



TM TECHNOLOGY SERVICES SDN BHD
CERTIFICATE AUTHORITY
(TMCA)

CERTIFICATION PRACTICE STATEMENT
(CPS)
VERSION 1.2.2

DATE OF PUBLICATION: 1st JULY 2024

COPYRIGHT ©2024 TM TECHNOLOGY SERVICES SDN BHD
ALL RIGHTS RESERVED

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

Revision History

Date	Version	Modification Type	Item/Ref. No.	Description	Author
7th July, 2023	1	New		Approved for publication.	TMCA CPS Committee
28th July 2023	1	Edits	Header	Change header from Telekom Malaysia Certificate Authority to TM Tech Certificate Authority	Amalia Binti Mohd Mahdzir
28th July 2023	1	Edits	Preface	Change TELEKOM MALAYSIA to TM Technology Services Sdn Bhd	Amalia Binti Mohd Mahdzir
7th August 2023	1	Edits	TOC	Add in missing numbering for item 8	Amalia Binti Mohd Mahdzir
7th August 2023	1.1	Revise	3.2.3	Review and add in verification process for Class 1 certificate.	TMCA CPS Committee
7th August 2023	1.1	Revise	6.8	Revised and edit TSA statement to no stipulation	TMCA CPS Committee
7th August 2023	1.1	Revise	9.8	Revised liability cap for Class 1 certificate	TMCA CPS Committee
19th February 2024	1.2	Revise	3.2.3	Remove clause 3.2.3 Class 3	TMCA CPS Committee
19th February 2024	1.2	Revise	4.3.2	Remove clause 4.3.2 Class 3 Digital Certificate Application Process Flow	TMCA CPS Committee
30 th MAY 2024	1.2	Revise		Pending Approval	TMCA CPS Committee
30 th MAY 2024	1.2.1	Revise	2.2	Remove CRL Confidentiality statement	TMCA CPS Committee
30 th MAY 2024	1.2.1	Edit	3.1.1	Add in BRN & TIN for corporate certificate	TMCA CPS Committee
30 th MAY 2024	1.2.1	Revise	3.1.5	Revised Distinguish names	TMCA CPS Committee
30 th MAY 2024	1.2.1	Revise	4.2.1	Revise numbering (RFC 7382)	TMCA CPS Committee
30 th MAY 2024	1.2.1	Edit	4.3.1	Edit DN terminology to subject	TMCA CPS Committee
30 th MAY 2024	1.2.1	Revise	4.3.3	Revised numbering (RFC 7382)	TMCA CPS Committee
30 th MAY 2024	1.2.1	Edit	4.4.2	Edit Publication of the Certificate by the CA	TMCA CPS Committee
30 th MAY 2024	1.2.1	Edits	4.5.2	Edit in DSA 1998 clause	TMCA CPS Committee
30 th MAY 2024	1.2.1	Edits	4.9.2	Edit in DSA 1998 Clause	TMCA CPS Committee
30 th MAY 2024	1.2.1	Revise	4.11	Revise numbering - Circumstances for Suspension	TMCA CPS Committee
30 th MAY 2024	1.2.1	Revise	5.4.6 /5.4.7	Omitted (RFC7382)	TMCA CPS Committee
30 th MAY 2024	1.2.1	Edit	9.11	Edit fee table	TMCA CPS Committee
30 th MAY 2024	1.2.1	Revise	9.1.2, 9.1.3. 9.1.4	Omitted (RFC7382)	TMCA CPS Committee
30 th MAY 2024	1.2.1	Edit	9.13	Edit Claims (DSA 1998)	TMCA CPS Committee
20th JUNE 2024	1.2.2	Revise	Preface	Add in brief explanation of Digital Certificate, Digital Signature, DSA 1997, DSR 1998, The Rights, Duties, and Liabilities of the Licensed CA, RA,	TMCA CPS Committee

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

				Subscribers, and Relying Parties	
1 st July 2024	1.2.2	Edit	1.3.1.2	Edit SubCA terminology to TMCA Trust Anchor	TMCA CPS Committee
1st July 2024	1.2.2	Revise	1.3.3	Revise Subscriber	TMCA CPS Committee
1st July 2024	1.2.2	Revise	1.3.4	Revise Relying Party	TMCA CPS Committee
1st July 2024	1.2.2	Revise	1.4.1	Revise Appropriate Certificate Uses – add in Class 3	TMCA CPS Committee
1st July 2024	1.2.2	Revise	2.2	Revise Repository	TMCA CPS Committee
1st July 2024	1.2.2	Revise	2.4	Revise Usage Accounting Processes	TMCA CPS Committee
1st July 2024	1.2.2	Revise	3.2.3	Revise Authentication of Individual Identity	TMCA CPS Committee
1st July 2024	1.2.2	Revise	4.1.2	Revise Enrolment Process and Responsibilities	TMCA CPS Committee
1st July 2024	1.2.2	Revise	4.2.1.3	Edit Class 3 Digital Certificate Application Process Flow	TMCA CPS Committee
1st July 2024	1.2.2	Revise	4.3.1	Revise CA Action During Certificate Issuance	TMCA CPS Committee
1st July 2024	1.2.2	Revise	5.7.3	Revise Entity Private Key Compromise Procedure	TMCA CPS Committee
1st July 2024	1.2.2	Edit	9.1	Edit Fee	TMCA CPS Committee
1st July 2024	1.2.2	Revise	9.4	Revise Privacy Plan	TMCA CPS Committee
1st July 2024	1.2.2	Revise	9.8	Revise Limitation of Liability	TMCA CPS Committee
1st July 2024	1.2.2	Revise	9.1.4	Revise Governing Law	TMCA CPS Committee

Notice

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

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

Contents

1	INTRODUCTION	15
1.1	OVERVIEW	15
1.2	DOCUMENT NAME AND IDENTIFICATION	15
1.3	PKI PARTICIPANTS	15
1.3.1	CERTIFICATION AUTHORITIES	15
1.3.2	REGISTRATION AUTHORITIES (RAS)	16
1.3.3	SUBSCRIBERS	16
1.3.4	RELYING PARTIES	19
1.3.5	OTHER PARTICIPANTS	20
1.4	CERTIFICATE USAGE	20
1.4.1	APPROPRIATE CERTIFICATE USES	21
1.4.2	PROHIBITED CERTIFICATE USES	23
1.5	POLICY ADMINISTRATION	23
1.5.1	ORGANISATION ADMINISTERING THE DOCUMENT	23
1.5.2	CONTACT PERSON	24
1.5.3	PERSON DETERMINING CP/CPS SUITABILITY FOR THE POLICY	24
1.5.4	CPS APPROVAL PROCEDURES	24
1.6	DEFINITIONS AND ACRONYMS	24
2	PUBLICATION AND REPOSITORY RESPONSIBILITIES	26
2.1	REPOSITORIES	26
2.2	PUBLICATION OF CERTIFICATION INFORMATION	26
2.2.1	TMCA STATEMENT ON REPOSITORY PUBLICATION CRITERIA	26
2.3	TIME OR FREQUENCY OF PUBLICATION	27
2.4	ACCESS CONTROLS ON REPOSITORIES	27
2.4.1	USAGE ACCOUNTING PROCESSES	27
2.4.2	ACCESS MANAGEMENT PROCESSES	28
2.4.3	COMPLIANCE AND LEGAL FRAMEWORK	28
3	IDENTIFICATION AND AUTHENTICATION	30
3.1	NAMING	30
3.1.1	TYPE OF NAMES	30
3.1.2	NEED FOR NAMES TO BE MEANINGFUL	30
3.1.3	ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS	30
3.1.4	RULES FOR INTERPRETING VARIOUS NAME FORMS	30
3.1.5	UNIQUENESS OF NAMES	30
3.1.6	RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS	30
3.1.7	PERSONAL IDENTIFICATION FOR SUSPENSION & REVOCATION OF DIGITAL CERTIFICATES	30
3.2	INITIAL IDENTITY VALIDATION	31
3.2.1	METHOD TO PROVE POSSESSION OF PRIVATE KEY	31
3.2.2	AUTHENTICATION OF ORGANISATION IDENTITY	31
3.2.3	AUTHENTICATION OF INDIVIDUAL IDENTITY	31

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

3.2.4	NON-VERIFIED SUBSCRIBER INFORMATION	32
3.2.5	VALIDATION OF AUTHORITY	32
3.2.6	CRITERIA FOR INTEROPERATION	32
3.3	IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS	32
3.3.1	IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY	32
3.3.2	IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION	32
3.4	IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS	32
4	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	34
4.1	CERTIFICATE APPLICATION	34
4.1.1	WHO CAN SUBMIT A CERTIFICATE APPLICATION?	34
4.1.2	ENROLMENT PROCESS AND RESPONSIBILITIES	34
4.2	CERTIFICATE APPLICATION PROCESSING	37
4.2.1	PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS	37
4.2.2	APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS	39
4.2.3	TIME TO PROCESS CERTIFICATE APPLICATIONS	39
4.3	CERTIFICATE ISSUANCE	40
4.3.1	CA ACTIONS DURING CERTIFICATE ISSUANCE	40
4.3.2	NOTIFICATIONS TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE	40
4.3.3	NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES	40
4.4	CERTIFICATE ACCEPTANCE	40
4.4.1	CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE	40
4.4.2	PUBLICATION OF THE CERTIFICATE BY THE CA	41
4.4.3	NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES	41
4.5	KEY PAIR AND CERTIFICATE USAGE	41
4.5.1	SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE	41
4.5.2	RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE	42
4.6	CERTIFICATE RENEWAL	42
4.6.1	CIRCUMSTANCES FOR CERTIFICATE RENEWAL	42
4.6.2	WHO MAY REQUEST RENEWAL	42
4.6.3	PROCESSING CERTIFICATE RENEWAL REQUESTS	42
4.6.4	NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER	43
4.6.5	CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE	43
4.6.6	PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA	43
4.6.7	NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES	43
4.7	CERTIFICATE RE-KEY	43
4.7.1	CIRCUMSTANCES FOR CERTIFICATE RE-KEY	43
4.7.2	WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY	43
4.7.3	PROCESSING CERTIFICATE RE-KEYING REQUESTS	43
4.7.4	NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER	43
4.7.5	CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE	43
4.7.6	PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA	43
4.7.7	NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES	44
4.8	CERTIFICATE MODIFICATION	44
4.8.1	CIRCUMSTANCES FOR CERTIFICATE MODIFICATION	44
4.8.2	WHO MAY REQUEST CERTIFICATE MODIFICATION	44
4.8.3	PROCESSING CERTIFICATE MODIFICATION REQUESTS	44
4.8.4	NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER	44
4.8.5	CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE	44
4.8.6	PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA	44

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

4.8.7	NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES	44
4.9	CERTIFICATE REVOCATION AND SUSPENSION	44
4.9.1	CIRCUMSTANCES FOR REVOCATION	44
4.9.2	WHO CAN REQUEST FOR REVOCATION	44
4.9.3	PROCEDURE FOR REVOCATION REQUEST	45
4.9.4	REVOCATION REQUEST GRACE PERIOD	45
4.9.5	TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST	45
4.9.6	REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES	45
4.9.7	CRL ISSUANCE FREQUENCY	45
4.9.8	MAXIMUM LATENCY FOR CRLs	45
4.10	CERTIFICATE STATUS SERVICES	46
4.10.1	OPERATIONAL CHARACTERISTICS	46
4.10.2	SERVICE AVAILABILITY	46
4.10.3	OPTIONAL FEATURES	46
4.11	CIRCUMSTANCES FOR SUSPENSION	46
4.11.1	WHO CAN REQUEST SUSPENSION	46
4.11.2	PROCEDURE FOR SUSPENSION REQUEST	46
4.11.3	LIMITS ON SUSPENSION PERIOD	47
4.12	END OF SUBSCRIPTION	47
4.13	KEY ESCROW AND RECOVERY	47
4.13.1	KEY ESCROW AND RECOVERY POLICY AND PRACTICES	47
4.13.2	SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES	47
5	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	48
5.1	PHYSICAL SECURITY CONTROL	48
5.1.1	SITE LOCATION AND CONSTRUCTION	48
5.1.2	PHYSICAL ACCESS	48
5.1.3	POWER AND AIR CONDITIONING	48
5.1.4	WATER EXPOSURES	48
5.1.5	FIRE PREVENTION AND PROTECTION	48
5.1.6	MEDIA STORAGE	48
5.1.7	WASTE DISPOSAL	48
5.1.8	OFFSITE BACKUP	49
5.2	PROCEDURAL CONTROLS	49
5.2.1	TRUSTED ROLES	49
5.2.2	NUMBER OF PERSONS REQUIRED PER TASK	49
5.2.3	IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE	49
5.2.4	ROLES REQUIRING SEPARATION OF DUTIES	49
5.3	PERSONNEL CONTROLS	49
5.3.1	QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS	49
5.3.2	BACKGROUND CHECK PROCEDURES	49
5.3.3	TRAINING REQUIREMENTS	49
5.3.4	RETRAINING FREQUENCY AND REQUIREMENTS	49
5.3.5	JOB ROTATION FREQUENCY AND SEQUENCE	50
5.3.6	SANCTIONS FOR UNAUTHORISED ACTIONS	50
5.3.7	INDEPENDENT CONTRACTOR REQUIREMENTS	50
5.3.8	DOCUMENTATION SUPPLIED TO PERSONNEL	50
5.4	AUDIT LOGGING PROCEDURES	51
5.4.1	TYPES OF EVENTS RECORDED	51
5.4.2	FREQUENCY OF PROCESSING LOG	51

