



MSC TRUSTGATE.COM SDN. BHD.

USER GUIDE

LHDN e-Invoice Organization Certificate

Version 1.5



MSC Trustgate.com Sdn. Bhd. (478231-x)

Suite 2-9, Level 2, Block 4801
CBD Perdana, Jalan Perdana
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia
Tel: +603 8318 1800
Fax: +603 8319 1800

Revision History

#	Date	Changes	Version
1	15 May 2024	First Version	1.0
2	11 June 2024	Add Section 7.1.3 Certificate Authority and Revocation Information	1.1
3	11 July 2024	Add: <ul style="list-style-type: none">1. Section 4.1 KeyStore Explorer2. Section 8 Updating Info in MyTrustID portal3. Section 9 Certificate Revocation	1.2
4	14 Aug 2024	<ul style="list-style-type: none">1. Replace the term 'Certificate Only' to 'Soft Certificate'2. Update:<ul style="list-style-type: none">i. Section 3.1 Required Information – Update link for LOAii. Section 4.1.2 Package & Pricing Page – Update type of certificate packagesiii. Section 4.1.3 Application Info page – Include Soft Certificate Optionsiv. Section 4.1.4 Disclaimer Page –Update the latest image of Subscriber Agreementv. Section 4.2.1 Roaming Certificate - Add email received by user for API Authentication token/ keyvi. Section 4.2.2 Soft Certificate – Update certificate activation according to the Soft Certificate Option3. Add Section 5.2.2.3 OpenSSL4. Add Appendices5. Add Section 7.3 Reissue Certificate	1.3
5.	23 May 2025	<ul style="list-style-type: none">1. Update:<ul style="list-style-type: none">i. Section 7.3 Reissue Certificate – Update certificate information to set and reset certificate PIN.	1.4

#	Date	Changes	Version
6	20 Aug 2025	1. Update: <ul style="list-style-type: none"> i. Section 4.1.2 Package & Pricing Page – Update certificate package for new & renew user. ii. Section 4.1.3 Application Info Page – Update additional supporting document which is consent letter to register LEI iii. Section 4 Purchasing Certificate – Update a reminder to user to renew the certificate one months before expiry date. 	1.5

Table of Contents

About This Guideline.....	6
1 Understanding Digital Certificates.....	7
1.1 What Are Digital Certificates?	7
1.2 Components of a Digital Certificate.....	7
1.3 Functions of Digital Certificates	7
1.4 Trust and Hierarchy	8
1.5 Conclusion.....	8
2 Types of Digital Certificates	9
3 Pre-requisites for Purchasing Digital Certificate	10
3.1 Required Information	10
3.2 Payment Method	10
4 Purchasing Certificate.....	11
4.1 Online Portal.....	11
4.1.1 Instructions Page	11
4.1.2 Package & Pricing Page	12
4.1.3 Application Info Page	13
4.1.4 Disclaimer Page.....	19
4.1.5 Payment Page	20
4.2 Activation.....	21
4.2.1 Roaming Certificate	21
4.2.2 Soft Certificate	24
5 Processing Time.....	27
6 Integration and Configuration.....	28
6.1.1 Roaming Certificate	28
6.1.2 Soft Certificate	28
6.1.3 Certificate Authority and Revocation Information	29
6.1.3.1 Root Certificate Authority (Root CA).....	29
6.1.3.2 Intermediate Certificate Authority (Intermediate CA)	30
6.1.3.3 Certificate Revocation List (CRL)	30
7 Update Info in MyTrustID portal	31
7.1 Login portal.....	31
7.2 Update CSR and the Supporting Documents.....	33
7.3 Reissue Certificate	38
8 Certificate Revocation.....	41
9 Support and Resources	42
10 Appendices.....	43
Appendix A: Generating Certificate Signing Request (CSR)	43
a) KeyStore Explorer.....	44
b) OpenSSL.....	56
c) Java Key Store (JKS).....	56

Appendix B: Import PEM file into Key Store	57
a) KeyStore Explorer.....	57
b) OpenSSL.....	60
c) Java Key Store (JKS).....	60
Appendix C: Export Key from Key Store to P12	61
a) KeyStore Explorer.....	61
b) OpenSSL.....	62
c) Java Key Store (JKS).....	63

About This Guideline

The User Guideline document aims to provide comprehensive guidance on the process of purchasing LHDN e-Invoice digital certificates from MSC Trustgate. Whether you're a new user seeking to acquire your first digital certificate or an existing user who is looking to renew your digital certificate, this guide has you covered.

In this guideline, you'll find detailed instructions on:

1. **Understanding Digital Certificates:** Gain insights into what digital certificates are, their importance, and how they function in securing online transactions and communications.
2. **Types of Digital Certificates:** Understand the various types of digital certificates offered by MSC Trustgate, including their features, use cases, and suitability for different applications.
3. **Prerequisites for Purchasing:** Learn about the prerequisites and requirements you need to fulfill before initiating the digital certificate purchase process.
4. **Purchasing Process:** Step-by-step instructions on how to request and purchase digital certificates from MSC Trustgate, including generating key pairs, submitting Certificate Signing Requests (CSRs), and completing the payment process.
5. **Processing Time:** Understand the expected processing time for your certificate request, including verification and validation procedures, as per MSC Trustgate's Certificate Practice Statement.
6. **Integration and Configuration:** Guidance on integrating and configuring MSC Trustgate's API with your e-Invoice software or system to obtain the XAdES digital signature structure. This guidance is applicable if you choose to purchase a Roaming Certificate.
7. **Support and Resources:** Access additional resources, FAQs, and contact information for MSC Trustgate's support team to assist you throughout the certificate purchasing process. Please note that this guideline does not include instructions on constructing XAdES digital signature structures for your e-Invoice documents or the related e-Invoice submission process. For further details, kindly refer to the LHDN website.

This User Guide aims to empower you with the knowledge and tools necessary to navigate the digital certificate purchasing process effectively. Should you have any questions or require further assistance, please don't hesitate to reach out to our support team.

All certificate issuance process is accordance with MSC Trustgate Certificate Practice Statement.

Let's get started on securing your e-Invoice with MSC Trustgate's LHDN e-Invoice Organization digital certificates!

1 Understanding Digital Certificates

Digital certificates play a crucial role to secure online communication, providing authentication, encryption, integrity and trust. Here's an overview of what digital certificates are and how they function:

1.1 What Are Digital Certificates?

A digital certificate, also known as a public key certificate, is a digital document issued by a trusted and qualified entity, or a licensed Certification Authority (CA). It serves as a form of identification, providing assurance of the authenticity and integrity of electronic documents, websites, and online communications.

1.2 Components of a Digital Certificate

1. **Public Key:** The key pair generated for cryptographic operations. The public key is embedded in the certificate and is used for encryption, digital signatures, and authentication.
2. **Private Key:** The corresponding key known only to the certificate owner, used for decrypting encrypted data, creating digital signatures, and proving ownership of the public key.
3. **Certificate Holder Information:** Details about the certificate holder or organization, such as name, email address, and organizational affiliation.
4. **Issuer Information:** Information about the Certification Authority (CA) that issued the certificate, including its name, digital signature, and validity period.
5. **Digital Signature:** A cryptographic signature created by the CA to verify the authenticity and integrity of the certificate. It ensures that the certificate has not been tampered with since it was issued.

1.3 Functions of Digital Certificates

1. **Authentication:** Digital certificates verify the identity of individuals, organizations, or websites in online interactions. They assure users that they are communicating with legitimate entities and not imposters.
2. **Digital Signatures:** Certificates enable the creation of digital signatures, which provide proof of the origin, identity, and integrity of electronic documents, transactions, and communications. Digital signatures validate the authenticity of the signer and ensure non-repudiation.

3. **Data Encryption:** Digital certificates facilitate secure communication by enabling encryption of data exchanged between parties. They ensure that sensitive information remains confidential and cannot be intercepted or tampered with by unauthorized parties.
4. **Non-repudiation or Content Commitment:** Digital certificates enable non-repudiation by associating digital signatures with the identity of the signer. When a user signs a document or message with their private key, the corresponding digital certificate verifies their identity. This provides strong evidence that the signer cannot later deny their involvement or the authenticity of the signed content.

1.4 Trust and Hierarchy

Digital certificates operate within a hierarchical trust model, where trust is established through a chain of trust anchored by trusted root CAs. Intermediate CAs issue certificates on behalf of the root CA, and end-entity certificates are issued to individuals, organizations, or devices.

1.5 Conclusion

In summary, digital certificates are essential tools for securing online transactions, communications, and data exchange. They provide authentication, encryption, and digital signature capabilities, ensuring the confidentiality, integrity, and authenticity of electronic information in today's digital world.

