



**Suruhanjaya Komunikasi dan Multimedia Malaysia**  
Malaysian Communications and Multimedia Commission

## **FREQUENTLY ASKED QUESTIONS - DIGITAL SIGNATURE**

**01 February 2023**

Document No : Frequently Asked Questions – Digital Signature  
Revision : Initial Version  
Date : 01 Feb 2023

© MCMC 2023. All rights reserved

# FREQUENTLY ASKED QUESTIONS - DIGITAL SIGNATURE

## TABLE OF CONTENTS

<b>PART A: GENERAL - ABOUT DIGITAL SIGNATURES</b> .....	3
1. What is a digital signature? .....	3
2. What is a digital certificate?.....	3
3. What is the difference between an electronic signature and a digital signature?.....	3
4. What are the key features of a digital signature?.....	4
5. What is the legal effect of a digital signature and an electronic signature? ..	4
6. What are the benefits of using a digital signature? .....	5
7. How secure is a digital signature? .....	6
8. How is a digital signature created? .....	7
<b>PART B: APPLYING FOR THE USAGE OF DIGITAL SIGNATURES</b> .....	8
1. How can I apply for a digital certificate to be used in digital signatures? ..	8
2. What is the general process for applying a digital certificate and using it in a digital signature?.....	8
3. What is a licensed Certification Authority (CA)?.....	9
4. What is the cost for using the digital signature? .....	9
5. What do the different classes of a digital certificate mean?.....	9
<b>PART C: APPLYING AS LICENSED CA, RECOGNISED REPOSITORY OR RECOGNISED DATE/TIME STAMP SERVICES</b> .....	10
1. What types of licence and recognitions are available under the DSA 1997 and the DSR 1998? .....	10
2. How can I apply to become a licensed CA, a recognised repository provider, or a recognised date/time stamp service provider? .....	11
3. A licensed CA may also become a recognised repository or a recognised date/time stamping service provider. When applying for both, should the application fees be paid separately? .....	11
4. What are the relevant information and documents to be provided and submitted together with the application(s)?.....	11
5. Can a company residing outside of Malaysia provide a recognised repository and a recognised date/time stamp service? .....	12
6. How long will the licence or certification of recognition be valid for, and how long will it take to process the licence / recognition?.....	12

7. Can a government agency apply to become a CA?.....	12
8. Is a licensed CA required to maintain a specific amount of working capital? .....	12
9. What is the standard time used for the provision of date/time stamp services?.....	13
10. Can a foreign entity be a shareholder in the company applying as a licensed CA?.....	13
11. Can a foreign entity apply as a licensed CA in Malaysia? .....	13
<b>PART D: FOREIGN CERTIFICATION AUTHORITY .....</b>	<b>14</b>
1. What are the requirements for recognition of foreign CA in Malaysia? ....	14
2. How to apply for recognition as a foreign CA in Malaysia?.....	14
3. Does a digital signature that has been issued or created by foreign CA have the same effect and validity in Malaysia?.....	14
<b>OTHER REFERENCES.....</b>	<b>15</b>

**INTRODUCTION**

This part provides an overview of the concept and adoption of a digital signature in Malaysia.

**1. What is a digital signature?**

The concept of a digital signature is equivalent to a handwritten signature, it allows you to sign a document electronically while validating the signer. It is created through a mathematical technique called an “asymmetric cryptography algorithm”. The following actions are made possible with the aid of this cryptographic operation:

- i. Proving the document's authenticity and the source;
- ii. Ensuring the document is not modified after being signed; and
- iii. Confirming the signer's identity by issuing a signer’s digital certificate that is attached to the signature.

**2. What is a digital certificate?**

A digital certificate is an electronic file containing information about an individual and his or her public key.

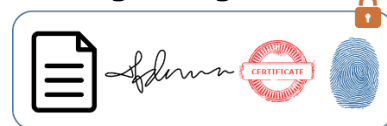
A digital certificate is digitally signed by a licensed Certification Authority (“CA”) and are required to create a digital signature. Digital certificates must only be issued by a licensed CA and are only valid for a specified time.

