



**TM TECHNOLOGY SERVICES SDN BHD
CERTIFICATION
AUTHORITY (TMCA)**

**CERTIFICATE POLICY (CP)
VERSION 1.1**

DATE OF PUBLICATION: 4TH MARCH 2024

**COPYRIGHT ©2024 TM TECHNOLOGY SERVICES SDN BHD
ALL RIGHTS RESERVED**



TM Technology Services Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

Revision History

Date	Version	Modification Type	Item/Ref. No.	Description	Author
7 th Nov, 2023	1.0	New		Approved for publication	TMCA CPS Committee
4 TH MARCH 2024	1.1	Revised	All	Approval for publication	TMCA CPS Committee

Notice

This document and the information contained in it is for PUBLIC use



TM Technology Services Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

DATE OF PUBLICATION: 4TH MARCH 2024	1
1 INTRODUCTION	12
1.1 OVERVIEW	12
1.2 DOCUMENT NAME AND IDENTIFICATION	13
1.3 PKI PARTICIPANTS	13
1.3.1 CERTIFICATION AUTHORITIES	13
1.3.1.1 CERTIFICATION AUTHORITY LICENSE	13
1.3.1.2 TMCA INFRASTRUCTURE	14
1.3.2 REGISTRATION AUTHORITIES (RAs)	14
1.3.2.1 SUB CERTIFICATE AUTHORITY (SUB CA)	14
1.3.3 SUBSCRIBERS	15
1.3.4 RELYING PARTIES	15
1.3.5 OTHER PARTICIPANTS	15
1.4 CERTIFICATE USAGE	15
1.4.1 APPROPRIATE CERTIFICATE USES	16
DEFINITION OF ASSURANCE LEVELS	17
1.4.2 PROHIBITED CERTIFICATE USES	17
1.5 POLICY ADMINISTRATION	17
1.5.1 ORGANISATION ADMINISTERING THE DOCUMENT	17
1.5.2 CONTACT PERSON	17
1.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE POLICY	19
1.5.4 CP APPROVAL PROCEDURES	19
1.6 DEFINITIONS AND ACRONYMS	19
2 PUBLICATION AND RESPIROTY RESPONSIBILITIES	21
2.1 REPOSITORIES	21
2.2 PUBLICATION OF CERTIFICATION INFORMATION	21
2.3 TIME OR FREQUENCY OF PUBLICATION	21
2.4 ACCESS CONTROLS ON REPOSITORIES	21

3 IDENTIFICATION AND AUTHENTICATION	22
3.1 NAMING	22
3.1.1 TYPE OF NAMES	22
3.1.2 NEED FOR NAMES TO BE MEANINGFUL	22
3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS	22
3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS	22
3.1.5 UNIQUENESS OF NAMES	22
3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS	22
3.2 INITIAL IDENTITY VALIDATION	22
3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY	22
3.2.2 AUTHENTICATION OF ORGANISATION IDENTITY	23
3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY	23
3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION	24
3.2.5 VALIDATION OF AUTHORITY	24
3.2.6 CRITERIA FOR INTEROPERATION	24
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS	24
3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY	24
3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION	24
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS	25
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	25
4.1 CERTIFICATE APPLICATION	25
4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION	25
4.1.2 ENROLMENT PROCESS AND RESPONSIBILITIES	25
4.2 CERTIFICATE APPLICATION PROCESSING	26
4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS	26
4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS	26
4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS	26
4.3 CERTIFICATE ISSUANCE	26
4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE	26
4.3.2 NOTIFICATIONS TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE	26
4.4 CERTIFICATE ACCEPTANCE	26



TM Technology Services Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

4.4.1	CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE	26
4.4.2	PUBLICATION OF THE CERTIFICATE BY THE CA	26
4.4.3	NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES	27
4.5	KEY PAIR AND CERTIFICATE USAGE	27
4.5.1	SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE	27
4.5.2	RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE	27
4.6	CERTIFICATE RENEWAL	27
4.6.1	CIRCUMSTANCES FOR CERTIFICATE RENEWAL	27
4.6.2	WHO MAY REQUEST RENEWAL	27
4.6.3	PROCESSING CERTIFICATE RENEWAL REQUESTS	27
4.6.4	NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER	27
4.6.5	CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE	28
4.6.6	PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA	28
4.6.7	NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES	28
4.7	CERTIFICATE RE-KEY	28
4.7.1	CIRCUMSTANCES FOR CERTIFICATE RE-KEY	28
4.7.2	WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY	28
4.7.3	PROCESSING CERTIFICATE RE-KEYING REQUESTS	28
4.7.4	NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER	28
4.7.5	CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE	28
4.7.6	PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA	28
4.7.7	NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES	28
4.8	CERTIFICATE MODIFICATION	28
4.8.1	CIRCUMSTANCES FOR CERTIFICATE MODIFICATION	28
4.8.2	WHO MAY REQUEST CERTIFICATE MODIFICATION	29
4.8.3	PROCESSING CERTIFICATE MODIFICATION REQUESTS	29
4.8.4	NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER	29
4.8.5	CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE	29
4.8.6	PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA	29
4.8.7	NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES	29
4.9	CERTIFICATE REVOCATION AND SUSPENSION	29
4.9.1	CIRCUMSTANCES FOR REVOCATION	29
4.9.2	WHO CAN REQUEST FOR REVOCATION	30
4.9.3	PROCEDURE FOR REVOCATION REQUEST	31
4.9.3.1	RENEWAL & UPDATED LIST OF REVOKED CERTIFICATES	31
4.9.4	REVOCATION REQUEST GRACE PERIOD	31
4.9.5	TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST	31
4.9.6	REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES	31



TM Technology Services Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

4.9.7	CRL ISSUANCE FREQUENCY	31
4.9.8	MAXIMUM LATENCY FOR CRLS	31
4.9.9	ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY	31
4.9.10	ON-LINE REVOCATION CHECKING REQUIREMENTS	31
4.9.11	OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE	31
4.9.12	SPECIAL REQUIREMENTS RE KEY COMPROMISE	31
4.9.13	CIRCUMSTANCES FOR SUSPENSION	31
4.9.14	WHO CAN REQUEST SUSPENSION	32
4.9.15	PROCEDURE FOR SUSPENSION REQUEST	32
4.9.16	LIMITS ON SUSPENSION PERIOD	32
4.10	CERTIFICATE STATUS SERVICES	32
4.10.1	OPERATIONAL CHARACTERISTICS	32
4.10.2	SERVICE AVAILABILITY	32
4.10.3	OPTIONAL FEATURES	32
4.11	END OF SUBSCRIPTION	33
4.12	KEY ESCROW AND RECOVERY	33
4.12.1	KEY ESCROW AND RECOVERY POLICY AND PRACTICES	33
4.12.2	SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES	33
5	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	34
5.1	PHYSICAL SECURITY CONTROLS	34
5.1.1	SITE LOCATION AND CONSTRUCTION	34
5.1.2	PHYSICAL ACCESS	34
5.1.3	POWER AND AIR CONDITIONING	34
5.1.4	WATER EXPOSURES	34
5.1.5	FIRE PREVENTION AND PROTECTION	34
5.1.6	MEDIA STORAGE	35
5.1.7	WASTE DISPOSAL	35
5.1.8	OFFSITE BACKUP	35
5.2	PROCEDURAL CONTROLS	35
5.2.1	TRUSTED ROLES	35
5.2.2	NUMBER OF PERSONS REQUIRED PER TASK	35
5.2.3	IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE	35
5.2.4	ROLES REQUIRING SEPARATION OF DUTIES	35
5.3	PERSONNEL CONTROLS	35
5.3.1	QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS	35



TM Technology Services Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

5.3.2	BACKGROUND CHECK PROCEDURES	35
5.3.3	TRAINING REQUIREMENTS	36
5.3.4	RETRAINING FREQUENCY AND REQUIREMENTS	36
5.3.5	JOB ROTATION FREQUENCY AND SEQUENCE	36
5.3.6	SANCTIONS FOR UNAUTHORISED ACTIONS	36
5.3.7	INDEPENDENT CONTRACTOR REQUIREMENTS	36
5.3.8	DOCUMENTATION SUPPLIED TO PERSONNEL	36
5.4	AUDIT LOGGING PROCEDURES	36
5.4.1	TYPES OF EVENTS RECORDED	36
5.4.2	FREQUENCY OF PROCESSING LOG	36
5.4.3	RETENTION PERIOD FOR AUDIT LOG	36
5.4.4	PROTECTION OF AUDIT LOG	37
5.4.5	AUDIT LOG BACKUP PROCEDURES	37
5.4.6	INCREMENTAL BACKUPS OF AUDIT LOGS ARE CREATED DAILY AND FULL BACKUPS SHALL BE PERFORMED WEEKLY BY AUTHORIZED TRUSTED PERSONNEL. THE BACKUP ARE STORED IN A SECURE LOCATION. AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)	37
5.4.7	NOTIFICATION TO EVENT-CAUSING SUBJECT	37
5.4.8	VULNERABILITY ASSESSMENTS	37
5.5	RECORDS ARCHIVAL	37
5.5.1	TYPES OF RECORDS ARCHIVED	37
5.5.2	RETENTION PERIOD FOR ARCHIVE	37
5.5.3	PROTECTION OF ARCHIVE	37
5.5.4	ARCHIVE BACKUP PROCEDURES	37
5.5.5	REQUIREMENTS FOR TIME-STAMPING OF RECORDS	37
5.5.6	ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)	37
5.5.7	PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION	37
5.6	KEY CHANGEOVER	38
5.7	COMPROMISE AND DISASTER RECOVERY	38
5.7.1	INCIDENT AND COMPROMISE HANDLING PROCEDURES	38
5.7.2	COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED	38
5.7.3	ENTITY PRIVATE KEY COMPROMISE PROCEDURES	38
5.7.4	BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER	38
5.8	CA OR RA TERMINATION	38
6	TECHNICAL SECURITY CONTROLS	39
6.1	KEY PAIR GENERATION AND INSTALLATION	39
6.1.1	KEY PAIR GENERATION	39

