3072 Bits)	sha384RSA	25 Years
11.	CN = Trustgate ID Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	433DB9E222A1EF0AF4F4C4DFAEE76643B9039F1758A13BDFBED36C7290114162	12c0c769d716b6395f0386dfd3a4310f	1623fb16a21d47aebd2149cebfafb69a084defe9	RSA (3072 Bits)	sha384RSA	25 Years
12.	CN = Trustgate MPKI Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	075CEA0ADE7133F67F3EB44815A07E6E4865534901FF1400C42A3C6D3123F95A	009a7ed31d3a6d7959fd3840ec3a3085a0	7b239af4d4285041c6a92550a1cdabaf213a7f38	RSA (3072 Bits)	sha384RSA	25 Years
13.	CN = Trustgate ECC Global Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	AFF58C68DFA45AF80B7D965545E8DC08221E527C8C1090E41270DD9FE7B523D6	00b250e71acf18397b15316921d33ecc49	dee7a462b667a762dadbb2024f7c6c8b088b6f26	ECC (384 Bits)	sha384ECDSA	25 Years

#	Subject DN	SHA256 Thumbprint	Serial Number	Subject Key Identifier	Key Size	Signature Algorithm	Validity
14.	CN = Trustgate ECC Time Stamping Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	BEFD8058D1CE9482799FD62275A2019A84E47F592E1B618D17E563C6540301A4	7dbfaa742a870ecd10441f7e239414d3	68f7475232f55aa586f9c0ee65349fa46c4f2136	ECC (384 Bits)	sha384ECDSA	25 Years
15.	CN = Trustgate ECC ID Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	843C2B01DF6A1FDBAF54F7F640F41187F1818A5E429EB457EF627014AF2F5AD6	5b9d7733c2996ae55cbbbb2deabee4f6	d06744f750fd6f6d08745648472c70762e93c047	ECC (384 Bits)	sha384ECDSA	25 Years
16.	CN = Trustgate ECC MPKI Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	1110EAA11E493C0E9448985D207DC40B7EE2C83EAF087F10BA172E2AC262F2C5	52dfcafca5a2fcac35ebe2e56dfd3a71	21a0d0ea2e5cad02a1c221322992c8e300753770	ECC (384 Bits)	sha384ECDSA	25 Years
17.	CN = Trustgate SMIME RSA Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	504B5D7CD5324FB393817075F3BBDCB990EC4C930CCD35E374F97D426B1DA0EB	12c84b2179f7b95c223e51927c51ee99	03f90b3c5a1dcd44a155a5f8cfe8bb456e24b8d5	RSA (3072 Bits)	sha384RSA	25 Years
18.	CN = Trustgate SMIME ECC Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	0E09801EB903A6F8DE6EF86799296C74B89AB8680C0AF3F2D870EAB6A095F63F	0091deb6bb1345e494052f4d8108d0919e	bd2b7d05bb5f13cca3410cef2ffaa3440c3d756b	ECC (384 Bits)	sha384ECDSA	25 Years
19.	CN = Trustgate SMIME Enterprise RSA Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	4027859768646C2235DD86CDF7D82AC345AA7F71F742DDFACE2A2D6FD51B41AC	4109174639de3a04b828d36ea78d04c0	8c0f3cee93c1ecbbbaba98054cf56fad00c9a749	RSA (3072 Bits)	sha384RSA	25 Years
