TM TECHNOLOGY SERVICES SDN BHD
CERTIFICATE AUTHORITY
(TMCA)

Essential Pre-Subscription Readings for TMCA Digital Certificates

VERSION 1.0

TMTECH-TMCA-PreSubscprtion-001

DATE OF PUBLICATION: 3rd JULY 2024

Revision History

Date	Version	Modification Type	Item/ Ref.No.	Description	Author
3rd July, 2024	1	New		Approved for publication.	TMCA CPS Committee

Reviewed by

Name: Nazman Fariz Mohd Noh

Designation: AGM ESS CYDEC

Date: : 3rd July 2024

Approved by

Name: TMCA CP CPS Committee

Designation: TMCA CP CPS Committee

Date: : 3rd July 2024

TOC

Contents

Introduction

Prior to accepting the terms & conditions of TMCA Digital Certificate it is advisable for potential Subscribersto have some pre-requisite knowledge of the following information:

a. Digital Certificates;
b. Digital Signatures;
c. Digital Signature Act 1997;
d. Digital Signature Regulations 1998;
e. The rights, duties and liabilities of the licensed CA, RA, Subscribers and relyingparties.

1 Digital Certificates

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

---

2 Digital Signatures

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

---

3 Digital Signature Act 1997 (Malaysia)

The **Digital Signature Act 1997** is a legislative framework established by the Malaysian government to regulate the use of digital signatures within the country. This Act provides legal recognition for digital signatures, making them legally

equivalent to handwritten signatures under certain conditions. It sets out the requirements for the licensing of Certification Authorities (CAs), the responsibilities of licensed CAs, and the standards for digital signatures to be considered valid. The Act aims to facilitate secure electronic commerce and communications by providing a trusted environment for digital transactions.

The copy of the document can be obtained from TMCA website at www.tmca.com.my

---

4 Digital Signature Regulations 1998 (Malaysia)

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

The copy of the document can be obtained from TMCA website at www.tmca.com.my

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

5.1 Licensed Certification Authorities (CAs)

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

5.2 Registration Authorities (RAs)

- **Rights:** RAs act on behalf of CAs to verify the identity of certificate applicants and facilitate the certificate issuance process.

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

5.3 Subscribers

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

5.4 Relying Parties

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

6 Restrictions and limitations

For subscribers (certificate holders) and relying parties (those who use certificates to verify identities or secure communications) of TMCA digital certificates, various restrictions and limitations may apply. The following outlines the specific constraints and conditions that subscribers and relying parties encounter upon subscribing to TMCA digital certificates.

6.1 Validity Period

Certificates have an expiration date and cannot be used beyond that without renewal.

6.2 Usage Restrictions

Certificates often specify their permitted uses (e.g., encryption, digital signatures.

Code signing, IoT device) and may restrict other uses.

6.3 Revocation

Certificates can be revoked if compromised or if the subscriber no longer meets requirements, making them invalid before their expiration date.

6.4 Trust Chain

Relying parties **need to trust** TM Technology Services Sdn Bhd Certificate Authority (TMCA) and verify the entire chain of trust up to TMCA trusted root CA.

The certificates can be obtained from TMCA website at www.tmca.com.my

Type of certificates:

- Root Certificates
- Intermediate Certificates TM Applied Business Root Certificate RSA R2
- Intermediate Certificates TM Applied Business Root Certificate ECC R2
- Intermediate Certificates TM Tech Class 2 RSA ROOT CA R1

6.4.1 How to trust TM Technology Services Sdn Bhd digital certificate

6.4.1.1 Windows (11)

To manually trust a digital certificate in Windows 11, you can follow these steps:

6.4.1.1.1 Importing a Certificate into Trusted Root Certification Authorities

1) Open the Run Dialog Box:

- Press `Win + R` to open the Run dialog box.

2) Open the Certificate Manager:

- Type `certmgr.msc` and press `Enter`. This opens the Certificate Manager.

3) Navigate to Trusted Root Certification Authorities:

- In the Certificate Manager window, expand the `Trusted Root Certification Authorities` folder.
- Click on the `Certificates` sub-folder.

4) Import the Certificate:

- Right-click on the `Certificates` sub-folder.
- Select `All Tasks` -> `Import`.

6.4.1.1.2 Certificate Import Wizard:

- In the Certificate Import Wizard, click `Next`.
- Click `Browse` and select the certificate file you want to trust (e.g., a `.crt`, `.pfx` or `.cer` file).
- Click `Next`.