**3. What is the difference between an electronic signature and a digital signature?**

**Electronic Signature**



**Digital Signature**



The primary distinction between a digital signature and an electronic signature is that the former provides integrity, authentication, and nonrepudiation for documents while safeguarding the interest of the signer, and is issued by a licensed CA, whereas the latter is subject to the risk of

tampering and has no authority in verifying the identity of the signer who electronically signs the document.

Electronic signatures are governed by the Electronic Commerce Act (“ECA 2006”); it provides for the legal recognition of electronic messages in commercial transactions, the use of electronic messages to fulfil legal requirements, as well as to enable and facilitate commercial transactions by electronic means. The ECA defines an electronic signature to mean “any letter, character, number, sound, or any other symbol, or any combination thereof, created in an electronic form adopted by a person as a signature.”

Digital signatures are governed by the Digital Signature Act (“DSA”) 1997. It is a signature generated using an asymmetric cryptosystem and verified by reference to the public key listed in a valid certificate issued by a licensed CA. Such a certificate is used to verify the identity of the signer of a message and to ensure the correctness and validity of information in electronic transactions. Digital signatures offer more security and protection compared to other types of electronic signatures as they are created based on a set of algorithms and a unique authentication process.

#### **4. What are the key features of a digital signature?**

The main characteristic of a digital signature is that the signer must be identified and verified by reference to the public key listed in a digital certificate that was issued by a licensed CA. Meanwhile, an electronic signature can be any letter, character, number, sound, or any other symbol, or any combination thereof, created in electronic form adopted by a person as a signature.

However, an electronic signature is harder to verify as compared to a digital signature because there is no digital certificate issued and attached to an electronic signature, whereas a digital certificate has the feature of preventing tampering. Thus, the electronic signature is less secure.

#### **5. What is the legal effect of a digital signature and an electronic signature?**

A digital signature is governed by the DSA 1997 and the Digital Signature Regulations 1998 (“DSR 1998”) under the purview of the Malaysian Communications and Multimedia Commission (“MCMC”). Subsection 62(2) of the DSA 1997 clearly states that a document signed with a digital signature has the same legally binding effect as a document signed with a handwritten signature, an affixed thumbprint, or any other mark.

An electronic signature is governed by the ECA 2006 under the purview of the Ministry of Domestic Trade and Cost of Living (“KPDNKSJ”). The communication of proposals and formation of legally binding contracts expressed and signed via any electronic format shall have legal effect and be binding on the parties involved, provided the conditions set out in Section 9 of the ECA 2006 are fulfilled. Under subsection 10(1) of the ECA 2006, it is stated that for any electronic document that requires a seal to be affixed, a digital signature must be used instead.

## 6. What are the benefits of using a digital signature?

<b>(a) Integrity</b>	<ul style="list-style-type: none"> <li>▪ The document remains exactly as it was signed and cannot be altered in any way after signing, without invalidating the signature.</li> <li>▪ Reduce and eliminate the possibility of the document being tampered with.</li> </ul>
<b>(b) Authentication</b>	<ul style="list-style-type: none"> <li>▪ Only the licensed CA is allowed to issue digital certificates.</li> <li>▪ The document has been verified as it came from the signer and no one else.</li> <li>▪ Minimises the risk of impersonation in digital communications.</li> </ul>
<b>(c) Nonrepudiation</b>	<ul style="list-style-type: none"> <li>▪ The document signer cannot deny his/her signature on the document. A digital signature provides added assurances of evidence in terms of the origin, identity, and status of an electronic document, transaction, or message. The signer’s identity is validated by the digital certificate, regardless of the output of the signature itself.</li> </ul>
<b>(d) Time-Stamped</b>	<ul style="list-style-type: none"> <li>▪ Time-stamping consists of associating a specific date and time with an event. It is a valuable complement to digital signing practices, enabling organisations to record when a digital item, such as a message, document, transaction, or piece of software, was signed. With an audit trail that is automatically timestamped, it is simple to trace.</li> </ul>
<b>(e) Legally binding</b>	<ul style="list-style-type: none"> <li>▪ A document signed with a digital signature is as legally binding as a document signed with a handwritten signature, an affixed thump-print,</li> </ul>

	or any other mark. It has a higher degree of evidential value.
<b>(f) Convenience</b>	<ul style="list-style-type: none"> <li>▪ The inevitable tedium of moving paperwork is one of the most inconvenient aspects of pen and paper signatures or, worse, paperwork getting lost. Digital signatures simplify the process. You can sign a document electronically, no matter where you are. All you need is an internet connection and access to a computer, laptop, or mobile device. For many businesses, this level of efficiency is hugely valuable because there is no need to wait on paperwork when closing a deal. You can complete the execution of time-sensitive documents on the spot; without asking customers to engage in extensive paper processes that risk slowing down transactions, reducing efficiency rates, or even losing a sale.</li> </ul>