20.	CN = Trustgate SMIME Enterprise ECC Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	E766F25782559C75324FDCCC53DDED1DE0A7BB16791CCBD0657EA873BECDACCA	7eb1f303670712bdb1d9a7342f64281a	4a2d6d1a968565f42b2c12e79b8210e6403d2823	ECC (384 Bits)	sha384ECDSA	25 Years
21.	CN = Trustgate TLS Basic RSA Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	002D96A8B5E7087B3B3CCC9ECFECF89FAA124DE61F390889C3C5FA29F16A9D6A	18ca67cce70774e9d2c250e954647a2b	83222e8f646af9903a43921d9c76a24dff7a19b8	RSA (3072 Bits)	sha384RSA	25 Years
22.	CN = Trustgate TLS RSA Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	B622543BC97CBDBC8D0890B36C4E613B105A8AF6C69B852B38B7D89B0AE0725B	71d237a2e3e87fcb41f2c1bad4b07d2f	d940c28832be18dec6ca582419db8b01bf843b09	RSA (3072 Bits)	sha384RSA	25 Years

#	Subject DN	SHA256 Thumbprint	Serial Number	Subject Key Identifier	Key Size	Signature Algorithm	Validity
23.	CN = Trustgate TLS High Assurance RSA Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	455FEC3946F62073AFD03C7B701E4188BB54EEB23D438599EAFFA51CAB9F86D5	0ea5a9c064eb815bc018ac1ee0a82fc1	84c1c69f02dad25dd796d880e5992aed144e0380	RSA (3072 Bits)	sha384RSA	25 Years
24.	CN = Trustgate TLS Basic ECC Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	6D0139F87DF6A4E18005AD41E11E29748FF44A7FB7A2429E5A4441AD65225322	00a29d37de5a72c989a01c842f10641601	dc1012f640e72a059269f7d8692a5f89e02b84cf	ECC (384 Bits)	sha384ECDSA	25 Years
25.	CN = Trustgate TLS ECC Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	7E3790A513679E0E21A53B7ECCC0CEC8B8B3649E15ABCD481C5ABB00CD0869AE	64acc74ac2c7ca0940954411db6e4235	d5d6bba6cf96c33b88311856f410085eceb53b9b	ECC (384 Bits)	sha384ECDSA	25 Years
26.	CN = Trustgate TLS High Assurance ECC Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	8FE689549B5A060DFE2C2C7052434C5013CD9BCA106A413EBA9021515BB1E5EB	00f811b549dfee67978ad82b9cf29a8508	11bf629fba9cb7d33ea29e37c38b3015709f8aa3	ECC (384 Bits)	sha384ECDSA	25 Years

C.2: Bridge CA Certificates

#	Subject DN	SHA256 Thumbprint	Serial Number	Subject Key Identifier	Key Size	Signature Algorithm	Validity
1.	CN = Trustgate Secure Server Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	1EA22856E474C9CF5B90F5117E17595A0FBE7E1AA3D172067676BED130C52CE6	1b848f53cde7c3447a4d955a6538b041	ab604e47e04232b9794441f682ab37efb9fcb059	RSA (3072 Bits)	sha384RSA	15 Years
2.	CN = Trustgate ID Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	45CD58326CC8D3637C4586717072A3849AA801B69811639AAE05CD53C1E59BCE	4439e6140906c826b709501bec8785ed	1623fb16a21d47aebd2149cebfafb69a084defe9	RSA (3072 Bits)	sha384RSA	15 Years