6.1.2	PRIVATE KEY DELIVERY TO SUBSCRIBER	39
6.1.3	PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER	39
6.1.4	CA PUBLIC KEY DELIVERY TO RELYING PARTIES	39
6.1.5	KEY SIZES	39
6.1.6	PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING	39
6.1.7	KEY USAGE PURPOSES (AS PER X.509 v3 KEY USAGE FIELD)	40
6.2	PRIVATE KEYS PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	40
6.2.1	CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS	40
6.2.2	PRIVATE KEY (N OUT OF M) MULTI PERSON CONTROL	40
6.2.3	PRIVATE KEY ESCROW	40
6.2.4	PRIVATE KEY BACKUP	40
6.2.5	PRIVATE KEY ARCHIVAL	40
6.2.6	PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE	40
6.2.7	PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE	40
6.2.8	METHOD OF ACTIVATING PRIVATE KEY	41
6.2.9	METHOD OF DEACTIVATING PRIVATE KEY	41
6.2.10	METHOD OF DESTROYING PRIVATE KEY	41
6.2.11	CRYPTOGRAPHIC MODULE RATING	41
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT	41
6.3.1	PUBLIC KEYS ARCHIVAL	41
6.3.2	CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIOD	41
6.4	ACTIVATION DATA	41
6.4.1	ACTIVATION DATA GENERATION AND INSTALLATION	41
6.4.2	ACTIVATION DATA PROTECTION	41
6.4.3	OTHER ASPECTS OF ACTIVATION DATA	41
6.5	COMPUTER SECURITY CONTROLS	42
6.5.1	SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS	42
6.5.2	COMPUTER SECURITY RATING	42
6.6	LIFE CYCLE TECHNICAL CONTROLS	42
6.6.1	SYSTEM DEVELOPMENT CONTROLS	42
6.6.2	SECURITY MANAGEMENT CONTROLS	42
6.6.3	LIFE CYCLE SECURITY CONTROLS	42
6.7	NETWORK SECURITY CONTROLS	42
6.8	TIME-STAMPING	43

7	CERTIFICATE, CRL, AND OCSP PROFILES	44
7.1	CERTIFICATE PROFILE	44
7.1.1	VERSION NUMBER(S)	44
7.1.2	CERTIFICATE EXTENSIONS	44
7.1.3	ALGORITHM OBJECT IDENTIFIERS	44
7.1.3.2	ENCRYPTION ALGORITHM OID	44
7.1.4	NAME FORMS	44
7.1.5	NAME CONSTRAINTS	44
7.1.6	CERTIFICATE POLICY OBJECT IDENTIFIER	44
7.1.7	USAGE OF POLICY CONSTRAINTS EXTENSION	44
7.1.8	POLICY QUALIFIERS SYNTAX AND SEMANTICS	44
7.1.9	PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION	44
7.2	CRL PROFILE	45
7.2.1	VERSION NUMBER(S)	45
7.2.2	CRL AND CRL ENTRY EXTENSIONS	45
7.3	OCSP PROFILE	45
7.3.1	VERSION NUMBER(S)	45
7.3.2	OCSP EXTENSION	45
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	45
8.1	FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT	45
8.2	IDENTITY/QUALIFICATIONS OF ASSESSOR	45
8.3	ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY	45
8.4	TOPICS COVERED BY ASSESSMENT	46
8.5	ACTIONS TAKEN AS RESULT OF DEFICIENCY	46
8.6	COMMUNICATIONS OF RESULTS	46
9	OTHER BUSINESS AND LEGAL MATTERS	47
9.1	FEES	47
9.1.1	CERTIFICATE ISSUANCE OR RENEWAL FEES	47
9.1.2	CERTIFICATE ACCESS FEES	47
9.1.3	REVOCATION OR STATUS INFORMATION ACCESS FEES	47



TM Technology Services Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

9.1.4	FEES FOR OTHER SERVICES	47
9.1.5	REFUND POLICY	47
9.2	FINANCIAL RESPONSIBILITY	47
9.2.1	INSURANCE COVERAGE	47
9.2.2	OTHER ASSETS	47
9.2.3	INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES	47
9.3	CONFIDENTIALITY OF BUSINESS INFORMATION	47
9.3.1	SCOPE OF CONFIDENTIAL INFORMATION	47
9.3.2	INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION	48
9.3.3	RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION	48
9.4	PRIVACY OF PERSONAL INFORMATION	48
9.4.1	PRIVACY PLAN	48
9.4.2	INFORMATION TREATED AS PRIVATE	48
9.4.3	INFORMATION NOT DEEMED AS PRIVATE	48
9.4.4	RESPONSIBILITY TO PROTECT PRIVATE INFORMATION	48
9.4.5	NOTICE AND CONSENT TO USE PRIVATE INFORMATION	48
9.4.6	DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS	48
9.4.7	OTHER INFORMATION DISCLOSURE CIRCUMSTANCES	48
9.5	INTELLECTUAL PROPERTY RIGHTS	48
9.6	REPRESENTATIONS AND WARRANTIES	48
9.6.1	CA REPRESENTATIONS AND WARRANTIES	48
9.6.2	RA REPRESENTATIONS AND WARRANTIES	49
9.6.3	SUBSCRIBERS REPRESENTATIONS AND WARRANTIES	49
9.6.4	RELYING PARTY REPRESENTATIONS AND WARRANTIES	49
9.6.5	REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS	49
9.7	DISCLAIMERS OF WARRANTIES	49
9.7.1	TMCA'S LIABILITY	49
9.7.2	RA'S LIABILITIES	49
9.7.3	SUBSCRIBER'S LIABILITIES	49
9.8	LIMITATIONS OF LIABILITY	49
9.9	INDEMNITIES	50
9.9.1	CA OBLIGATIONS	50



TM Technology Services Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

9.9.2 RA OBLIGATIONS	50
9.9.2.2 OBSERVANCE OF CERTIFICATE POLICY	50
9.9.2.3 RECEIPT OF APPLICATIONS FOR CERTIFICATION SERVICES	51
9.9.2.4 PROTECTION OF PRIVATE INFORMATION & SAFEKEEPING OF DATA SECURITY	51
9.9.2.5 SAFEGUARD OF FACILITIES & PERSONNEL	51
9.9.3 SUBSCRIBER OBLIGATIONS	51
9.9.3.2 GENERATION OF KEY PAIR	51
9.9.3.3 PROTECTION & SAFEKEEPING OF PRIVATE KEYS	51
9.9.3.4 USE OF PRIVATE KEY	51
9.9.3.5 VERIFICATION OF DIGITAL CERTIFICATES	52
9.9.4 RELYING PARTY OBLIGATIONS	52
9.9.5 REPOSITORY OBLIGATIONS	52
9.10 TERM AND TERMINATION	52
9.10.1 TERM	52
9.10.2 TERMINATION	52
9.10.3 EFFECT OF TERMINATION AND SURVIVAL	52
9.11 INDIVIDUAL NOTICES AND COMMUNICATION WITH PARTICIPANTS	52
9.12 AMENDMENTS	53
9.12.1 PROCEDURE FOR AMENDMENT	53
9.12.2 NOTIFICATION MECHANISM AND PERIOD	53
9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED	53
9.13 DISPUTE RESOLUTION PROCEDURES	53
9.14 GOVERNING LAW	53
9.15 COMPLIANCE WITH APPLICABLE LAW	53
9.16 MISCELLANEOUS PROVISIONS	53
9.16.1 ENTIRE AGREEMENT	53
9.16.2 ASSIGNMENT	53
9.16.3 SEVERABILITY	53
9.16.4 ENFORCEMENT (ATTORNEY'S FEE AND WAIVER OF RIGHTS)	53
9.16.5 FORCE MAJEURE	53
9.17 OTHER PROVISIONS	54
APPENDIX A – APPLICATION FORM FOR TMCA DIGITAL CERTIFICATE	55

1 INTRODUCTION

1.1 Overview

TMCA Certificate Policy (CP) (hereinafter, TMCA) applies to the services of TMCA that are associated with the issuance of and management of digital certificates issued under Root Certification Authority (Root CA) managed by TMCA. Root CA can be used to manage certificate hierarchies of certification authorities as well as of end entity certificates.

The CP is organised as follows:

Section Number	Description
1	This section provides information on TMCA infrastructure, the roles and responsibilities of the stakeholders.
2	This section explains about publication and repository responsibilities.
3	This section explains the procedures and operational requirements for the identification and authentication during initial registration.
4	This section explains the procedures and operational requirements for the application, issuance, revocation, suspension and renewal of digital certificate.
5	This section outlines the critical security measures and controls employed by TMCA in providing trustworthy certification services.
6	This section outlines the used to define the security measures taken by TMCA to protect its cryptographic key and activation data.
7	This section defines the certificate, CRL, and OCSP format and use.
8	This section provides information about assessment, assessor scope and what to be observed in the audit.
9	This section outlines the important legal provisions. In this section, fees, TMCA's, RA's, Relying Parties' and Subscriber's obligations, limitations and warranties will be highlighted.

