TM Applied Business

TELEKOM MALAYSIA CERTIFICATION AUTHORITY (TMCA)

CERTIFICATE POLICY (CP)
VERSION 5.3

DATE OF PUBLICATION: 20th January 2022

Revision History

Date	Version	Modification Type	Item/Ref. No.	Description	Author
30th Nov, 2012	1.0	New		Draft document based on RFC 2527 for review and approval.	TMCA CPS Committee
29th Sept, 2014	2.0	Update	2.13.2 and 2.13.3	Include Webtrust for CA compliance statement. Approved and release for publication.	TMCA CPS Committee
29th Sept, 2016	3.0	Update	3.1.5	Deletion of "In addition, TMCA shall incorporate additional controls that include face-to-face verification" Approved and releases for publication	TMCA CPS Committee
5th June, 2018	4.0	Update	1.4 and Appendix B	Updating the new office address and contact details	TMCA CPS Committee
27th June, 2019	4.1	Annual Revision	-	No changes	TMCA CPS Committee
20th March, 2020	5.0	Update	-	Updating CP according to RFC3647. Approved and release for publication.	TMCA CPS Committee
13th May, 2020	5.1	Update	1.3.1, 1.4.1, 1.4.2, 3.2, 4.3.1, 4.10.3, 5.1, 7.3, and 9.13	Updating minor deviations in CP based on RFC3647. Approved and release for publication.	TMCA CPS Committee
24th June, 2021	5.2	Update	6.1.3	Update the key delivery method. Approved and release for publication.	TMCA CPS Committee
20th January, 2022	5.3	Update	1.5.1, 1.5.2, 3.1.1	Updating the new office address and individual certificate description	TMCA CPS Committee

Notice

1 INTRODUCTION

1.1 Overview

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

The CP is organised as follows:

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

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

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

a. Digital Certificates;

b. Digital Signatures;

c. Digital Signature Act 1997;

d. Digital Signature Regulations 1998;

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

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

1.2 Document Name and Identification

In compliance with the Malaysia's Digital Signature Act 1997 (hereinafter referred to as the "DSA") and the Digital Signature Regulations 1998 (hereinafter referred to as the "DSR"), TMCA CP is intends to prescribe all matters concerning TELEKOM MALAYSIA 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 CP can be found on the TMCA repository at http://www.tmca.com.my/repository. This CP may be updated from time to time.

1.3 PKI Participants

TMCA CP 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

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

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

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

Certification Authority License

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

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

1.3.1.1 TMCA Infrastructure

TMCA infrastructure provides the standard trust model as shown below:

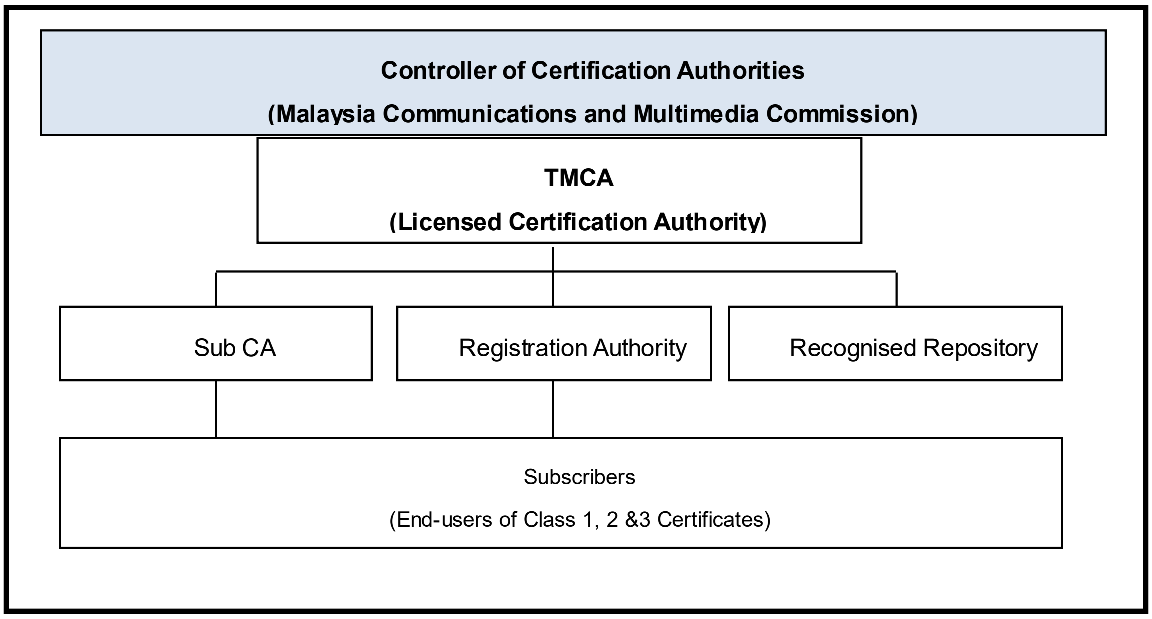

Controller of Certification Authorities
(Malaysia Communications and Multimedia Commission)
TMCA
(Licensed Certification Authority)
Sub CA
Registration Authority
Recognised Repository
Subscribers
(End-users of Class 1, 2 &3 Certificates)

Figure 1 TMCA Infrastructure

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

1.3.2 Registration Authorities (RAs)

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

1.3.2.1 Sub Certificate Authority (Sub CA)

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

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

1.3.3 Subscribers

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

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

1.3.4 Relying Parties

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

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

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

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

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

TMCA reserves the rights to amend this CP at any time and the amendments to this CP shall be made available at TMCA's web site, https://www.tmca.com.my.Amendments shall become effective automatically within fourteen (14) working days of the CP 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 CP. The publication date is equivalent to the effective date of the CP.

1.4.1 Appropriate Certificate Uses

TMCA offers the following certificate classes:

Class	Usage	Assurance Level	Subscribers
Class 1 Digital Certificates	This class of digital certificate is used for encryption and decryption of electronic data. As authentication of the user is simple sufficed with email authentication, the digital certificates are not to be used to digitally sign a business transaction. Class 1 digital certificates do not provide assurance on the identity of the Subscriber.	Low	Individual – Malaysian and Foreigner

Class	Usage	Assurance Level	Subscribers
Class 2 Digital Certificates	This class of digital certificate is used for digitally sign an online business transaction and as the digital signing is legally accepted, verification of user is mandatory. Class 2 digital certificates provide assurance on the identity of the Subscriber. Class 2 certificates are mainly used for user authentication and online secure transactions in the following services: • e-Financial Services • e- Government Services • e-Stock Broking Services • e-Commerce • Electronic Approval • e-Document Services • e-Insurance Services This class of digital certificate is applicable for individual user certificate and server certificate.	Medium	Individual
			SME/ Corporation/ Government
			Organization Members
			Organization
			NGO
	Secure Web Transaction	Medium	Web Server Operator
Class 3 Digital Certificate	This class of digital certificate is used for 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.	High	Individual
			Organization

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:

Telekom Applied Business Sdn Bhd (455343-U)
Level 15, Menara TM ONE,
60000 Kuala Lumpur,
Tel: +603 2241 4917

1.5.2 Contact Person

Compliance Officer
Telekom Applied Business Sdn Bhd (455343-U)
Level 15, Menara TM ONE,
60000 Kuala Lumpur,
Tel: +603 2241 4917

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

1.5.3 Person Determining CP suitability for the Policy

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

1.5.4 CP Approval Procedures

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

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

TMCA reserves the rights to amend this CP at any time and the amendments to this CP shall be made available at TMCA's web site, https://www.tmca.com.my.Amendments shall become effective automatically within fourteen (14) working days of the CP 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 CP. The publication date is equivalent to the effective date of the CP.