3.	CN = Trustgate MPKI Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	8E800BF38414B142440CD175398D29075C6946F0EC048A02357DCC5BEADEA32C	00a9ea80b7d36e51dd8c6fd9d5ccbfa616	7b239af4d4285041c6a92550a1cdabaf213a7f38	RSA (3072 Bits)	sha384RSA	15 Years
4.	CN = Trustgate ECC Time Stamping Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	27A491B41594F31517130E4B7EA94EB38C529358E0987E48849E3F9BC8C6D166	559e48dc4a24dec8df91fbc00a0f6e97	68f7475232f55aa586f9c0ee65349fa46c4f2136	ECC (384 Bits)	sha384ECDSA	15 Years
5.	CN = Trustgate ECC ID Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	FB5EF4B679D073B4D0C4DFA469288A0C3BB949CFF7699A6141B46E2B1EDAC017	53eed85c50effee9195b5606af10c569	d06744f750fd6f6d08745648472c70762e93c047	ECC (384 Bits)	sha384ECDSA	15 Years
6.	CN = Trustgate ECC MPKI Root CA O = MSC Trustgate.com Sdn. Bhd C = MY	C1D86D24AAE0EF5FB7070DFBB685AAC62F0E4420907DA5C26B24BAE96A39BDCE	00880e69fe2dbe15590c75e3a83f8f330a	21a0d0ea2e5cad02a1c221322992c8e300753770	ECC (384 Bits)	sha384ECDSA	15 Years

C.3: Subordinate CA Certificates

#	Subject DN	SHA256 Thumbprint	Serial Number	Subject Key Identifier	Key Size	Signature Algorithm	Validity
1.	CN = MSC Trustgate.com Class 2 MPKI CA O = MSC Trustgate.com Sdn. Bhd. C = MY	CC6ADC88D783574EA3E4F5114FF3AE4DB5B1470934242C62471B124A419C2F94	74f79fea598446997a1cf7d53e0e797a	8a904f921fbd19396012f93fe75f2f5716c42286	RSA (2048 Bits)	sha256RSA	10 Years
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	029f18639809be29e1f9b4d747ed8af4	555caac636b361bf30a441acba2d9bdf58d28401	RSA (2048 Bits)	sha256RSA	10 Years
3.	CN = Bank Negara Malaysia Class 2 CA-G3 O = MSC Trustgate.com Sdn. Bhd. C = MY	A4166F2E0125B553E84CBA1B7D240369AB2A5AB1846C0EF14E2332CEBD39E180	0c0996dcf45f3898f9de146c9fb8c1f2	4cb88bb74bb5b3f92b563685845a1b2f2810b278	RSA (2048 Bits)	sha256RSA	10 Years
4.	CN = INTECH-KLIS CA OU = Remote Signing System O = IDAMAN NURANI TECHNOLOGIES SDN. BHD C = MY,	D0D6BA9EA1822C1C57F96F39BEE2A47A431889B7FD4C3BA25FB2200DC1873EBF	0dd4440ff954d2e5e51487e4d24f9092	ab539e3d6e303789042bb25ace85bc781d94fdd9	RSA (2048 Bits)	sha256RSA	15 Years
5.	CN = ABMB-MFA CA OU = Remote Signing System O = Alliance Bank Malaysia Berhad C = MY	F26EDD6166A7507C20C641D2961349E1875C2144C040D507EEA6EA7E173F43D7	1f1fbf124eb3872e663c56ac88829224	eee08f65bbebb49b0933497a750558dc2302b9d3	RSA (2048 Bits)	sha256RSA	15 Years
6.	CN = Trustgate Time Stamping Services CA (ECC) O = MSC Trustgate.com Sdn. Bhd. C = MY	67AC1B817817B9C626D6D3E8487A1C7FEC8AA27336D50148580F88BB67FFB7FF	45fe0985dc94accc26f309492cc18479	5146b3587866ed571800f03ea98cbae3e8e635eb	ECC (384 Bits)	sha384ECDSA	15 Years