Note: It is important that potential Subscribers to fully understand the contents of this CP before submitting application for a digital certificate.

Prior to accepting the terms & conditions of this CP, it is advisable for potential Subscribers to have some pre-requisite knowledge of the following information:

- a. Digital Certificates;
- b. Digital Signatures;
- c. Digital Signature Act 1997;
- d. Digital Signature Regulations 1998;

TM Technology Services Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

- e. The rights, duties and liabilities of the licensed CA, RA, Subscribers and relying parties.

All the above information can be obtained from TMCA website at www.tmca.com.my.

1.2 Document Name and Identification

In compliance with the Malaysia's Digital Signature Act 1997 (hereinafter referred to as the "DSA") and the Digital Signature Regulations 1998 (hereinafter referred to as the "DSR"), TMCA CP is intends to prescribe all matters concerning TM Technology Services Sdn Bhd Certification Authority (hereinafter referred to as "TMCA") and the certification services including certificate issuance and management, operation of certification systems, and responsibilities and liabilities of the related parties such as TMCA , Registration Authority (hereinafter referred to as the "RA") and its Subscribers.

The CP is named as the "TM Technology Services Sdn Bhd Certificate Policy". The version number and date of the document is provided herein on the cover page:

Object Identifier (OID)" for this CP is: 1.2.410.20004.5.2

This CP can be found on the TMCA repository at <https://www.tmca.com.my/info/legalRepository>. ThisCP may be updated from time to time.

1.3 PKI Participants

TMCA CP provides information about the policies, employed by TMCA to perform certification services.

1.3.1 Certification Authorities

TM Technology Services Sdn Bhd is a licensed certification authority (TMCA) granted by MCMC, operates in compliance with the requirements of the DSA and the DSR to provide certification services. TMCA uses a highly technological and trustworthy certificate management system to provide public key certification services to its Subscribers, and also to conform to the current industry standard.

In digital business environment, TMCA's trust model involves a combination of secure technology with reliable and visible processes for the identification and authentication of all parties in the TMCA infrastructure.

In compliance of the requirements of DSA and DSR, TMCA's public key certification services have been designed to address the requirements of a diverse group of users.

1.3.1.1 Certification Authority License

TMCA is licensed to issue digital certificates to individual/business/organisation.

The digital certificates can be used to improve the security in digital transactions in the public and private sectors.

1.3.1.2 TMCA Infrastructure

TMCA infrastructure provides the standard trust model as shown below:

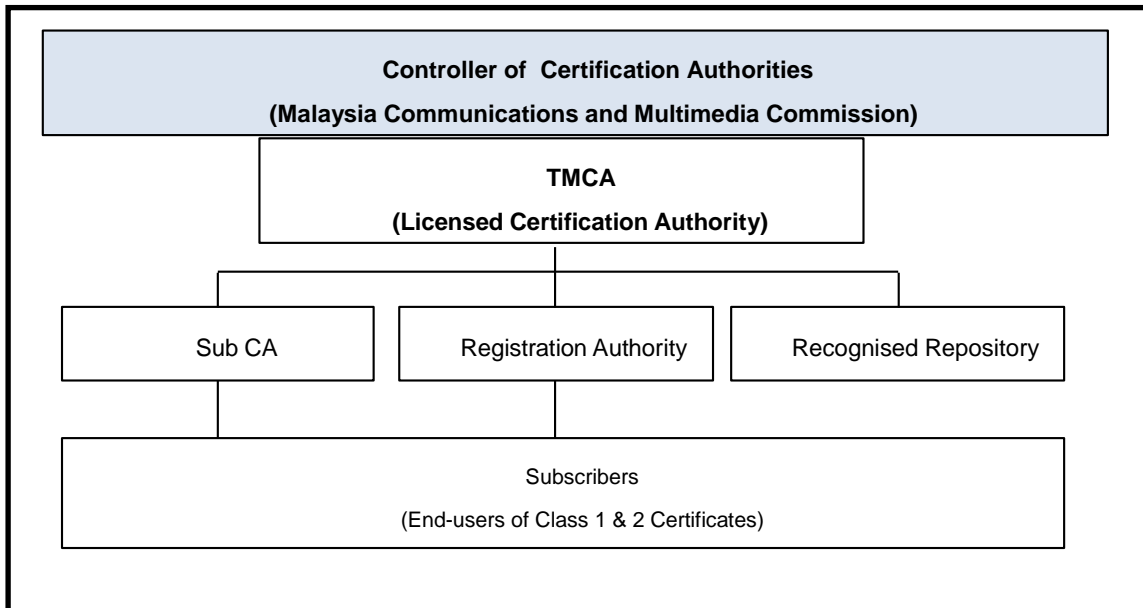


Figure 1 TMCA Infrastructure

Roles and responsibilities of the stakeholders in the TMCA infrastructure are stated in the sub-sections below:

1.3.2 Registration Authorities (RAs)

RAs are trusted entities appointed by TMCA to assist Subscribers in applying for certificates, to approve certificate requests and/or to help TMCA in revoking certificates. The functions that the RAs shall carry out shall also include personal authentication, token distribution, revocation reporting and name assignment. The organisations that are appointed as Registration Authority (RA) for TMCA shall be officially published on TMCA’s website, <https://www.tmca.com.my>, and other printed materials deemed necessary and copyrighted by the management of TMCA. The list of TMCA’s Registration Authorities is available at the website.

1.3.2.1 Sub Certificate Authority (Sub CA)

In a distributed trust model, organisations may wish to become the issuer of Subscriber’s certificates. A Sub CA shall be the party who accepts applications, verifies, issues and revokes Subscriber certificates, subject to the agreement between TMCA and the party being the Sub CA.

Sub CA has the authority to act as its own RA as depicted in Figure 1 above.

1.3.3 Subscribers

These are the Subscribers/end-users of TMCA services. They could be individuals or organisations who hold and/or rely on digital certificates in electronic transactions. Subscribers need not necessarily be a natural person; it could also be a certificate using system such as a secure web server or any organisation. Each Subscriber could own as many certificates as it needs and may use them for different purposes.

The proposed usage will be determined by the certificate classes that they have applied for.

1.3.4 Relying Parties

Relying Parties are the entities who, by using another's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate relies on the validity of the certificate that bind the Subscriber's name to a public key.

Relying Parties may use information in the certificate to determine the suitability of the certificate for a particular use and does so at their own risk. TMCA's Relying Parties are individuals or applications that accept secure transactions from Subscribers of TMCA.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

TMCA offers the following certificate classes:

Class	Usage	Assurance Level	Subscribers
Class 1 Digital Certificates	This class of digital certificate is used for encryption and decryption of electronic data. As authentication of the user is simple sufficed with email authentication, the digital certificates are not to be used to digitally sign a business transaction. Class 1 digital certificates do not provide assurance on the identity of the Subscriber.	Low	Individual – Malaysian and Foreigner
Class 2 Digital Certificates	<p>This class of digital certificate is used for digitally sign an online business transaction and as the digital signing is legally accepted, verification of user is mandatory. Class 2 digital certificates provide assurance on the identity of the Subscriber. Class 2 certificates are mainly used for user authentication and online secure transactions in the following services:</p> <ul style="list-style-type: none"> • Digital Financial Services • Digital Government Services • Digital Stock Broking Services • Digital Commerce • Digital Approval • Digital Document Services • Digital Insurance Services <p>This class of digital certificate is applicable for individual user certificate and server certificate.</p>	Medium	Individual
			SME/ Corporation/ Government
			Organization Members
			Organization
			NGO
	Secure Web Transaction	Medium	Web Server Operator

Definition of Assurance Levels

Assurance levels for the certificate classes are defined as follows:

Assurance Level	Description
Low	Certificates have either no authentication purposes for non-repudiation or no proof of identity of Subscriber. For example, the encryption application enables a Relying Party to use the Subscriber's certificate to encrypt messages to the Subscriber, although the Sending Relying Party cannot be sure that the recipient is in fact the person named in the certificate
Medium	Certificates are suitable for securing some inter- and intra-organizational, commercial, and personal email requiring a medium level of assurance of the Subscriber's identity.

1.4.2 Prohibited Certificate Uses

All certificate usages not listed in 1.4.1 are prohibited.

Certificates use is restricted by using certificate extension on key usage and extended key usage. Certificates do not guarantee that the subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A certificate only establishes that the information in the certificate was verified as reasonably correct when the certificate is issued.

Certificates issued pursuant to this CP may not be used:

- a) for any application requiring fail-safe performance such as: (i) the operation of nuclear power facilities; (ii) air traffic control systems; (iii) aircraft navigation systems; (iv) weapons control systems; (v) any other system whose failure could lead to injury, death or environmental damage; or
- b) where prohibited by law.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

Subscribers are advised to visit TMCA's web site at <https://www.tmca.com.my> for relevant information and assistance.