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

5.4.3	RETENTION PERIOD FOR AUDIT LOG	51
5.4.4	PROTECTION OF AUDIT LOG	51
5.4.5	AUDIT LOG BACKUP PROCEDURES	51
5.4.6	VULNERABILITY ASSESSMENTS	51
5.5	RECORDS ARCHIVAL	52
5.5.1	TYPES OF RECORDS ARCHIVED	52
5.5.2	RETENTION PERIOD FOR ARCHIVE	52
5.5.3	PROTECTION OF ARCHIVE	52
5.5.4	ARCHIVE BACKUP PROCEDURES	52
5.5.5	REQUIREMENTS FOR TIME-STAMPING OF RECORDS	52
5.5.6	ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)	52
5.5.7	PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION	52
5.6	KEY CHANGEOVER	52
5.7	COMPROMISE AND DISASTER RECOVERY	53
5.7.1	INCIDENT AND COMPROMISE HANDLING PROCEDURES	53
5.7.2	COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED	53
5.7.3	ENTITY PRIVATE KEY COMPROMISE PROCEDURES	53
5.7.4	BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER	53
5.8	CA OR RA TERMINATION	54
6	TECHNICAL SECURITY CONTROLS	55
6.1	KEY PAIR GENERATION AND INSTALLATION	55
6.1.1	KEY PAIR GENERATION	55
6.1.2	PRIVATE KEY DELIVERY TO SUBSCRIBER	55
6.1.3	PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER	55
6.1.4	CA PUBLIC KEY DELIVERY TO RELYING PARTIES	55
6.1.5	KEY SIZES	55
6.1.6	PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING	55
6.1.7	KEY USAGE PURPOSES (AS PER X.509 v3 KEY USAGE FIELD)	55
6.2	PRIVATE KEYS PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	56
6.2.1	CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS	56
6.2.2	PRIVATE KEY (N OUT OF M) MULTI PERSON CONTROL	56
6.2.3	PRIVATE KEY ESCROW	56
6.2.4	PRIVATE KEY BACKUP	56
6.2.5	PRIVATE KEY ARCHIVAL	56
6.2.6	PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE	56
6.2.7	PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE	56
6.2.8	METHOD OF ACTIVATING PRIVATE KEY	56
6.2.9	METHOD OF DEACTIVATING PRIVATE KEY	56
6.2.10	METHOD OF DESTROYING PRIVATE KEY	56
6.2.11	CRYPTOGRAPHIC MODULE RATING	57
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT	57
6.3.1	PUBLIC KEYS ARCHIVAL	57
6.3.2	CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIOD	57
6.4	ACTIVATION DATA	57
6.4.1	ACTIVATION DATA GENERATION AND INSTALLATION	57
6.4.2	ACTIVATION DATA PROTECTION	57
6.4.3	OTHER ASPECTS OF ACTIVATION DATA	57
6.5	COMPUTER SECURITY CONTROLS	57
6.5.1	SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS	57

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

6.5.2	ENFORCED SEPARATION OF DUTIES FOR TRUSTED ROLES IDENTIFICATION AND AUTHENTICATION OF TRUSTED ROLES AND ASSOCIATED IDENTITIES	57
6.5.3	COMPUTER SECURITY RATING	57
6.6	LIFE CYCLE TECHNICAL CONTROLS	58
6.6.1	SYSTEM DEVELOPMENT CONTROLS	58
6.6.2	SECURITY MANAGEMENT CONTROLS	58
6.6.3	LIFE CYCLE SECURITY CONTROLS	58
6.7	NETWORK SECURITY CONTROLS	58
6.8	TIME-STAMPING	58
7	CERTIFICATE, CRL, AND OCSP PROFILES	59
7.1	CERTIFICATE PROFILE	59
7.1.1	VERSION NUMBER(S)	59
7.1.2	CERTIFICATE EXTENSIONS	59
7.1.3	ALGORITHM OBJECT IDENTIFIERS	59
7.1.4	NAME FORMS	59
7.1.5	NAME CONSTRAINTS	59
7.1.6	CERTIFICATE POLICY OBJECT IDENTIFIER	59
7.1.7	USAGE OF POLICY CONSTRAINTS EXTENSION	59
7.1.8	POLICY QUALIFIERS SYNTAX AND SEMANTICS	59
7.1.9	PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION	59
7.2	CRL PROFILE	59
7.2.1	VERSION NUMBER(S)	59
7.2.2	CRL AND CRL ENTRY EXTENSIONS	60
7.3	OCSP PROFILE	60
7.3.1	VERSION NUMBER(S)	60
7.3.2	OCSP EXTENSION	60
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	61
8.1	FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT	61
8.2	IDENTITY/QUALIFICATIONS OF ASSESSOR	61
8.3	ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY	61
8.4	TOPICS COVERED BY ASSESSMENT	61
8.5	ACTIONS TAKEN AS RESULT OF DEFICIENCY	61
8.6	COMMUNICATIONS OF RESULTS	61
9	OTHER BUSINESS AND LEGAL MATTERS	62
9.1	FEES	62
9.1.1	CERTIFICATE ISSUANCE OR RENEWAL FEES	62
9.1.2	CERTIFICATE ACCESS FEES (OMITTED)	62
9.1.3	REVOCATION OR STATUS INFORMATION ACCESS FEES (OMITTED)	62
9.1.4	FEES FOR OTHER SERVICES	62
9.1.5	REFUND POLICY	62
9.2	FINANCIAL RESPONSIBILITY	63
9.2.1	INSURANCE COVERAGE	63
9.2.2	OTHER ASSETS	63
9.2.3	INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES	63

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION	63
9.3.1 SCOPE OF CONFIDENTIAL INFORMATION	63
9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION	63
9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION	63
9.4 PRIVACY OF PERSONAL INFORMATION	63
9.4.1 PRIVACY PLAN	63
9.4.2 INFORMATION TREATED AS PRIVATE	70
9.4.3 INFORMATION NOT DEEMED AS PRIVATE	70
9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION	70
9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION	70
9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS	70
9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES	70
9.5 INTELLECTUAL PROPERTY RIGHTS	72
9.6 REPRESENTATIONS AND WARRANTIES	72
9.6.1 CA REPRESENTATIONS AND WARRANTIES	72
9.6.2 RA REPRESENTATIONS AND WARRANTIES	72
9.6.3 SUBSCRIBERS REPRESENTATIONS AND WARRANTIES	72
9.6.4 RELYING PARTY REPRESENTATIONS AND WARRANTIES	72
9.6.5 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS	72
9.7 DISCLAIMERS OF WARRANTIES	72
9.7.1 TMCA'S LIABILITY	72
9.7.2 RA'S LIABILITIES	72
9.7.3 SUBSCRIBER'S LIABILITIES	72
9.8 LIMITATIONS OF LIABILITY	72
9.8.1 TMCA LIABILITY CAP / RELIANCE LIMIT	72
9.8.2 RA LIABILITY	73
9.9 INDEMNITIES	73
9.10 TERM AND TERMINATION	73
9.10.1 TERM	73
9.10.2 TERMINATION	73
9.10.3 EFFECT OF TERMINATION AND SURVIVAL	73
9.11 INDIVIDUAL NOTICES AND COMMUNICATION WITH PARTICIPANTS	73
9.12 AMENDMENTS	73
9.12.1 PROCEDURE FOR AMENDMENT	73
9.12.2 NOTIFICATION MECHANISM AND PERIOD	73
9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED	73
9.13 DISPUTE RESOLUTION PROCEDURES	73
9.13.1 CLAIMS	73
9.14 GOVERNING LAW	74
9.15 COMPLIANCE WITH APPLICABLE LAW	74
9.16 MISCELLANEOUS PROVISIONS	74
9.16.1 ENTIRE AGREEMENT	74
9.16.2 ASSIGNMENT	74
9.16.3 SEVERABILITY	74
9.16.4 ENFORCEMENT (ATTORNEY'S FEE AND WAIVER OF RIGHTS)	74
9.16.5 FORCE MAJEURE	74
9.17 OTHER PROVISION	74
9.17.1 PERSONAL DATA	74
9.17.2 RIGHT TO AUDIT	74
1 APPENDIX A – APPLICATION FORM FOR TMCA DIGITAL CERTIFICATE	76

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

2 APPENDIX B – APPLICATION FORM FOR TMCA DIGITAL CERTIFICATE (BUS/GOV/NGO)

79

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

PREFACE

Objectives of TMCA CPS

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"), this Certification Practice Statement (CPS) 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. This documentation named Certification Practice Statement ("CPS") has been prepared by TMCA, in order to identify the policies and rules to be followed in the course of activities of TMCA certificate services, follows the framework and structure outlined in the Internet Engineering Task Force RFC 7382

Overview of TMCA CPS

TMCA CPS provides information about the policies, practices and procedures employed by TMCA to perform certification services. This document outlines the standard procedures of issuing, managing, suspending, revoking and renewing digital certificates by TMCA. The CPS 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 CPS before

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

submitting application for a digital certificate.

Prior to accepting the terms & conditions of this CPS, it is advisable for potential Subscribersto 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;
- 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

Digital Certificates

Digital Certificates are electronic credentials that are used to establish the identity of entities such as individuals, organizations, or devices in digital communications. They serve a similar purpose to physical identification documents, like a passport or driver's license, but in the digital realm. A digital certificate contains a public key, the identity of the certificate holder, and is issued by a trusted third party known as a Certificate Authority (CA). The CA digitally signs the certificate to attest to the validity of the holder's identity and the association with the public key. Digital certificates enable secure, encrypted communications and are fundamental to the operation of Public Key Infrastructure (PKI). TMCA as licenced CA in Malaysia generate Digital Certificates.

Digital Signatures

Digital Signatures are cryptographic mechanisms that provide a secure and tamper-evident way to sign electronic documents. They ensure the authenticity, integrity, and non-repudiation of the signed document. A digital signature is created using the signer's private key, and it can be verified by anyone using the corresponding public key, which is typically embedded in a digital certificate. When a document is signed digitally, any alteration to the document after signing will invalidate the signature, alerting the recipient to potential tampering. Digital signatures are widely used in electronic transactions, legal agreements, and official communications to ensure security and trust.

Digital Signature Act 1997 (Malaysia)

The Digital Signature Act 1997 is a legislative framework established by the Malaysian government to regulate the use of digital signatures within the country. This Act provides legal recognition for digital signatures, making them legally equivalent to handwritten signatures under certain conditions. It sets out the requirements for the licensing of Certification Authorities (CAs), the responsibilities of licensed CAs, and the standards for digital signatures to be considered valid. The Act aims to facilitate secure electronic commerce and communications by providing a trusted environment for digital transactions.

Digital Signature Regulations 1998 (Malaysia)

The Digital Signature Regulations 1998 were introduced to support and implement the provisions of the Digital Signature Act 1997. These regulations detail the operational requirements and standards that licensed Certification Authorities (CAs) must adhere to. They cover aspects such as the application process for CA licenses, the obligations of CAs, the procedures for issuing and managing digital certificates, and the compliance requirements. The regulations ensure that CAs operate in a secure and reliable manner, providing a trustworthy infrastructure for digital signatures in Malaysia.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

The Rights, Duties, and Liabilities of the Licensed CA, RA, Subscribers, and Relying Parties

Licensed Certification Authorities (CAs)

- **Rights:** Licensed CAs have the authority to issue, manage, and revoke digital certificates. They can charge fees for their services and enter into agreements with subscribers and relying parties.
- **Duties:** CAs must adhere to the standards and regulations set forth in the Digital Signature Act 1997 and Digital Signature Regulations 1998. They must ensure the accuracy and security of the digital certificates they issue and maintain robust systems to prevent fraud and misuse.
- **Liabilities:** CAs are liable for any damages resulting from the failure to comply with legal and regulatory requirements, including issuing false or fraudulent certificates.