2 Types of Digital Certificates

There are 2 types of certificates or services for one (1) unit of Organization Certificate:

Certificate/Service Type	Annual Unit Price (RM)	Remarks
Soft Certificate	1,500	<ul style="list-style-type: none"> It is the organization or service provider's responsibility to securely manage its private key. The organization or service provider is accountable for conducting digital signing in accordance with the XAdES standard for e-Invoices. There is no integration with MSC Trustgate
Roaming Digital Certificate	15,000	<ul style="list-style-type: none"> MSC Trustgate securely manages the organization's private key in a Hardware Security Module (HSM). MSC Trustgate offers digital signature services adhering to the XAdES standard for e-Invoices, aiming to streamline processes and save resources for the organization or service provider. Integration with MSC Trustgate is facilitated via REST API for digital signing services.

3 Pre-requisites for Purchasing Digital Certificate

3.1 Required Information

Before you apply for a digital certificate, please make sure if you have the following detail ready:

1. Applicant's government issued photo-ID such as MyKad for Malaysian or passport for non-Malaysian and the applicant's contact information (such as phone and address).
2. Letter of Authorization – a letter signed by Director(s) of the Company under the Company's Letterhead to authorize a person to apply digital certificate for your organization, including the information of your company. (<https://www.msctrustgate.com/mytrustid/LOA>).
3. Certificate Signing Request (CSR) file in PKCS#10 format (for purchasing Soft Certificate). Refer to [Appendices A](#) for instructions on generating a CSR.

3.2 Payment Method

Payment can be made via online portal (FPX or Credit Card) or bank transfer to:

Bank: **CIMB Bank**

Account No: **8003227066**

Account Name: **MSC Trustgate.com Sdn Bhd**

4 Purchasing Certificate

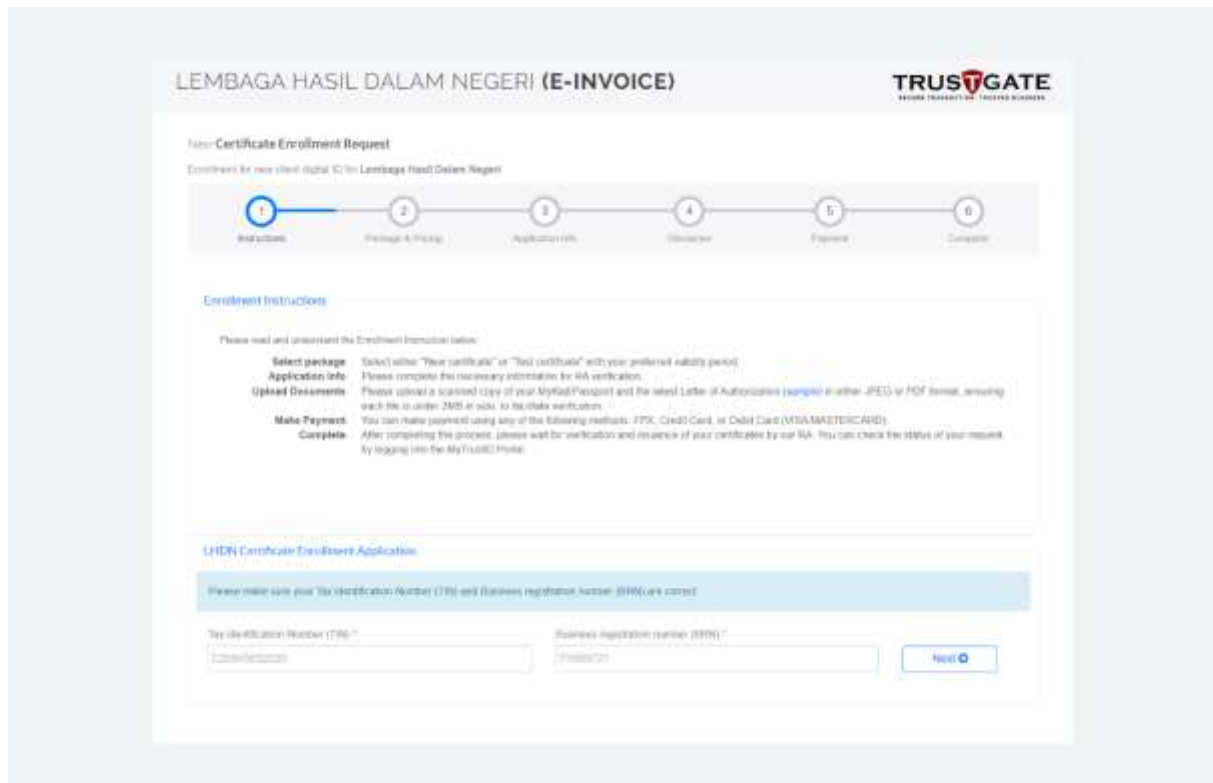
To expedite the certificate request process, we recommend purchasing the LHDN e-Invoice Organization Certificate through our online portal.

Customers are reminded to renew at least one month before the expiry date to ensure the remaining validity period is preserved.

4.1 Online Portal

4.1.1 Instructions Page


1. **Open Online Portal.** Click on the following link to start the registration process:
<https://www.msctrustgate.com/mytrustid/enrollment?q=lhdn>
2. **Read Enrollment Instructions.** Before proceeding, read and understand the Enrollment Instructions provided.
3. **Letter of Authorization.** If you are unsure about the Letter of Authorization, click the [Sample] button to view a sample in the Enrollment Instructions section. Note that the Letter of Authorization must be uploaded in the Application Info page.
4. **Enter Organization Identification.** To proceed with the LHDN Certificate Enrollment Application, enter your organization's Tax Identification Number (TIN) and Business Registration Number (BRN) in the respective fields.
5. **Verify Information.** Make sure the TIN and BRN numbers are CORRECT.
6. **Proceed to Next Step.** Click the 'Next' button to continue.



4.1.2 Package & Pricing Page

1. In the Package & Pricing page, there are two sections.
2. The first section is for selecting the Package that you want to purchase. The available package will vary depending on user type.
3. For new user, six package options are available which is New User - Soft Certificate (1 year validity), New User - Soft Certificate (1 year validity + LEI), New User - Soft Certificate (2 years validity), New User - Soft Certificate (2 years validity + LEI), New User - Roaming Certificate (1 year validity) and New User - Roaming Certificate (1 year validity + LEI). You can choose one of the listed packages.
4. For renew user, there are six types of packages which is Renew User - Soft Certificate (1 year validity), Renew User - Soft Certificate (1 year validity + LEI), Renew User - Soft Certificate (2 years validity), Renew User - Soft Certificate (2 years validity + LEI), Renew User - Roaming Certificate (1 year validity) and Renew User - Roaming Certificate (1 year validity + LEI). You can choose one of the listed packages.
5. The second section is Pricing & Description, which is automatically filled based on the chosen package.
6. Next, click the 'Next' button to proceed.
7. Alternatively, you can click the 'Back' button to return to the previous page.

LEMBAGA HASIL DALAM NEGERI (E-INVOICE)



New Certificate Enrollment Request

Enrollment for new client digital ID for Lembaga Hasil Dalam Negeri

1
Instructions

2
Package & Pricing

3
Application Info

4
Subscriber Agreement & Disclaimer

5
Payment

6
Complete

Package

A Legal Entity Identifier (LEI) is a global ID that uniquely identifies your company in financial and cross-border transactions.

Package *

Select Package

Select Package

New User - Soft Certificate - 1 year - MYR1500.00

New User - Soft Certificate + LEI - 1 year - MYR1700.00

New User - Soft Certificate - 2 years - MYR3000.00

New User - Soft Certificate + LEI - 2 years - MYR3400.00

New User - Roaming Certificate - 1 year - MYR15000.00

New User - Roaming Certificate + LEI - 1 year - MYR16200.00

Pricing & Description

Description

Description

Validity (Days)

Validity

Subtotal (RM)

Subtotal

Tax (SST 8%)

Tax

Total Amount (MYR)

Total Amount

Back

Next

Type of Package for new user

4.1.3 Application Info Page


1. There are four sections that you are required to fill in:
 - a. Applicant Information
 - b. Company Information
 - c. Personnel Information
 - d. Supporting Documents

Additionally, there is an CSR Information section if you choose to purchase a Soft Certificate.

2. Under the Application Information section, you need to provide the following information:
 - Nationality
 - MyKad No (Malaysian Identification Card Number)
 - Email
 - Full Name
 - Mobile No

3. Under the Company Information section, you need to provide the following information:
 - Organization ID
 - Registration No
 - Company Name
 - Company Address
 - Postcode
 - City
 - State
 - Country (select from drop-down menu)
4. In the Personnel Information section, you need to provide the following information:
 - Designation
 - Office Phone No
 - Fax No
5. In the Supporting Documents section, you are required to upload:
 - Image of your MyKad/Passport
 - Company's Letter of Authorization signed by your company's director or owner indicating that you are authorized to request the digital certificate on behalf of the company.
 - SSM Corporate Information.
 - **Additional supporting documents:** The Vetting Team will request a Consent Letter for LEI registration. This requirement only applies if the user selects a package that includes LEI.