For further assistance, please contact:

TM Technology Services Sdn Bhd (200201003726 [571389-H])
 Level 28, TM Annexe2
 Jalan Pantai Baru
 59100Kuala Lumpur

1.5.2 Contact Person

TMCA Manager



TM Technology Services Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4TH MARCH 2024

TM Technology Services Sdn Bhd (200201003726 [571389-H])
Level 28, TM Annexe2
Jalan PantaiBaru
59100Kuala Lumpur
Tel: +^6013 3999398

For Business inquiries on certification services, and other technical inquiries, please email to: tmca.helpdesk@tm.com.my

TM Technology Services Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

1.5.3 Person Determining CPS suitability for the Policy

TMCA CP/CPS committee determines CPS suitability for the policy.

1.5.4 CP Approval Procedures

TMCA may make changes, as and when required, to its operating practices in order to improve its certification services, and some of these changes may require amendments to the CP.

This CP and any subsequent amendments shall be managed, reviewed and approved by the management of TMCA.

TMCA reserves the rights to amend this CP at any time and the amendments to this CP shall be made available at TMCA's web site, <https://www.tmca.com.my>.

Note, once the amendments have become effective, they shall supersede the earlier version of the CP. The publication date is equivalent to the effective date of the CP.

1.6 Definitions and Acronyms

Acronyms and Abbreviations Used in CP

Acronyms/Abbreviations	Description
CA	Certification Authority
CP	Certificate Policy
CRL	Certificate Revocation List
DN	Distinguished Name
DSA	Digital Signature Act 1997
DSR	Digital Signature Regulations 1998
ECC	Elliptic curve cryptography
eKYC	Electronic Know Your Customer
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
IP	Internet Protocol

Acronyms/Abbreviations	Description
ISO	International Standard Organisation



TM Technology Services Sdn Bhd Certification Authority (TMCA)		Version 1.1
Certificate Policy (CP)		Publication Date: 4 TH MARCH 2024
ITU	International Telecommunications Union	
OCSP	Online Certificate Status Protocol (OCSP)	
PIN	Personal Identification Number	
PKI	Public Key Infrastructure	
RA	Registration Authority	
RP	Registration Personnel	
RSA	RSA (which stands for Rivest , Shamir and Adleman who first publicly described it) is an algorithm for public-key cryptography . It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be sufficiently secure given sufficiently long keys and the use of up-to-date implementations.	
SHA	Secure Hash Algorithm .	
SSL	Secure Socket Layer	
TM Tech	TM Technology Services Sdn Bhd (200201003726 [571389-H])	
TMCA	TM Technology Services Sdn Bhd Certification Authority	

Acronyms/Abbreviations	Description
URL	Uniform Resource Locator
WWW	World Wide Web
X.509	ITU-T standard for certificates format
MCMC	Malaysian Communications and Multimedia Commission
CSR	Certificate Signing Request

2 PUBLICATION AND RESPIATORY RESPONSIBILITIES

2.1 Repositories

TMCA's repository function is obligated to publish certificates and certificate revocation lists in a timely manner.

2.2 Publication of Certification Information

Each CA shall store its Certificates and CRL in TMCA Repository. TMCA will ensure unrestricted access to Certificate status information for all applicable Relying Parties.

Certificates are internal and external to TMCA available via LDAP directories. This CP will be stored on a Web server and made available through <https://www.tmca.com.my>. All PKI information not included in TMCA Repository or on the above mentioned website is considered confidential by TMCA and is not publicly available.

2.3 Time or Frequency of Publication

TMCA shall undergo with a minimum of once per year and makes appropriate changes to the Certification Practice Statement and Certification Policy.

TMCA renews and updates the CRL at least once every 24 hours.

2.4 Access Controls on Repositories

End users may search for TMCA certificates or CRLs using http queries or the LDAP protocol. TMCA repository is accessible via http query and LDAP query.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Type of Names

- a. For names used in the basic domain of digital certificates and the Certificate Revocation List (CRL) and OCSP (Online Certificate Status Protocol), the method of ITU-T X.500 DN (Distinguished Name) is applied.
- b. Information contained in digital certificates and the CRL and OCSP is as follows:
 - ① Individual Certificate: Real name as in Mykad, MyTentera, Polis Diraja Malaysia Card or Passport; with/without *Mykad Number, MyTentera Number, Polis Diraja Malaysia Number, Passport Number or Email Address (optional)*
 - ② Corporate Certificate: Real company name as in Company Registration, Company ID, and Email Address.
 - ③ Server Certificate: Company Real Name as in Company Registration and Internet Domain Name (URLs for WWW); or Device Serial Number and MAC address

3.1.2 Need for Names to be Meaningful

TMCA uses distinguished names to identify both Subject and issuer of the certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

The use of pseudonyms for CA subscribers names are not permitted except for Class 1.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

TMCA verifies the uniqueness of Subscriber's DN (Distinguished Name).

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2 Initial Identity Validation

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

3.2.1 Method to Prove Possession of Private Key

On receiving application for issuance of a certificate, TMCA verifies whether the Public Key submitted by the Subscriber matches the Private Key owned by the Subscriber through the following:

- a. In applying for issuance of a certificate, the Subscriber should use application form

TM Technology Services Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

prepared by TMCA.

- b. TMCA verifies whether the Public Key matches the Private Key based on information contained in application form.
- c. In the case of Class 2 digital certificates, there is a strong requirement to secure the private key, and TMCA shall verify it against the key held by the Subscriber.

3.2.2 Authentication of Organisation Identity

As stipulated in Section “3.2.3 Authentication of Individual Identity”

3.2.3 Authentication of Individual Identity

TMCA verifies personal identity of the applicant by service type as follows:

Class	Subscribers	Identification
Class 1	Individual/Business	Verification via email.
Class 2 (Individual / Business /NGO)	Individual	Manual verification of ID if Subscriber visits to TMCA Office or Authorised RA Office. If Subscriber applies online, verification via supporting documents must be attached. If Subscriber is a member of corporate organisation, verification via company email or internal authentication should be sufficient. In addition, TMCA shall incorporate additional controls that include face-to-face or eKYC verification.
	SME/Corporation/Organisation	Manual verification of ID and supporting documents if Subscriber representative visits to TMCA Office or Authorised RA Office. If Subscriber applies online, verification via supporting must be attached. If Subscriber is a member of corporate organisation, verification via company email or internal authentication should be sufficient. In addition, TMCA shall incorporate additional controls that include face-to-face or eKYC verification.
	Server Operator	Manual verification of ID if Subscriber visits to TMCA Office or Authorised RA Office. If Subscriber applies online, verification via supporting documents must be attached. If Subscriber is a member of corporate organisation, verification via company email or internal authentication should be sufficient.

Note:

1. In case the identity of the Subscriber is already verified by Authorised RA by following the same procedures used by TMCA, the Subscriber may be regarded as having fulfilled the requirement of identity verification as stipulated in this CP.
2. In case of a reputable organisation is also an Authorised RA, option shall be given to the organisation to efficiently authenticate their employees or customers who intend to be a Subscriber of TMCA, via other means besides the manual verification or eKYC. For example, if the organisation has Single Sign On (SSO) services and/or Identity Management services, these systems can be capitalised to authenticate the Subscribers.

3.2.4 Non-Verified Subscriber Information

Non-verified subscriber information includes:

1. Subscriber's name in Class 1 certificates
2. Any other information designated as non-verified in the certificate.

3.2.5 Validation of Authority

TMCA 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 with human resources department letter of authority and by presenting official id where the relationship of the Applicant with the organization is certified.

3.2.6 Criteria for Interoperation

No stipulation

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Before the expiration of an existing certificate, the Subscriber is required to obtain a new certificate to maintain the continuity of the certificate usage. This process is called Re-Key. The Subscribers are required to generate a new key pair to replace the expiring key pair. Subscribers may also request a new certificate by using an existing key pair. This process is called Renewal.

3.3.2 Identification and Authentication for Re-Key After Revocation

There is no Re-Key after revocation. The Subscriber shall submit a new application after revocation.

3.4 Identification and Authentication for Revocation Requests

The procedures for personal identification for suspension/revocation of a digital certificate are similar to procedures of personal identification for issuance of a digital certificate.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Application of certificate can be submitted by anyone who complies the provisions specified in the TMCA Application form, CP/CPS and any relevant End-User Agreements.

TMCA holds the rights to reject certificate applications.

4.1.2 Enrolment Process and Responsibilities

TMCA maintains systems and processes that sufficiently authenticate the Applicant's identity for all certificates under this CP. Applicants must submit sufficient information to allow TMCA and RA successfully perform required verifications. TMCA and RA shall protect and securely store information presented by Applicants.



TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Subscriber should personally visit TMCA Office or TMCA's Authorised RA for registration or access TMCA website to apply online. Subscriber may require undergoing personal identification process as stipulated in Section "3.1 Naming" for Issuance/Suspension/Revoke/Reinstatement/Cancellation of Digital Certificates in the CP.

TMCA shall maintain systems and processes to authenticate the Applicant's identity in compliance with this CP. Initial validation shall be performed by the validation team or by the RA appointed by TMCA.

TMCA and the RA shall ensure all communication and information regarding certificate issuance are made secure and auditable.

4.2.2 Approval or Rejection of Certificate Applications

After a Certificate Applicant submits a Certificate Application, TMCA shall approve or reject the application after verification process. If the validation is failed, the Certificate Application is rejected.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Accepted certificate applications as described in section 4.2.2 are processed by TMCA. The RA that performs validation shall ensure that all information is verified and authenticated in a secure manner when submitting to TMCA.

However, issuance of digital certificates may be delayed or rejected if the information presented by the Subscriber is inaccurate.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

TMCA shall notify the Subscriber of the Issuance of a certificate upon issuance.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

TMCA issues certificate to the Subscriber upon successful processing of the application and the acceptance of the certificate by the Subscriber based on the Terms & Conditions and Acceptance Notice stated in the application form.