1.6 Definitions and Acronyms

Acronyms and Abbreviations Used in CP

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

Acronyms/Abbreviations	Description
ISO	International Standard Organisation
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 *OCSP responders*.
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
RP	Registration Personnel
RSA	RSA (which stands for Rivest, Shamir and Adleman who first publicly described it) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be sufficiently secure given sufficiently long keys and the use of up-to-date implementations.
SHA-1	SHA-1 is a cryptographic hash function designed by the National Security Agency and published by the NIST as a U.S. Federal Information Processing Standard. SHA stands for Secure Hash Algorithm.
SSL	Secure Socket Layer
TAB	Telekom Applied Business Sdn. Bhd,
TMCA	Telekom Malaysia Certification Authority

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

2 PUBLICATION AND RESPITORY RESPONSIBILITIES

2.1 Repositories

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

2.2 Publication of Certification Information

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

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

2.3 Time or Frequency of Publication

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

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

2.4 Access Controls on Repositories

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Type of Names

a. For names used in the basic domain of digital certificates and the Certificate Revocation

List (CRL) and OCSP (Online Certificate Status Protocol), the method of ITU-T X.500 DN (Distinguished Name) is applied.

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

① Individual Certificate: Real name as in Mykad, MyTentera, Polis Diraja Malaysia Card or Passport; *Mykad Number, MyTentera Number, Polis Diraja Malaysia Number, Passport Number or Email Address (optional)*

② Corporate Certificate: Real name as in Company Registration, Company ID, and E-mail Address.

③ 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 verifies the uniqueness of Subscriber’s DN (Distinguished Name).

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

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

a. In applying for issuance of a certificate, the Subscriber should use application form prepared by TMCA.

b. TMCA verifies whether the Public Key matches the Private Key based on information contained in application form.

c. In the case of Class 2 and 3 digital certificates, there is a strong requirement to secure the private key, and TMCA shall verify it against the key held by the Subscriber.

3.2.2 Authentication of Organisation Identity

As stipulated in Section "3.2.3 Authentication of Individual Identity"

3.2.3 Authentication of Individual Identity

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

Class	Subscribers	Identification
Class 1	Individual/Business	No verification is required. Sufficed with email authentication.
Class 2 (Individual / Business /NGO)	Individual	Manual verification of ID if Subscriber visits to TMCA Office or Authorised RA Office. If Subscriber applies online, verification via supporting documents must be attached. If Subscriber is a member of corporate organisation, verification via company email or internal authentication should be sufficient. In addition, TMCA shall incorporate additional controls that include face-to-face verification.
	SME/Corporation/Organisation	Manual verification of ID if Subscriber visits to TMCA Office or Authorised RA Office. If Subscriber applies online, verification via supporting must be attached. If Subscriber is a member of corporate organisation, verification via company email or internal authentication should be sufficient. In addition, TMCA shall incorporate additional controls that include face-to-face verification.
	Server Operator	Manual verification of ID if Subscriber visits to TMCA Office or Authorised RA Office. If Subscriber applies online, verification via supporting documents must be attached. If Subscriber is a member of corporate organisation, verification via company email or internal authentication should be sufficient. In addition, TMCA shall incorporate additional controls that include face-to-face verification.
Class 3 (Individual / Business /NGO)	Individual	Manual verification of ID if Subscriber visits to TMCA Office or Authorised RA Office. If Subscriber applies online, verification via supporting documents must be attached. If Subscriber is a member of corporate organisation, verification via company email or internal authentication should be sufficient. In addition, TMCA shall incorporate additional controls that include face-to-face verification.

Class	Subscribers	Identification
	Corporation/Organisation/NGO	Manual verification of ID if Subscriber visits to TMCA Office or Authorised RA Office. If Subscriber applies online, verification via supporting documents must be attached. If Subscriber is a member of corporate organisation, verification via company email or internal authentication should be sufficient. In addition, TMCA shall incorporate additional controls that include face-to-face 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 CP.
2. In case of a reputable organisation is also an Authorised RA, option shall be given to the organisation to efficiently authenticate their employees or customers who intend to be a Subscriber of TMCA, via other means besides the manual verification. 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

TMCA shall disclose all the Cross Certificates that identify TMCA as Subject.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

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

3.3.2 Identification and Authentication for Re-Key After Revocation

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

3.4 Identification and Authentication for Revocation Requests

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

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	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. He requires present for face-to-face verification at the office of Authorized RA. All supporting documents in Section 3.2.1.1 (a) 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 - Corporate/SME	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. He requires present for face-to-face verification at the office of Authorized RA. All supporting documents in Section 3.2.2.1 (b) 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	1. Business Owner is a person who represents for the business is the ‘applicant’ and his identity shall be verified by Authorized RA during the face-to-face verification process. All supporting

Roles	Responsibilities
	documents in Section 3.2.2.2 (a) 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 – Individual Business	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. He requires present for face-to-face verification at the office of Authorized RA. All supporting documents in Section 3.2.2.12(b) 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	1. Authorized Officer from the voluntary organization is the 'applicant' responsible for applying digital certificates for the voluntary organization. All supporting documents in Section 3.2.2.3 (a) 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	1. Legal Agent acting as proxy for the voluntary organization is the 'applicant' responsible for applying digital certificates for the voluntary organization. All supporting documents in Section 3.2.3.1 (b) 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	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. All supporting documents in Section 3.2.3.1 (a) 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	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 in Section 3.2.3.2 (a) must be submitted together with the

Roles	Responsibilities
	application form. 2. Authorized RA must perform quality factors of selection, for example, not to approve the application if the applicant has criminal records.

4.2 Certificate Application Processing

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.

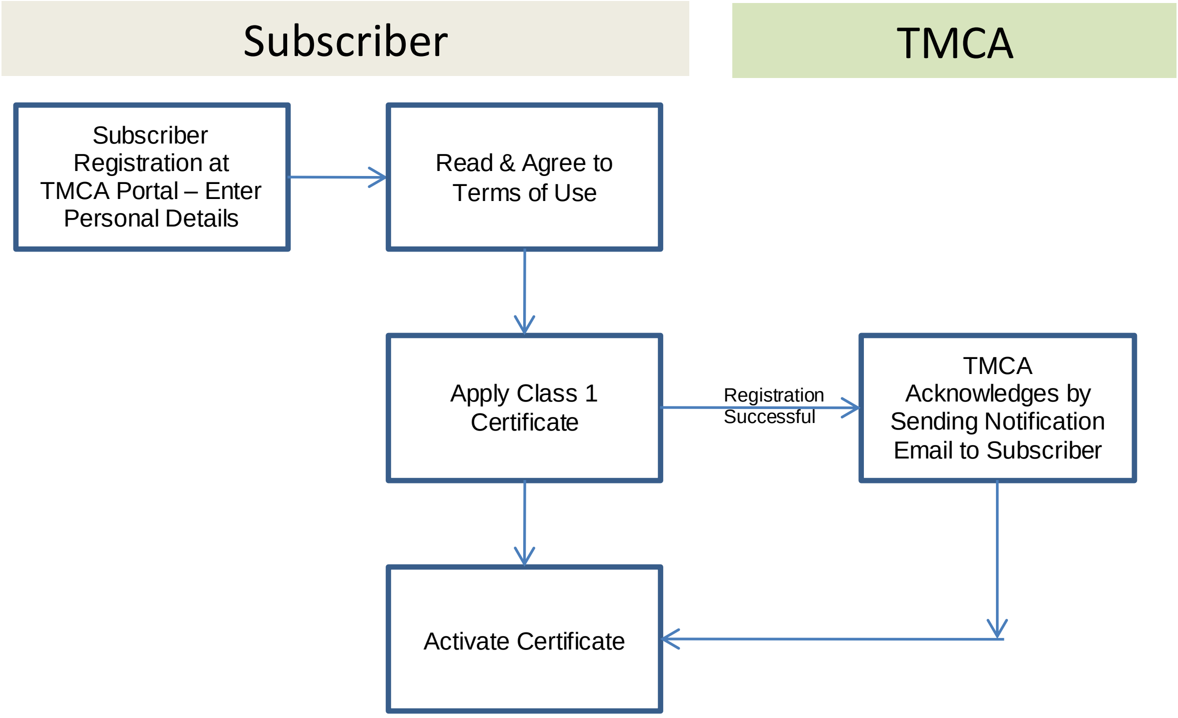

Subscriber
TMCA
Subscriber Registration at TMCA Portal – Enter Personal Details
Read & Agree to Terms of Use
Apply Class 1 Certificate
Registration Successful
TMCA Acknowledges by Sending Notification Email to Subscriber
Activate Certificate

Figure 2 Class 1 Digital Certificate Application Process Flow

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 website/Authorised Registration Authority (RA), fill in the form with required details and supporting documents and submit it personally to the Authorised RA for processing. Subscriber must first verify and confirm the application information captured by Authorised RA into system is correct before the key pair generation process. TMCA will acknowledge receipt of the Certificate Signing Request (CSR) from Authorised RA after the registration has been successfully completed at the Authorised 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 Authorised RA, TMCA will send the approval notification to the Authorised RA.