LEMBAGA HASIL DALAM NEGERI (E-INVOICE)



New Certificate Enrollment Request

Enrollment for new client digital ID for Lembaga Hasil Dalam Negeri

1
Instructions

2
Package & Pricing

3
Application Info

4
Subscriber Agreement & Disclaimer

5
Payment

6
Complete

Applicant Information

Nationality *

MyKad No *

Email *

Full Name *

Mobile No *

Company Information

Tax Identification Number (TIN) *

Business registration number (BRN) *

Company Name *

Company Address *

Postcode *

City *

State *

Country *

Personnel Information

Designation

Office Phone No

Fax No

E-Invoice Information

Business registration number (BRN)

Tax Identification Number (TIN) *

Email *

Supporting Documents

Please upload scanned copy of your MyKad/Passport and Letter of Authorization that has been signed by director.

MyKad / Passport *

Letter of Authorization (Signing Authority) *

SSM Corporate Information *

Select a file

Select a file


Select a file

[Back](#)

[Next](#)

New Certificate (Roaming Certificate)

6. If you are purchasing a Soft Certificate, an additional section called Soft Certificate Options will appear. You can choose from two options:
 - i. PKCS#12 format (P12) – Create a CSR directly through the portal by filling out the required fields in the CSR Information section.

LEMBAGA HASIL DALAM NEGERI (E-INVOICE)


New Certificate Enrollment Request

Enrollment for new client digital ID for Lembaga Hasil Dalam Negeri

1 Instructions
2 Package & Pricing
3 Application Info
4 Subscriber Agreement & Disclaimer
5 Payment
6 Complete

Soft Certificate Options

Soft Certificate Options *

Select Soft Certificate Option

Select Soft Certificate Option

PKCS#12 format (P12)

PEM format (Require to upload your own CSR)

Malaysian

MyKad No *

Example: 889201040201

Email *

Email

Full Name *

Full Name

Mobile No *

Mobile No

Company Name *

Company Name

Company Address *

Address

Postcode *

Postcode

City *

City

State *

State

Country *

Select Country

Personnel Information

Designation

Example: CEO

Office Phone No

Office No

Fax No

Fax No

E-Invoice Information

Business registration number (BRN)

Business registration number (BR)

Tax Identification Number (TIN)*

Tax Identification Number (TIN)

Email *

Email

Supporting Documents

Please upload scanned copy of your MyKad/Passport and Letter of Authorization that has been signed by director.

MyKad / Passport *

Letter of Authorization (Signing Authority) *

SSM Corporate Information *

Select a file

Select a file

Select a file

Back
Next

New Certificate (Soft Certificate)

LEMBAGA HASIL DALAM NEGERI (E-INVOICE)

New Certificate Enrollment Request

Guidance for new client digital ID for Lembaga Hasil Dalam Negeri

1
Instructions

2
Package & Pricing

3
Application Info

4
Subscriber Agreement & Declaration

5
Payment

6
Complete

Soft Certificate Options

Soft Certificate Options *

PKCS#12 format (P12)

CSR Details

Common Name (CN) The company or organization name * <input style="width: 95%;" type="text" value="Example: MSC TRUSTGATE SDN BHD"/>	Serial Number (SN) The Business Registration Number (BRN) * <input style="width: 95%;" type="text" value="109401014945"/>
Organization Name (O) The company or organization name * <input style="width: 95%;" type="text" value="Example: MSC TRUSTGATE SDN BHD"/>	Organization Identifier (ORG_ID) The Tax Identification Number (TRN) * <input style="width: 95%;" type="text" value="C088122/000"/>
Country (C) The country of the organization - 3-letter ISO code * <input style="width: 95%;" type="text" value="Select Country"/>	

Applicant Information

Nationality *

MyKad No *

Email *

Full Name *

Mobile No *

Company Information

Tax Identification Number (TRN) *

Business registration number (BRN) *

Company Name *

Company Address *

Postcode *

City *

State *

Country *

Personal Information

Designation *

Office Phone No *

Fax No *

e-Invoice Information

Business registration number (BRN) *

Tax Identification Number (TRN) *


Email *

Supporting Documents

Please upload scanned copy of your MyKad/Passport and Letter of Authorization that has been signed by director.

MyKad / Passport *	<input type="button" value="Select a file"/>
Letter of Authorization (Signing Authority) *	<input type="button" value="Select a file"/>
SOM Corporate Information *	<input type="button" value="Select a file"/>

New Certificate (Soft Certificate) (PKCS#12 format)

- 

LEMBAGA HASIL DALAM NEGERI (E-INVOICE)

New Certificate Enrollment Request

Enrollment for new client digital ID for Lembaga Hasil Dalam Negeri

- Initiation
 - Packages & Pricing
 - Application Info**
 - Subscription Agreement & Disclosure
 - Payment
 - Complete

Self-Certificate Options

Self-Certificate Options *

(PKM format (Require to upload your own CSR))

CSR Data:

Please CSR information here.

Your CSR should start with ---BEGIN NEW CERTIFICATE REQUEST--- and end with ---END NEW CERTIFICATE REQUEST---

CSR Information

Applicant Information

Nationality *

Malaysian

MyKad No. *

Example: 888811040201

Email *

Email

Full Name *

Full Name

Mobile No. *

Mobile No.

Company Information

Tax Identification Number (TIN) *

CN001227000

Business registration number (BRN) *

199401014945

Company Name *

Company Name

Company Address *

Address

Postcode *

City *

State *

Country *

Personal Information

Designation *

Example: CEO

Office Phone No.

Office No.

Fax No.

Fax No.

E-Invoice Information

Business registration number (BRN) *

Business registration number (BRN)

Tax Identification Number (TIN) *

Tax Identification Number (TIN)

Email *

Email

Supporting Documents

Please upload scanned copy of your MyKad Passport and Letter of Authorization that has been signed by Director.

MyKad / Passport *

Letter of Authorization (Signing Authority) *

SBM Corporate Information *

Select a file

Select a file

Select a file

Back
Next

18 | Page

4.1.4 Disclaimer Page

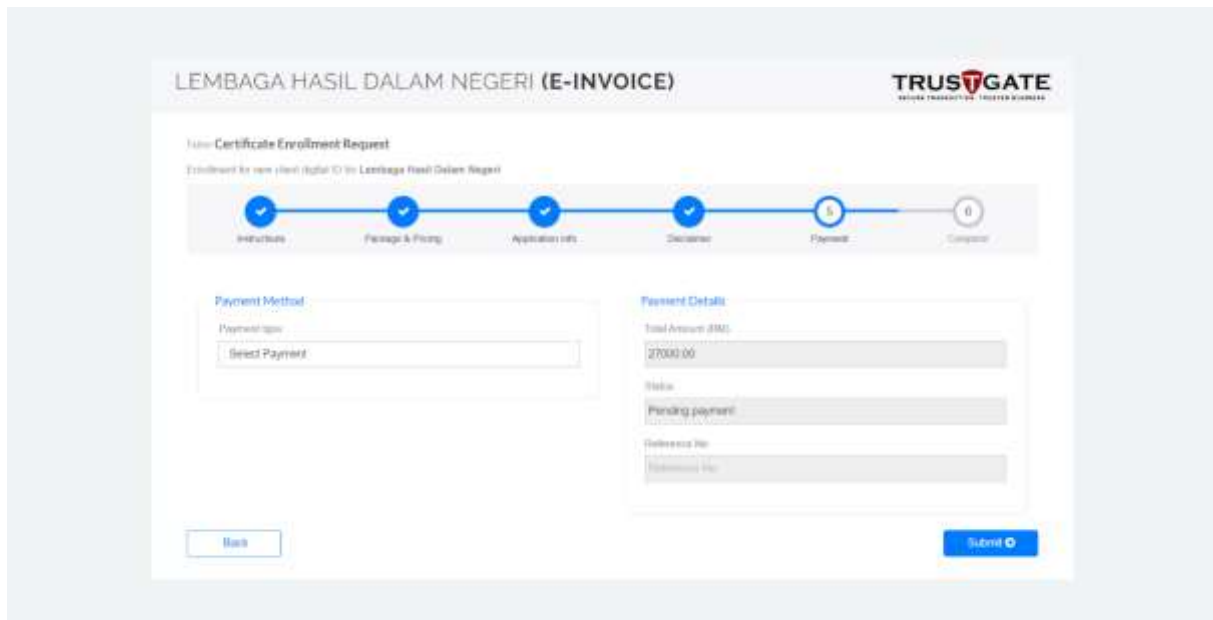
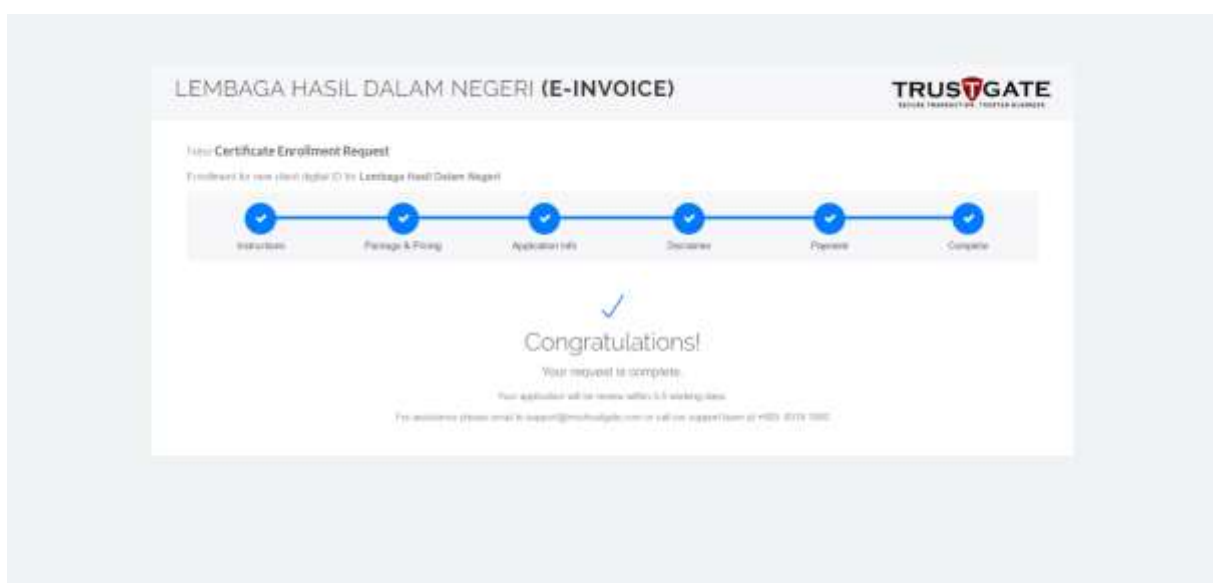
1. On the Disclaimer page, you can read the Subscriber Agreement.
2. After reading the agreement, tick the box provided to agree and confirm that all the information provided is true and accurate, and that you agree with the Subscriber Agreement.
3. To proceed, click 'Save and proceed' button.