The Subscriber is obligated to verify all details contained with the certificate, any error or omission found must be communicated immediately to TMCA.

4.4.2 Publication of the Certificate by the CA

No stipulation.

TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The Subscribers are required to use a Private Key and certificate only for appropriate applications as set forth in this CP and in consistency with applicable certificate content (e.g. key usage field).

The Subscribers must protect their Private Keys to avoid disclosure or misuse by third parties. Use of a Private Key and certificate are subject to the terms of the Subscriber Agreement and using the certificate within the scope and authority defined in the legal regulations, this CP and the CPS documents.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties are obligated to check the validity of certificates only for appropriate applications as set forth in this CP and in consistency with applicable certificate content (e.g. key usage field), successfully perform Public Key operations as a condition of relying on a certificate, assume responsibility to check the status of a certificate using appropriate mechanism available to verify the certificate.

Relying parties are under obligation to use a trustworthy system defined under the legislation and standard during these operations. TMCA will not be responsible for the relying parties not fulfilling the conditions stated above before relying on the certificates.

4.6 Certificate Renewal

Certificate Renewal is the issuance of a new certificate without changing the Public Key or any other information.

4.6.1 Circumstances for Certificate Renewal

- a. Renewal of digital certificates refers to issuance of a new digital certificate to extend the validity of the original certificate using the same Public Key and the same DN (Distinguished Name). Subscribers who require their digital certificates renewed should apply at least 30 days prior to the expiration of their original certificate.

4.6.2 Who May Request Renewal

The Subscriber or his Authorised Representative can apply for renewal of a digital certificate.

4.6.3 Processing Certificate Renewal Requests

TMCA shall request additional information upon processing the renewal request.

4.6.4 Notification of New Certificate Issuance to Subscriber

TMCA shall notify the Subscriber of the Issuance of a certificate upon issuance.



TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As per 4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

No stipulation.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 Certificate Re-Key

Certificate Re-key is the application for issuance of a new certificate that certifies the new public key. The requirements for certificate Re-keying is as stipulated in Section “4.3 Certificate Issuance”

4.7.1 Circumstances for Certificate Re-Key

No stipulation.

TMCA shall perform Certificate Re-Key if the certificate has been erased from medium storage such as token or lost or device malfunction.

4.7.2 Who May Request Certification of a New Public Key

The Subscriber of the issued certificate may request for re-key.

4.7.3 Processing Certificate Re-Keying Requests

An Issuing CA may request additional information before processing a re-key or reissue request and may re-validate the Subscriber subject to re-verification of any previously validated data. In the case of a reissuance, authentication through a suitable challenge response mechanism is acceptable.

4.7.4 Notification of New Certificate Issuance to Subscriber

As stipulated in Section “4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate”

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As stipulated in Section “4.4.1 Conduct Constituting Certificate Acceptance”

4.7.6 Publication of the Re-Keyed Certificate by the CA

As stipulated in Section “4.4.2 Publication of Certificate by CA”

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As stipulated in Section “4.4.3 Notification of Certificate Issuance by the CA to Other Entities”

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification is defined as the production of a new Certificate that has details which differ

TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

from a previously issued Certificate. The new modified Certificate may or may not have a new Public Key and may or may not have a new 'Valid to' date.

1. Issuing CAs shall treat modification in the same was a 'New' issuance.
2. Issuing CAs may modify Certificates that have either been previously renewed or previously re-keyed. The original Certificate may be revoked after modification is complete, however, the original Certificate must not be further renewed, re-keyed or modified.

4.8.2 Who May Request Certificate Modification

The Subscriber or his Authorised Representative may request for certificate modification.

4.8.3 Processing Certificate Modification Requests

An Issuing CA may request additional information before processing certificate modification and may re-validate the Subscriber subject to re-verification of any previously validated data.

4.8.4 Notification of New Certificate Issuance to Subscriber

As stipulated in Section "4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate"

4.8.5 Conduct Constituting Acceptance of Modified Certificate

As stipulated in Section "4.4.1 Conduct Constituting Certificate Acceptance"

4.8.6 Publication of the Modified Certificate by the CA

As stipulated in Section "4.4.2 Publication of Certificate by CA"

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

As stipulated in Section "4.4.3 Notification of Certificate Issuance by the CA to Other Entities"

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

TMCA revokes the corresponding certificate due to one of the following reasons:

- ① In the event the Subscriber or his Authorised Representative applies to TMCA for revocation.
- ② In the event TMCA discovers that the Subscriber obtains his digital certificate by fraud, forgery, or other illegal means.
- ③ In the event TMCA discovers the death, missing, or dissolution of the Subscriber or his organisation.
- ④ In the event TMCA discovers the Subscriber's Private Key has been lost, damaged, stolen, or compromised.



TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4TH MARCH 2024

- ⑤ In the event the Subscriber violates any of these rules mentioned in the CPS.
- ⑥ In the event the designation of TMCA as a licensed Certification Authority is cancelled by MCMC.
- ⑦ In the event that the Subscriber discovers that his Private Key has weakness, lost, damaged, stolen or compromised.

4.9.2 Who Can Request for Revocation

The Subscriber or his Authorised Representative can apply for revocation of a digital certificate.

TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

4.9.3 Procedure for Revocation Request

The entity or the Subscribers must list out their identities and explain the reason for requesting the revocation. TMCA and the RA authenticate and log each revocation request.

TMCA or the RA shall revoke the certificate if the request is authenticated as originated from the Subscriber or authorized personnel in the organization listed in the certificate.

Issuing CAs and RAs will record each request for revocation and authenticate the source, taking appropriate action to revoke the Certificate if the request is authentic and approved. Once revoked, the serial number of the Certificate and the date and time shall be added to the appropriate CRL.

4.9.3.1 Renewal & Updated List of Revoked Certificates

Once a digital certificate is successfully revoked, TMCA shall update the list of revoked digital certificates promptly.

4.9.4 Revocation Request Grace Period

Once the identity of the Subscriber and reasons for request for revocation is confirmed and accepted, TMCA shall within a commercially reasonable period of time revoke the corresponding certificate.

4.9.5 Time Within Which CA Must Process the Revocation Request

TMCA shall begin investigating the revocation request within 24 hours after the submission.

4.9.6 Revocation Checking Requirements for Relying Parties

An Authorised party shall only rely on a Certificate's contents after checking with the applicable CRL for the latest Certificate status information, either manually or automatically.

4.9.7 CRL Issuance Frequency

The CRL are issued every 24 hours.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation.

4.9.9 On-Line Revocation/Status Checking Availability

TMCA shall provide online certificate status checking service through OCSP protocol.

4.9.10 On-Line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Re Key Compromise

As stipulated in "Section 4.9.1 Circumstances for Revocation"

4.9.13 Circumstances for Suspension

Certificate Suspension for certificates issued by TMCA is not provided.



TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

4.9.14 Who Can Request Suspension

Certificate Suspension for certificates issued by TMCA is not provided.

4.9.15 Procedure for Suspension Request

Certificate Suspension for certificates issued by TMCA is not provided.

4.9.16 Limits on Suspension Period

Certificate Suspension for certificates issued by TMCA is not provided.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

TMCA shall make certificate status information available via CRL and/or OCSP. TMCA shall list revoked certificates on the appropriate CRL where they remain until one additional CRL is published after the end of the certificate's validity period.

4.10.2 Service Availability

The service shall be available 24 hours a day, 7 days a week.

4.10.3 Optional Features

No stipulation.



TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.



TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Security Controls

5.1.1 Site Location and Construction

TMCA CA operation shall be performed in secured facilities protected against external threats and high security areas and various security areas have been designated and equipped with logical and physical controls to make CA operations accessible by authorized personnel only.

The site location combined with other physical security protection mechanisms such door locks and intrusion sensors shall protect from unauthorized access to CA equipment and data records.

5.1.2 Physical Access

TMCA shall ensure that the facilities used for Certificate life cycle management are operated in an environment that physically protects the services from Compromise through unauthorized access to systems or data. An authorized employee should always accompany any unauthorized person entering a physically secured area. Physical protections should be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the systems hosting the CA operations. No parts of the CA premises shall be shared with other organizations within this perimeter.

5.1.3 Power and Air Conditioning

TMCA shall ensure that the power and air conditioning facilities are sufficient to support the operation of the CA system, ventilation and protection.

5.1.4 Water Exposures

TMCA shall ensure that the CA system is protected from water exposure

5.1.5 Fire Prevention and Protection

TMCA shall ensure that the CA system is protected with a fire suppression system.



TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

5.1.6 Media Storage

Backup of all records including the cryptographic key material of TMCA operations are kept in appropriate secure media.

5.1.7 Waste Disposal

TMCA shall ensure all information and documents relating to certificate services stored in electronic or paper based be destroyed and disposed of pursuant to relevant procedures if no longer be used or no need to be stored. Cryptographic equipment shall be reset to clear all key material according to the manufacturer's instruction manual before its being disposed of.

5.1.8 Offsite Backup

TMCA maintains a remote backup storage of subscriber certificates, including CRL (Certificates Revocation List), for 10 years after the corresponding digital certificates are voided.