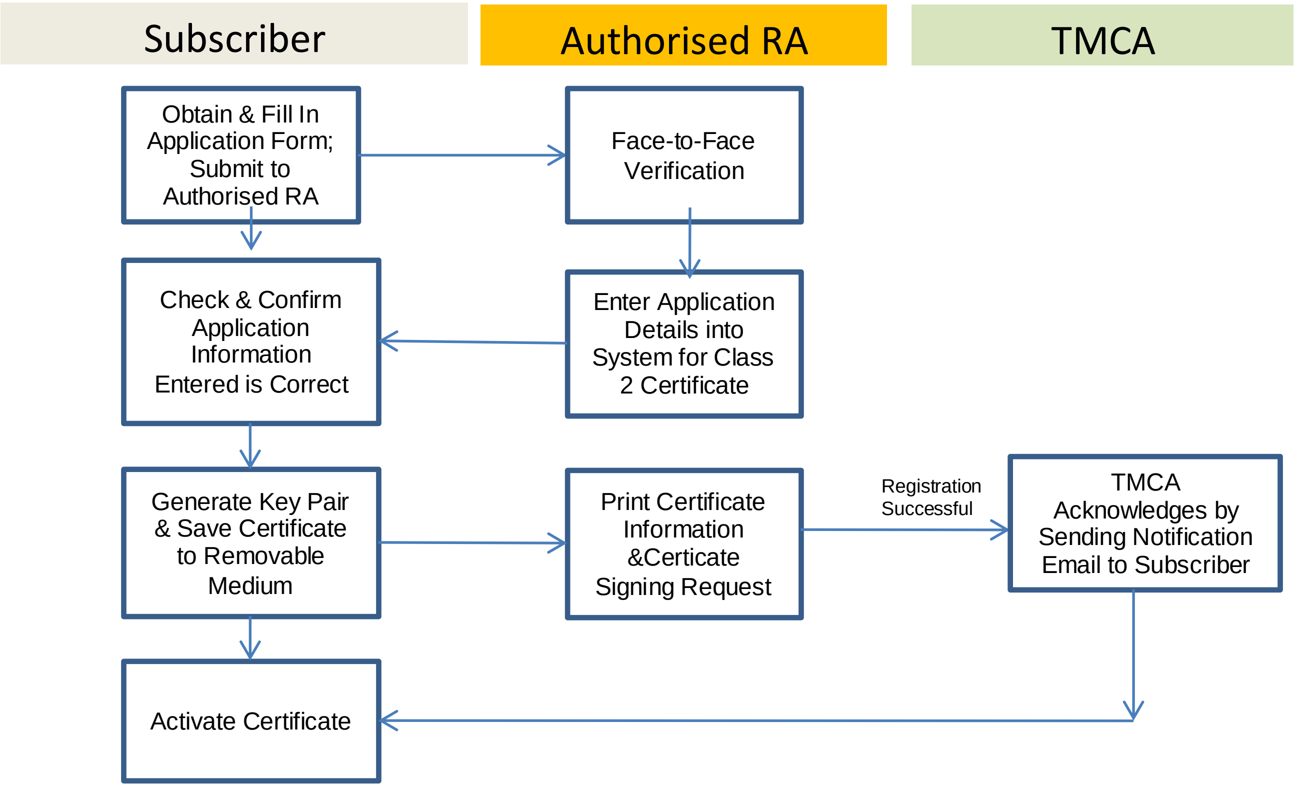

Subscriber
Authorised RA
TMCA
Obtain & Fill In Application Form; Submit to Authorised RA
Face-to-Face Verification
Check & Confirm Application Information Entered is Correct
Enter Application Details into System for Class 2 Certificate
Generate Key Pair & Save Certificate to Removable Medium
Print Certificate Information &Certicate Signing Request
Registration Successful
TMCA Acknowledges by Sending Notification Email to Subscriber
Activate Certificate

Figure 3 Class 2 Digital Certificate Application Process Flow

Class 3 Digital Certificate Application Process Flow

This process flow is similar to that of Class 2 described in Section 4.1.2 above.

The authentication of *Class 3 Individual* certificates is based on personal presence of the applicant before the Authorised RA or TMCA Management Representative. Authorised RA or TMCA Management Representative shall check the identity of the applicant against passport or driver's license and one other identification credential.

The authentication of *Class 3 Organisation* certificates is based on authentication of the organisation and a confirmation from the organisation of the employment and authorisation of the person who has submitted the application on behalf of the organisation as described in Section 3.2.2 of the CP. TMCA may also have occasion to approve applications for the organisations based on confirmation of their identity in connection with their employment or retention as an independent contractor and background checking procedures.

Dissemination and Publication of Digital Certificate Process Flow

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

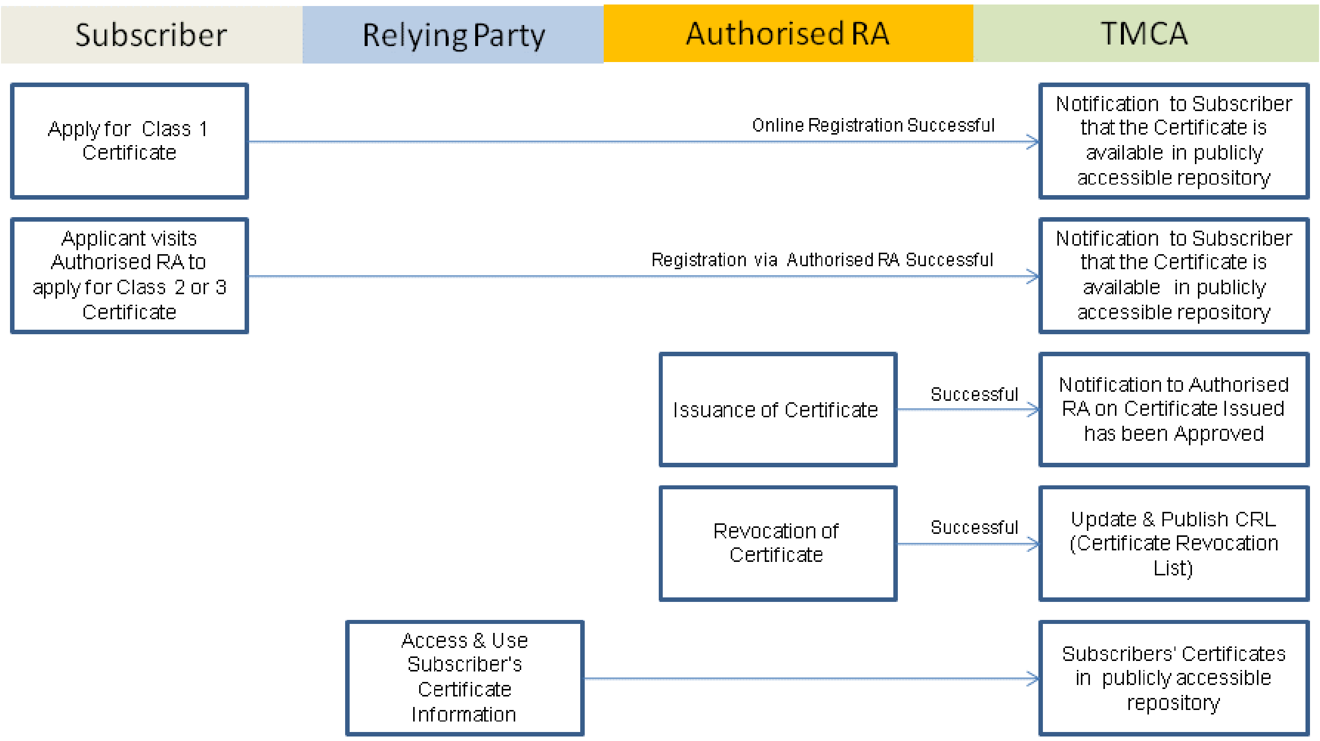

Subscriber
Relying Party
Authorised RA
TMCA
Apply for Class 1 Certificate
Online Registration Successful
Notification to Subscriber that the Certificate is available in publicly accessible repository
Applicant visits Authorised RA to apply for Class 2 or 3 Certificate
Registration via Authorised RA Successful
Notification to Subscriber that the Certificate is available in publicly accessible repository
Issuance of Certificate
Successful
Notification to Authorised RA on Certificate Issued has been Approved
Revocation of Certificate
Successful
Update & Publish CRL (Certificate Revocation List)
Access & Use Subscriber's Certificate Information
Subscribers' Certificates in publicly accessible repository

Figure 4 Dissemination and Publication of Digital Certificate Process Flow

4.2.1 Performing Identification and Authentication Functions

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

4.2.2 Approval or Rejection of Certificate Applications

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

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

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

① Personal identification of subscriber, as stipulated in Section "3.1 Naming".