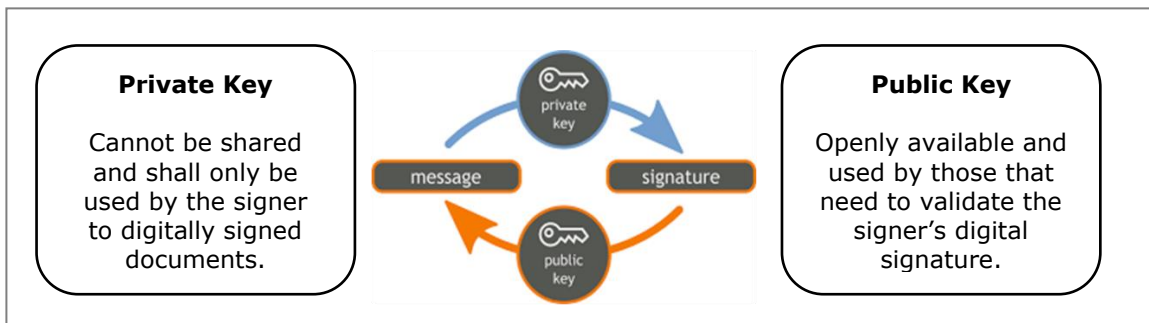
## 7. How secure is a digital signature?

<b>(a) Virtually impossible to forge</b>	Digital signatures are validated or verified by the digital certificate. A person cannot digitally sign a document without the signer's private key. Hence, document forging would be impossible.
<b>(b) Entity verification</b>	For a digital certificate to be issued in connection with the use of digital signatures, an identity verification of the person applying for the digital certificate will need to be performed. Only after the verification process has been completed successfully will the digital certificate be issued.
<b>(c) No modification</b>	All documents signed will be encrypted upon signing, which will make it impossible for the document to be tampered with. Modification of the documents would invalidate the digital signature. Therefore, no modification is allowed on a digitally signed document, which is valid.
<b>(d) Trusted third party</b>	The digital signature is only valid when it is signed through the service and platform provided by a trusted third party, which are the licensed CAs.
<b>(e) Trustworthy system</b>	A licensed CA must satisfy the requirements of using a trustworthy system for the generation and management of key pairs and certificates in accordance with the DSA 1997 and the DSR 1998.

<b>(f) Compliance monitoring</b>	A licensed CA is required to comply with a set of requirements that are imposed and assessed yearly through an annual compliance audit conducted by a qualified auditor registered with MCMC. This must be in line with international standards for CA worldwide—WebTrust for CA Audit.
----------------------------------	---

## 8. How is a digital signature created?

Under the PKI protocol, a digital signature is formed using two lengthy numbers, known as keys, based on an asymmetric cryptosystem. The keys function as a pair of related keys, a public key, and a private key. The keys are connected to a unique digital identity, or digital certificate. The digital signature is created by encrypting the hash data using the sender's private key. The recipient then decrypts it and compares it to the attachment using the public key. Hashing is the concept of transforming a string of characters into another value for the purpose of security.
















## PART B: APPLYING FOR THE USAGE OF DIGITAL SIGNATURES

### INTRODUCTION

This part gives a general overview of how to apply for a digital certificate that can be used in digital signatures. Listed below are organisations licensed and recognised by MCMC in relation to the provisioning of CA, Repository & Date/Time Stamping services. For more information, please contact any of the licensed CAs listed in the following link: [List of Certification Authorities and Recognition](#).