5.2 Procedural Controls

5.2.1 Trusted Roles

All TMCA personnel that have access to or control over PKI operations including Certificate issuance, Use, Suspension and Revocation shall, for purposes of TMCA CP, be considered as serving in a Trusted Role. Such personnel include, but is not limited to, CA Operators, RA, system administration personnel, engineering personnel, security management and managers who are designated to oversee the operations of TMCA.

5.2.2 Number of Persons Required per Task

No stipulation.

5.2.3 Identification and Authentication for Each Role

Trusted Roles for CA's have their identity and authorisation verified before they are:

- Included in the access list for the CA site
- Included in the access list for physical access to the CA System, and
- Given an account on the PKI system

5.2.4 Roles Requiring Separation of Duties

No stipulation.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

TMCA carries out checks to establish the background, qualifications, and experience needed to perform within the competence context of the specific job.

5.3.2 Background Check Procedures

No stipulation.



TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

5.3.3 Training Requirements

TMCA shall makes available training for their personnel to carry out CA or RA functions. Training topics include the operation of the CA software and hardware, operational and security procedures, disaster recovery and business continuity operations, and requirements of TMCA CPS.

5.3.4 Retraining Frequency and Requirements

No stipulation.

5.3.5 Job Rotation Frequency and Sequence

TMCA shall conduct job rotation for all critical posts to provide continuity and integrity of TMCA service.

5.3.6 Sanctions for Unauthorised Actions

Appropriate disciplinary actions shall be applied to TMCA personnel attempting unauthorized actions.

5.3.7 Independent Contractor Requirements

Contracted Personnel shall sign a confidentiality (nondisclosure) agreement as part of their initial terms and conditions of contract or employment.

5.3.8 Documentation Supplied to Personnel

TMCA make available documentation including TMCA CPS, TMCA CP, security policy, system documents to personnel, during training or employment.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

TMCA shall stores all records related to the key generating system, certificate generating system, management system, directory system, and time-stamping system in file logs and manages them accordingly.

5.4.2 Frequency of Processing Log

Audit logs should be reviewed periodically for any event of malicious activities and following each critical operation.

5.4.3 Retention Period for Audit Log

No stipulation.



TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

5.4.4 Protection of Audit Log

Audit logs are protected by physical and electronic security measures, and can be accessed by authorized personnel by configuring its system and established operational procedures. The records of the event shall be protected from alteration and data tempering and separate from its originally generated.

5.4.5 Audit Log Backup Procedures

5.4.6 Incremental backups of audit logs are created daily and full backups shall be performed weekly by authorised Trusted Personnel. The backup are stored in a secure location. Audit Collection System (Internal vs. External)

No stipulation.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

No stipulation.

5.5 Records Archival

5.5.1 Types of Records Archived

TMCA includes reasonably sufficient detail of the records to show validity of the proper operation of the CA system and of generated certificates according to this CP and the corresponding CPS.

5.5.2 Retention Period for Archive

TMCA shall archive the original records and the copies are archived secure sites for ten (10) years.

5.5.3 Protection of Archive

All archives created for TMCA shall be logically secured and shall be stored in adequately safeguarded locations owned or managed by TMCA.

5.5.4 Archive Backup Procedures

No Stipulation.

5.5.5 Requirements for Time-Stamping of Records

No stipulation.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

5.6 Key Changeover

No stipulation.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

No stipulation.

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

TMCA has a maintenance services with vendor to ensure the stability of the system and application.

In the event of computing resources (virtual machine) malfunction, software and data corruption, TMCA technical team will restores the system immediately using dual backup system resources, as well as engaging the vendor to provide the support.

The downtime may be vary depending on situation and resources. Approximately 6 hours of downtime for full restoration.

When major data such as Subscribers' certificates are damaged or lost, TMCA restores them immediately using backup data.

5.7.3 Entity Private Key Compromise Procedures

If the TMCA Private Key is Compromised, TMCA shall revoke the CA certificate.

5.7.4 Business Continuity Capabilities After a Disaster

TMCA has the capability to restore or recover essential operations within twenty-four (24) hours following a disaster with, at a minimum, support for the following functions:

- Certificate issuance,
- Certificate revocation,
- Publication of revocation information, and
- Provision of key recovery information for customers.

5.8 CA or RA Termination

Validity of digital certificates issued by TMCA shall be terminated in the event one of the following arises:

- a. The term of the digital certificate's validity elapses.
- b. The designation of TMCA as a licensed Certification Authority is cancelled by MCMC.
- c. The digital certificate issued by TMCA is suspended.
- d. The digital certificate issued by TMCA is revoked.
- e. The CA certificate issued by Root CA to TMCA is revoked.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

TMCA shall perform the generation of key pairs for:

- (a) All CA key pairs are generated in pre-planned Key Generation Ceremonies in accordance to the requirements of the Key Ceremony guidelines and meeting FIPS 140-1 level 3 cryptographic requirements. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by TMCA.
- (b) Generation of RA key pairs will be performed by Authorised RA by using cryptographic software provided and meeting FIPS 140-1 level 3 cryptographic requirements.
- (c) Generation of end-user Subscriber key pairs will be performed by the Subscriber. This is applicable for all classes of digital certificates and the appropriate tools/software shall be used by meeting FIPS 140-1 level 3 cryptographic requirements.

6.1.2 Private Key Delivery to Subscriber

Private Keys may be delivered via electronic communication (e.g. e-mail) or hardware token to the Subscriber where the private key must be protected from activation, compromise, or modification during the delivery process.

6.1.3 Public Key Delivery to Certificate Issuer

The CA Certificate containing the Public Key corresponding to the CA's signing key is delivered to each End-User electronically via email or using hardware token.

6.1.4 CA Public Key Delivery to Relying Parties

The certificates of TMCA are distributed to Relying Parties for certificate path validation purposes. TMCA's Public Keys are published at www.tmca.com.my.

6.1.5 Key Sizes

TMCA uses the following sizes and hash values to employ secure and reliable algorithms for digital signature and key encryption:

- a. For RSA and Digital Signature Algorithm (: 1024 bit or higher;
- b. For ECC: 160 bit or higher;
- c. For SHA-1: 160 bit or higher;
- d. For SHA-2: 2048 bit or higher.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key use with the RSA algorithm defined in PKCS-1 shall be generated and checked in accordance with PKCS-1.

TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

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

TMCA certificate extensions are defined by the X.509 v.3 standard.

TMCA uses certain constraints and extensions for its public PKI services which may limit the role and position of TMCA or subscriber certificate so that such subscribers can be identified under varying roles. As key usage extension limits the technical purposes for which a public key listed in a certificate may be used.

TMCA own certificates may contain a key usage extension that limits the functionality of a key to only signing certificates, certificate revocation lists, and other data.

6.2 Private Keys Protection and Cryptographic Module Engineering Controls

TMCA stores Private Keys and key generating modules in a secure storage device which is not connected to internal or external LAN and the secured storage device is protected from physical intrusion. The Private Keys are stored in access-authorised smart cards that are safe from leakage or tampering due to the use of double encryption method.

6.2.1 Cryptographic Module Standards and Controls

No stipulation.

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

The storage of the private key of TMCA requires multiple controls by appropriately authorised members of staff serving in trustworthy positions.

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

All Key Pairs will be backed-up. Backed-up keys are stored in encrypted form and protected at a level similar to or higher than the level stipulated for the primary version of the key.

6.2.5 Private Key Archival

TMCA private Signature keys and Subscriber Private Signature keys are not archived.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

After generation, the Private Keys are directly stored in the HSM box/smart card.

If a copy of the subject's keys is not required to be kept by the CA, once delivered to the subscriber, the private key must be maintained under the subscriber's sole control. Any copies of the subject's keys held by the CA must be destroyed.

6.2.7 Private Key Storage on Cryptographic Module

Digital signature modules used by TMCA are sealed; access-authorised, and equipped with functions that protect Private Keys from leakage or tampering.

TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

6.2.8 Method of Activating Private Key

The Private Key shall be protected from exposure and unauthorised usage using Subscriber' password. Each invocation of certificate function requires insertion of the Password associated with the Key Pair.

6.2.9 Method of Deactivating Private Key

HSM automatically deactivates all active Private Keys once the module itself is deactivated.

6.2.10 Method of Destroying Private Key

In the event that it's Licensed CA (Certification Authority) Certificate expires or when Private Root Keys are damaged or leaked or compromised, TMCA shall completely erase their physical storage media.

6.2.11 Cryptographic Module Rating

All Key Pairs are generated and stored in a hardware cryptographic module (Hardware Security Module, HSM) with FIPS 140 level approved method.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Keys Archival

TMCA stores certificates containing Public Keys in directory during the term of validity of the certificates or until the certificates are revoked.

6.3.2 Certificate Operational Periods and Key Pair Usage Period

Key Pairs used to perform TMCA functions have a maximum validity of twenty (20) years. All other Key Pairs will have a maximum validity of three (3)years. Key Pairs are not to be used beyond their validity period.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

All password is unique and unpredictable and offers a security level appropriate to that of the protected Key Pair.

6.4.2 Activation Data Protection

Password used for Key Pair activation must be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

TMCA utilises TMCA System that provides the following minimum functionalities:

- Access control to TMCA services and Trusted Roles
- Enforced separation of duties for Trusted Roles identification and authentication of Trusted Roles and associated identities
- Use of cryptography for session communication and database security
- Archival of TMCA and Subscriber history and audit data
- Audit of security-related events
- Self-test of security-related CA services
- Trusted path for identification of Trusted Roles and associated identities, and
- Recovery mechanisms for keys and the TMCA System.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

All software components of the PKI developed by TMCA are developed in conditions and following a process that ensure their security. TMCA uses CMMI processes during the design and development of their software. TMCA ensures, during software updates, the origin and integrity of the software.