7.	CN = Trustgate Time Stamping Services CA O = MSC Trustgate.com Sdn. Bhd. C = MY	7348112B9D8DF0042E920E202D532F6CA89A352BEDC59B8E85947C86F88B5EED	2041904eaf1b4af03c4f7f53cc74a83f	6bc9c97b0423d3de8ff444f5dd6ea687027a9880	ECC (384 Bits)	sha384ECDSA	15 Years

#	Subject DN	SHA256 Thumbprint	Serial Number	Subject Key Identifier	Key Size	Signature Algorithm	Validity
8.	CN = MyTrust Class 2 ECC Individual CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	F040B8C96223510A3190E0E85233159986BD26187D11C909D65AB8E0D298AA22	31748e2e336007c8d0d52f5d7c6053b7	e6a213f17f466916e0eda45699e1cc58bfc73ef2	ECC (384 Bits)	sha384ECDSA	15 Years
9.	CN = Bursa Anywhere CA OU = Remote Signing System O = Bursa Malaysia Berhad C = MY	2D01696CC852C4CE5317778A9FA16BBEA14CDEE10F5FBA91A3B37D8FF52768E5	1bf8459a40c5b0c65a3e602a1c3e06f4	3f8471db708f0d0199b845a4bf5bd0da820603b5	ECC (384 Bits)	sha384ECDSA	15 Years
10.	CN = GPKI CA ECC OU = MAMPU, O = MSC Trustgate.com Sdn. Bhd C = MY	567EF5A4C14641BC6B46452540F187B5686407DF4BDD51E5A3B1C79E678F97B8	2dfffda9b6cf352f36d3ff2b798f54ed	6598b4ea5fe27f1d2d15e01e0a6263bd6b3a8526	ECC (384 Bits)	sha384ECDSA	15 Years
11.	CN = MyLawyer ID CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	3B89B1CED28ED8045BA39015FAEB6C7FBF7D5E6A046B2F0198B846D7BEDA0006	4a4418e9745a0820a6788f2a985841d7	11f11c8192ff90d924d4349deb647ab0288c1e14	ECC (256 Bits)	sha256ECDSA	15 Years
12.	CN = MyTrust Class 3 ECC Enterprise CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	8EA69844C4A6BDA29FC13FD65A2371E9E689C22C1BF6585432406B527F86730F	32640e34187668c98d426cf5bbdb4c3c	b49bf36badb1745162af38142d5a623d14b2f779	ECC (384 Bits)	sha384ECDSA	15 Years
13.	CN = MyTrust Class 2 RSA Individual CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	35F1FAF93C2FAB2BF302F551525C587FD4D434BB6BB247ED75B50DB0F2FE2AB3	0924eaaa2c4c4e70645a95c8676bb338	545f5b34bc3acc4f2d9b47d858fbef3673c2a9b4	RSA (2048 Bits)	sha256RSA	15 Years
14.	CN = MyTrust Class 2 RSA Enterprise CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	1B1EE0498319BF0A223D4917A41A454D4EA08F44C5C8BD26F65121256377CB6A	7306eb97981bb42a3190caaca7be3382	60d7f177ed658e5eb4bf9248918c165e0a8e4578	RSA (2048 Bits)	sha256RSA	10 Years
15.	CN = PayNet CA O = Payments Network Malaysia Sdn Bhd C = MY	B70119C3B78800839F1A5246CB1DF54F2F148012F785371755669B278D0384AF	29ce7b42b0abe8e6c0e6a7bc2df5e7ad	c4619cb76a58a4baa03c39bdad9aea899fd7f472	RSA (2048 Bits)	sha384RSA	10 Years