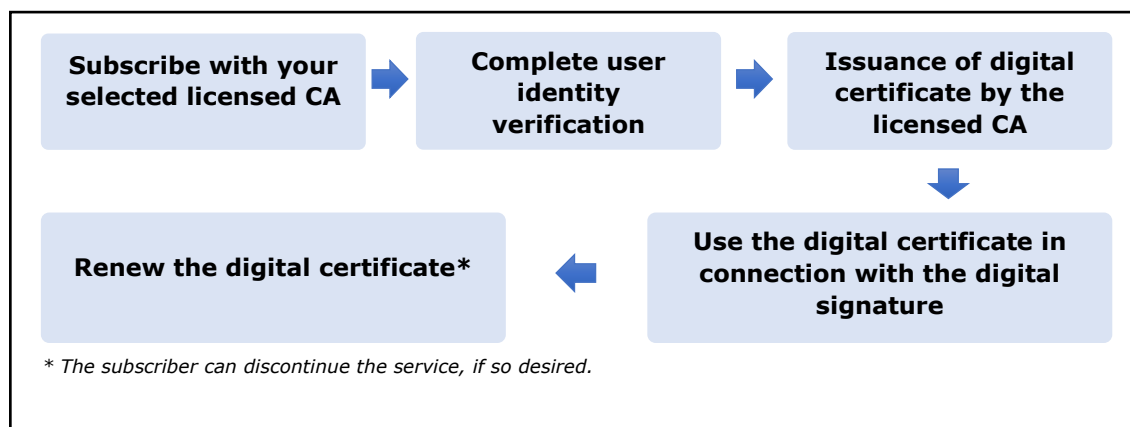
LICENSED CAs	RECOGNITION FOR REPOSITORY	RECOGNITION FOR DATE/ TIME STAMP (DTS) SERVICES
<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">    </div> <div style="text-align: center;">    </div> </div> <ul style="list-style-type: none"> <li>▪ Issuance of digital certificate to the subscriber (digital identity); and</li> <li>▪ Ensures use of a trustworthy system.</li> </ul>	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">    </div> <div style="text-align: center;">    </div> </div> <ul style="list-style-type: none"> <li>▪ A system for storing and retrieving certificates and other information relevant to digital signatures; and</li> <li>▪ A recognised repository shall:                             <ul style="list-style-type: none"> <li>• Maintain a publicly accessible database required under the Act</li> <li>• Publish the certification authority disclosure record.</li> </ul> </li> </ul>	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">    </div> <div style="text-align: center;">  </div> </div> <ul style="list-style-type: none"> <li>▪ If a time-stamp is required under any written law, a time-stamp by a recognised date/time stamp service is required;</li> <li>▪ Date and time at which the document is signed or executed; and</li> <li>▪ Admissible in evidence in all legal proceedings.</li> </ul>

### 1. How can I apply for a digital certificate to be used in digital signatures?

You can apply for a digital certificate to be used in digital signatures by registering as a subscriber to one of the MCMC’s licensed Certification Authorities (“CA”).

### 2. What is the general process for applying a digital certificate and using it in a digital signature?

The general process to apply for a digital certificate and use it in a digital signature is simplified as per the diagram below:



### 3. What is a licensed Certification Authority (CA)?

A CA is an organisation that acts to validate the identities of entities (such as websites, email addresses, companies, or individual persons) and bind them to cryptographic keys through the issuance of electronic documents known as digital certificates. Licensed CA means a CA to whom a licence has been issued by the MCMC and whose licence is in effect (valid).

### 4. What is the cost for using the digital signature?

As per the licence condition, the cost of the digital certificate is according to specific classes and is subject to approval by MCMC. In general, the fees levied are as shown below:

Services	Fees Levied
Class 1	Not more than RM50
Class 2	Not more than RM120
Class 3	Not more than RM3400

The final cost of using the digital signature may vary depending on your requirements, the type of class used, the type of services offered, as well as the hardware and software that may be involved.

### 5. What do the different classes of a digital certificate mean?

There are three (3) classes of digital certificates: Class 1, Class 2, and Class 3. Different risk levels, the effects of data compromise, and their purposes are reflected by the classes. The level of trust or security that it delivers increases with the value that the class number typically represents, with Class 1 being the lowest level and Class 3 being the highest level. You may contact any of the licensed CAs to learn more about which class will best suit your needs.