[illegible]

Subscriber Agreement

4.1.5 Payment Page

1. There are three payment options listed under the Payment Method section:
 - FPX – Click the ‘Pay Now’ button, and the page will redirect to Merchant’s Portal
 - Credit/ Debit Card – Click the ‘Pay Now’ button, then the page will redirect to Internet Payment Gateway. This page requires user to enter credit card details to proceed.
 - Others (Bank Transfer) – Click the ‘Upload Proof of Payment’ button to upload the payment receipt (For the amount exceeding RM10,000).
2. You can confirm the amount you need to pay under the Payment Details section.
3. Click the ‘Submit’ button to make payment.

MSC Trustgate takes up to 5 working days to process your application.

1. After your request has been verified and validated, MSC Trustgate will email you to indicate that your request for the LHDN e-Invoice Organization Certificate has been approved and is ready to activate. This notification will be sent to the email address you provided during the registration process.
2. You should set your Certificate PIN using the link provided via email.



3. Enter your new PIN and reenter it for confirmation, then click the 'Submit' button to proceed.
4. Once you have completed the set Certificate PIN process, your certificate will be successfully activated and ready to use for submitting e-Invoices.

TRUSTGATE
RECEIPT MANAGEMENT SYSTEM
MyTrust ID

Setting Digital Certificate Activation

Please ensure your details are correct before setting your PIN.
Your PIN should at least contain 8 characters. You should always remember this PIN as you will be required to enter during any digital signature process.

Please enter your PIN:

[Customer Support & Contact](#)
© 2024 MAC Trusmi. All rights reserved.

Set Certificate PIN process

TRUSTGATE
RECEIPT MANAGEMENT SYSTEM
MyTrust ID

Setting Digital Certificate Activation

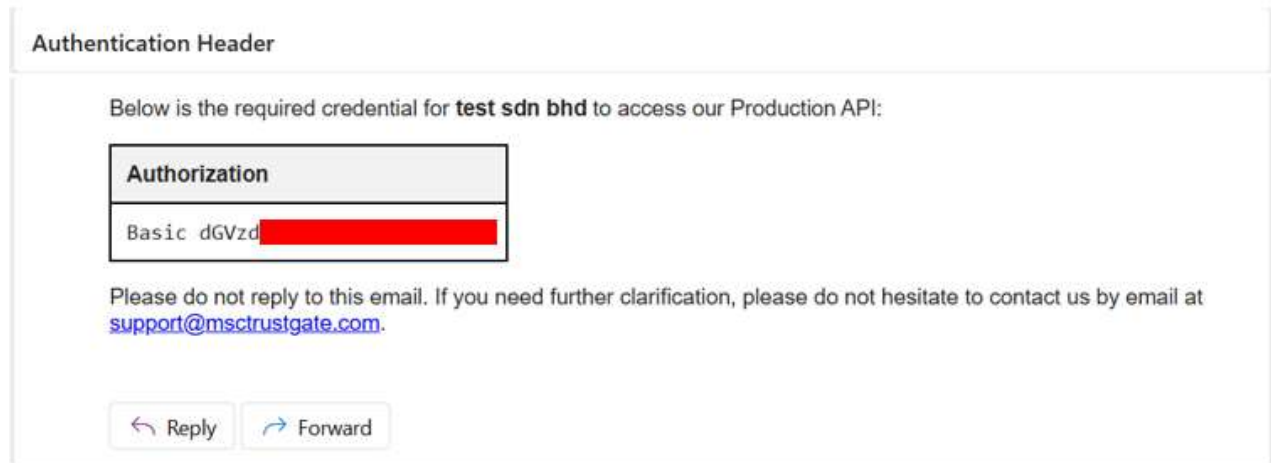
Please ensure your details are correct before setting your PIN.
Your PIN should at least contain 8 characters. You should always remember this PIN as you will be required to enter during any digital signature process.

Your certificate has been successfully activated. You may now proceed with digital signing activity.

[Customer Support & Contact](#)
© 2024 MAC Trusmi. All rights reserved.

Certificate successfully activated

5. At the same time, you will receive an email with API Authentication token/ key for integration purpose.
6. If you haven't received the API Authentication token/ key yet, feel free to reach out via email to support@msctrustgate.com for assistance.

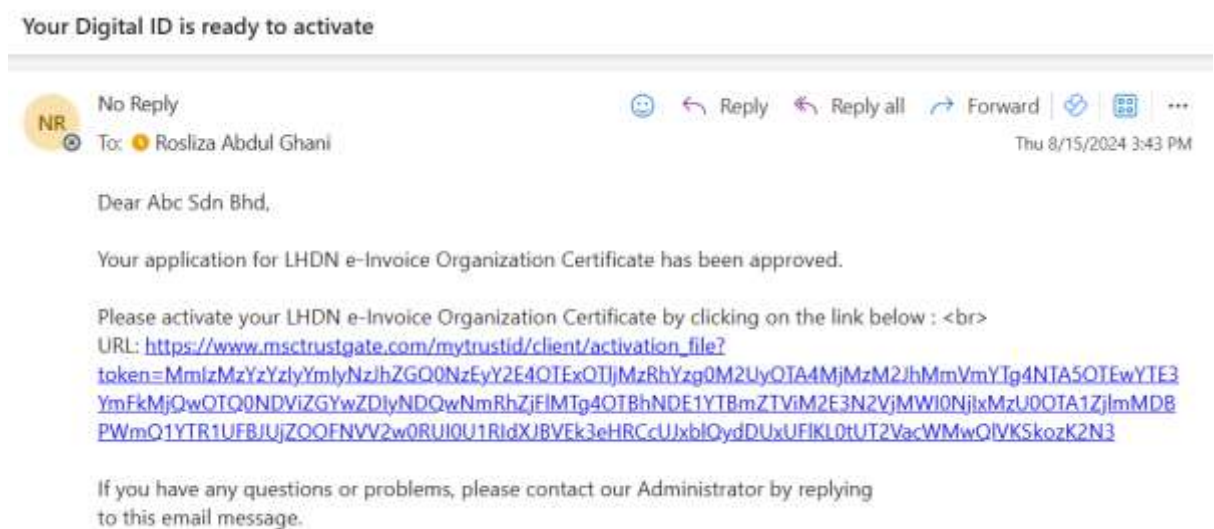


Email received by user with API authentication token/ key

4.2.2 Soft Certificate

After your request has been verified, validated, and approved, MSC Trustgate will email to you ¹ based on the Soft Certificate options you selected during purchasing in Step 6 in [Section 4.1.3](#).


- i. If you choose PKCS#12 format (P12) option:
 1. MSC Trustgate will email you to indicate that your request for the LHDN e-Invoice Organization Certificate has been approved and is ready to activate.
 2. You should set your PIN to download a P12 file using the link provided via email.



Email received by user

¹ This notification will be sent to the email address you provided during the registration process.

3. Enter your new PIN and reenter it for confirmation, then click the 'Submit' button to proceed.



MyTrust ID

Soft Certificate Activation

Please ensure your details are correct before setting your PIN. Your PIN should at least contain 8 characters. You should always remember this PIN as you will be required to enter during any digital signature process.