Registration Authorities (RAs)

- **Rights:** RAs act on behalf of CAs to verify the identity of certificate applicants and facilitate the certificate issuance process.
- **Duties:** RAs must follow the procedures and guidelines established by the CAs and regulatory authorities to ensure accurate identity verification and secure handling of applicant information.
- **Liabilities:** RAs share responsibility with CAs for the accuracy of identity verification and can be held liable for any negligence or misconduct in the verification process.

Subscribers

- **Rights:** Subscribers have the right to obtain and use digital certificates for secure communications and transactions. They can request the revocation of their certificates if they are compromised.
- **Duties:** Subscribers must provide accurate information during the certificate application process, protect their private keys, and use their digital certificates responsibly.
- **Liabilities:** Subscribers are liable for any misuse of their digital certificates and private keys, including any unauthorized transactions resulting from their negligence.

Relying Parties

- **Rights:** Relying parties have the right to trust and use the digital certificates issued by licensed CAs for verifying digital signatures and secure communications.
- **Duties:** Relying parties must exercise due diligence in verifying the validity and status of digital certificates before relying on them for critical transactions.
- **Liabilities:** Relying parties are responsible for any consequences of relying on expired, revoked, or fraudulent certificates without proper verification.

Amendment, Publication & Notification of CPS

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

TMCA reserves the rights to amend this CPS at any time and the amendments to this CPS shall be made available at TMCA's web site, <https://www.tmca.com.my>. Amendments shall become effective automatically within fourteen (14) working days of the CPS being posted at the web site and

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

unless TMCA explicitly states otherwise prior to the end of the fourteen (14) days period.
Note, once the amendments have become effective, they shall supersede the earlier version of the CPS. The publication date is equivalent to the effective date of the CPS.

Customer Service & Other Information

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

59100 Kuala Lumpur

Tel No: 60133999398

For Business inquiries on certification services, and other technical inquiries:

Please email to: tmca.helpdesk@tm.com.my

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

1 INTRODUCTION

1.1 Overview

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"), this Certification Practice Statement (CPS) 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.

This CPS describes:

- Participants
- Publication of the certificates and Certificate Revocation Lists (CRLs)
- How certificates are issued, managed, re-keyed, renewed, and revoked
- Facility management (physical security, personnel, audit, etc.)
- Key management
- Audit procedures
- Business and legal issues

Certification Authority License

TMCA is licensed to issue digital certificates to individual/business/organization. The digital certificates can be used to improve the security in e-transactions in the public and private sectors.

1.2 Document Name and Identification

The name of this document is "TM TECH CERTIFICATE AUTHORITY CERTIFICATION PRACTICE STATEMENT (TMCA CPS)"

1.3 PKI Participants

Note that in a PKI the term "subscriber" refers to an individual or organization that is a subject of a certificate issued by a CA. The term is used in this fashion throughout this document, without qualification, and should not be confused with the networking use of the term to refer to an individual or organization that receives service from an ISP. In such cases, the term "network subscriber" will be used. Also note that, for brevity, this document always refers to PKI participants as organizations or entities, even though some of them are individuals.

TMCA CPS provides information about the policies, practices and procedures employed by TMCA to perform certification services. This document outlines the standard procedures of issuing, managing, suspending, revoking and renewing digital certificates by TMCA.

1.3.1 Certification Authorities

TM Technology Services Sdn Bhd (TMCA) is a licensed certification authority 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

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

1.3.1.1 Certification Authority License

TMCA is licensed to issue digital certificates to individual/business/organization/government agency

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:

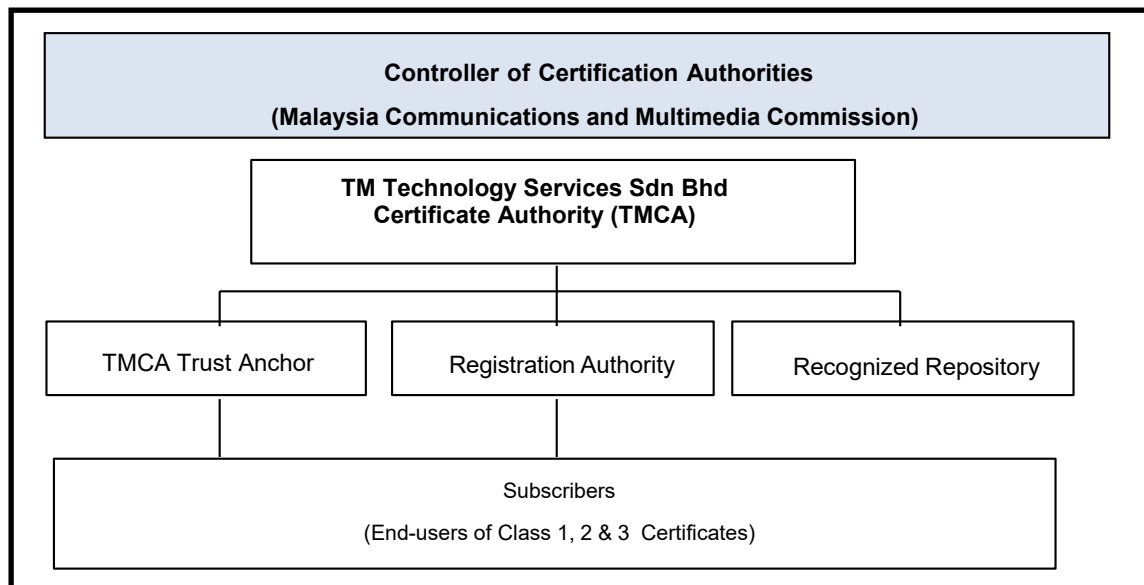


Figure 1 TMCA Infrastructure

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

1.3.1.3 TMCA Trust Anchor

In a distributed trust model, organizations may wish to become the issuer of Subscriber's certificates. TMCA Trust Anchor shall be the party who accepts applications, verifies, issues and revokes Subscriber certificates

TMCA operates in compliance with Malaysian laws by having a TMCA Trust Anchor internally within the organization. This means that TMCA assumes the responsibilities of both the primary CA and any subordinate roles necessary for the effective management of its certification services.

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.

1.3.3 Subscribers

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

These are the Subscribers/end-users of TMCA services. They could be individuals or organizations 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 organization. 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 prior to subscriptions, use and rely upon a certificate, subscriber are encourage to read through the information with regards to certificates and it's uses.

1.3.3.1 The restrictions and limitations

1.3.3.1.1 Usage Restrictions

Purpose-Specific Use: Digital certificates are often issued for specific purposes, such as email encryption, digital signatures, or server authentication. Subscribers must use the certificate only for its intended purpose.

1.3.3.1.2 Compliance with Policies

Subscribers must adhere to the policies and procedures outlined by the TMCA.

1.3.3.1.3 Non-Transferability

The subscriber cannot transfer their certificate to another individual or entity.

1.3.3.1.4 Security Limitations

a. Key Protection:

Subscribers must protect their private keys. If a private key is compromised, the associated certificate must be revoked, and the subscriber may need to obtain a new certificate. Subscriber to immediately notify the TMCA of the compromise of the subscriber's private key.

b. Password Management:

If a certificate is protected by a password, the subscriber is responsible for keeping that password secure. Losing the password can render the certificate unusable.

1.3.3.2 Management Limitations

1.3.3.2.1 Renewal and Revocation

Digital certificates have a finite validity period. Subscribers are responsible for renewing their certificates before they expire. Additionally, subscribers must promptly request the revocation of their certificates if they believe the certificate has been compromised.

1.3.3.2.2 Updates to Information:

If there are changes to the information contained in the certificate (e.g., a change in the subscriber's name or organizational details), the subscriber may need to update the certificate or obtain a new one.

1.3.3.3 Legal and Regulatory Constraints

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

1.3.3.3.1 Acceptance of the certificate

Before communicating any certificate to another person, or otherwise inducing their use or reliance on it, the subscriber must accept the certificate. Upon such acceptance, certain representations by the subscriber will be implied.

1.3.3.3.2 Due Diligence

The subscriber has a duty to exercise due diligence in verifying the authenticity and validity of the digital signature or certificate. To confirm that the certificate is valid and not revoked or suspended, please check at TMCA repository. The repository link is embedded in the digital certificate at Details>CRLDistribution Points, e.g.: URL= <http://www.tmca.com.my/crl/eCert2.crl>

Subscribers should use the received certificate to verify that the digital signature was created during the operational period of the certificate by the private key corresponding to the public key listed in the certificate and that the message associated with the digital signature received has not been altered.

1.3.3.3.3 Jurisdictional Compliance

Subscribers must comply with the legal and regulatory requirements of the jurisdictions in which they operate. This can include data protection laws, export controls, and other relevant regulations.

1.3.3.3.4 Audit and Logging

Subscribers may be required to maintain logs and records of their certificate usage for auditing purposes. This is often necessary for compliance with security and regulatory standards.

1.3.3.4 Technical Limitations

1.3.3.4.1 Compatibility

Subscribers must ensure that their systems and applications are compatible with the digital certificates they are using. This includes ensuring that their software supports the encryption algorithms and protocols specified by the certificate.

1.3.3.4.2 Certificate Chain

The trustworthiness of a digital certificate relies on the trustworthiness of the issuing CA and the certificate chain. Subscribers must ensure that the entire certificate chain is valid and trusted by their systems.

Understanding these restrictions and limitations is crucial for the effective and secure use of digital certificates.

1.3.3.4.3 Signature Longevity

It is important to re-sign data over time to maintain the signature security. Data with digital signatures may need to be re-signed before the security value of an available digital signature decreases with time. Digital signatures might need to be re-signed periodically to ensure their continued validity and security as cryptographic standards evolve and certificates expire or get revoked.

1.3.3.4.4 Time stamping requirement

If a time-stamp is required under any written law or if a particular time may be significant with regard to the use of digitally signed data, a time-stamp by a recognised DTS service should be appended or attached to the message or digital signature or other document.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

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.

1.3.4.1 Recipient of the subscriber's digital signature

1.3.4.1.1 Rights

a. Verification

The recipient has the right to verify the authenticity and integrity of the digital signature.

b. Reliance

They can rely on the digital signature as evidence of the signer's identity and intention.

c. Enforcement

The recipient can enforce the signed document or transaction in accordance with applicable laws and agreements.

d. Confidentiality

They may have rights regarding the confidentiality and privacy of the information contained in the signed document.

e. Non-repudiation

The recipient has the right to assert that the signer cannot deny their involvement in signing the document.

1.3.4.1.2 Duties

a. Due Diligence

The recipient has a duty to exercise due diligence in verifying the authenticity and validity of the digital signature. To confirm that the certificate is valid and not revoked or suspended, please check at TMCA repository. The repository link is embedded in the digital certificate at Details>CRL Distribution Points, e.g.: URL= <http://www.tmca.com.my/crl/eCert2.crl>

b. Protection

They must take reasonable steps to protect the integrity of the signed document and the associated digital signature.

c. Compliance

The recipient may have a duty to comply with any legal or regulatory requirements regarding the handling of

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

digitally signed documents.

d. Non-alteration

They should not alter the signed document in any way that would compromise its integrity or invalidate the digital signature.

e. Notification

If there are any discrepancies or issues with the signed document or digital signature, the recipient may have a duty to notify the appropriate parties.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

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 CPS.

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

TMCA reserves the rights to amend this CPS at any time and the amendments to this CPS shall be made available at TMCA's web site, <https://www.tmca.com.my>. Amendments shall become effective automatically within fourteen (14) working days of the CPS being posted at the web site and unless TMCA explicitly states otherwise prior to the end of the fourteen (14) days period.

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

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

1.4.1 Appropriate Certificate Uses

TMCA offers the following certificate classes:

Class	Usage	Assurance Level	Subscribers
Class 1 Digital Certificates	Class 1 Digital Certificates are ideal for personal use where basic security and identity verification are needed, such as securing email communication and accessing websites securely. This class of digital certificate is used for encryption and decryption of electronic data. As authentication of the user is simple sufficed with signed application form and email authentication, the digital certificates are not to be used to digitally sign a business transaction. Class 1 digital certificates provide low assurance on the identity of the Subscriber. For higher security needs, such as financial transactions or enterprise authentication, higher-class certificates are recommended	Low	Individual – Malaysian and Foreigner

Class	Usage	Assurance Level	Subscribers
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 / organization 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, organization certificate and server certificate.</p>	Medium	Individual
			SME/ Corporation/ Government
			Organization Members
			Organization
			NGO
	Secure Web Transaction	Medium	Web Server Operator
Class 3 Digital Certificate	<p>Certificates are individual and organizational Certificates that provide a high level of assurance of the identity of the Subject as compared to Class 1 and 2.</p> <p>Common Uses for Class 3 Digital Certificates</p> <ul style="list-style-type: none"> • High-Value Transactions • E-Governance 		

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

	<ul style="list-style-type: none"> • Enterprise Security. • Digital Signatures • SSL/TLS Certificates. • Code Signing • Smart Cards and Tokens <p>This class of digital certificate is used for digital signature, servers and software signing, for which independent verification and checking of identity and authority is done by the issuing certificate authority (CA) or Authorized RA. Application requires Notary Public endorsement.</p>		
--	---	--	--

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

1.4.1.1 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.
High	These are the Class 3 Individual and Organizational certificates that provide a high level of assurance of the identity of the Subscriber in comparison with Class 1 and 2.