② The uniqueness of DN (Distinguished Name) submitted by the Subscriber

i. 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.

ii. 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.

b. 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 "3.1 Personal Identification for Issuance of Digital Certificate" and Section "1.3.2 Registration Authorities (RAs)".

c. 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.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

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

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

TMCA issues certificate to the Subscriber upon successful processing of the application and the acceptance of the certificate by the Subscriber based on the Terms & Conditions and Acceptance Notice stated in the application form. The Subscriber is advised to verify all details contained with the certificate, any error or omission found must be communicated immediately to TMCA.

4.4.2 Publication of the Certificate by the CA

No stipulation.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and 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 CP.

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

TMCA reserves the rights to amend this CP at any time and the amendments to this CP shall be made available at TMCA's web site, https://www.tmca.com.my.Amendments shall become effective automatically within fourteen (14) working days of the CP 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 CP. The publication date is equivalent to the effective date of the CP.

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.

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 withTMCA CP.
- Verify the status of certificates at the time of reliance.

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

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, as stipulated in Section "3.1.6 Personal Identification for Renewal of Digital Certificates".

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.

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”

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:

① In the event the Subscriber or his Authorised Representative applies to TMCA for revocation.

② In the event TMCA discovers that the Subscriber obtains his digital certificate by fraud, forgery, or other illegal means.

③ In the event TMCA discovers the death, missing, or dissolution of the Subscriber or his organisation.

④ In the event TMCA discovers the Subscriber's Private Key has been lost, damaged, stolen, or compromised.

⑤ In the event the Subscriber violates any of these rules mentioned in the CPS.

⑥ In the event the designation of TMCA as a licensed Certification Authority is cancelled by MCMC.

⑦ In the event that the Subscriber discovers that his Private Key has weakness, lost, damaged, stolen or compromised.

4.9.2 Who Can Request for Revocation

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

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 access to TMCA website to revoke the certificate online. 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 should 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 aCertificate'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.

4.9.9 On-Line Revocation/Status Checking Availability

No stipulation.

4.9.10 On-Line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements re Key Compromise

As stipulated in “Section 4.9.1 Circumstances for Revocation”

4.9.13 Circumstances for Suspension

Certificate Suspension for certificates issued by TMCA is not provided.

4.9.14 Who Can Request Suspension

Only the Subscriber or his Authorised Representative can apply for suspension of a digital certificate.

4.9.15 Procedure for Suspension Request

a. Subscribers should personally visit TMCA Office or TMCA’s Authorised RA for suspension of digital certificate or access to TMCA website to apply online. 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 should be informed of change of certificate status once the suspension process has been successfully completed.

4.9.16 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.

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 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Security Controls

5.1.1 Site Location and Construction

No stipulation.

5.1.2 Physical Access

TMCA safeguards 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 security controlled area.

b. TMCA controls access to the controlled area by using 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 maintains and regularly reviews a log that records any entries into the controlled area.

f. TMCA 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 deploys UPS system that shall ensure uninterrupted services in case of power failures. TMCA 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.

TMCA also use air-conditioning system and raised floor to ensure optimum ventilation and protection.

5.1.4 Water Exposures

TMCA installs the core certification systems at a reasonable height to protect them from flood damage.

5.1.5 Fire Prevention and Protection

TMCA 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.

5.1.8 Offsite Backup

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

5.2 Procedural Controls

5.2.1 Trusted Roles

All TMCA personnel that have access to or control over PKI operations including Certificate issuance,Use, Suspension and Revocation shall, for purposes of TMCA CP,be considered as serving in a Trusted Role. Such personnel includes, 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 aTrusted Role for a CA shall:

- Be appointed in writing by TMCA
- Not be assigned other duties that may conflict with the duties defined for the Trusted Role
- Be a permanent employee or other authorised individual, and
- Have sufficient expertise and knowledge required for the performance of their duties.

5.3.2 Background Check Procedures

No stipulation.

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.

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 systems.

5.3.7 Independent Contractor Requirements

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

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

TMCA 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

No stipulation.

5.4.4 Protection of Audit Log

As part of this CA's system backup procedures, audit trail files are backed up to media 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 and stored in a secure area storage facility (e.g. safe box).

5.4.6 Audit Collection System (Internal vs. External)

No stipulation.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

No stipulation.

5.5 Records Archival

5.5.1 Types of Records Archived

The minimum records to be archived, in relation to allactions and information that is relevant to each certificateapplication and to the generation, issuance, distribution,usage, suspension, revocation, renewal and expiration of allcertificates 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 in physically separate and secure sites for ten (10) years.

5.5.3 Protection of Archive

All archives created for TMCA shall be logically secured and shall be stored in adequately safeguarded locations owned or managed by TMCA. 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. Electronic documents are safely stored with Digital Signatures.

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 regularly 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.

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

When system resources or software are damaged, TMCA restores the system immediately using dual backup system resources and software. The maximum downtime period is 4 (four) hours.

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

5.7.3 Entity Private Key Compromise Procedures

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

5.7.4 Business Continuity Capabilities After a Disaster

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

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

5.8 CA or RA Termination

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

a. The term of the digital certificate's validity elapses.

b. The designation of TMCA as a licensed Certification Authority is cancelled by MCMC.

c. The digital certificate issued by TMCA is suspended.

d. The digital certificate issued by TMCA is revoked.

e. The CA certificate issued by Root CA to TMCA is revoked.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

TMCA shall perform the generation of key pairs for:

(a) All CA key pairs are generated in pre-planned Key Generation Ceremonies in accordance to the requirements of the Key Ceremony guidelines and meeting FIPS 140-1 level 3 cryptographic requirements. The activities perfomed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by TMCA.

(b) Generation of RA key pairs will be performed by Authorised RA by using cryptographic software provided and meeting FIPS 140-1 level 3 cryptographic requirements.

(c) Generation of end-user Subscriber key pairs will be performed by the Subscriber. This is applicable for all classes of digital certificates and the appropriate tools/software shall be used by meeting FIPS 140-1 level 3 cryptographic requirements.

6.1.2 Private Key Delivery to Subscriber

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

.

6.1.3 Public Key Delivery to Certificate Issuer

The CA Certificate containing the Public Key corresponding to the CA’s signing key is delivered to each End-User eletronically 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 certificates, certificate revocation lists, and other data.

6.2 Private Keys Protection and Cryptographic Module Engineering Controls

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

6.2.1 Cryptographic Module Standards and Controls

No stipulation.

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

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

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

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

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer Into or From a Cryptographic Module

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

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

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

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

6.2.9 Method of Deactivating Private Key

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

6.2.10 Method of Destroying Private Key

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

6.2.11 Cryptographic Module Rating

All Key Pairs are generated and stored in a hardware cryptographic module (Hardware Se curity 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 asecurity 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
- Enforced separation of duties for Trusted Roles identification and authentication of Trusted Roles and associated identities
- Use of cryptography for session communication and database security
- Archival of TMCA and Subscriber history and audit data
- Audit of security-related events
- Self-test of security-related CA services
- Trusted path for identification of Trusted Roles and associated identities, and
- Recovery mechanisms for keys and the TMCA System.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

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

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

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

6.6.1 System Development Controls

No stipulation.