6.4.1.1.3 Place the Certificate in the Trusted Root Certification Authorities Store:

- Ensure the option `Place all certificates in the following store` is selected.
- The selected store should be `Trusted Root Certification Authorities`.
- Click `Next`.

6.4.1.1.4 Complete the Import Process:

- Click `Finish` to complete the import process.
- You should see a message saying that the import was successful.

6.4.1.1.5 Confirming the Certificate is Trusted

- **Verify the Certificate**:
  - In the Certificate Manager, within the `Trusted Root Certification Authorities` -> `Certificates` sub-folder, look for the imported certificate.
  - Double-click the certificate to open its details.
  - Ensure that it says "This certificate is OK" under the `General` tab, indicating that the certificate is trusted.

6.4.1.1.6 Using the Certificate in Applications

- After importing the certificate into the Trusted Root Certification Authorities store, it will be trusted by default for all applications that use the Windows Certificate Store. This includes browsers like Microsoft Edge and Chrome, email clients, and other applications that rely on the Windows Certificate Store for secure communications.

6.4.1.1.7 Additional Notes

- **Administrator Rights**: You may need administrator rights to perform these actions, especially when importing a certificate into the Trusted Root Certification Authorities store.
- **Security Considerations**: Only import certificates from trusted sources to avoid compromising the security of your system. Importing an untrusted or malicious certificate could expose your system to security risks.

By following these steps, you can manually trust a digital certificate in Windows 11, ensuring that the certificate is recognized as valid and trusted by your system and its applications.

6.4.1.2 IOS

To manually trust a digital certificate on an iOS device, such as macbook, an iPhone or iPad, you can follow these steps:

6.4.1.2.1 Importing and Trusting a Digital Certificate on iOS

1) **Obtain the Certificate File**

   - Ensure you have the digital certificate file (usually in `.crt`, `.cer`, `.pfx` or `.pem` format) accessible on your iOS device. You can email it to yourself, download it from a website, or use a cloud storage service like iCloud, Dropbox, or Google Drive.

2) **Install the Certificate**

   - Open the certificate file on your iOS device. You can do this by tapping the certificate file in your email, browser, or cloud storage app.
   - When you tap the certificate file, you should see an option to install it. Tap `Install`.

3) **Complete the Installation**

   - If prompted, enter your device passcode.
   - Tap `Install` again on the warning screen to confirm the installation of the certificate.
   - Tap `Done` when the installation is complete.

6.4.2 Trusting the Installed Certificate

1) **Open Settings**

   - Go to the `Settings` app on your iOS device.

2) **Navigate to General**

   - Scroll down and tap `General`.

3) **Go to About**

   - Scroll down and tap `About`.

4) **View Certificate Trust Settings:**

- Scroll down and tap `Certificate Trust Settings`. This section displays the list of installed root certificates.

5) **Enable Full Trust for the Certificate:**

- Find the certificate you just installed in the list.
- Toggle the switch next to the certificate to enable full trust for it. This makes the certificate trusted by your device for secure connections.

6.4.3 Additional Notes

- **Profile Installation**: Sometimes, the certificate installation might be part of a configuration profile. In that case, you need to install the configuration profile first by going to `Settings` -> `General` -> `Profiles` (if available) and following the prompts.
- **Security Considerations**: As with any system, ensure you only install and trust certificates from trusted sources to avoid compromising the security of your device. Trusting a malicious certificate could expose your device to security risks.

By following these steps, you can manually trust a digital certificate on an iOS device, allowing it to be recognized as valid and trusted for secure communications and applications on your iPhone or iPad.

6.5 Key Size and Algorithm Restrictions

Certificates may have limitations on the cryptographic key size and algorithms used, affecting their security and compatibility. TMCA aims to use algorithms approved by NIST and widely recommended globally, thereby ensuring high security standards for our certificates

6.6 Legal and Compliance Requirements

Depending on the jurisdiction and application, there may be legal and regulatory restrictions on how certificates are used and managed.

6.7 Certificate Policies and Practices

TMCA define policies and practices that govern the issuance and management of certificates in our TM TECH TMCA CPS (Certification Practice Statements) which subscribers and relying parties must comply with.

The copy of the document can be obtained from TMCA website at www.tmca.com.my

7 Your Continued Use of Our Services

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

8 Contact Information

We understand that you may have questions or concerns about our privacy practices. For specific inquiries related to TMCA's data handling practices, you can contact the TMCA Manager at:

TMCA Manager:

Email: elia@tm.com.my

Phone: +6013 3999398

We strive to respond to all inquiries promptly and within the timeframes required by applicable data protection laws.