1.4.2 Prohibited Certificate Uses

All certificate usages not listed in 1.4.1 are prohibited.

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

Tel: +6013 3999398

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

1.5.2 Contact Person

TMCA Manager
TM Technology Services Sdn Bhd (200201003726 [571389-H])
Level 28, TM Annexe 2
Jalan Pantai Baru
59100 Kuala Lumpur
Tel: +6013 3999398

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

1.5.3 Person Determining CP/CPS suitability for the Policy

TMCA CP/CPS committee determines CP and CPS suitability for the policy based on therecommendations received from the assessor.

1.5.4 CPS 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 CPS.
This CPS and any subsequent amendments shall be managed, reviewed and approved bythe management of TMCA.

TMCA reserves the rights to amend this CPS at any time and the amendments to this CPSshall be made available at TMCA's web site, <https://www.tmca.com.my>. Amendments shallbecome effective automatically within fourteen (14) working days of the CPS being posted at the web site and unless TMCA explicitly states otherwise prior to the end of the fourteen (14) days period.

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

1.6 Definitions and Acronyms

Acronyms and Abbreviations Used in CPS

Acronyms/Abbreviations	Description
ARL	Authority Revocation List
CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DSA	Digital Signature Act 1997
Acronyms/Abbreviations	Description
DSA	Digital Signature Algorithm(in cryptography)
DSR	Digital Signature Regulations 1998

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

ECC	Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
IP	Internet Protocol
ISO	International Standard Organization
ITU	International Telecommunications Union
OCSP	The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 2560 and is on the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI). Messages communicated via OCSP are encoded in ASN.1 and are usually communicated over HTTP. The "request/response" nature of these messages leads to OCSP servers being termed <i>OCSP responders</i> .
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
RP	Registration Personnel
TMCA	TM Tech Certificate Authority

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

2 PUBLICATION AND REPOSITORY 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

As per the CP, certificates and CRLs, MUST be made available for downloading by all relying parties, to enable them to validate this data.

TMCA 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 are available via LDAP directories. This CPS will be stored on a Web server and made available through <https://www.tmca.com.my>.

2.2.1 TMCA Statement on Repository Publication Criteria

At TMCA, the integrity and security of our repository are paramount. The publication of information within our repository is governed by stringent criteria to ensure accuracy, trustworthiness, and compliance with legal and regulatory standards.

2.2.1.1 Authorized Publishers

The following entities are authorized to publish information in the repository:

2.2.1.1.1 CA Administrators

Individuals with designated administrative roles within the CA organization are granted the authority to publish and manage information. These administrators undergo rigorous background checks and receive comprehensive training on compliance and security protocols.

Accredited Subordinate CAs: Subordinate Certificate Authorities that have been accredited by the primary CA are also authorized to publish information. This accreditation is contingent upon meeting the CA's stringent security and operational standards.

2.2.1.1.2 External Auditors

Independent auditors, who perform regular assessments of the CA's practices, may publish audit reports and findings, subject to confidentiality agreements and oversight by the CA administrators.

2.2.1.2 Legal Means and Criteria Enforcement:

The criteria for publishing information in the repository are legally enforced through a combination of internal policies, contractual agreements, and regulatory compliance mechanisms:

2.2.1.3 Internal Policies and Procedures

TM CA maintains a comprehensive set of internal policies and procedures that define the roles and responsibilities of authorized publishers, as well as the types of information that may be published. These policies are regularly reviewed and updated to ensure alignment with best practices and regulatory requirements.

2.2.1.4 Contracts and Agreements

All authorized publishers are bound by contractual agreements that explicitly outline their duties, the scope of their publishing rights, and the legal ramifications of non-compliance. These contracts are legally binding and enforceable.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

2.2.1.5 Regulatory Compliance

TMCA operates in compliance with relevant national and international standards, such as the WebTrust for Certification Authorities, Digital Signature Act 1997, and Digital Signature Regulation 1998

Compliance with the standards is verified through regular third-party audits, ensuring that TMCA adheres to the highest levels of security and operational integrity.

2.2.1.6 Audit and Monitoring

Continuous monitoring and periodic audits are conducted to ensure adherence to the established publishing criteria. Any deviations or violations are promptly addressed through corrective actions, which may include revocation of publishing rights and legal consequences.

By adhering to these stringent criteria and legal means, TMCA ensures that the information published in our repository is reliable, secure, and compliant with all applicable laws and regulations.

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.

2.4.1 Usage Accounting Processes

As a trusted Certificate Authority (CA), we are committed to maintaining a secure and transparent repository service. To ensure the integrity and proper usage of our repository, we have established comprehensive processes for accounting for its usage and managing access to the information published within it.

2.4.1.1 Logging and Monitoring

All interactions with the repository, including information publication, access requests, and data retrieval, are meticulously logged.

Advanced monitoring systems are employed to track and analyze these logs for any unauthorized or unusual activities.

2.4.1.2 Access Control

Access to the repository is restricted to authorized personnel and entities, as defined in our internal access control policies.

Multi-factor authentication (MFA) and role-based access control (RBAC) mechanisms are implemented to ensure that only eligible users can access specific information.

2.4.1.3 Usage Audits

Regular audits are conducted to review repository usage and access logs. These audits help identify any discrepancies or potential security breaches.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

Independent external auditors may also be engaged to perform periodic reviews of our processes and controls.

2.4.1.4 Usage Reporting

Detailed usage reports are generated and reviewed by CA administrators on a regular basis. These reports include metrics such as access frequency, data modification records, and user activity summaries.

Significant findings from these reports are escalated to senior management for further action.

2.4.2 Access Management Processes

2.4.2.1 User Authentication

Users accessing the repository are authenticated through secure login protocols, which may include password protection, biometric verification, and hardware tokens.

User credentials are managed and stored in compliance with industry standards to prevent unauthorized access.

2.4.2.2 Authorization Levels

Different levels of access rights are assigned based on user roles and responsibilities. This ensures that users can only access information pertinent to their functions.

Access rights are reviewed and updated regularly to accommodate changes in user roles or organizational structure.

2.4.2.3 Data Encryption

Information published in the repository is encrypted both in transit and at rest to safeguard against unauthorized access and data breaches.

Encryption keys are managed securely, with regular rotation and strict access controls.

2.4.2.4 Access Reviews and Revocation

Periodic access reviews are conducted to verify that users still require access to the repository. Any unnecessary access rights are promptly revoked.

Immediate revocation procedures are in place for users who leave the organization or no longer require access due to role changes.

2.4.3 Compliance and Legal Framework

2.4.3.1 Regulatory Adherence

Our repository services comply with relevant national and international regulations, including data protection laws and cybersecurity standards.

TMCA adhere to frameworks such as the PDPA and the WebTrust for Certification Authorities, ensuring our practices meet the highest standards of security and accountability.

2.4.3.2 Legal Agreements

Access to the repository is governed by legal agreements that outline the terms and conditions of use, including user responsibilities and consequences of misuse.

All authorized users and entities must agree to these terms before accessing the repository.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

By implementing these rigorous processes for usage accounting and access management, TMCA ensures the security, integrity, and reliability of the information published in our repository, fostering trust and confidence among all stakeholders.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Type of Names

For names used in the basic domain of digital certificates and the Certificate RevocationList (CRL) and OCSP (Online Certificate Status Protocol), the method of ITU-T X.500 DN (Distinguished Name) is applied.

Information **contained** in digital certificates and the CRL and OCSP is as follows:

a. Individual Certificate:

Real name as in Mykad, MyTentera, Polis Diraja MalaysiaCard or Passport; *May include - Mykad Number, MyTentera Number, Polis Diraja Malaysia Number, Passport Number or Email Address (optional)*

b. Corporate Certificate:

Real name as in Company Registration, Company ID, and E- mail Address. May include Business Registration Number(BRN) and Tax Identification Number(TIN)

c. Server Certificate:

Real Name as in Company Registration and Internet Domain Name (URLs for WWW).

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 names are not permitted.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

TMCA certifies Subject names that are unique among the certificates that it issues. Although it is desirable that these Subject names be unique throughout the PKI, to facilitate certificate path discovery, such uniqueness is not required, nor is it enforced through technical means. TMCA generates Subject names to minimize the chances that two entities in the PKI will be assigned the same name. Specifically, Subject|SerialNumber

3.1.6 Recognition, Authentication, and Role of Trademarks

Because the Subject names are not intended to be meaningful, TMCA makes no provision either to recognize or to authenticate trademarks, service marks, etc.

This CPS, and the information which it contains, is the property of TM Technology Services Sdn Bhd and its affiliates and licensors, and is protected from unauthorised copying and dissemination by Malaysian copyright law, trademark law, international conventions and other intellectual property laws.

3.1.7 Personal Identification for Suspension & Revocation of Digital Certificates

As stipulated in Section "3.2.3 Authentication of Individual Identity", for the individual/registered representative.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

In the event that the key pair is generated by the certificate applicant, the possession of the private key, shall be proven by sending the certificate signing request (CSR) or the application which includes its public key, to TMCA.

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	Email verification for the Class 1 certificate and application form with supporting documents must be attached.
Class 2 (Individual / Business /NGO)	Individual	Manual verification of ID if Subscriber visits to TMCA Office or Authorised RA Office. Supporting documents must be attached. If Subscriber is a member of corporate organisation, verification via company email or internal authentication should be sufficient. Alternatively, identities may be confirmed against a reliable third party database. In addition, TMCA shall incorporate additional controls that include face-to-face or eKYC verification.
	SME/Corporation/Organisation	Manual verification of ID if Subscriber visits to TMCA Office or Authorised RA Office. All supporting must be attached. Confirmation of organization identity is based upon the official identification document issued by government agencies. (e.g.: SSM Digital CTC). In addition, wherever applicable, a letter of representative authorisation from the organization. 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. All supporting must be attached. Confirmation of organization identity is based upon the official identification document issued by government agencies. (e.g.: SSM Digital CTC). In addition, wherever applicable, a letter of representative authorisation from the organization. TMCA shall incorporate additional controls that include face- to-face or eKYC verification.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

Class 3 (Individual / Business /NGO)	Individual	The application shall be certified by a notary public duly appointed under the Notaries Public Act 1959. All supporting documents must be attached. TMCA application shall include physical face to face verification.
	Corporation/Organisation/NGO	The application shall be certified by a notary public duly appointed under the Notaries Public Act 1959. All supporting documents must be attached. TMCA application shall include physical face to face verification.

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 CPS.
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. 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

All information in the certificates issued by TMCA will be verified.

3.2.5 Validation of Authority

No stipulation.

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 certificate renewal process is similar to an application for a new certificate unless agreed upon the relying parties between the Certification Authority and the Sub CA subscriber. 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

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

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. The Subscriber/customer also has the option to do it online through TMCA web-site www.tmca.com.my via digitally signed form. Revocation requests can be placed directly to www.tmca.com.my or via the revocation form in the TMCA repository at <http://www.tmca.com.my/repository>.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

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.