≡
Abc Sdn Bhd

👤
C1853629080

📠
478231X

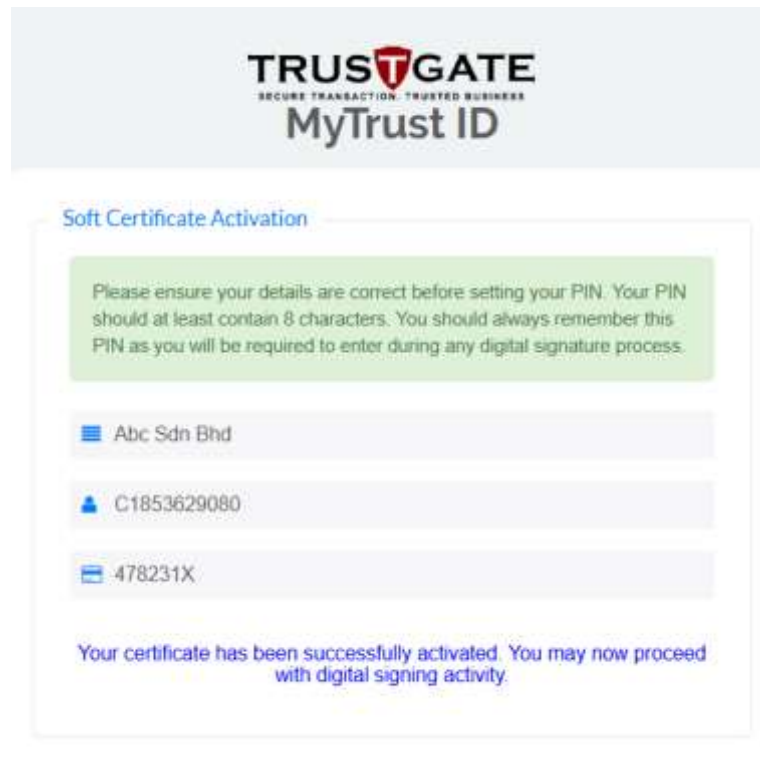
Please enter your PIN.

🔒

🔒

Submit ➔

Set PIN process



TRUSTGATE
SECURE TRANSACTION. TRUSTED BUSINESS
MyTrust ID

Soft Certificate Activation

Please ensure your details are correct before setting your PIN. Your PIN should at least contain 8 characters. You should always remember this PIN as you will be required to enter during any digital signature process.

Abc Sdn Bhd

C1853629080

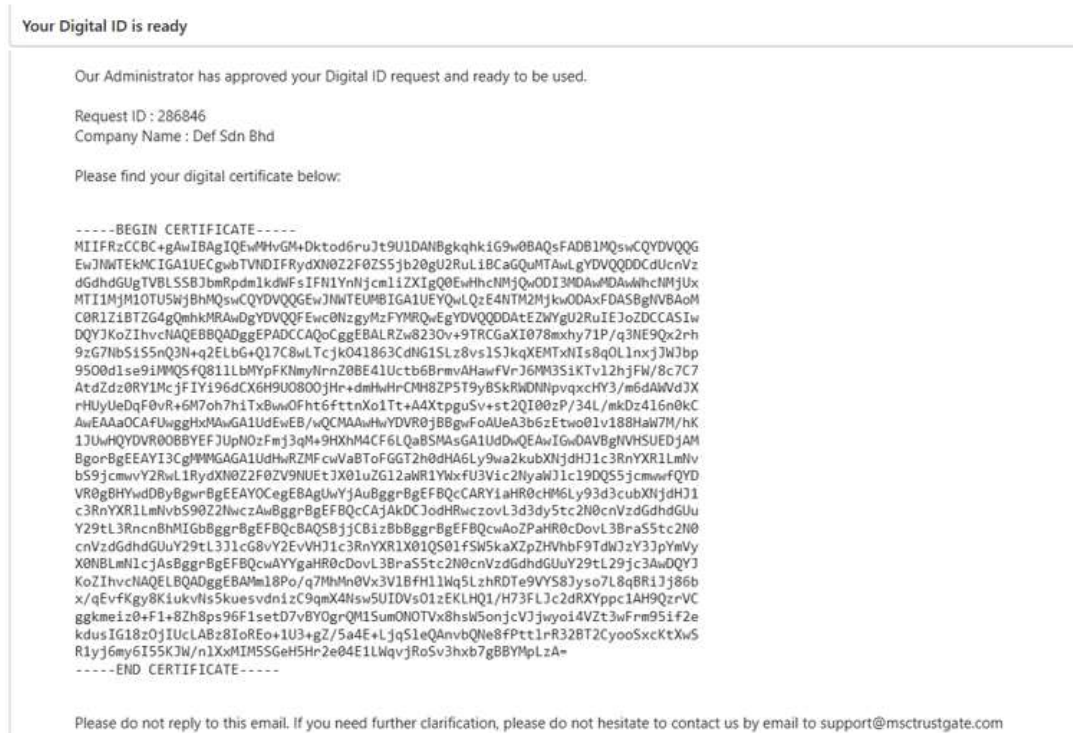
478231X

Your certificate has been successfully activated. You may now proceed with digital signing activity.

Soft Certificate Successfully Activated

4. Once you have completed set PIN process, your P12 file will auto download.
5. Please check your **Download** folder to view the file.
6. You can save and use the P12 file for eInvoice purpose.

- ii. If you choose PEM format option (which requires uploading your own CSR), you will receive your certificate via email. You are then required to install or store the certificate according to the requirements of your software or system for e-Invoice.



Digital Certificate received by the user via email

5 Processing Time

All Certificate Requests will be processed up to 5 working days, inclusive of verification and validation procedures, in accordance with MSC Trustgate Certificate Practice Statement. The duration of the process may also be influenced by the completeness of information provided, as outlined in the pre-requisite section.

6 Integration and Configuration

6.1.1 Roaming Certificate

If you purchase a Roaming Certificate, MSC Trustgate will create, manage, and store your private key in a Hardware Security Module (HSM) to ensure a high level of security for your key. MSC Trustgate will also assist you in creating the digital signature in accordance with the XAdES standard as outlined by LHDN.

You only need to prepare your e-Invoice document in XML or JSON format and pass it to MSC Trustgate through an API. The API will return a signed e-Invoice using your LHDN e-Invoice Organization Certificate, ready to be submitted to LHDN.

For more detailed information, please refer to the [eInvoice TGAPI RoamingCertificate](#) document.

6.1.2 Soft Certificate

There is no integration if you purchase the Soft Certificate. You are responsible for creating, managing, and storing your private key, as well as creating the digital signature in the XAdES standard as outlined by LHDN.

6.1.3 Certificate Authority and Revocation Information

6.1.3.1 Root Certificate Authority (Root CA)

The Root CA is the top-most authority in the hierarchy of digital certificates. It's crucial as it forms the trust anchor for all certificates issued beneath it.

You may download the Root CA certificate here:

https://www.msctrustgate.com/cacerts/Trustgate_MPKI_RCA.cer

or copy the following text:

```
-----BEGIN CERTIFICATE-----
MIIEEdTCCAt2gAwIBAgIRAJp+0x06bXlZ/ThA7DowhaAwDQYJKoZIhvcNAQEMBQAw
VDELMakGA1UEBhMCTVxJDAiBgNVBAoMG01TQyBUcnVzdGdhGUuY29tIFNkbi4g
QmhkLjEfmB0GA1UEAwVWVHJ1c3RnYXR1IE1QS0kgUm9vdCBDQTAeFw0yMDYw
MDAwMDBaFw00NzA0MDQyMzU5MDBaMFQxZCZAJBgNVBAYTAk1ZMSQwIgYDVQQK
BtN U0MgVHJ1c3RnYXR1LmNvbSBtZG4uIEJoZC4xHzAdBgNVBAMMF1RydXN0Z2F0ZSBN
UETJIFJvb3QgQ0EwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQD
GKv/GY0UiBRUghsTHuUfGzDVwlJuMqO9bcspES00411YA7U7ZDbSVVfAYADtUk
jXjX5Jt vavNC6Rq/7uuyIVKkoq9a94eFS5owybiYZTdUJhDLh58JJXdQQfLr
QGzqPjG4s3CX9qsqSr7c9Ii3aW0mVE/AxpDKoD7fTFEeUAFqL2jkLeeuemCTsk
xQQbbqQ2ZW/bv rBX0wxVGbo/Is8LorESUo6RAkHM9PeUGrSj7gtfFNhWgnbkCJ
137pQQNRmLflQdX NOGKuYVFWLeeDf+GFb9uhHQYneGusaehyAKN6vz2nztpCcA
18M/DZBo1zSiMyeyC N61hOcnIU5l6soA9RbIR8W3uOg5KkIyP1h81nayke1Qym
02Ty1FxmQ9RfaLCXY5i L6Rm81sxlPq7liUaLFKSra/VsU/gX9ZCvmDX0Y6AJJ/
3V1vTDG2nDtHsMc2wCQ6d AoaExtIjYUYnORC3TMzb9ED8opxpiGsTJdn4T/4cK
6ZHUwiumoUGMyw0RrcCAwEA AaNcMEAwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ
4EFgQUeyOa9NQoUEHGqSVQoc2r ryE6fzgwDgYDVR0PAQH/BAQDAgEGMA0GCS
qGSIb3DQEBAUAA4IBgQCQF2KMdQmW CKKmuihO0EGfNrBVP+vQOjMOg98Utge
XnuOS40jfdj+dCiBP7ayMqQYKBuj0aYFr Gb4IsyXIKBaDMJBkqKo3QLUjsDV
6BBOEeplqN0DeAouLSq/rc62gH1IvelwpQCPE WxBqO5baSiew6p2sErkbwJWqz
/XiFm2j/CjNbhJAfI9zDLIEUP5k2pRw+lBSRgPX /k4hQBK1+3SGxEqL3PJgp
5LFaWugSzJCcVXr6KQXnlbtQLM65Tz8SnpUmnfQEgN Fp1RJ4YT79ijdtRWUuZD
2rMxgW4DwWDbAboA8W2jRM580ltMoc0kYAc7zF80Q+Z8 jqfKV5an5+GdDwtslyr
Bk0o0oXBoXQqdLEhdqtGxKBC7PfwkMVh7/4Idk68cQIzL LGlK/t/tON8yZJsGB
EDyWanRRs+kPTxzFSw4bY7jupVwuJ7Q46J65y/CR9pOkJLq KmCgat4f/e22h3ub
8py+u5Yvm2Oq2z1YBs+chYcJmbWyoT+lxTjG82o=
-----END CERTIFICATE-----
```