#	Subject DN	SHA256 Thumbprint	Serial Number	Subject Key Identifier	Key Size	Signature Algorithm	Validity
16.	CN = MyTrust Digital ID Class 3 CA OU = MyTrust Gateway, O = MSC Trustgate.com Sdn. Bhd, C = MY	94B349BC4BE13041EA9A47315CE22E0EA327873FADA258EDC99B91F56F0F8439	6e8f6812d27111357bbf0d703635d68e	38a29bdc0e9b49ae4d8b53077892ea6261a63b82	ECC (384 Bits)	sha384ECDSA	15 Years
17.	CN = Trustgate Extended Validation Server CA O = MSC Trustgate.com Sdn. Bhd. C = MY	80689FEA931C13B6399096B44989CF2DDB3BB42DBFBAC25D56D274B9FEC23968	00ec4a1578a32003767f5b20b80b0dad05	d47bc6c114bcf57826bc6d2c3e7515174ba205c0	RSA (2048 Bits)	sha384RSA	15 Years
18.	CN = Trustgate Secure Server CA O = MSC Trustgate.com Sdn. Bhd. C = MY	D25E03BDBF23BF7772167268834F1FFC094CEF1D9A27C320FEB8320EF1813DBC	00b52e33ec2c56b59a04965d35d17dc028	d5b5c719032d3bc09960623e5e6ce227d20a38d9	RSA (2048 Bits)	sha384RSA	15 Years
19.	CN = Trustgate Basic Server CA O = MSC Trustgate.com Sdn. Bhd. C = MY	F6330ED89B22D8C06E46B2F733DA812374CD853B89EF1D6222B9162B0A00CAFD	00c3af2ed14fde0fe371612dbff8bd9388	ab4ba7463a645dfca85deed6ac080a9ce76345e0	RSA (2048 Bits)	sha384RSA	15 Years
20.	CN = Trustgate S/MIME Individual CA O = MSC Trustgate.com Sdn. Bhd. C = MY	2CFE9402F6DDAAA69154A541D713B8B7C7F83D33FAA696F8F0D1FB87271F3AE0	0085834d4e496c6aa2dfa2f8368b47bc88	2047fcb34bf41b3295d7d5acd57b27a986c71dd9	RSA (2048 Bits)	sha384RSA	15 Years
21.	CN = Trustgate S/MIME Organization CA O = MSC Trustgate.com Sdn. Bhd. C = MY	B4AEF17549780191EEF9E9592D40E378CE491781C0066B4D82E4F5D67B3C0134	00dcd1aaf8b041f1478e24cce037454559	f28cc1bf53f6a50b4dab6e3ec8268bf783628a24	RSA (2048 Bits)	sha384RSA	15 Years
22.	CN = Trustgate Document Signing CA O = MSC Trustgate.com Sdn. Bhd. C = MY	CA3A2B1EA210207F7D7A08BBC86EFDD391B1726EC7DD5357CC7576B7092C58CF	32d31f77b35a0212203c915c2bd63a00	7d790a3da6dd67567ff68dc6a047c628d8f5bc69	RSA (2048 Bits)	sha384RSA	15 Years
23.	CN = Trustgate MPKI Individual Subscriber CA O = MSC Trustgate.com Sdn. Bhd. C = MY	2685AD25E4393E39944F95FEACB704261DD88BFD3100A06756A563D2CAB499DA	008020df6b273f58369e9ed911ecfed0ee	780ddbeb312dc28d25bf5f3c1da5bb33f84ad495	RSA (2048 Bits)	sha384RSA	15 Years
24.	CN = MyKad ID CA O = MSC Trustgate.com Sdn. Bhd. C = MY	0AE0DF704E86B6845CD0F94B0A4A51F27E8A5194D39A94BF32560F09ACEA4F88	00b71b4254797d9028605d67c010abc5f8	d64b037e1a9c763b070e954adbf82252a6bd1e20	RSA (2048 Bits)	sha384RSA	15 Years

#	Subject DN	SHA256 Thumbprint	Serial Number	Subject Key Identifier	Key Size	Signature Algorithm	Validity
25.	CN = GPKI CA O = MSC Trustgate.com Sdn. Bhd. C = MY	962AD5D1976B0F65895788371795A1D4DEA139B82974E0E8E1EE518AEC1D6713	2dfffda9b6cf352f36d3ff2b798f54ed	6598b4ea5fe27f1d2d15e01e0a6263bd6b3a8526	ECC (384 Bits)	sha384ECDSA	15 Years