6.6.2 Security Management Controls

No stipulation.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

a. TMCA manages operation of the core certification systems and keeps monitoring the system current status and trend.

b. For control of access networks, TMCA employs firewall systems.

c. To protect network service from illegal intrusion, TMCA deploys intrusion detection systems.

6.8 Time-Stamping

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

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version Number(s)

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

7.1.2 Certificate Extensions

Certificate extensions are processed in accordance with RFC5280.

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

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

7.1.3 Algorithm Object Identifiers

7.1.3.1 Signature Algorithm OID

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

7.1.3.2 Encryption Algorithm OID

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

7.1.4 Name Forms

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

7.1.5 Name Constraints

Each distinguished name (DN) of an TMCA CertificateSubject includes 'O = TM'.

7.1.6 Certificate Policy Object Identifier

No stipulation.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

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

7.3 OCSP Profile

No stipulation.

7.3.1 Version Number(s)

No stipulation.

7.3.2 OCSP Extension

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency and Circumstances of Assessment

TMCA shall undergo with a minimum of once per year as part of its annual PKI audit. All audits shall be performed in compliance with TMCA CP and WebTrust for Certification Authorities version 2.0 Program.. The audit also checks the consistency with Certification Practice Statement and Certification Policy.

8.2 Identity/Qualifications of Assessor

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

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

8.3 Assessor’s Relationship to Assessed Entity

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

8.4 Topics covered by Assessment

Each audit will include, but is not limited to, compliance with TMCA CP and WebTrust for Certification Authorities version 2.0 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 bepublicly available. Audit results will be made available to TMCA internal departments.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

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

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

All collected or processed personal data within TMCA is kept confidential and handled in full compliance witha 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

9.4.2 Information Treated as Private

Non-public Subscriber information is treated as private.

9.4.3 Information Not Deemed as Private

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

9.4.4 Responsibility to Protect Private Information

No stipulation.

9.4.5 Notice and Consent to Use Private Information

No stipulation.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

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

a. CP and CPS

b. Certificates

c. Revocation Information

d. TMCA's root keys and root certificates

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

No stipulation.

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscribers Representations and Warranties

No stipulation.

9.6.4 Relying Party Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

9.7.1 TMCA's Liability

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

9.7.2 RA's Liabilities

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

9.7.3 Subscriber's Liabilities

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

9.8 Limitations of Liability

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

Class	Liability Caps
Class 1	No liability
Class 2	Ringgit Malaysia Twenty Five Thousand (RM25,000.00)
Class 3	Ringgit Malaysia Five Hundred Thousand (RM500,000.00)

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

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

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

9.9 Indemnities

9.9.1 CA Obligations

TMCA shall be obliged to:

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

9.9.2 RA Obligations

9.9.2.1 Operation of RAs

a. To perform identity verification services, TMCA may outsource the functions to several Registration Authorities (RAs). RAs are reputable organisations that are capable to carry out the functions without compromising to the security procedures adopted by TMCA. Before RAs are appointed, the RAs need to sign up contract with TMCA and acceptance test will be carried out to ensure they are in compliance to the procedures.

b. The main functions of RAs are as follows:

   i. Receipt of application for certification services such as:

      - Issuance
      - Renewal
      - Suspension
      - Reinstatement
      - Revocation

   ii. Personal identification of applicants.

   iii. Requesting TMCA to issue applicants' certificates and notifying to applicants.

   iv. Other functions related to certification services as commissioned by TMCA.

9.9.2.2 Observance of Certificate Policy

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

9.9.2.3 Receipt of Applications for Certification Services

a. Registration Authorities must accept only those applications with accurate information and until verifications are completed, applications are not treated as "accepted". For personal identification, Registration Authorities observe specific guidelines set by TMCA.

b. Once the reception process is completed, Registration Authorities issue receipt slips prepared by TMCA.

c. Registration Authorities are prohibited from refusing receipt of certificate applications without valid reasons. If applications are rejected, Registration Authorities should clearly state the reasons the applications are rejected.

9.9.2.4 Protection of Private Information & Safekeeping of Data Security

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

9.9.2.5 Safeguard of Facilities & Personnel

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

9.9.3 Subscriber Obligations

9.9.3.1 Provision of Accurate Information

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

9.9.3.2 Generation of Key Pair

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

9.9.3.3 Protection & Safekeeping of Private Keys

a. Subscribers are responsible at all time for the safekeeping of Private Keys to prevent their loss, damage, theft, or being compromised.

b. In the event that the Private Keys belonging to the Subscribers have been lost, damaged, stolen, or compromised, Subscribers should immediately notify TMCA via email or call TMCA Data Center.

c. TMCA after further verification shall determine as to whether to revoke the Subscriber's digital certificate. This is to prevent further damage due to miss-use of the Subscriber's digital certificates by an unauthorised person.

9.9.3.4 Use of Private Key

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

9.9.3.5 Verification of Digital Certificates

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

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

9.9.4 Relying Party Obligations

Relying Party obligations are:

- Restrict reliance on certificates issued by TMCA to the purposes for those certificates, in accordance withTMCA CP.
- Verify the status of certificates at the time of reliance.
- Confirm the validity, issuing body, types, and purpose of the corresponding digital certificates before conducting e-business using digital certificates.
- Verify and confirm whether the digital certificates are suspended or revoked of their

validity by using CRL.

- Damages if any due to users not observing the above confirmation process shall be exclusively borne by the Relying Parties.
- Agree to be bound by the provisions of limitations of liability as described in the CP upon reliance on a certificate issued by the TMCA.

9.9.5 Repository Obligations

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

9.10 Term and Termination

9.10.1 Term

No stipulation.

9.10.2 Termination

No stipulation.

9.10.3 Effect of Termination and Survival

No stipulation.

9.11 Individual Notices and Communication with Participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

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

9.12.2 Notification Mechanism and Period

No stipulation.

9.12.3 Circumstances Under Which OID Must Be Changed

No stipulation.

9.13 Dispute Resolution Procedures

No stipulation.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

The use of TMCA certificates shall always comply with the applicable law. This CP will be interpreted and applied in pursuant to the Digital Signature Act 1998 and other related Laws of Malaysia.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

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

No stipulation.

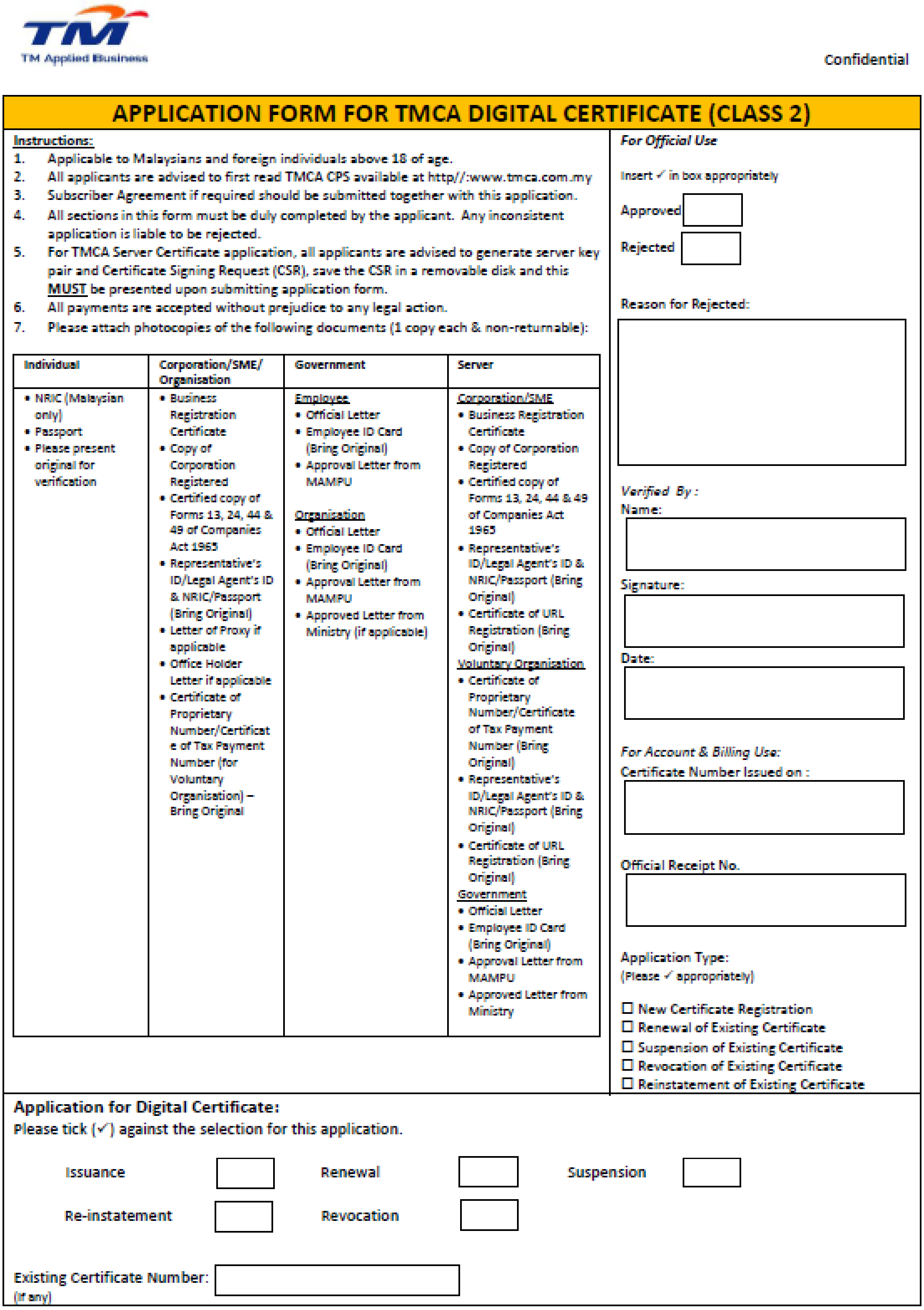
9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.