4.1.2 Enrolment Process and Responsibilities

The roles & responsibilities of the respective applicants are listed as follows:

Roles	Responsibilities
Authorized Officer – Corporate/SME	<ol style="list-style-type: none"> 1. An Authorized Officer is a 'trusted person' appointed by his company to oversee the use of digital certificate for his organization. This person who is the 'Applicant' responsible for applying the digital certificate on behalf of his company. A representative authorisation letter is required. 2. He requires eKYC verification or present for face-to-face verification at the office of Authorized RA. All supporting documents must be submitted together with the application form. Authorized RA must perform quality factors of selection, for example, not to approve the application if the applicant has criminal records.
Legal Agent – Corporate/SME	<ol style="list-style-type: none"> 1. Legal Agent for Corporate/SME is acting as a proxy for the company (client) who is entrusted with sourcing and obtaining digital certificates from TMCA for the company. In this case, the Legal Agent is the 'applicant' applying the digital certificates for his client. A representative authorisation letter is required. He requires eKYC verification or present for face-to-face verification at the office of TMCA or Authorized RA. All supporting documents must be submitted together with the application form. 2. Authorized RA must perform quality factors of selection, for example, not to approve the application if the applicant has criminal records.
Business Owner – Individual Business	<ol style="list-style-type: none"> 1. Business Owner is a person who represents for the business is the 'applicant' and his identity shall be verified via eKYC verification or by Authorized RA during the face-to-face verification process. All supporting documents must be submitted together with the application form. 2. Authorized RA must perform quality factors of selection, for example, not to approve the application if the applicant has criminal records.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

Roles	Responsibilities
Legal Agent – Individual Business	<ol style="list-style-type: none"> 1. Legal Agent for Individual Business is acting as a proxy for the company (client) who is entrusted with sourcing and obtaining digital certificates from a known and trusted CA for the company. In this case, the Legal Agent is the 'applicant' applying the digital certificates for his client. A representative authorisation letter is required. He requires eKYC verification or present for face-to-face verification at the office of AuthorizedRA. All supporting documents must be submitted together with the application form. 2. Authorized RA must perform quality factors of selection, for example, not to approve the application if the applicant has criminal records.
Authorized Officer – Voluntary Organization	<ol style="list-style-type: none"> 1. Authorized Officer from the voluntary organization is the 'applicant' responsible for applying digital certificates for the voluntary organization. A representative authorisation letter is required. All supporting documents must be submitted together with the application form. 2. Authorized RA must perform quality factors of selection, for example, not to approve the application if the applicant has criminal records.
Legal Agent – Voluntary Organization	<ol style="list-style-type: none"> 1. Legal Agent acting as proxy for the voluntary organization is the 'applicant' responsible for applying digital certificates for the voluntary organization. A representative authorisation letter is required. All supporting documents must be submitted together with the application form. 2. Authorized RA must perform quality factors of selection, for example, not to approve the application if the applicant has criminal records.
Government Employee	<ol style="list-style-type: none"> 1. Government Employee is the representative from the government agency or department, who has been given the authority to apply digital certificates for the agency. A representative authorisation letter is required. All supporting documents must be submitted together with the application form. 2. Authorized RA must perform quality factors of selection, for example, not to approve the application if the applicant has criminal records.
Ministry's Authorized Officer	<ol style="list-style-type: none"> 1. Ministry's Authorized Officer is the representative from the ministry, who has been given the authority to apply digital certificates for the ministry. All supporting documents must be submitted together with the application form. 2. Authorized RA must perform quality factors of selection, for example, not to approve the application if the applicant has criminal records.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

Notary Public	<ol style="list-style-type: none"> 1. Notaries Public are appointed by the Attorney General of Malaysia under The Notaries Public Act 1959. An experienced legal professionals, often lawyers, who meet specific qualifications and criteria set out by the Attorney General's Office. 2. Notaries Public are trusted public officers whose role is crucial in preventing fraud and ensuring the integrity of documents used in legal and commercial matters.
---------------	---

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 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 CPS. TMCA shall incorporate additional controls that include face- to-face or eKYC verification.

4.2.1.1 Class 1 Digital Certificate Application Process Flow

This is an online registration process for Class 1 digital certificate application, in which the applicant can apply for the digital certificate at TMCA portal at his convenience. The email verification will be incorporated as part of the registration process, therefore, the email address of the applicant must be valid before TMCA is able to acknowledge the application and then send a notification email for him to activate the certificate.

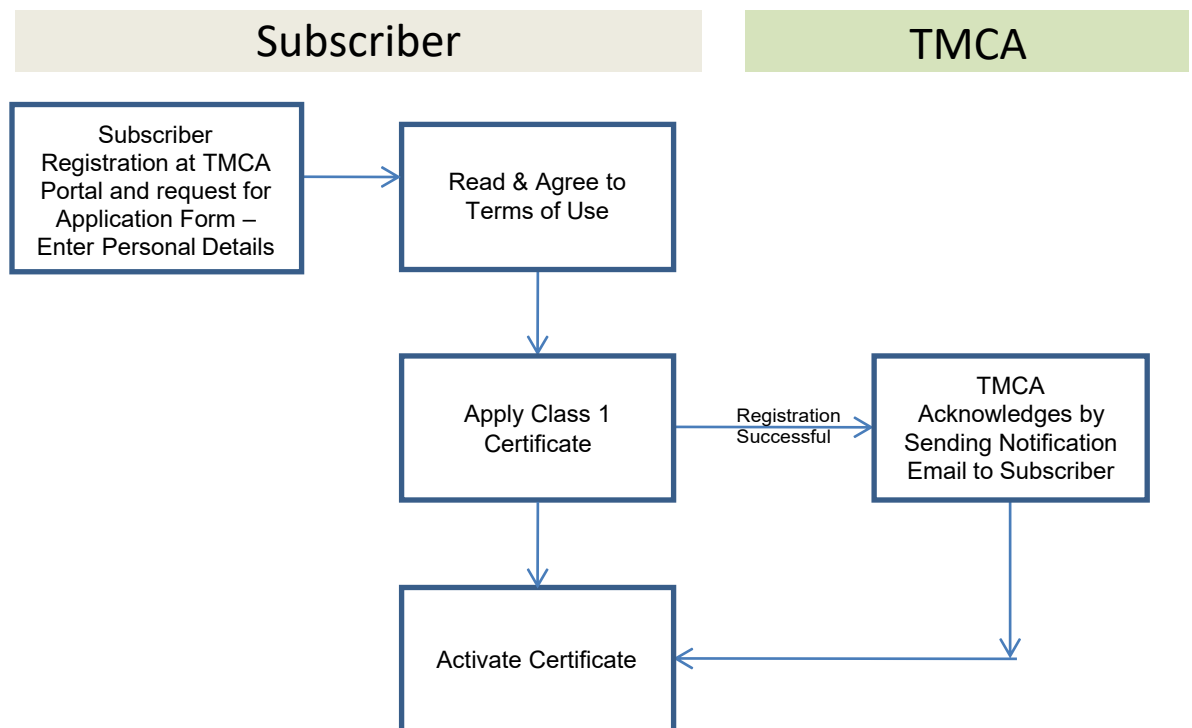


Figure 2 Class 1 Digital Certificate Application Process Flow

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

4.2.1.2 Class 2 Digital Certificate Application Process Flow

This is a Class 2 digital certificate application process flow, in which the applicant will obtain the application form from TMCA or Authorized Registration Authority (RA), fill in the form with required details and supporting documents and submit it personally to TMCA or Authorized RA for processing. Subscriber must first verify and confirm the application information captured by Authorized RA into system is correct before the key pair generation process. If, applicable, TMCA will acknowledge receipt of the Certificate Signing Request (CSR) from Authorized RA after the registration has been successfully completed at the Authorized RA's side. TMCA will, in turn, send out the notification email to the Subscriber to activate the certificate.

In the case of digital certificate has been successfully issued by Authorized RA, TMCA will send the approval notification to the Authorized RA.

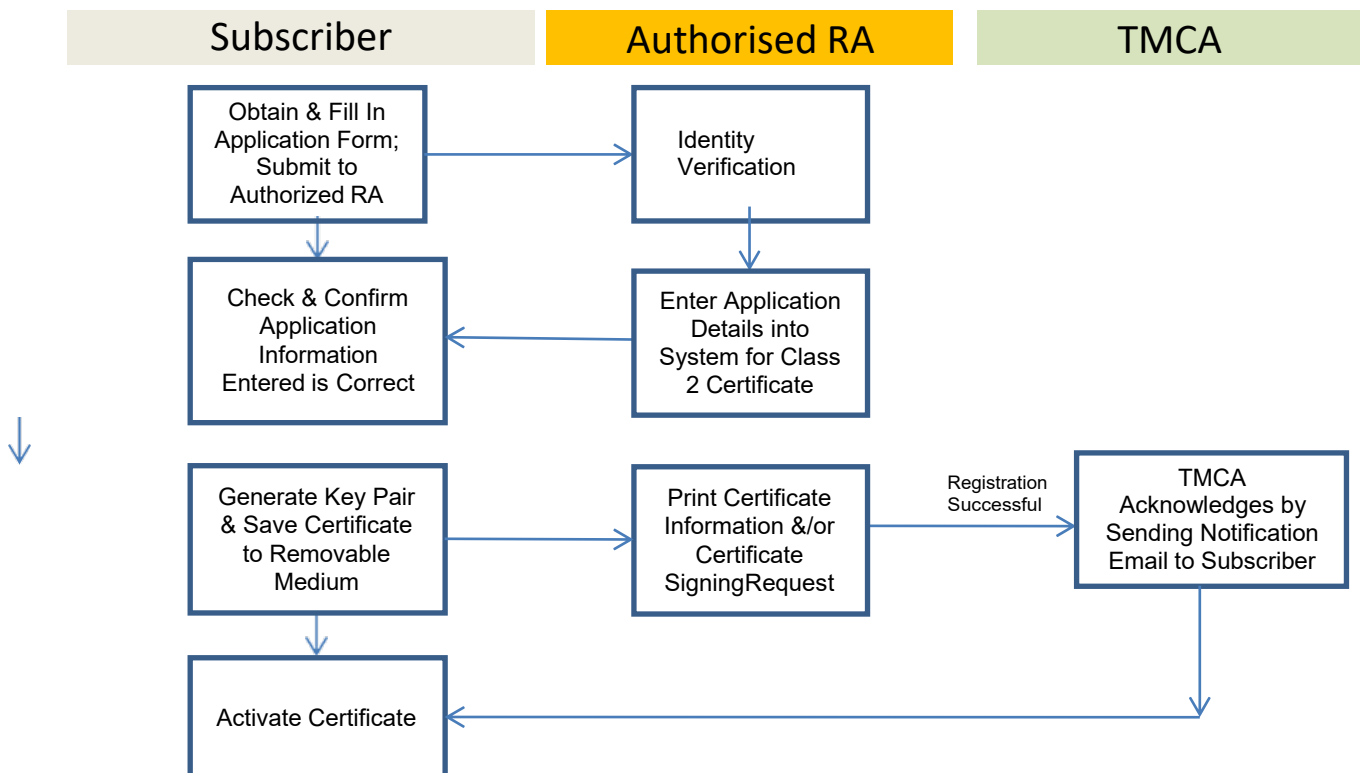


Figure 3 Class 2 & 3 Digital Certificate Application Process Flow

4.2.1.3 Class 3 Digital Certificate Application Process Flow

This process flow is similar to that of Class 2 described in Section 4.2.1.2 above.

The authentication of *Class 3 Individual* certificates is based on personal presence of the applicant before the Authorized RA or TMCA Management Representative. Authorized RA or TMCA Management Representative shall check the identity of the applicant against passport or driver's license and one other identification credential. **The application shall be certified by a notary public duly appointed under the Notaries Public Act 1959. All supporting documents must be attached.**

The authentication of *Class 3 Organization* certificates is based on authentication of the organization and a confirmation from the organization of the employment and authorization of the person who has submitted the application on behalf of the organization as described in Section 3.2.2 of the CPS. The application shall be certified by a notary public duly appointed under the Notaries Public Act 1959. All supporting documents must be attached. TMCA may also have occasion to approve applications for the organizations based on confirmation of their identity in connection with their employment or retention as an independent contractor and background checking procedures.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

4.2.1.4 Dissemination and Publication of Digital Certificate Process Flow

This process flow shows the dissemination and publication of digital certificates for TMCA:

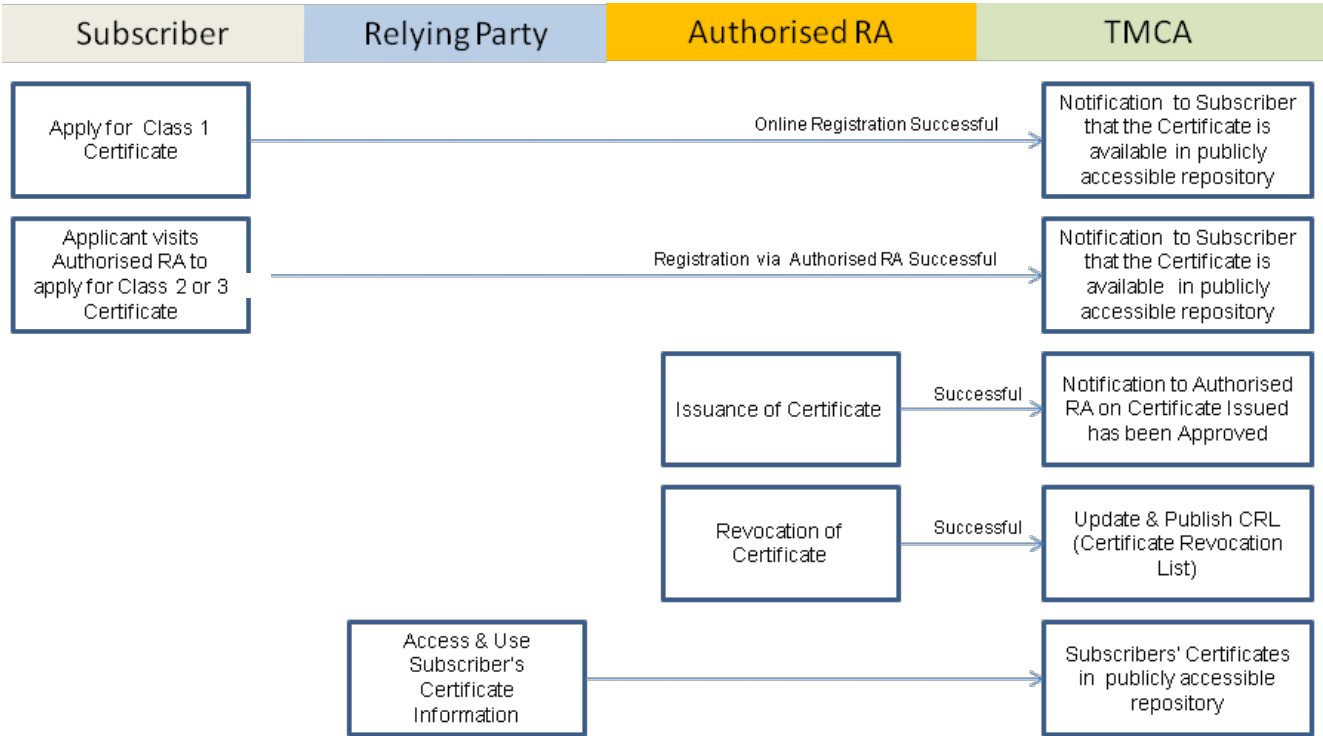


Figure 4 Dissemination and Publication of Digital Certificate Process Flow

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.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Before issuing digital certificates, TMCA will perform the following verification:

Identification of subscriber, as stipulated in section "3. Identification and Authentication".
The uniqueness of DN(Distinguished Name)/Subject submitted by the Subscriber

Digital Certificate issued by TMCA contains the following details:

- ① Subscriber's name.
- ② Subscriber's Public Key.
- ③ Method of digital signature used by the Subscriber and TMCA.
- ④ Serial number of the digital certificate.
- ⑤ Validity of the digital certificate.
- ⑥ Name of TMCA as an issuer of the digital certificate.
- ⑦ Scope of digital certificate's use and restrictions to its application
- ⑧ Other information on representation in case the Subscriber holds representation rights for a third party.

Server Certificate issued by TMCA contains the following details:

- ① Subscriber's name.
- ② Subscriber's Public Key.
- ③ Method of digital signature used by the Subscriber and TMCA.
- ④ Serial number of the digital certificate.
- ⑤ Validity of the digital certificate.
- ⑥ Name of TMCA as an issuer of the digital certificate.
- ⑦ Scope of digital certificate's use and restrictions to its application
- ⑧ Other information on representation in case the Subscriber holds representation rights for a third party.

Under normal circumstances, digital certificates are issued within 1 to 3 working days from the date of application. However, this is subjected to the Subscriber has filed the application form correctly together with other supporting documents and TMCA has also completed the personal identification process as stipulated in section "3. Identification and authentication" and section "1.3.2 Registration Authorities (RAs)".
Upon successfully completed the certificate issuance process, TMCA shall send notification email to Subscriber to activate the certificate.

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

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.

4.3.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

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

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

4.4.2 Publication of the Certificate by the CA

Certificates will be published at <https://tmca.com.my> once issued, following the conduct described in Section 4.4.1. This will be done within 24 hours

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key pair and Certificate Usage

The certificates containing public key that is intended for verifying digital signature created using the corresponding private key, must be utilized exclusively for their intended purposes. Certificates shall not be used in an illegal or discriminatory manner including, but not limited to, trafficking of illegal material, engaging in activities that compromise national security and utilising the certificate for accessing illegal material. In the event of any illegal use of certificates, it is within the purview of TMCA to promptly revoke the certificate without issuing prior notice to the subscriber. Furthermore, any future applications submitted by the subscriber may face adverse consideration as a consequence of such misuse. This policy is in place to maintain the integrity and legal standing of digital certificates issued by TMCA.

4.5.1 Subscriber Private Key and Certificate Usage

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.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

4.5.2 Relying Party Public Key and Certificate Usage

Relying Party shall Restrict reliance on certificates issued by TMCA to the purposes for those certificates, in accordance with TMCA CPS.

- 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 CPS upon reliance on a certificate issued by the TMCA.

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.
- b. TMCA shall notify Subscribers via email for renewal of digital certificates at least 60 days prior to the expiration of the existing digital certificates.

4.6.2 Who May Request Renewal

The Subscriber or his Authorised Representative can apply for renewal of a digital certificate. Once a digital certificate is renewed, the originally issued certificate before application for renewal shall be revoked. Before renewal, TMCA shall verify the following:

- a. Personal identification of Subscriber.
- b. The uniqueness of DN (Distinguished Name) submitted by the Subscriber.
- c. To safeguard certificate integrity, the private key generation for Class 2 certificate can be performed by Subscriber or CA.
- d. Subscriber should be informed of change of certificate status once the renewal process has been successfully completed.

4.6.3 Processing Certificate Renewal Requests

TMCA shall request additional information upon processing the renewal request.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

4.6.4 Notification of New Certificate Issuance to Subscriber

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

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

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

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.

4.7.2 Who May Request Certification of a New Public Key

As stipulated in Section "4.1 Certificate Application"

4.7.3 Processing Certificate Re-Keying Requests

As stipulated in Section "4.2 Certificate Application Processing"

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"

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

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

No stipulation.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

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

- a. In the event the Subscriber or his Authorised Representative applies to TMCA for revocation.
- b. In the event TMCA discovers that the Subscriber obtains his digital certificate by fraud, forgery, or other illegal means.
- c. In the event TMCA discovers the death, missing, or dissolution of the Subscriber or his organisation.
- d. In the event TMCA discovers the Subscriber's Private Key has been lost, damaged, stolen, or compromised.
- e. In the event the Subscriber violates any of these rules mentioned in the CPS.
- f. In the event the designation of TMCA as a licensed Certification Authority is cancelled by MCMC.
- g. 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. Subscriber to immediately notify TMCA of any compromise of the subscriber's private key.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

4.9.3 Procedure for Revocation Request

4.9.3.1 Application for Revocation of Digital Certificate

- a. Subscribers should personally visit TMCA Office or TMCA's Authorised RA for revocation of digital certificate or email TMCA to revoke the certificate. Depending on the class of TMCA certificates being sought, Subscribers may require to undergo personal identification process as stipulated in Section "3.1.7 Personal Identification for Suspension & Revocation of Digital Certificates" of the CP. For Class 1 certificate revocation, Subscriber requires to be authenticated by using their password and selects a valid reason from the system for the revocation.
- b. Subscriber shall be informed of change of certificate status once the revocation process has been successfully completed.

4.9.3.2 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 revoke the corresponding certificates promptly.

4.9.5 Time Within Which CA Must Process the Revocation Request

TMCA processes 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

No stipulation.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

4.9.8.1 On-Line Revocation/Status Checking Availability

No stipulation.

4.9.8.2 On-Line Revocation Checking Requirements

No stipulation.

4.9.8.3 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.8.4 Special Requirements re Key Compromise

As stipulated in "Section 4.9.1 Circumstances for Revocation"

4.10 Certificate Status Services

4.10.1 Operational Characteristics

No stipulation.

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.

4.11 Circumstances for Suspension

Digital certificate suspension may occur under various circumstances, among them are:

- a) Security Threats or Compromise
- b) Illegal or Prohibited Activities
- c) Non-Compliance with Policies
- d) Request for Suspension
- e) Breach of Trust
- f) Failure to Meet Industry Standards
- g) Emergencies or National Security Concerns
- h) Technical Issues or Errors

4.11.1 Who Can Request Suspension

Suspension of a digital certificate can be requested by :

- a) Certificate Holder
- b) Certificate Authority (CA)
- c) Registration (Authority)

4.11.2 Procedure for Suspension Request

- a. Subscribers should personally visit TMCA Office or TMCA's Authorised RA for suspension of digital certificate. Depending on the class of TMCA certificates being sought, Subscribers may require to undergo personal identification process as stipulated in Section "3.1.7 Personal Identification for Suspension & Revocation of Digital Certificate" of the CP.
- b. Subscriber shall be informed of change of certificate status once the suspension process has been successfully completed.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

4.11.3 Limits on Suspension Period

TMCA renews and updates the list of suspended certificates with immediate effect. The information shall be posted on a directory service. At the time of which the information is posted on directory service shall be construed as the time of announcement.

Suspension period will be maximum of 6 months

4.12 End of Subscription

No stipulation.

4.13 Key Escrow and Recovery

4.13.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.13.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Security Control

5.1.1 Site Location and Construction

No stipulation.

5.1.2 Physical Access

TMCA subscribe to services in safeguarding the sites where the core certification systems are installed to prevent damage due to intrusion, illegal access and fire.

- a. TMCA installs and operates the core certification systems in a separate securitycontrolled area.
- b. TMCA subscribe to secured controlled area which uses multi-layer access systems, which use a combination of passwords and smart-card.
- c. TMCA installs the core certification systems in a secure cabinet.
- d. TMCA ensures that all non-TMCA Authorised Personnel are accompanied by the TMCA person-in-charge or the Authorised Officer whenever the non-TMCA Authorised Personnel wishes to enter the security area where the core certification systems are installed.
- e. TMCA subscribed to the controlled area which maintains and regularly reviews a log that records any entries into the controlled area.
- f. TMCA subscribe to the controlled area that maintains an alarm system by installing the following surveillance control systems:
 - CCTV camera monitoring system
 - Intrusion detection system

5.1.3 Power and Air Conditioning

TMCA subscribed to controlled area that deploys UPS system that shall ensure uninterrupted services in case of power failures. The controlled area also ensures all essential power is also connected to TM's standby generator system. The UPS has the capabilities to offer 99.99% power uptime availability to support all CA systems. The controlled area also uses air-conditioning system and raised floor to ensure optimum ventilation and protection.

5.1.4 Water Exposures

TMCA subscribe to controlled area that installs the core certification systems at a reasonable height to protect them from flooddamage.

5.1.5 Fire Prevention and Protection

TMCA subscribe to the controlled area that installs fire detector, portable fire extinguisher, and automatic fire extinguishing facilities to prevent the core certification systems from fire damage.

5.1.6 Media Storage

Critical system data is incrementally backed-up on a daily basis. Full back-ups are performed on a weekly, monthly and annual basis. TMCA controls physical access to its major storage media that are stored in safes.

5.1.7 Waste Disposal

TMCA shreds and crushes documents, diskettes, and other items to prevent information from such materials from being leaked.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

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 CPS, 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.

Individuals assigned to a Trusted Role for a CA shall:

- a. Be appointed in writing by TM Technology Services Sdn Bhd
- b. Not be assigned other duties that may conflict with the duties defined for the Trusted Role and
- c. Have sufficient expertise and knowledge required for the performance of their duties.

5.3.2 Background Check Procedures

All operative personnel in TMCA are required to go through a stringent background check upon joining and on an annual basis.

5.3.3 Training Requirements

TMCA 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.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

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

TMCA's policies and procedures specify the sanctions against personnel for unauthorized actions, unauthorised use of authority, and unauthorised use of system

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 employment or training.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

TMCA 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

Event logs are reviewed at least on a monthly basis by CA management. The review must be documented including findings, notifications to senior management, actions taken and issue resolution.

5.4.3 Retention Period for Audit Log

Audit Log will be archive for 10 years

5.4.4 Protection of Audit Log

As part of this CA's system backup procedures, audit trail files are backed up prior to shutdown of intermittent operation of the off-line CA system and thereafter archived by the system administrator.

The logged events must be inspected to identify incidents with high severity and to eliminate "false positives". Events that are considered "high severity" could cause a risk for system availability or represent a security breach or an attempted breach, such as multiple incorrect logons of a user account, attempts of unauthorized access to systems and resources and unauthorized alterations of critical and security related system parameters.