26.	CN = eP ID CA O = MSC Trustgate.com Sdn. Bhd. C = MY	85FD130D83DBE0049818DCDB12203F6C16616289CE7EE2E6C14F03BD29FADA64	0084f9cd9ce8766571978fc790187350fc	9de185ec63061a154faf4919442fb5ccaed1ee78	RSA (2048 Bits)	sha384RSA	15 Years
27.	CN = NPRA ID CA O = MSC Trustgate.com Sdn. Bhd. C = MY	AC717550BB1446C617128B723E36D46B9CDE7AD58D89F2AE325BDD13036E95C0	305eba080a1d6f877f0cbe469ef5877f	e5c309f05853ed34158451bdd47d04f4ba99c254	RSA (2048 Bits)	sha384RSA	15 Years
28.	CN = Healthcare ID CA O = MSC Trustgate.com Sdn. Bhd. C = MY	FBE9A14D3CAA3F72D0A402E5AE41581EAF1D7A79F12B4E3E722450B8372F1205	00863f1e682ef8898f01fd09e4a066287e	02f72a5afaa34a696dcd170cf8248e7e3c450715	RSA (2048 Bits)	sha384RSA	15 Years
29.	CN = ABMB-MFA CA - G2 O = MSC Trustgate.com Sdn. Bhd. C = MY	E623BD036F1C56E664536DE064710494816CEE48BCD5A5F36AAD744AC31CEF44	532e5372d5193cf4454b45735e1c7394	7327d516db0f319573f64af3b287bc4e2e8504e4	RSA (2048 Bits)	sha384RSA	15 Years
30.	CN = PayNet CA - G2 O = MSC Trustgate.com Sdn. Bhd. C = MY	56B97166434D8BDE298B353F6F800A70BE185A23FF97274EE0A7765CEAEB78D0	104ee2d2031bbb8ac91f122845ef45e1	0b0f86d741829b0efe5ccc3744d6f0a8034bdcbf	RSA (2048 Bits)	sha384RSA	15 Years
31.	CN = Trustgate ECC Time Stamping Services CA O = MSC Trustgate.com Sdn. Bhd. C = MY	7348112B9D8DF0042E920E202D532F6CA89A352BEDC59B8E85947C86F88B5EED	2041904eaf1b4af03c4f7f53cc74a83f	6bc9c97b0423d3de8ff444f5dd6ea687027a9880	ECC (384 Bits)	sha384ECDSA	15 Years
32.	CN = Trustgate ECC Document Signing CA O = MSC Trustgate.com Sdn. Bhd. C = MY	3E7CDC64E3FAD792A86BB130E1256C261BCD3B9049171B22F7A28439643ECF28	00a8edafb4e1460420e3a0da807f71d9fd	c9fedf4d25307080668f63956f3d4cd6f0a494f8	ECC (384 Bits)	sha384ECDSA	15 Years
33.	CN = Trustgate ECC MPKI Individual Subscriber CA O = MSC Trustgate.com Sdn. Bhd. C = MY	E10696EFAF72D5E0D0B62A80E687D4852227C30BAC367768F1451873A5C5BAB1	404f8ed0902e42b4cc0b4ab1c0151c33	11e5e1621ced21fbcc758681750c3d7692a270a9	ECC (384 Bits)	sha384ECDSA	15 Years
34.	CN = Bursa Anywhere CA - G2 O = MSC Trustgate.com Sdn. Bhd. C = MY	9A7BC4FDC454F1B920BFF8A7E7D578CC805F2C0C09B7ADE2B68C484EAFA7DA0C	00cee0600a39b695fbbf7f1099a2a478a3	456671a5c31f674695c1a83a3ef4cc991881f546	ECC (384 Bits)	sha384ECDSA	15 Years

#	Subject DN	SHA256 Thumbprint	Serial Number	Subject Key Identifier	Key Size	Signature Algorithm	Validity
35.	CN = GPKI CA ECC - G2 O = MSC Trustgate.com Sdn. Bhd. C = MY	229028210BE6A3B6176E8F5441B5EE629DA94BF28F425BA997F2E5AD5D7F8812	008d3842634d7914d84649345da01d51a1	8837629cbf1e5b2312438f4338531ba69707c22e	ECC (384 Bits)	sha384ECDSA	15 Years