6.1.3.2 Intermediate Certificate Authority (Intermediate CA)

The Intermediate CA issues certificates to end entities or another intermediate CAs. It helps in creating a chain of trust from the Root CA to the end-user certificate.

You may download the Intermediate CA certificate here:

https://www.msctrustgate.com/cacerts/Trustgate_MPKI_IS_CA.cer

or copy the following text:

```
-----BEGIN CERTIFICATE-----
MIIFZDCCA8ygAwIBAgIRAIAG32snP1g2np7ZEez+0O4wDQYJKoZIhvcNAQEMBQAw
VDELMakGA1UEBhMCTVxJDAiBgNVBAoMG01TQyBUcnVzdGdhGDUuY29tIFNkbi4g
QmhlLjEfmB0GA1UEAwVWVHJ1c3RnYXRlIElQS0kgUm9vdCBDQTAeFw0yMjA0MDcw
MDAwMDBaFw0zNzA0MDUyMzU5MDBaMGUCZAJBgNVBAYTAk1ZMSQwIgYDVQQKDBtN
U0MgVHJ1c3RnYXRlLmNvbSBtZG4uIEJoZC4xMDAuBgNVBAMMJ1RydXN0Z2F0ZSBN
UETtJIEluZG12aWR1YWwU3Vic2NyaWJlcjBDbDQTCASiwdQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBANta8491VimDL6pQfbB1K2wYnAePYXIXtA0Bp0ZEzv7BIJaD
7skW7habTKvfnjl1wkyxEPf6KTY1Y86TRBdKyyqvlMNRMAeq5OSPLk52bRkWCm
GK1DRodEANztvy575AJz3vubJP/WRhEKVCr4IYb072X8mluAtZTU7DYR0XPMzat
RZELbHij82YGB9fUjWdwM5K5pfDP+B19THxFwJzswZlbHmgT868cWPHLWMLD4jG
UssJh30SxMuCXArxdWG2wc5TLP46mCwAbRxI0yWMcnbaK6v/9ekrHkTBoBE5Ud+M
1RRRCaqbjMbqlc3SlQRLXpHEgQZ+ySdwpOPT69cCAwEAAaOACA4wgGgAMBIGAlUd
EwEB/wQIMAYBAf8CAQAwHwYDVR0jBBGwFoAUeyOa9NQoUEHGqSVQoc2rryE6fzgw
HQYDVR0OBByEFHgN2+sxLcKNJb9fPB2luzP4StSVMA4GA1UdDwEB/wQEAwIBBjAT
BgNVHSUEDDAKBggrBgEFBQcDAjBIBgNVHR8EQTA/MD2gO6A5hjdodHRwczovL3Br
aS5tc2N0cnVzdGdhGDUuY29tL2Nybc9jZHAvcvVwby90Z21wa2lyY2EuY3JSMHwG
A1UdIAR1MHMwcyYlKwYBBAGDgnoBAQIwYjAuBggrBgEFBQcCARYiaHR0cHM6Ly93
d3cubXNjdHJ1c3RnYXRlLmNvbS90Z2NwcZAwBggrBgEFBQcCAjAkDCJodHRwczov
L3d3dy5tc2N0cnVzdGdhGDUuY29tL3RncnBhMfCcGCCsGAQUFBwEBBEswSTBHBggr
BgEFBQcwAoY7aHR0cHM6Ly93d3cubXNjdHJ1c3RnYXRlLmNvbS9jYWNlcjRzL1Ry
dXN0Z2F0ZV9NUETtJX1JDQ55jZXIwDQYJKoZIhvcNAQEMBQADggGBAEYbYrOQVXIA
D+OegmIlpQpnyCrE6aH6ndNPgZw8wNgR8tVDgZt9q9q6AdIUdQzDHF2NqZG9T4oY
UhZLnG8dKALZOlcrQ2hrIqc8sr/AOPkfiOcbWNGLCCho6Q/FzLLUjcazTFs8l2dxe
QqLOfECZVfP8g75RdaMBvTPx7tzoen4xUkM1QDz57hTYwR/L2gEWN0vla7y8bYME
orZEDi+Jqkidh8kLIu+DsMBsISyWkbkLln41vSS97wuKuZ9Y3pIssctrrWPGrupU
qhc5GldiLAmuPM+yarmPSkndAokOrVleOwdj8t343FlGmNEj94DXxh8edYznEMPD
v0brMq5by9rBtu7KofJUpkYqu8T/+Qt5y/GO41Z5Hf7/H9IBXgIrycFfd07wVJHM
XbAxpLvczFrQoU7lUvE+Qo271bP17XiR61ZdAGBTwJm9yQGQyUBAx2+A5aGYQ0+
7WlKV7uiCf2LYs8Mv6rf8TpPzzo+JyTmLpX4Y8MfGpZ2LzWcXu62ww==
-----END CERTIFICATE-----
```

6.1.3.3 Certificate Revocation List (CRL)

The CRL contains a list of certificates that have been revoked by the CA before their expiration date and should no longer be trusted. It's important to configure systems to check the CRL to ensure revoked certificates are not used. The CRL is periodically updated by MSC Trustgate. Please configure your system to download the CRL at least once a day to ensure certificate revocation status is checked against the most recent list.

You may download the CRL here:

http://pki.msctrustgate.com/crl/cdp/Trustgate_MPKI_Individual_Subscriber_CA.crl

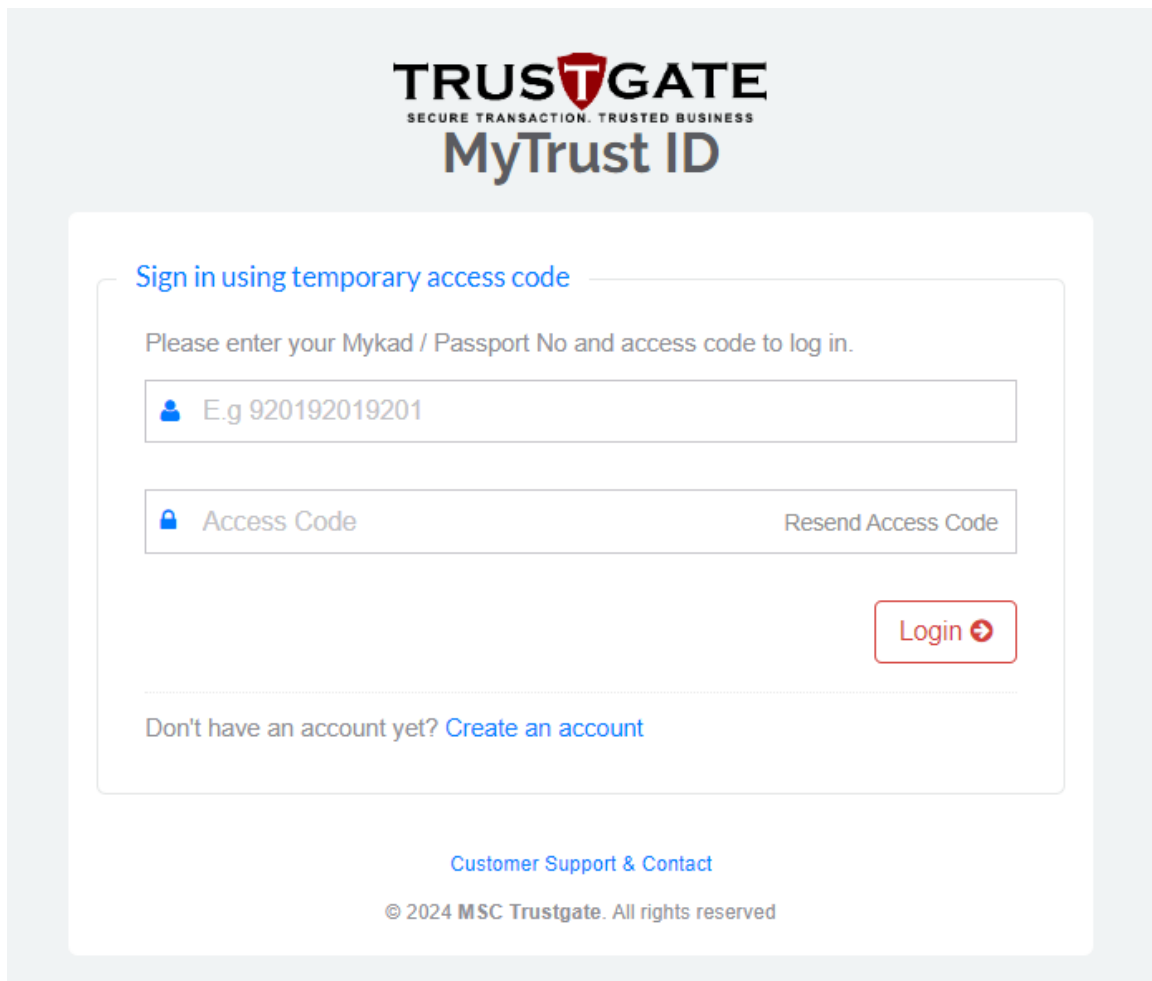
7 Update Info in MyTrustID portal

The MyTrustID portal is a self-service online platform for managing your certificates and certificate requests. Follow the steps below to update the Certificate Signing Request (CSR) and supporting documents.

Please note that this action can only be performed when the status is 'Submitted'.

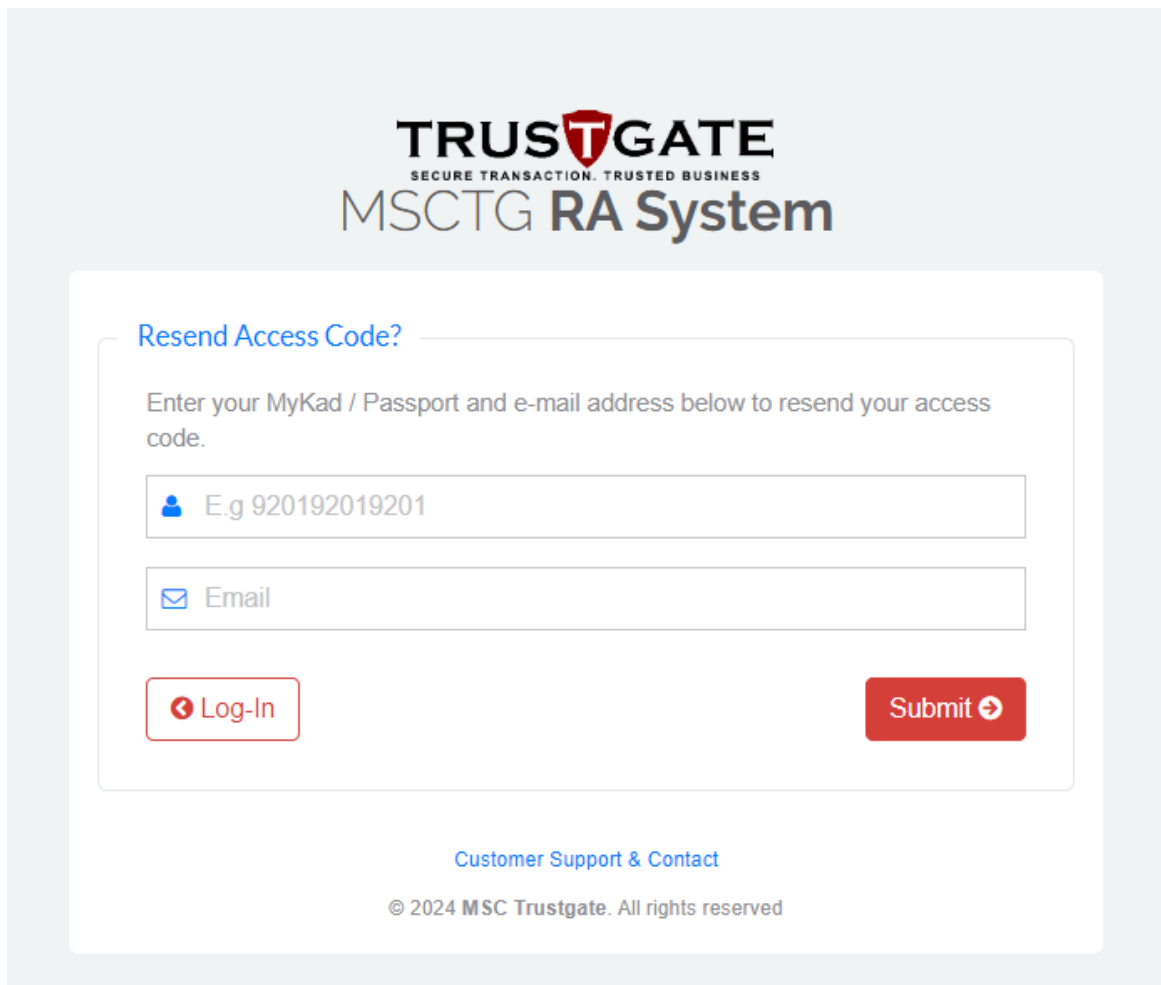
7.1 Login portal

1. **Click Link:** Click on the link below to update the info in MyTrustID portal:
<https://www.msctrustgate.com/mytrustid/client/login>
2. **Login portal:** Enter your Maykad/ Passport No and access code to login the portal.
3. **Forgot Access Code:** If you forgot the access code, you could click 'Resend Access Code' to request new access code.

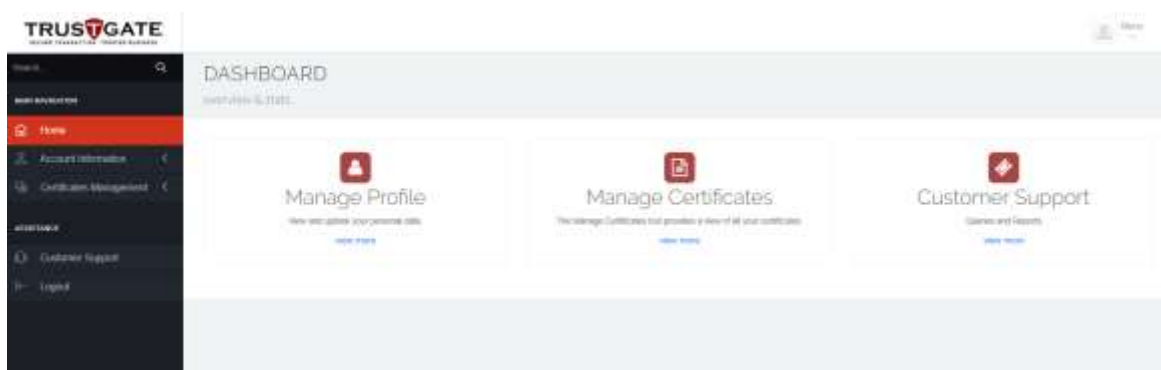


The screenshot shows the MyTrust ID login interface. At the top, the TRUSTGATE logo is displayed with the tagline 'SECURE TRANSACTION. TRUSTED BUSINESS' and 'MyTrust ID' below it. The main heading is 'Sign in using temporary access code'. Below this, a prompt asks the user to 'Please enter your Mykad / Passport No and access code to log in.' There are two input fields: the first is for the Mykad/Passport No, with a placeholder 'E.g 920192019201' and a user icon; the second is for the Access Code, with a lock icon and a 'Resend Access Code' link. A red 'Login' button with a right arrow is positioned to the right of the Access Code field. At the bottom of the login area, there is a link 'Don't have an account yet? Create an account'. Below the login area, there is a link 'Customer Support & Contact' and a copyright notice '© 2024 MSC Trustgate. All rights reserved'.

4. **Resend Access Code:** Enter Mykad/ Passport No and email address to receive new access code.