Development and testing infrastructures are separated from the production infrastructure of the PKI.

TMCA ensures that all software updates are done in a secure way. Updates are performed by personnel in a Trusted Role.

6.6.1 System Development Controls

No stipulation.

6.6.2 Security Management Controls

No stipulation.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

- a. TMCA manages operation of the core certification systems and keeps monitoring the system current status and trend.
- b. For control of access networks, TMCA employs firewall systems.
- c. To protect network service from illegal intrusion, TMCA deploys intrusion detection systems.



TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

6.8 Time-Stamping

CA event protocols are being signed and time stamped. TMCA shall provide a time stamp service for use with document signing certificates.

TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version Number(s)

Certificates issued under this CP are constructed according to X.509 Version 3.

7.1.2 Certificate Extensions

Certificate extensions are processed in accordance with RFC5280.

All Certificates issued under this CP contain the X.509 Certificate Policy extension. This extension is not marked critical.

All Certificates issued under this CP contain the X.509 key usage extension. This extension is marked critical.

7.1.3 Algorithm Object Identifiers

7.1.3.1 Signature Algorithm OID

For signatures, SHA-2 hashing with RSA Encryption (OID 1.2.840.113549.1.1.11) is being used.

7.1.3.2 Encryption Algorithm OID

For encryption, the RSA algorithm (OID 1.2.840.113549.1.1.1) is being used.

7.1.4 Name Forms

Reference can be made to Appendix A “Application Form for TMCA Digital Certificate” and Appendix B “TMCA Subscriber Agreement”.

7.1.5 Name Constraints

Each distinguished name (DN) of an TMCA Certificate Subject includes ‘O = TM’.

7.1.6 Certificate Policy Object Identifier

No stipulation.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

TMCA populates the policy qualifiers extension with a general disclaimer and reference to the URL and e-mail address through which TMCA CP and other related documents can be obtained.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.



TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

7.2 CRL Profile

7.2.1 Version Number(s)

CRL issued under this CP are constructed according to X.509 Version 2.

7.2.2 CRL and CRL Entry Extensions

All software within TMCA PKI correctly processes CRL extensions as specified in RFC5280.

7.3 OCSP Profile

No stipulation.

7.3.1 Version Number(s)

No stipulation.

7.3.2 OCSP Extension

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency and Circumstances of Assessment

TMCA shall undergo with a minimum of once per year as part of its annual PKI audit. All audits shall be performed in compliance with TMCA CP and WebTrust for Certification Authorities version 2.2.2 Program. The audit also checks the consistency with Certification Practice Statement and Certification Policy.

8.2 Identity/Qualifications of Assessor

The compliance audit TMCA shall be performed by a certified public accounting firm with a demonstrated competency in the evaluation of Certification Authorities and Registration Authorities.

Internal auditors must have IT auditing experience and must be employed by TMCA.

8.3 Assessor's Relationship to Assessed Entity

Assessor shall be organizationally independent of the TMCA's operational and policy authorities.



TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

8.4 Topics covered by Assessment

Each audit will include, but is not limited to, compliance with TMCA CP and WebTrust for Certification Authorities version 2.2.2 Program.

Topics covered by each audit will include but are not limited to:

- a. CA environmental controls
- b. CA physical security controls
- c. Key life cycle management controls
- d. Certificate life cycle management controls
- e. CA infrastructure or administrative controls.

8.5 Actions Taken as Result of Deficiency

If a compliance audit shows deficiencies of TMCA, a determination of action to be taken shall be made. TMCA is responsible for developing and implementing a corrective action plan.

8.6 Communications of Results

The compliance auditor shall report the results of a compliance audit to TMCA.

TMCA shall treat audit results as sensitive commercial information and it will not be publicly available. Audit results will be made available to TMCA internal departments.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

TMCA reserves the right to require payment of a fee for delivery of TMCA services. Fees may differ depending on Certificate type and may be regularly increased or decreased at the exclusive discretion of TMCA. The corresponding pricelist is exclusive internal information to TMCA.

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

No stipulation.

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

All collected or processed personal data within TMCA is kept confidential and handled in full compliance with a applicable data protection legislation (Personal Data Protection Act). Certificate status information is not regarded as confidential and therefore public available via CRL.

9.3.1 Scope of Confidential Information

No stipulation.

TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

9.3.2 Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

No stipulation.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

TMCA's privacy plan can be found in www.tmca.com.my

9.4.2 Information Treated as Private

Non-public Subscriber information is treated as private.

9.4.3 Information Not Deemed as Private

Subscriber information issued in the certificates, certificate directory, and online CRLs is not deemed private information, subject to applicable law.

9.4.4 Responsibility to Protect Private Information

No stipulation.

9.4.5 Notice and Consent to Use Private Information

No stipulation.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

TMCA shall be permitted to disclose confidential and/or private information if required to do so by law or regulation. This section is subject to applicable laws.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

TMCA retains all rights, title, interest, including without intellectual property rights to the following:

- a. CP and CPS
- b. Certificates
- c. Revocation Information
- d. TMCA's root keys and root certificates

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

No stipulation.

TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscribers Representations and Warranties

No stipulation.

9.6.4 Relying Party Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

9.7.1 TMCA's Liability

TMCA shall not be held liable for losses due to false or forged signatures if they have complied with the Act, or for punitive or exemplary damages

9.7.2 RA's Liabilities

- In case Registration Authorities cause Subscribers and users to suffer damages by violating provisions in the CP, RAs shall be subject to the same liabilities as those applicable to TMCA, as shown in section "2.6.4 Limitations of liability."
- As a security for such Liability for Damages, Registration Authorities may subscribe to public liability insurance.

9.7.3 Subscriber's Liabilities

In case, Subscribers have caused TMCA to suffer losses due to violation of Subscribers' responsibilities in pursuant to the CP, TMCA shall have the rights to claim the losses from the Subscribers

9.8 Limitations of Liability

In addition to Applicable Laws, Subscriber Agreement and Relying Parties Agreement, TMCA shall limit TMCA's liability not exceeding the liability caps described below:

Class	Liability Caps
Class 1	No liability
Class 2	Ringgit Malaysia Twenty Five Thousand (RM25,000.00)

The liability of Subscribers shall be as set forth in the applicable Subscriber Agreement.

The Liability of Authorised RAs and TMCA shall be set out in the agreement(s) between them.

The liability of Relying Parties shall be set forth in the applicable Relying Parties Agreements.

9.9 Indemnities

9.9.1 CA Obligations

TMCA shall be obliged to:

- Operate in full accordance with this CP, as well as with any applicable laws of the governing jurisdiction.
- Frequently verify that its RA's comply with the relevant provisions of the CP.
- Publish Certificates in TMCA Repository and maintain Certificate status information therein in a manner accessible to all Relying Parties.
- Provide prompt notice in case of compromise of its own private key(s).
- Provide support to subscribers and relying parties as described in this CP.
- Issue electronic certificates in accordance with this CP.
- Revoke certificates issued according to this CP upon receipt of a valid and authenticated request to revoke a certificate from an RA and Subscriber, and
- Notify relying parties of certificate revocation by publishing CRLs on the TMCA repository.

9.9.2 RA Obligations

9.9.2.1 Operation of RAs

- a. To perform identity verification services, TMCA may outsource the functions to several Registration Authorities (RAs). RAs are reputable organisations that are capable to carry out the functions without compromising to the security procedures adopted by TMCA. Before RAs are appointed, the RAs need to sign up contract with TMCA and acceptance test will be carried out to ensure they are in compliance to the procedures.
- b. The main functions of RAs are as follows:
 - i. Receipt of application for certification services such as:
 - Issuance
 - Renewal
 - Suspension
 - Reinstatement
 - Revocation
 - ii. Personal identification of applicants.
 - iii. Requesting TMCA to issue applicants' certificates and notifying to applicants.
 - iv. Other functions related to certification services as commissioned by TMCA.

9.9.2.2 Observance of Certificate Policy

In providing licensed certification services, Registration Authorities must observe the rules in this CP and carry out registration functions faithfully.

TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

9.9.2.3 Receipt of Applications for Certification Services

- a. Registration Authorities must accept only those applications with accurate information and until verifications are completed, applications are not treated as "accepted". For personal identification, Registration Authorities observe specific guidelines set by TMCA.
- b. Once the reception process is completed, Registration Authorities issue receipt slips prepared by TMCA.
- c. Registration Authorities are prohibited from refusing receipt of certificate applications without valid reasons. If applications are rejected, Registration Authorities should clearly state the reasons the applications are rejected.

9.9.2.4 Protection of Private Information & Safekeeping of Data Security

Registration Authorities protect the private information obtained in performing the certification services and at all-time TMCA shall safeguard the security of data.

9.9.2.5 Safeguard of Facilities & Personnel

In performing the certification services, Registration Authorities must also observe security guidelines for facilities and personnel as set by TMCA.

9.9.3 Subscriber Obligations

9.9.3.1 Provision of Accurate Information

Subscriber must at all-time provide accurate and factual information demanded by TMCA. In the event that the information provided by the Subscriber is incomplete, false and misleading, TMCA shall have the rights to revoke the digital certificate issued without prior notice to the Subscriber.

9.9.3.2 Generation of Key Pair

Pursuant to Section 6.1 of the CP, Subscribers can generate Key Pair by using the system provided by TMCA. Optionally, Subscriber is able to generate Key Pair by using standard PKI software.