**PART C: APPLYING AS LICENSED CA, RECOGNISED REPOSITORY OR RECOGNISED DATE/TIME STAMP SERVICES**

**INTRODUCTION**

An overview of Malaysia's licensing and recognition procedures for the provision of CA, Repository and Date Time/Stamping services are provided in this section. Please contact the Numbering and Electronic Addressing Management Department at [neamd@mcmc.gov.my](mailto:neamd@mcmc.gov.my) for more information or clarification if your specific question is not addressed in this section of the FAQ.

For more information, you may refer to the [Licensing Guidebook - Digital Signature](#), which is available on MCMC's Official Website.

**1. What types of licence and recognitions are available under the DSA 1997 and the DSR 1998?**

CATEGORIES	TYPE	DEFINITION AS PER THE DSA 1997 AND THE DSR 1998
<b>Licence</b>	<b>Certification Authority</b>	i. CA means "a person who issues a certificate."
		ii. Licensed CA means "a CA to whom a licence has been issued by MCMC and whose licence is in effect."
<b>Certification of Recognition</b>	<b>Repository</b>	i. A system for storing and retrieving certificates and other information relevant to digital signatures.  ii. Recognised Repository means a repository recognised by the MCMC under section 68 of the DSA 1997.
	<b>Date/Time Stamp services</b>	i. Time-Stamp means to append or attach to a message, digital signature or certificate a digitally signed notation indicating at least the date, time and identity of the person appending or attaching the notation.  ii. Recognised Date/Time Stamp Services means a date/time stamp services recognised by MCMC under section 70 of the DSA 1997.

CATEGORIES	TYPE	DEFINITION AS PER THE DSA 1997 AND THE DSR 1998
	<b>Foreign Certification Authority</b>	A foreign CA will be recognised subject to the fulfilment of the requirements stipulated in the DSA 1997 and the DSR 1998 and in the event that an international treaty, agreement, or convention concerning the recognition of its certificates has been concluded to which Malaysia is a party.

**2. How can I apply to become a licensed CA, a recognised repository provider, or a recognised date/time stamp service provider?**

For more information, please refer to the [Licensing Guidebook - Digital Signature](#), which is available on the MCMC's official website. The guidebook sets the criteria as well as all relevant processes and procedures with regards to the application to become a licensed CA, recognised repository provider, or recognised date/time stamp service provider.

**3. A licensed CA may also become a recognised repository or a recognised date/time stamping service provider. When applying for both, should the application fees be paid separately?**

Even though multiple applications may be made simultaneously, each application will be identified and handled separately. A RM2,500.00 application fee is therefore required for each licence application and recognition that is requested.

**4. What are the relevant information and documents to be provided and submitted together with the application(s)?**

In general, the applicant must provide all relevant information and documents as specified in Form 1. This shall include, but is not be limited to, all the evidence of the company's establishment; audited financial information and reports; a list of manpower to demonstrate the capability of managing the operation; and, for the operational stage, a performance audit report to demonstrate assurance of the capability of operating using a trustworthy system. The applicant also must provide any other relevant information requested by MCMC.

**5. Can a company residing outside of Malaysia provide a recognised repository and a recognised date/time stamp service?**

No. In accordance with Regulations 48 and 61 of the DSR 1998, eligibility of a recognised repository and/or recognised date/time stamp services is that the entity must be a body corporate incorporated in Malaysia or a partnership within the meaning of the Partnership Act 1961 and maintains a registered office in Malaysia.

**6. How long will the licence or certification of recognition be valid for, and how long will it take to process the licence / recognition?**

The licence and recognition issued by MCMC shall be for a period not exceeding five (5) years, subject to MCMC's assessment based on the qualification requirements as per the DSA 1997 and the DSR 1998. A complete application will ordinarily be processed within sixty (60) days after the receipt of all information and documents asked for by MCMC. MCMC reserves the right to determine if an application is complete and if the information provided is sufficient for its purposes.