36.	CN = MyLawyer ID CA - G2 O = MSC Trustgate.com Sdn. Bhd. C = MY	EF4C2488FA68ABAA945445254C3DEB49EF8269F736593F093493B41C7103ADF3	0089312c5ed6b24a6fd27381c6b3fe17bf	14e872374c9590fb4322426affd4eff5e3fdfb29	ECC (384 Bits)	sha384ECDSA	15 Years
37.	CN = Trustgate Digital ID Class 3 CA O = MSC Trustgate.com Sdn. Bhd. C = MY	7EC5C9AB617519B1655CB0587B68E668B974F8A9B098405416159ADA6D03FF3A	00c190d449caff4d5368ebaa7e8711ba00	29bc0d9c211748425dd9676b6cdaad7e74d15087	ECC (384 Bits)	sha384ECDSA	15 Years
38.	CN = Trustgate SMIME Basic RSA CA O = MSC Trustgate.com Sdn. Bhd. C = MY	6AABC6A71C014A2AECBE446A9C98EC05908F63B2C2D21536DABE386F719A3606	00cf761633616fdda9c66142ce699a90af	11e3e9c41e9121261524f194e1eb5ad8b1005f3d	RSA (2048 Bits)	sha384RSA	15 Years
39.	CN = Trustgate SMIME Standard RSA CA O = MSC Trustgate.com Sdn. Bhd. C = MY	A14A4C5C832BF6E9CE159B5245A70EFC2A2FA3560EC2191D084246BC72D8B20F	75c22d006b9412676b58b92e776da46a	7ed98d7df4bb8bf76395477bbc152b47fef50a4b	RSA (2048 Bits)	sha384RSA	15 Years
40.	CN = Trustgate SMIME Enterprise RSA CA O = MSC Trustgate.com Sdn. Bhd. C = MY	98F9400AB4E27EFE6E40039AF79ED67D8F3B3827E84CAF63010CDF5515D4A223	00b9f700a0322a620ba89224d22285f67d	66ad1c23221de899b41b96f8e45e1196546787db	RSA (2048 Bits)	sha384RSA	15 Years
41.	CN = Trustgate SMIME Organization RSA CA O = MSC Trustgate.com Sdn. Bhd. C = MY	6BBE5F6621F8AC75B50D68B447B554E28649E105418AC298BC84F52981AFF658	46ea29770949107bf18e3acc7bab6b18	f89a1072f545e53b1ce1b3e77d84f78f2d87b0c5	RSA (2048 Bits)	sha384RSA	15 Years
42.	CN = Trustgate SMIME Basic ECC CA O = MSC Trustgate.com Sdn. Bhd. C = MY	DC453E098780C277DD3780578D0001EEE614BBA885F89211E477CA3E3871EC6F	50a68d9e06b46a8ead0d792f63565547	1f8b256250ba30879cea47f6d4dbe13b99ad8da3	ECC (384 Bits)	sha384ECDSA	15 Years
43.	CN = Trustgate SMIME Standard ECC CA O = MSC Trustgate.com Sdn. Bhd. C = MY	B13AC2DA0B36F819FFFB56DAC80A9C48A4C1E83D37E9EB40F57B7E290C22EEB9	00847426ee964a21479175e5433f8ba6d3	ee4f35fa44afdefc78f2e1eaf039dc8f9504ae29	ECC (384 Bits)	sha384ECDSA	15 Years

#	Subject DN	SHA256 Thumbprint	Serial Number	Subject Key Identifier	Key Size	Signature Algorithm	Validity
44.	CN = Trustgate SMIME Enterprise ECC CA O = MSC Trustgate.com Sdn. Bhd. C = MY	6DC156503B110B7D2BA0CFB0CF91F1CEC702A1A69CDAD4EC81B68F8FBACA48E9	09867beebeae1508a3be5262e4d26efd	bb30e70ff2d0570a306b24dae8a1d9f54bc27784	ECC (384 Bits)	sha384ECDSA	15 Years