9.9.3.3 Protection & Safekeeping of Private Keys

- a. Subscribers are responsible at all time for the safekeeping of Private Keys to prevent their loss, damage, theft, or being compromised.
- b. In the event that the Private Keys belonging to the Subscribers have been lost, damaged, stolen, or compromised, Subscribers should immediately notify TMCA via email or call TMCA Data Center.
- c. TMCA after further verification shall determine as to whether to revoke the Subscriber's digital certificate. This is to prevent further damage due to miss-use of the Subscriber's digital certificates by an unauthorised person.

9.9.3.4 Use of Private Key

Subscribers should use the Private Key that matches the Public Key contained in the TMCA-issued digital certificate.

TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

9.9.3.5 Verification of Digital Certificates

On receiving new digital certificates, Subscriber should verify the correctness of the information stored in the digital certificate such as distinguished name, the validity, issuing body, their types, and services.

In the event that the Subscriber discovers that some information may be invalid, the Subscriber must inform TMCA immediately via email or call TMCA Data Center. After further verification, TMCA shall determine whether to revoke the Subscriber's digital certificate and issue a new digital certificate.

9.9.4 Relying Party Obligations

Relying Party obligations are:

- Restrict reliance on certificates issued by TMCA to the purposes for those certificates, in accordance with TMCA CP.
- Verify the status of certificates at the time of reliance.
- Confirm the validity, issuing body, types, and purpose of the corresponding digital certificates before conducting e-business using digital certificates.
- Verify and confirm whether the digital certificates are suspended or revoked of their validity by using CRL.
- Damages if any due to users not observing the above confirmation process shall be exclusively borne by the Relying Parties.
- Agree to be bound by the provisions of limitations of liability as described in the CP upon reliance on a certificate issued by the TMCA.

9.9.5 Repository Obligations

TMCA's repository function is obligated to publish certificates and certificate revocation lists in a timely manner.

9.10 Term and Termination

9.10.1 Term

No stipulation.

9.10.2 Termination

No stipulation.

9.10.3 Effect of Termination and Survival

No stipulation.

9.11 Individual Notices and Communication with Participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

Editorial changes may be made to this CP and Glossary without notification of Subscribers and with creating a new version.

9.12.2 Notification Mechanism and Period

No stipulation.

9.12.3 Circumstances under Which OID Must Be Changed

No stipulation.

9.13 Dispute Resolution Procedures

No stipulation.

9.14 Governing Law

This CP is governed in accordance with the laws of Malaysia. Applicants, Subscribers, and Relying Parties irrevocably consent to jurisdiction of the courts of Malaysia.

9.15 Compliance with Applicable Law

The use of TMCA certificates shall always comply with the applicable law. This CP will be interpreted and applied in pursuant to the Digital Signature Act 1997 and other related Laws of Malaysia.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

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

No stipulation.

9.16.5 Force Majeure

No stipulation.



TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

9.17 Other Provisions

No stipulation.



TM Technology Service Sdn Bhd Certification Authority (TMCA)	Version 1.1
Certificate Policy (CP)	Publication Date: 4 TH MARCH 2024

Appendix A – Application Form for TMCA Digital Certificate



CONFIDENTIAL

TMCA DIGITAL CERTIFICATE APPLICATION FORM (INDIVIDUAL)

1. Applicable to Malaysians and foreign individuals above 18 of age.
 2. All applicants are advised to first read TMCA CPS available at <https://tmca.com.my/>
 3. Subscriber Agreement if required should be submitted together with this application.
 4. All sections in this form must be duly completed by the applicant. Any inconsistent application is liable to be rejected.
 6. All payments are accepted without prejudice to any legal action.
 7. For any replacement of certificates in due to the wrong/misleading information provided and/or changes required initiated by the subscriber, the chargeable amount shall be imposed to the subscriber at the certificate cost.
 8. Please attach an image of the following document:
 - NRIC (Malaysian only) or,
 - Passport
- Individual Identity document verification is via online eKYC, Commissioner of Oath/Professional Bodies/HR endorsement or face to face verification by appointed RA

PERSONAL DETAIL

Name (as in NRIC/Passport) _____

NRIC /Passport No _____

Date of Birth (dd/mm/yyyy) _____

Email Address _____

Correspondence Address _____

Postcode _____

Telephone Number _____

DECLARATION

I declare all the above information is true and valid to the best of its knowledge and hereby grant TMCA permission to verify the information from whatever sources. TMCA considers appropriate with the understanding that TMCA is bound by the Digital Signature Act 1997 and Digital Signature Regulations 1998 not to release such information unless required to do so by law or by an authority of higher order. Further, I agree to be bound by the Terms & Conditions as stated overleaf or any amendments made thereto and I declare that I have verified of all that is contained in the Acceptance Notice overleaf.

Signature of Applicant



Name of Applicant

Date

TERMS & CONDITIONS DECLARATION

You must read the following Terms & Conditions carefully before applying for, accepting or using TMCA Digital Certificate. If you do not agree to the Terms & Conditions, please refrain from applying, accepting or using the digital certificate. By agreeing to the Terms & Conditions, you are entering into an agreement with Telekom Applied Business Sdn. Bhd. (hereinafter referred to as "TMCA Subscriber Agreement"). This subscriber agreement will become effective once you submit the certificate application to Telekom Applied Business Sdn. Bhd. (TMCA). By submitting TMCA Subscriber Agreement and this application form, you are requesting TMCA to issue TMCA Digital Certificate to you. You must understand fully the information provided by TMCA and must familiar with the following terms:

- DIGITAL SIGNATURE ACT 1997 & DIGITAL SIGNATURE REGULATIONS 1998
- CERTIFICATION PRACTICE STATEMENT (CPS)
 - TMCA Digital Certificate services are governed by TMCA CPS. You agree to use the digital certificate and any related services provided by TMCA only in accordance with the CPS, which is published at TMCA's website, <http://www.tmca.com.my>.
- RIGHTS, DUTIES & LIABILITIES OF TMCA
 - TMCA provides limited warranties, disclaims all other warranties, including warranties of merchantability or fitness for a particular purpose, limits liability and excludes all liability for incidental, consequential, and punitive damage as stated in the CPS.

TMCA DIGITAL CERTIFICATE APPLICATION FORM (INDIVIDUAL)



CONFIDENTIAL

- All the information provided by the Subscriber in this application form will be kept confidential and will not be disclosed to any third party unless:
 - It is permitted by written law to be used for other purposes; or
 - The person affected has given that person's written consent for the data to be used for other purposes
- TMCA reserves the rights to amend this Terms & Conditions at any time and the amendments this Terms & Conditions shall be made available at this application form and TMCA's web site, <https://www.tmca.com.my>.
- **RIGHTS, DUTIES & LIABILITIES OF THE SUBSCRIBER**
 - You demonstrate your knowledge and acceptance of the terms of this subscriber agreement by either
 - Submitting this application for TMCA Digital Certificate; or
 - Using TMCA Digital Certificate, whichever occurs first.

ACCEPTANCE NOTICE

The following information will be incorporated in your selected class digital certificate.

- A statement stating that the type of certificate is in accordance with the regulation;
- The serial number of the certificate;
- The name of the subscriber as per application form;
- The distinguished name of the subscriber as per application form;
- The public key corresponding to the private key;
- An identifier of the algorithms with which the subscriber's public key is intended to be used;
- Validity period of the certificate as per application form;
- The distinguished name of TMCA;
- An identifier of the algorithms used to sign the certificate;
- A statement indicating the location of TMCA CPS, the method or procedures by which it may be retrieved, its form and structure, its authorship and its release date.


Other information required by the Digital Signature Regulations 1998 (Regulation 38) but not listed above shall be incorporated by reference to TMCA CPS.

By accepting this digital certificate, I hereby declare that:

1. The subscriber rightfully holds the private key corresponding to the public key listed in the certificate;
2. All representations made to TMCA or its Registration Authorities of the information listed in the certificate are true;
3. All material representations made to TMCA or its Registration Authorities (RA) or made in the certificate and not confirmed by TMCA or RA in issuing the certificate are true;
4. Acknowledge that the selected class digital certificate may only be used subject to the terms specified in TMCA CPS;
5. The subscriber agrees to assume duty to exercise reasonable care on protection and maintenance of the private key;
6. The subscriber undertakes to indemnify TMCA for any loss or damage caused by issuance or publication of the certificate in reliance on:
 - a) A false and material misrepresentation of fact by the subscriber;
 - b) The failure by the subscriber to disclose a material fact.
 If the representation or failure to disclose was made either with intent to deceive the Licensed Certificate Authority or a person relying on the certificate, or with negligence.


Agreement to Terms & Conditions and Certificate Information

Signature of Subscriber

 RIGHT CLICK ON IMAGE AND CHOOSE CHANGE PICTURE	Name	_____
	NRIC/Passport No	_____
	Date	_____

Verified By Authorised TMCA Personnel/RA

Signature of Authorised TMCA Personnel/RA

 RIGHT CLICK ON IMAGE AND CHOOSE CHANGE PICTURE	Name	_____
	NRIC/Passport No	_____
	Date	_____

Page 2 of 3



CONFIDENTIAL

IMAGES OF SUPPORTING DOCUMENT

Please attach a clear and readable image of your identity document:

- For NRIC or MYENTERA - Front and back page for card type identity document **OR**



- Passport - details page