**7. Can a government agency apply to become a CA?**

No. A person who wants to carry on or operate as a CA must satisfy the requirements set forth in Regulation 6 of the DSR 1998, which include but are not limited to the following:

- a) It is a body corporate incorporated in Malaysia or a partnership within the meaning of the Partnership Act 1961; and
- b) It maintains a registered office in Malaysia.

**8. Is a licensed CA required to maintain a specific amount of working capital?**

A licensed CA must keep and maintain its working capital of at least Malaysian Ringgit Six Million (RM6, 000,000.00) at all times to enable it to carry on or operate as a CA and this is specified in the CA's licence condition. This is stipulated as a licence condition.

Working capital is the total amount of available capital invested in a company's operating cycle, and it is used by businesses to meet their daily operating expenses. The working capital can be derived by comparing the current assets with the current liabilities on the balance sheet.

## 9. What is the standard time used for the provision of date/time stamp services?

The standard time used for date/time-stamping is synchronised with Malaysian Standard Time (MST). It is 8 hours ahead of Coordinated Universal Time (UTC) which is managed by the official timekeeper of Malaysia, i.e.: National Metrology Laboratory (SIRIM). Further information can be obtained from the [Guidelines for Recognised Date/Time Stamp Services](#) which is available at the MCMC's official website.

## 10. Can a foreign entity be a shareholder in the company applying as a licensed CA?

Yes. However, pursuant to the licence condition of a licensed CA, a written approval from MCMC is required before a licensed CA is allowed to have foreign shareholding.

Definition of a foreign entity would be as follows:

**"foreigner"** means:-

- (a) a person who is not a Malaysian citizen; or
- (b) a company incorporated in Malaysia of which not less than 51% of the shares in the company are owned by a foreign person or a foreign company;

**"foreign company"** means-

- (a) a company, corporation, society, association or other body incorporated outside Malaysia; or
- (b) an unincorporated society, association or other body which under the law of its place of origin may sue or be sued, or hold property in the name of the secretary or other officer of the body or association duly appointed for that purpose and which does not have its head office or principal place of business in Malaysia.

## 11. Can a foreign entity apply as a licensed CA in Malaysia?

Yes. However, all the CA infrastructure must be physically established in Malaysia.

## **INTRODUCTION**

This part provides an overview of the procedures needed to recognise foreign CAs in Malaysia. Please contact the Numbering and Electronic Addressing Management Department at [neamd@mcmc.gov.my](mailto:neamd@mcmc.gov.my) for more information or clarification if your specific question is not addressed in this section of the FAQ.

For more information, you may refer to the [Licensing Guidebook - Digital Signature](#) which is available on MCMC's official website.

### **1. What are the requirements for recognition of foreign CA in Malaysia?**

The process for the recognition of a foreign CA shall be in accordance with the DSA 1997 and the DSR 1998, specifically with the PART X - Recognition of Foreign Certification Authorities of the DSR 1998.

Secondly, an international treaty, agreement, or convention concerning the recognition of its certificates must be shown to have been concluded to which Malaysia is a party. This entity then can be considered to enable recognition of a foreign CA. Please note that the decision to recognise a foreign CA in Malaysia vests solely with MCMC.

### **2. How to apply for recognition as a foreign CA in Malaysia?**

An application to be a recognised foreign CA shall be made in writing to MCMC. Please refer to regulations 72 of DSR 1998 and [Licensing Guidebook - Digital Signature](#) which are available on MCMC's official website, with regards to the application for the said recognition.

### **3. Does a digital signature that has been issued or created by foreign CA have the same effect and validity in Malaysia?**

A digital signature issued or created by a foreign CA or issued or created outside of Malaysia will not have the same effect and validity in Malaysia.

A digital signature issued or created by a foreign CA has the same effect and validity in Malaysia only if the foreign CA is a recognised foreign CA issued with recognition under DSR 1998 regulation 73.

## **OTHER REFERENCES**

1. Digital Signature Act 1997
2. Digital Signature Regulations 1998
3. Guidelines for Audit of Certification Authorities
4. Guidelines for Recognised Date/Time Stamp Services
5. Licensing Guidebook - Digital Signature
6. WebTrust Principles and Criteria for Certification Authorities
7. List of Certification Authorities and Recognition
8. <https://www.mcmc.gov.my/en/media/video-gallery/digital-signature-act-1997>