Appendix A – Application Form for TMCA Digital Certificate



TM Applied Business

Confidential

APPLICATION FORM FOR TMCA DIGITAL CERTIFICATE (CLASS 2)

Instructions:

1. Applicable to Malaysians and foreign individuals above 18 of age.
2. All applicants are advised to first read TMCA CPS available at http//:www.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 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. Please attach photocopies of the following documents (1 copy each & non-returnable):

Individual	Corporation/SME/ Organisation	Government	Server
• NRIC (Malaysian only) • Passport • Please present original for verification	• Business Registration Certificate • Copy of Corporation Registered • Certified copy of Forms 13, 24, 44 & 49 of Companies Act 1965 • Representative's ID/Legal Agent's ID & NRIC/Passport (Bring Original) • Letter of Proxy if applicable • Office Holder Letter if applicable • Certificate of Proprietary Number/Certificate of Tax Payment Number (for Voluntary Organisation) – Bring Original	Employee • Official Letter • Employee ID Card (Bring Original) • Approval Letter from MAMPU Organisation • Official Letter • Employee ID Card (Bring Original) • Approval Letter from MAMPU • Approved Letter from Ministry (if applicable)	Corporation/SME • Business Registration Certificate • Copy of Corporation Registered • Certified copy of Forms 13, 24, 44 & 49 of Companies Act 1965 • Representative's ID/Legal Agent's ID & NRIC/Passport (Bring Original) • Certificate of URL Registration (Bring Original) Voluntary Organisation • Certificate of Proprietary Number/Certificate of Tax Payment Number (Bring Original) • Representative's ID/Legal Agent's ID & NRIC/Passport (Bring Original) • Certificate of URL Registration (Bring Original) Government • Official Letter • Employee ID Card (Bring Original) • Approval Letter from MAMPU • Approved Letter from Ministry

For Official Use

Insert ✓ in box appropriately

Approved □

Rejected □

Reason for Rejected:

Verified By :

Name:

Signature:

Date:

For Account & Billing Use:

Certificate Number Issued on :

Official Receipt No.

Application Type:
(Please ✓ appropriately)

□ New Certificate Registration
□ Renewal of Existing Certificate
□ Suspension of Existing Certificate
□ Revocation of Existing Certificate
□ Reinstatement of Existing Certificate

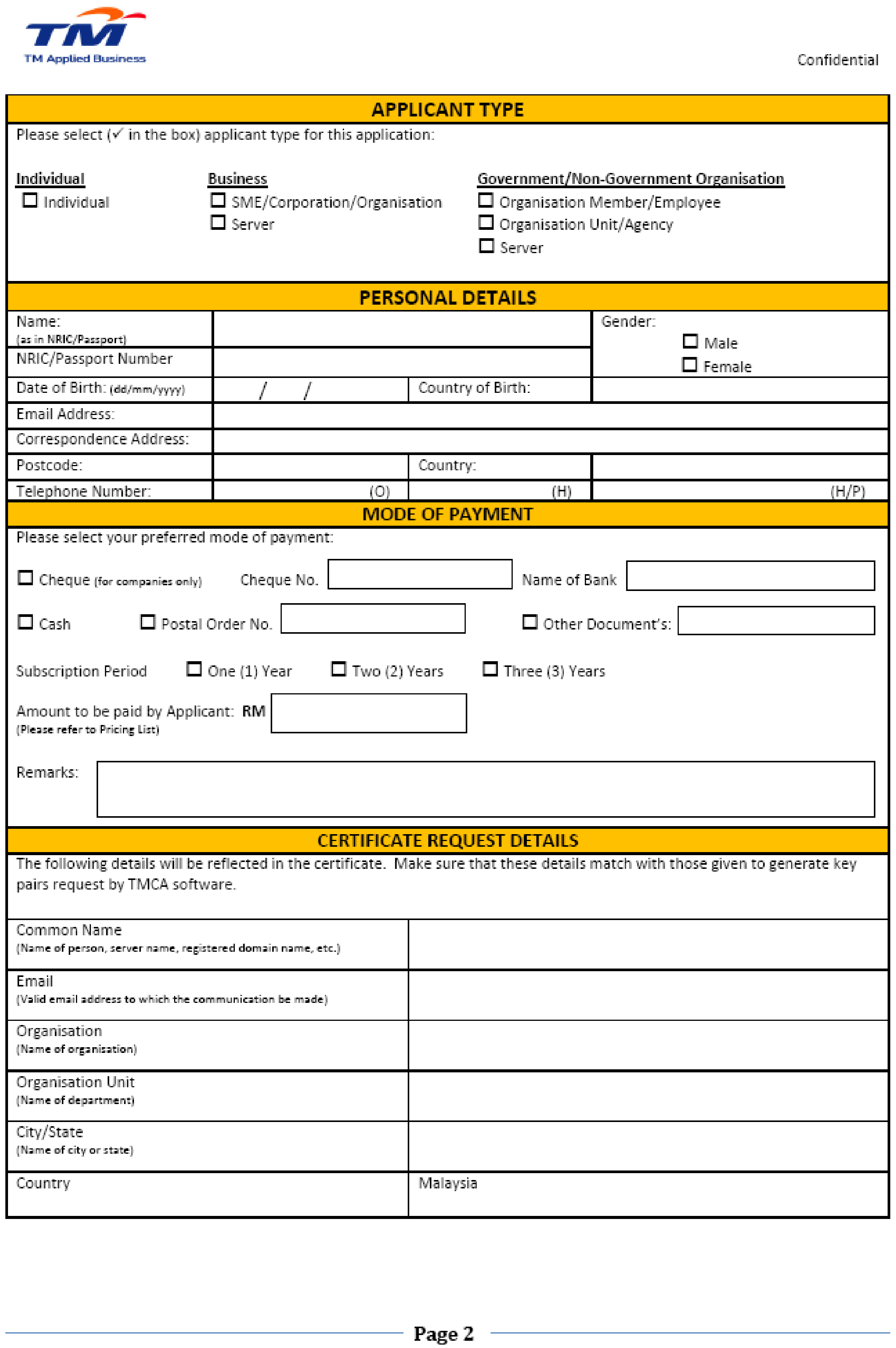
Application for Digital Certificate:

Please tick (✓) against the selection for this application.