45.	CN = Trustgate SMIME Organization ECC CA O = MSC Trustgate.com Sdn. Bhd. C = MY	DE81B6BF29E0B2FC37F9E278480201A53515AA476ABBCAB454929EA97A3740AF	2aebfd22983f824dab9121bb82b13883	9c8f986977cd12b9bddfddc31c7f4572aa2033c1	ECC (384 Bits)	sha384ECDSA	15 Years
46.	CN = Trustgate TLS DV RSA CA O = MSC Trustgate.com Sdn. Bhd. C = MY	B900574E70C3925FA8A64CB0E0B1E349F87A5B658F84C9C2F33EE4A793A2DED9	00d08f36c5483595abf8d711850d726224	01f6b50bc5cb49e6efc7e1ade7df85714e03057a	RSA (2048 Bits)	sha384RSA	15 Years
47.	CN = Trustgate TLS OV RSA CA O = MSC Trustgate.com Sdn. Bhd. C = MY	EAB6A9F072FC20161375977CF7B2469610790DAF9A277C509378E98D483794E3	7a08d1746cbd280c5467649fe6ca9f2a	99c81532f155e815b47158303f90a38edd2c6b48	RSA (2048 Bits)	sha384RSA	15 Years
48.	CN = Trustgate TLS EV RSA CA O = MSC Trustgate.com Sdn. Bhd. C = MY	4E035B43435561F36F3F4DA4706268747F8263FA21778EDF1F5F29C3C09893F1	00f52df047297866a29f3e97106c95d2da	111e2aa1f319d775f19360516af99875994e5d0c	RSA (2048 Bits)	sha384RSA	15 Years
49.	CN = Trustgate TLS DV ECC CA O = MSC Trustgate.com Sdn. Bhd. C = MY	F8908E9D0066F8535B6AF52FBEE7988438C421DCC13EF8CB1DC2C54888FBC273	7f1393d035d770c9281486959b9ce718	1d62c54a1bd48fbe56066daa626c02529b20e241	ECC (384 Bits)	sha384ECDSA	15 Years
50.	CN = Trustgate TLS OV ECC CA O = MSC Trustgate.com Sdn. Bhd. C = MY	448C5ECB1B9B2E390C05C2F1D4E9DF32F8BF3C9A10876C5BF94F6C74AE243C99	00b30a9e3ff81f2cb44edc8816e4d03a49	96afff26cfcb2d230e3ddc3baa327a216b0c7eab	ECC (384 Bits)	sha384ECDSA	15 Years
51.	CN = Trustgate TLS EV ECC CA O = MSC Trustgate.com Sdn. Bhd. C = MY	A223DDCD91B2781BD46B085F3BE48AA63E21177C3B9936066EB3D7ABD4853EFC	4bb5fbc91e349c9df9dfaab4a779bdcd	b4b60f49b479264a7248f5150fdcc852658de2b5	ECC (384 Bits)	sha384ECDSA	15 Years
52.	CN=Trustgate ECC MPKI Admin CA O=MSC Trustgate.com Sdn. Bhd. C=MY	44FB07085AC1BF5780D3C477039FA0CB70BCB391C23CB85EE7884BC3DC75FDD6	651126d24cf6e9897c7b3844d1d1ae23	92a183b21b5cd66d0c16d36ca88e0f3c6a9f8f06	ECC (384 Bits)	sha384ECDSA	15 Years

#	Subject DN	SHA256 Thumbprint	Serial Number	Subject Key Identifier	Key Size	Signature Algorithm	Validity
53.	CN=SARAWAKPASS DIGITAL IDENTITY CA O=SARAWAK GOVERNMENT S=SARAWAK C=MY	17FFE1E156453016E7262E2DAF4E7B4FFEEF9752718D24DB71C295DE76A52C82	3d3c815201b2bf93605a5e40367e88c5	2a0daf6037f9af063a4246f2e38ce00078c7dca9	ECC (384 Bits)	sha384ECDSA	15 Years
54.	CN=SARAWAKPASS DIGITAL SIGNING CA O=SARAWAK GOVERNMENT S=SARAWAK C=MY	37981ECB721573CF7705A3A9F628A2EF47C3234994D272A57C94CDD8794A1947	6493c3a69641f446c8eadc94a6e835b5	f812ede7281c00080f37b32035385ed93da9f151	ECC (384 Bits)	sha384ECDSA	15 Years