The event logs of HSM are monitored with on-line monitoring software in short time intervals. Detected events are rated and significant events will trigger an e-mail notification sent to alert the CA operations team. The CA operations team reviews the situation in real-time, and performs the necessary steps to notify about and to resolve the problem. Access to the logs is secure and available only to the CA operations team.

5.4.5 Audit Log Backup Procedures

Data backup are produced daily and full system backup are produced monthly and yearly. Audit log files shall be backed-up.

5.4.6 Vulnerability Assessments

No stipulation.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

5.5 Records Archival

5.5.1 Types of Records Archived

The minimum records to be archived, in relation to allocations and information that is relevant to each certificate application and to the generation, issuance, distribution, usage, suspension, revocation, renewal and expiration of all certificates issued by TMCA shall include

- Certification Practice Statement
- Certificate Policy
- Subscriber Agreement
- Registration records
- Key generation requests, including whether or not key generation was successful
- Certificate generation requests, including whether or not Certificate generation was successful
- Certificate issuance and Revocation records
- Audit records, including security related events
- Contract materials
- Signing keys for Certification Authorities, Registration Authorities, CRL's and OCSP Responders

5.5.2 Retention Period for Archive

TMCA regularly archives the original records and the copies are archived 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 environments owned or managed by TMCA. Physical archives shall be located in an environment which is protected from environmental factors such as temperature and humidity.

To prevent forgery of, tampering, or damage to archival records, TMCA archives records as follows:

- a. Digital documents are safely stored with controlled access rights and digitally signed.
- b. Hard copy documents are stored in locked cabinets.

5.5.4 Archive Backup Procedures

All electronic records, including digital copies of physical documents, shall be backed up and stored in secure area or secure facilities. Records that consist only in a physical form will not be backed up by TMCA.

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.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

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 24 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. Subscriber to immediately notify the TMCA of the compromise of the subscriber's private key.

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.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

5.8 CA or RA Termination

In the event that TMCA ceases operation, the Controller (MCMC) shall appoint another licensed certification authority to take over the certificates issued by the certification authority

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

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 Authorized 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 DSA: 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.

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

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

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-authorized 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.

6.2.8 Method of Activating Private Key

The Private Key shall be protected from exposure and unauthorised usage using Subscriber's 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.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

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 unauthorised 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

6.5.2 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.

6.5.3 Computer Security Rating

No stipulation.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

6.6 Life Cycle Technical Controls

All software components of the PKI are developed in conditions and following processes that ensure their security. 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.

6.8 Time-Stamping

Certificates, CRLs, and other revocation database entries shall contain time and date information.

The system time on TMCA is updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every 24 hours. All times are traceable to a real time value distributed National Metrology Institute of Malaysia (NMIM) and are updated when a leap second occurs as notified by the appropriate body

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 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 CPS contain the X.509 Certificate Policy extension. This extension is not marked critical.

All Certificates issued under this CPS 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 TMCA Certificate Subject includes 'O = TM Technology Services Sdn Bhd. '.

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 CPS and other related documents can be obtained.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

CRL issued under this CPS 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.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

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 audit shall be performed in compliance with DSA 1997 and WebTrust for Certification Authorities Program.

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 TM Technology Services Sdn. Bhd.

8.3 Assessor's Relationship to Assessed Entity

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

8.4 Topics covered by Assessment

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

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

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

CLASS CATEGORY	SERVICE	FEES (PER CERTIFICATE)
CLASS 1		
Digital Certificate Soft Cert	Digital Signature, Data Encipherment	RM50
CLASS 2		
Digital Certificate Roaming	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment	RM8-RM120
Digital Certificate Soft Cert	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment	RM80
Digital Certificate Token	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment	Certificate : RM80 Token : RM 100
Digital Certificate RRP	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment	RM80
Digital Certificate Training/Temporary	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment	RM40
CLASS 3		
Digital Certificate Roaming	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment	RM3,400

9.1.2 Certificate Access Fees (OMITTED)

No stipulation.

9.1.3 Revocation or Status Information Access Fees (OMITTED)

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No refund will be granted for unused certificate once it is generated and handed over to subscriber. However, in circumstances where the information on the certificate is incorrect due to causes by TMCA or it's RA, TMCA will issue a new certificate free of charge.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

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 an 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.

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

9.4.1.1 Data Collection

Details on what personal information is collected from certificate applicants. This may include

- a) names,
- b) copy of NRIC/MyTentera/passport and number
- c) email addresses
- d) telephone number
- e) organizational affiliations
- f) other relevant contact information.

9.4.1.2 Purpose of Data

9.4.1.2.1 Names, copy of NRIC/Military ID/Passport

The collection of names and copies of identification documents such as NRIC, Military ID, or Passport is essential to verify the identity of the certificate applicant. This information ensures that the certificate is issued to the correct individual or authorized representative of an organization, thereby enhancing the trustworthiness and security of digital transactions and communications.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

9.4.1.2.2 Email Addresses

Email addresses are collected to facilitate communication with the certificate applicant throughout the certificate issuance process. They are used for sending notifications, updates, and verification requests related to the application, issuance, renewal, or revocation of digital certificates. This ensures timely and secure correspondence between the TMCA and the certificate applicant.

9.4.1.2.3 Telephone Number

The collection of telephone numbers enables the TMCA to contact the certificate applicant quickly and efficiently when necessary. It may be used to verify information provided during the application process, confirm identity, or address any issues that arise during certificate issuance or management. This enhances the security and reliability of the certificate issuance process.

9.4.1.2.4 Organizational Affiliations

Information regarding organizational affiliations is gathered to accurately attribute digital certificates to the respective organizations or entities. This helps in verifying the legitimacy and authority of the certificate applicant to act on behalf of their organization, ensuring that digital certificates are issued to authorized personnel and entities only.

9.4.1.2.5 Other Relevant Contact Information

Additional contact information, such as mailing addresses or secondary email addresses, may be collected to ensure comprehensive communication capabilities between the TMCA and the certificate applicant. This information supports efficient correspondence and facilitates the management of digital certificate-related inquiries, updates, and notifications.

9.4.1.2.6 CTC eInfo SSM (Company Search Report from Suruhanjaya Syarikat Malaysia) and Letter of Proxy on Company Letterhead

The collection of Certified True Copy (CTC) of eInfo SSM and Letter of Proxy on Company Letterhead is necessary to verify the legal status and authorization of the certificate applicant within their organization.

These documents help confirm that the applicant has the authority to request and manage digital certificates on behalf of the company, ensuring that certificates are issued to authorized personnel only and aligning with regulatory requirements.

These purposes collectively support the TMCA's commitment to verifying identities, ensuring the integrity of digital certificates, maintaining communication with certificate applicants, and upholding security standards in digital transactions and communications.

9.4.1.3 Use of Data

At TMCA, we collect various types of personal and company information from certificate applicants to facilitate the issuance, management, and verification of digital certificates. The data collected serves the following purposes:

9.4.1.3.1 Verification of Identity

Names and copies of identification documents such as NRIC, Military ID, or Passport are collected to verify the identity of the certificate applicant. This ensures that digital certificates are issued to the correct individual or authorized representative.

9.4.1.3.2 Communication

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

Email addresses and telephone numbers are used to communicate with certificate applicants throughout the certificate issuance process. This includes sending notifications, updates, and verification requests related to application status, certificate issuance, renewal, or revocation.

9.4.1.3.3 Authorization and Affiliation

Organizational affiliations and relevant contact information are collected to verify the affiliation of the certificate applicant with their organization or entity. This helps ensure that certificates are issued to authorized personnel and entities only, maintaining the integrity and authenticity of digital transactions.

9.4.1.3.4 Legal Compliance

Certified True Copy (CTC) of eInfo SSM and Letter of Proxy on Company Letterhead are collected to comply with regulatory requirements and to verify the legal status and authorization of the certificate applicant within their organization. This ensures that certificates are issued in accordance with applicable laws and regulations.

9.4.1.3.5 Security and Trust

The data collected is crucial for maintaining the security and trustworthiness of digital certificates issued by TMCA. By accurately verifying identities and affiliations, we help protect against fraudulent activities and unauthorized certificate issuance, thereby safeguarding digital transactions and communications.

Overall, the use of this data is fundamental to our commitment to providing secure and reliable digital certificates, enhancing trust in online interactions, and ensuring compliance with legal and regulatory standards.

9.4.1.4 Data Retention

At TMCA, we adhere to strict data protection practices to ensure the security and integrity of personal information collected during the certificate issuance process. In compliance with regulatory requirements, all data provided by certificate applicants, including names, identification documents (such as NRIC, Military ID, or Passport copies), email addresses, telephone numbers, organizational affiliations, and other relevant contact information, will be securely stored for a period of 10 years from the date of collection.

This data retention period is necessary to meet legal and regulatory obligations, including but not limited to auditing, compliance, and dispute resolution purposes. During this period, stringent measures are implemented to safeguard the confidentiality and integrity of stored data, including encryption, access controls, and regular security audits.

At the end of the retention period, data that is no longer required for legal, regulatory, or operational purposes will be securely and permanently deleted in accordance with our data retention and disposal policies.

By storing data for the specified period, TMCA ensures continued compliance with applicable laws and regulations, as well as maintaining the ability to verify identities, manage certificate lifecycles, and uphold the security and trustworthiness of our digital certificate services.

9.4.1.5 Data Security

At TMCA, we prioritize the protection of personal data to ensure confidentiality, integrity, and availability throughout its lifecycle. To achieve this, we have implemented robust data security measures, including:

9.4.1.5.1 Encryption

Personal data collected, processed, and stored by [Certificate Authority Name] is encrypted using strong encryption algorithms. This ensures that sensitive information remains protected against unauthorized access and breaches.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

9.4.1.5.2 Access Controls

Access to personal data is strictly controlled and restricted to authorized personnel only. Role-based access controls (RBAC) are enforced to ensure that individuals have access only to the information necessary for their specific duties.

9.4.1.5.3 Secure Storage

Personal data is stored in secure environments that meet industry standards for physical and logical security. This includes data centers with access controls, surveillance, and environmental controls to prevent unauthorized access or physical theft.

9.4.1.5.4 Regular Security Audits

TMCA conduct regular security audits and assessments of our systems, infrastructure, and processes to identify and address potential vulnerabilities. These audits are performed by independent third-party security experts to ensure impartial evaluation and compliance with industry standards.

9.4.1.5.5 Incident Response

TMCA maintains a comprehensive incident response plan to promptly address and mitigate any security incidents or breaches. This includes procedures for incident detection, investigation, containment, and remediation to minimize impact and prevent recurrence.

9.4.1.5.6 Employee Training

All employees undergo regular training on data protection practices and security protocols to ensure awareness of their responsibilities in safeguarding personal data.

9.4.1.5.7 Compliance with Standards

TMCA adhere to relevant data protection laws and regulations, including but not limited to PDPA and industry-specific standards. Our data security measures are continuously updated to align with evolving legal requirements and best practices.

By implementing these data security measures, TMCA maintains a secure environment for handling personal data, thereby ensuring the trust, reliability, and integrity of our digital certificate services.

9.4.1.6 TMCA Data Sharing Statement

TMCA respects the privacy of its users and is committed to protecting their personal data. This Data Sharing Statement outlines the conditions under which TMCA may share personal data with third parties.

9.4.1.6.1 General Principles

TMCA will only share personal data with third parties when it is necessary to:

- a. Deliver our services and fulfill our contractual obligations.
- b. Comply with legal or regulatory requirements.
- c. Protect the rights, property, or safety of TMCA, our users, or others.
- d. Prevent or investigate fraud or other illegal activities.

TMCA will only share personal data with trusted third parties who have implemented appropriate technical and organizational measures to protect the data.

We will take steps to ensure that any third-party recipient of personal data uses the data only for the purposes for

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

which it was disclosed and in accordance with applicable data protection laws.

9.4.1.6.2 Service Providers

TMCA may share personal data with service providers who assist us in operating our business and providing our services. These service providers may include data processing companies, customer support providers, and marketing agencies.

9.4.1.6.3 Law Enforcement and Regulatory Authorities

TMCA may share personal data with law enforcement or regulatory authorities if required by law or if we believe that such disclosure is necessary to protect the rights, property, or safety of TMCA, our users, or others.

9.4.1.7 Your Rights

Depending on your location, you may have certain rights with respect to your personal data, such as the right to access, rectify, erase, or restrict the processing of your personal data. For more information about your rights, please contact us.

9.4.1.8 Changes to this Data Sharing Statement

TMCA may update this Data Sharing Statement from time to time. We will post any changes on our website.

9.4.1.9 Individual Rights

At TMCA, we understand that you have rights regarding your personal data. This statement explains the rights you have under applicable data protection laws and regulations.