Issuance □ Renewal □ Suspension □

Re-instatement □ Revocation □

Existing Certificate Number: ____________
(If any)



TM Applied Business

Confidential

APPLICANT TYPE

Please select (✓ in the box) applicant type for this application:

Individual	**Business**	**Government/Non-Government Organisation**
□ Individual	□ SME/Corporation/Organisation	□ Organisation Member/Employee
	□ Server	□ Organisation Unit/Agency
		□ Server

PERSONAL DETAILS

Name: (as in NRIC/Passport)			Gender: □ Male □ Female
NRIC/Passport Number			
Date of Birth: (dd/mm/yyyy)	/ /	Country of Birth:	
Email Address:			
Correspondence Address:			
Postcode:		Country:	
Telephone Number:	(O)	(H)	(H/P)

MODE OF PAYMENT

Please select your preferred mode of payment:

□ Cheque (for companies only) Cheque No. ______ Name of Bank ______

□ Cash □ Postal Order No. ______ □ Other Document's: ______

Subscription Period □ One (1) Year □ Two (2) Years □ Three (3) Years

Amount to be paid by Applicant: **RM** ______
(Please refer to Pricing List)

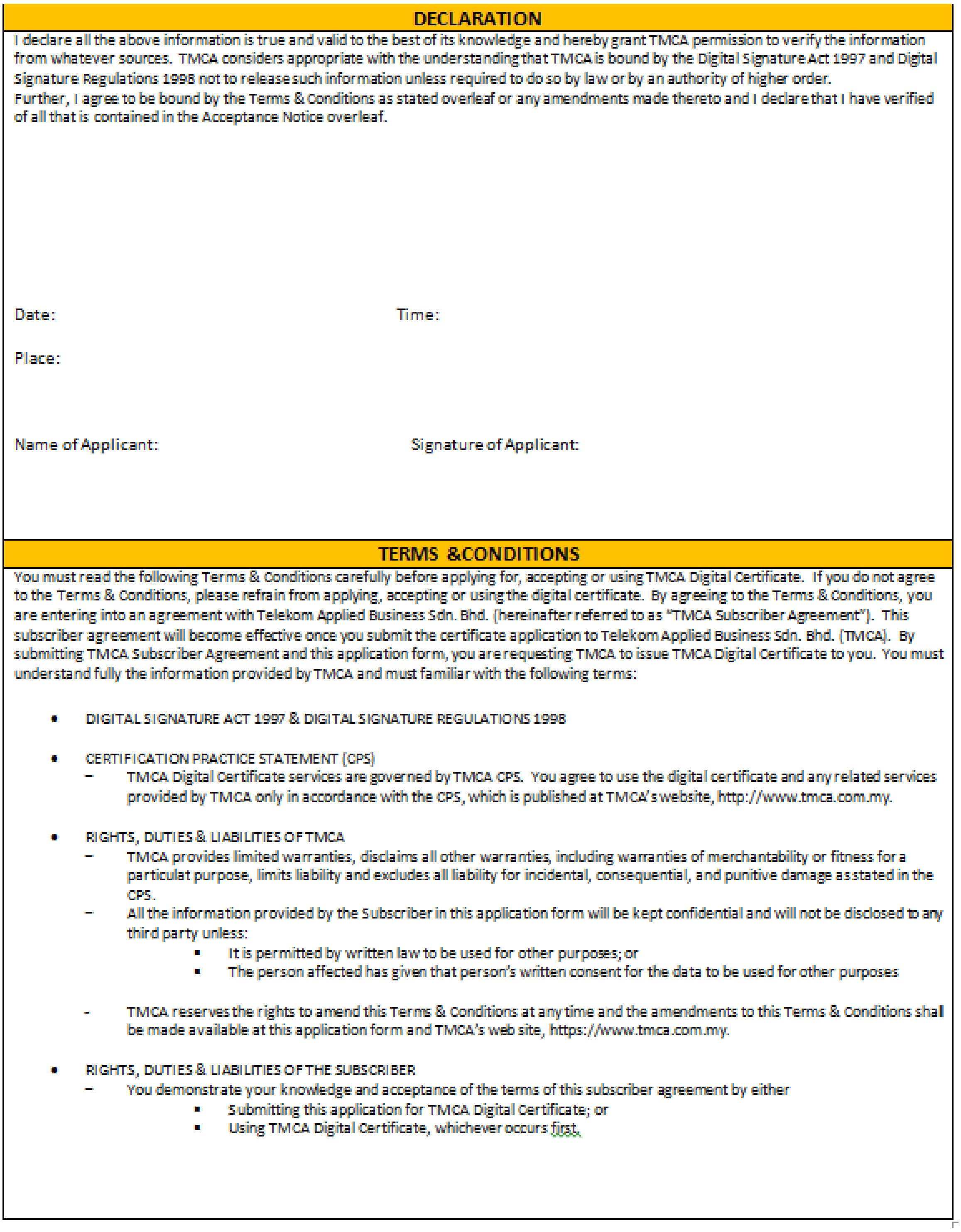
Remarks: ______

CERTIFICATE REQUEST DETAILS

The following details will be reflected in the certificate. Make sure that these details match with those given to generate key pairs request by TMCA software.

Common Name (Name of person, server name, registered domain name, etc.)	
Email (Valid email address to which the communication be made)	
Organisation (Name of organisation)	
Organisation Unit (Name of department)	
City/State (Name of city or state)	
Country	Malaysia

Page 2



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.

Date: Time:

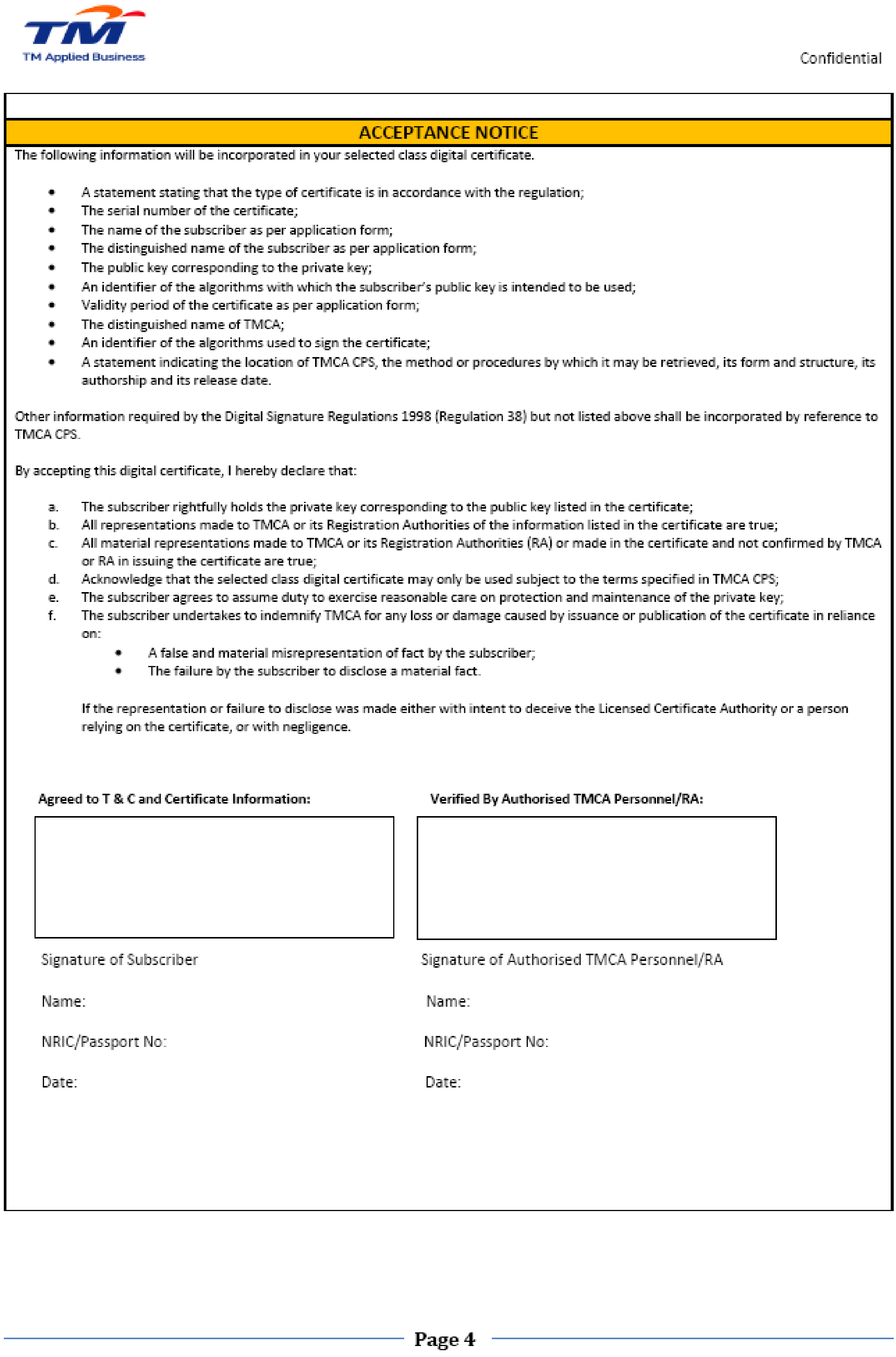
Place:

Name of Applicant: Signature of Applicant:

TERMS &CONDITIONS

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 particulat purpose, limits liability and excludes all liability for incidental, consequential, and punitive damage as stated in the CPS.
  - 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 to 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.



TM Applied Business

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:

a. The subscriber rightfully holds the private key corresponding to the public key listed in the certificate;
b. All representations made to TMCA or its Registration Authorities of the information listed in the certificate are true;
c. 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;
d. Acknowledge that the selected class digital certificate may only be used subject to the terms specified in TMCA CPS;
e. The subscriber agrees to assume duty to exercise reasonable care on protection and maintenance of the private key;
f. The subscriber undertakes to indemnify TMCA for any loss or damage caused by issuance or publication of the certificate in reliance on:
    - A false and material misrepresentation of fact by the subscriber;
    - 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.

Agreed to T & C and Certificate Information:

Signature of Subscriber

Name:

NRIC/Passport No:

Date:

Verified By Authorised TMCA Personnel/RA:

Signature of Authorised TMCA Personnel/RA

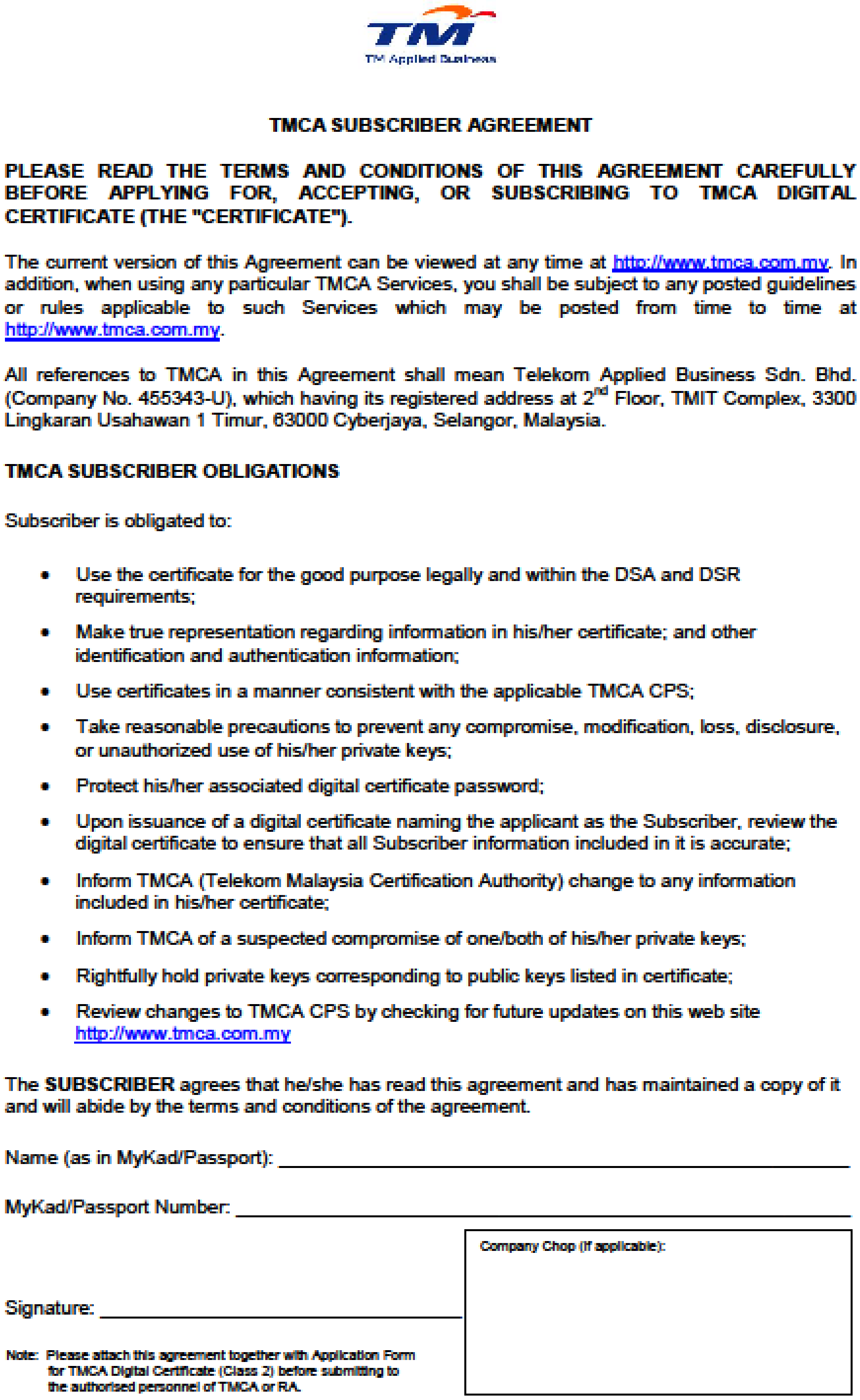
Name:

NRIC/Passport No:

Date:

Page 4

Appendix B – TMCA Subscriber Agreement (Online & Downloadable Versions)



TMCA SUBSCRIBER AGREEMENT

PLEASE READ THE TERMS AND CONDITIONS OF THIS AGREEMENT CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR SUBSCRIBING TO TMCA DIGITAL CERTIFICATE (THE "CERTIFICATE").

The current version of this Agreement can be viewed at any time at http://www.tmca.com.my. In addition, when using any particular TMCA Services, you shall be subject to any posted guidelines or rules applicable to such Services which may be posted from time to time at http://www.tmca.com.my.

All references to TMCA in this Agreement shall mean Telekom Applied Business Sdn. Bhd. (Company No. 455343-U), which having its registered address at 2nd Floor, TMIT Complex, 3300 Lingkaran Usahawan 1 Timur, 63000 Cyberjaya, Selangor, Malaysia.

TMCA SUBSCRIBER OBLIGATIONS

Subscriber is obligated to:

- Use the certificate for the good purpose legally and within the DSA and DSR requirements;
- Make true representation regarding information in his/her certificate; and other identification and authentication information;
- Use certificates in a manner consistent with the applicable TMCA CPS;
- Take reasonable precautions to prevent any compromise, modification, loss, disclosure, or unauthorized use of his/her private keys;
- Protect his/her associated digital certificate password;
- Upon issuance of a digital certificate naming the applicant as the Subscriber, review the digital certificate to ensure that all Subscriber information included in it is accurate;
- Inform TMCA (Telekom Malaysia Certification Authority) change to any information included in his/her certificate;
- Inform TMCA of a suspected compromise of one/both of his/her private keys;
- Rightfully hold private keys corresponding to public keys listed in certificate;
- Review changes to TMCA CPS by checking for future updates on this web site http://www.tmca.com.my

The **SUBSCRIBER** agrees that he/she has read this agreement and has maintained a copy of it and will abide by the terms and conditions of the agreement.

Name (as in MyKad/Passport): ______________________________

MyKad/Passport Number: ______________________________

Company Chop (If applicable):

Signature: ______________________________

Note: Please attach this agreement together with Application Form for TMCA Digital Certificate (Class 2) before submitting to the authorised personnel of TMCA or RA.