9.4.1.10 What Personal Data Do We Collect?

As a Certificate Authority (CA), TMCA typically collect the following types of personal data to issue and manage digital certificates:

9.4.1.10.1 Identification Information

Name, NRIC, Passport details, organization affiliation (if applicable), and contact details (e.g., email address).

9.4.1.10.2 Technical Data

Information about your device and interactions with our CA services, such as IP address and certificate issuance/renewal history.

9.4.1.11 Your Rights Regarding Your Personal Data

Depending on your location and applicable data protection laws, you may have the following rights:

9.4.1.11.1 Right to Access

You may request a copy of the personal data TMCA hold about you.

9.4.1.11.2 Right to Rectification

If you believe your personal data is inaccurate or incomplete, you may request that TMCA correct or update it.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

9.4.1.11.3 Right to Erasure (Right to be Forgotten)

In certain circumstances, you may request that TMCA erase your personal data. However, this right may be limited in some situations, such as where we are required by law to retain your data.

9.4.1.11.4 Right to Restrict Processing

You may request that TMCA restrict the processing of your personal data, meaning we can no longer use it for certain purposes (e.g., marketing).

9.4.1.11.5 Right to Data Portability

You may have the right to receive your personal data in a structured and commonly used format and to transmit it to another CA (where technically feasible).

9.4.1.12 Exercising Your Rights

If you wish to exercise any of your rights described above, please submit a written request to tmca.helpdesk@tm.com.my. We will respond to your request within a reasonable timeframe, as required by law.

9.4.1.13 Verification Process

To protect your privacy and security, TMCA may require verification of your identity before processing your request. This may involve requesting additional information to confirm your identity.

9.4.1.14 Exceptions to Your Rights

In some cases, TMCA may not be able to fully comply with your request, for example, if it interferes with our legal obligations or the rights of others. However, we will always explain the reasons for any limitations.

9.4.1.15 Changes to this Individual Rights Statement

TMCA may update this Individual Rights Statement from time to time. We will post any changes on our website.

9.4.1.16 Compliance with Malaysian Personal Data Protection Act (PDPA)

TMCA are committed to complying with the Malaysian Personal Data Protection Act (PDPA) of 2010. We take the protection of your personal data seriously and strive to ensure its lawful and responsible processing. Here is how TMCA comply with the PDPA

9.4.1.16.1 Data Protection Principles

TMCA adhere to the seven data protection principles outlined in the PDPA, including: processing personal data for a lawful purpose, obtaining your consent, and ensuring the accuracy and security of your data.

9.4.1.16.2 Registration with PDPC

TM Technology Services Sdn Bhd is registered with the Personal Data Protection Commissioner (PDPC) as a data user.

9.4.1.16.3 Limited Data Collection

TMCA only collect the personal data necessary to fulfill our obligations as a CA, such as identification information for certificate issuance and technical data for service delivery.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

9.4.1.16.4 Data Security Measures

TMCA implement robust technical and organizational measures to protect your personal data from unauthorized access, disclosure, alteration, or loss.

9.4.1.16.5 Data Retention

TMCA retain your personal data only for as long as necessary to fulfill the purposes for which it was collected or as required by law.

9.4.1.16.6 Individual Rights

TMCA respect your rights under the PDPA, including the right to access, rectify, erase, or restrict processing of your personal data. For more information about your rights, please see our Individual Rights Regarding Your Personal Data statement.

9.4.1.16.7 Changes to this Compliance Statement

TMCA may update this Compliance Statement to reflect changes in the PDPA or our data practices. We will post any changes on our website.

9.4.1.17 Policy Updates

9.4.1.17.1 Policy Updates and Communication

TMCA reserves the right to update this CPS from time to time. We will make reasonable efforts to communicate any material changes to the CPS to affected parties. This may include:

9.4.1.17.1.1 Posting the updated CPS on our website

TMCA will prominently display the revised CPS on our website with an effective date.

9.4.1.17.1.2 Direct notification

In some cases, TMCA may send direct notification (e.g., email) to users who have actively interacted with our services and provided contact information.

9.4.1.17.1.3 Public announcement

For significant changes, TMCA may issue a public announcement through industry channels or media outlets.

9.4.1.17.1.4 Frequency of Updates

TMCA may update the CPS for various reasons, including:

9.4.1.17.1.5 Changes in Law or Regulations

To comply with changes in applicable data protection laws or industry standards.

9.4.1.17.1.6 Changes in Our Practices

To reflect changes in our data collection, processing, or security practices.

9.4.1.17.1.7 New Technologies or Services

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

To accommodate the introduction of new technologies or services offered by our CA.

TMCA will strive to provide reasonable notice of any material changes to the CPS. However, we encourage you to periodically review the CPS on our website for the latest version.

9.4.1.18 Your Continued Use of Our Services

By continuing to use our TMCA services after the revised CPS becomes effective, you are deemed to have accepted the changes.

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

The restrictions and limitations for subscribers of digital certificates typically revolve around the usage, management, and security of the certificates. Here are some common ones:

9.4.7.1 Usage Restrictions

9.4.7.1.1 Purpose-Specific Use

Digital certificates are often issued for specific purposes, such as email encryption, digital signatures, or server authentication. Subscribers must use the certificate only for its intended purpose.

9.4.7.1.2 Compliance with Policies

Subscribers must adhere to the policies and procedures outlined TMCA. This includes following any guidelines for key management and certificate usage.

9.4.7.1.3 Non-Transferability

Digital certificates are typically non-transferable. The subscriber cannot transfer their certificate to another individual or entity.

9.4.7.2 Security Limitations

9.4.7.2.1 Key Protection

Subscribers must protect their private keys. If a private key is compromised, the associated certificate must be revoked, and the subscriber may need to obtain a new certificate.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

9.4.7.2.2 Password Management

If a certificate is protected by a password, the subscriber is responsible for keeping that password secure. Losing the password can render the certificate unusable.

9.4.7.3 Management Limitations

9.4.7.3.1 Renewal and Revocation

Digital certificates have a finite validity period. Subscribers are responsible for renewing their certificates before they expire. Additionally, subscribers must promptly request the revocation of their certificates if they believe the certificate has been compromised.

9.4.7.3.2 Updates to Information

If there are changes to the information contained in the certificate (e.g., a change in the subscriber's name or organizational details), the subscriber may need to update the certificate or obtain a new one.

9.4.7.4 Legal and Regulatory Constraints

9.4.7.4.1 Jurisdictional Compliance

Subscribers must comply with the legal and regulatory requirements of the jurisdictions in which they operate. This can include data protection laws, export controls, and other relevant regulations.

9.4.7.5 Audit and Logging

Subscribers may be required to maintain logs and records of their certificate usage for auditing purposes. This is often necessary for compliance with security and regulatory standards.

9.4.7.6 Technical Limitations

9.4.7.6.1 Compatibility

Subscribers must ensure that their systems and applications are compatible with the digital certificates they are using. This includes ensuring that their software supports the encryption algorithms and protocols specified by the certificate.

9.4.7.6.2 Certificate Chain

The trustworthiness of a digital certificate relies on the trustworthiness of the issuing CA and the certificate chain. Subscribers must ensure that the entire certificate chain is valid and trusted by their systems.

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

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.

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 CPS, RAs shall be subject to the same liabilities as those applicable to TMCA

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

9.8.1 TMCA Liability Cap / Reliance Limit

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

The reliance limit for each certificate will remain constant, regardless of the number of digital signatures, transactions, or claims associated with it. If the total liability exceeds the cap, the available liability cap will be allocated primarily to the earliest claims until final dispute resolution is reached, unless directed otherwise by a

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

court of competent jurisdiction.

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

9.8.2 RA Liability

RAs shall subject to the same liabilities as applicable to TMCA

9.9 Indemnities

TMCA assumes no financial responsibility for improperly used certificates, CRLs, etc

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 CPS 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

9.13.1 Claims

All claims will be acknowledged by us by email

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

Notification of incident, loss or damage. When loss or damage under the user of Digital Certificate occurs, the subscriber should notify us of the incident as soon as possible. Any loss or damage caused by theft/burglary must be reported to the local police. A copy of the police report should also be obtained to be produced as evidence for the claim.

9.14 Governing Law

This CPS is governed in accordance with the laws of Malaysia, i.e Digital Signature Act (1997) 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 CPS 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

TMCA shall not be liable for any losses, costs, expenses, liabilities, damages, or claims arising out of or related to delays in performance or from failure to perform its obligations if such failure or delay is due to circumstances beyond TMCA's reasonable control, including 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 Provision

9.17.1 Personal Data

TMCA are subjected to the PDPA Act 2010 (Act 709) and registered and party with the Jabatan Perlindungan Data Peribadi (JPDP). All the obligation stipulated in the act is deemed to be accepted by all parties as final and will not be subjected to any other obligations. The personal data involved shall be protected under the law.

9.17.2 Right to audit


TMCA has been deemed been audit by its independent external auditor appointed by MCMC and shall not be subjected to any other audit requirements as stipulated by any other written law as it will conflicting the jurisdiction

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024

among government agencies i.e., MCMC and any other Commissions and legislations

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

1 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



SAMPLE SIGNATURE

RIGHT CLICK ON IMAGE AND
CHOOSE CHANGE PICTURE

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)

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024



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

 <p>SAMPLE SIGNATURE</p> <p>RIGHT CLICK ON IMAGE AND CHOOSE CHANGE PICTURE</p>	Name	<input type="text"/>
	NRIC/Passport No	<input type="text"/>
	Date	<input type="text"/>

Verified By Authorised TMCA Personnel/RA

Signature of Authorised TMCA Personnel/RA

 <p>SAMPLE SIGNATURE</p> <p>RIGHT CLICK ON IMAGE AND CHOOSE CHANGE PICTURE</p>	Name	<input type="text"/>
	NRIC/Passport No	<input type="text"/>
	Date	<input type="text"/>

TMCA DIGITAL CERTIFICATE APPLICATION FORM (INDIVIDUAL)



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



TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1 st JULY 2024

2 Appendix B – Application Form for TMCA Digital Certificate (BUS/GOV/NGO)



CONFIDENTIAL

TMCA DIGITAL CERTIFICATE APPLICATION FORM (BUSINESS / GOVERNMENT / NGO)

1. Applicable to Malaysians and foreign corporation / SME / ORGANIZATION.
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.
5. For TMCA Server/SSL Certificate application, all applicants are advised to generate server key pair and Certificate Signing Request (CSR), save the CSR in a removable disk and this MUST be presented upon submitting application form.
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. Verification supporting documents *(please attach a certified copy of the following document)*:
 - a. For Corporation/SME/Organization,
 - Digitally Certified SSM e-info business/corporate information
 - Business Registration Certificate
 - Corporation Registered
 - Forms 13, 24, 44 & 49 of Companies Act 1965
 - Representative's ID/Legal Agent's ID & MyKad/ Valid Passport
 - Letter of Proxy if applicable
 - Office Holder Letter if applicable
 - Certificate of Proprietary Number
 - Proof Tax Identification Number (TIN)
 - b. For Government Organization
 - Official Letter
 - Employee ID Card
 - Approval Letter from MAMPU
 - Approved Letter from Ministry (if applicable)
 - c. For Government Employee
 - Official Letter
 - Employee ID Card
 - Approval Letter from MAMPU

Document verification is via online eKYC/ eKYB, Commissioner of Oath/Professional Bodies/HR endorsement or face to face verification by appointed RA

Application Type

Business

- SME /Corporation/ Organization ☐
- Server ☐

Government / Non-Government Organization

- Organization Member/Employee ☐
- Organization Unit / Agency ☐
- Server ☐

CERTIFICATE REQUEST DETAIL

Name *(as in official registration certificate)*

Registration No (ie. BRN)

Common Name (if any)

Server & Platform

Organization / Unit

Business Address

Email address

Telephone Number

Tax Identification Number (TIN)

REPRESENTATIVE PERSONAL DETAIL

Name *(as in NRIC/Passport)*

NRIC /Passport No

Date of Birth (dd/mm/yyyy)

Email Address

Telephone Number

Page 1 of 3

TMCA DIGITAL CERTIFICATE APPLICATION FORM (BUS/GOV/NGO)

add in page 2

TM Tech Certification Authority (TMCA)	Version 1.2.2
Certification Practice Statement (CPS)	Publication Date: 1st JULY 2024



CONFIDENTIAL

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 Subscriber Obligation, Terms & Conditions and Certificate Information

Signature of Subscriber Representative

	Name	_____
	NRIC/Passport No	_____
	Date	_____

Verified By Authorised TMCA Personnel/RA

Signature of Authorised TMCA Personnel/RA

	Name	_____
	NRIC/Passport No	_____
	Date	_____