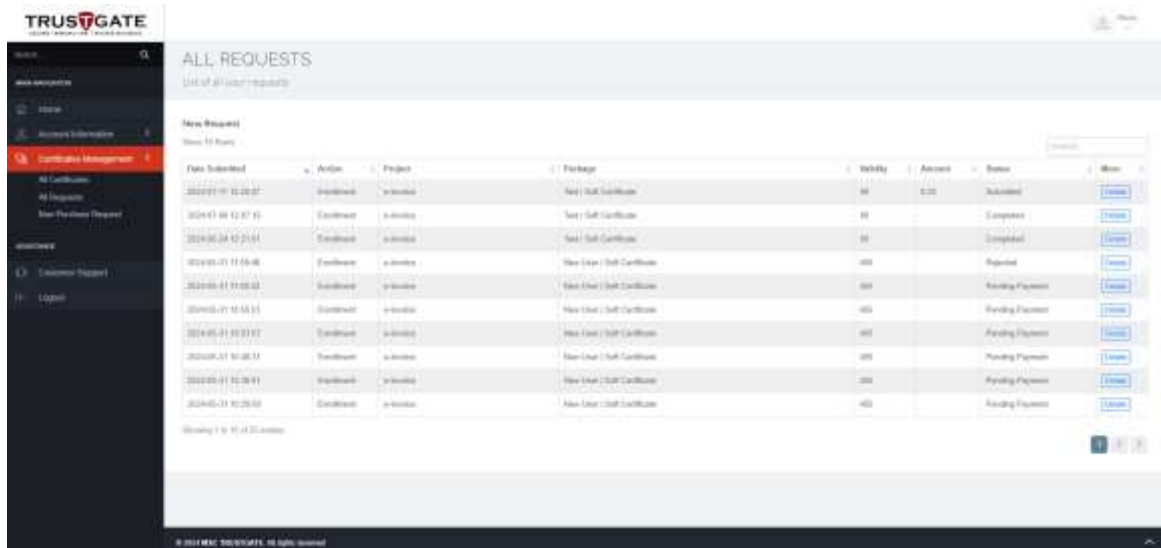


5. **View Dashboard:** After log in the portal, you will view the dashboard as in the picture below.



7.2 Update CSR and the Supporting Documents

1. **Update Info:** To update the supporting document or CSR information, click the 'Certificate Management' section on the left side bar. Then, choose 'All Requests'.
2. **All Requests:** In the 'All Requests' section, locate the certificate request you want to update. Click the 'Details' button for the specific certificate request you wish to update.



The screenshot shows the 'ALL REQUESTS' page in the TRUSTGATE system. The left sidebar contains navigation options: Home, Account Information, Certificate Management (selected), All Certificates, All Requests, New Pending Request, and Logout. The main content area displays a table of certificate requests with columns: Date Submitted, Action, Project, Package, Validity, Amount, Status, and More. The table lists 10 requests, with the first two being 'Completed' and the remaining eight being 'Pending Payment'. Each row has a 'Details' button for further action.

Date Submitted	Action	Project	Package	Validity	Amount	Status	More
2024-01-10 10:20:07	Completed	in-house	New Self-Certificate	90	0.00	Completed	Details
2024-01-10 12:57:15	Completed	in-house	New Self-Certificate	90		Completed	Details
2024-01-10 12:57:15	Completed	in-house	New Self-Certificate	90		Completed	Details
2024-01-11 05:46	Completed	in-house	New User Self-Certificate	90		Rejected	Details
2024-01-11 05:46	Completed	in-house	New User Self-Certificate	90		Pending Payment	Details
2024-01-11 05:46	Completed	in-house	New User Self-Certificate	90		Pending Payment	Details
2024-01-11 05:46	Completed	in-house	New User Self-Certificate	90		Pending Payment	Details
2024-01-11 05:46	Completed	in-house	New User Self-Certificate	90		Pending Payment	Details
2024-01-11 05:46	Completed	in-house	New User Self-Certificate	90		Pending Payment	Details
2024-01-11 05:46	Completed	in-house	New User Self-Certificate	90		Pending Payment	Details

Showing 1 to 10 of 10 entries

3. Action: Click 'Modify' button to update the CSR information.

The screenshot displays the TRUSTGATE Certificate Management interface. The left sidebar contains navigation links: Home, Account Information, Certificate Management (selected), All Certificates, All Requests, New Certificate Request, Customer Support, and Logout. The main content area is titled 'CERTIFICATE MANAGEMENT' and includes a 'Download Certificate Request' button. The interface is divided into several sections:

- Request Information:** Includes fields for Index, Date Submitted, Status, Project Information, Project Name, Organization Name, Organization ID, and Personal Information (Nationality, MyID No, Full Name, Email, Mobile No, Address, City, Postcode, State, Country).
- Company Information:** Includes fields for Company ID, Registration No, Company Name, Address, City, Postcode, State, and Country.
- Additional Information:** Includes fields for MyID No, CERTIFICATE ID, and User ID.
- Requesting Comments:** Includes fields for MyID No, Request, Request ID, and User ID.

On the right side, there are sections for 'Package Information' and 'Certificate Signing Request Information'. The 'Certificate Signing Request Information' section is highlighted with a red box and contains the CSR text. Below this, there is a 'Modify' button, also highlighted with a red box. The 'Modify' button is located at the bottom right of the interface.

CSR

4. CSR Information: Update the CSR information in the mark box.

The screenshot shows the TRUSTGATE LHDN e-Invoice Organization Certificate form. The form is titled "LEMBAGA HASIL DALAM NEGERI (E-INVOICE)". It contains several sections for user information:

- Personal Information:** Includes fields for Name (MIDNAGA), Full Name (MAGG), Nationality (Malaysia), Mobile No. (012-3456789), Email (magg@trustgate.com), Address (12345), Postcode (50100), City (Kuala Lumpur), State (Selangor), and Country (MY).
- Company Information:** Includes fields for Company Name (Trust Gate), Company ID (12345678), Registration No. (123456789), Address (12345), Postcode (50100), City (Kuala Lumpur), State (Selangor), and Country (MY).
- Additional Information:** Includes fields for TIN (123456789), SSK Number (123456789), and Bank (Bank).

The CSR Information section is highlighted with a red box. It contains a text area for the CSR request, which is currently empty. Below the text area is a "Submit" button.

5. Invalid CSR: If you enter the invalid CSR, the message of invalid CSR is displayed on the screen.

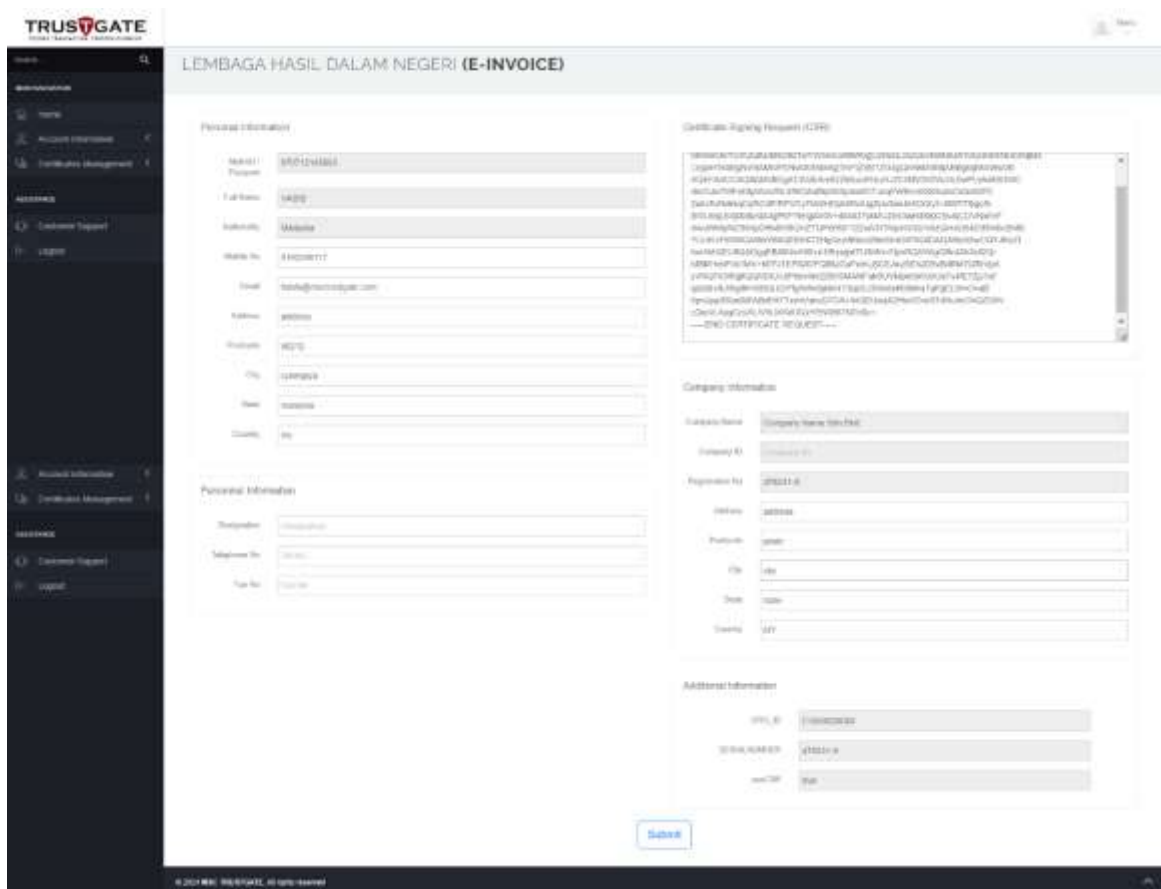
The screenshot shows the TRUSTGATE LHDN e-Invoice Organization Certificate form with an error message displayed. The error message is a black box with white text that reads: "www.trustgate.com says: Invalid CSR. Please make sure CSR is in the right format". Below the error message is a red box highlighting the CSR Information section, which is currently empty. The "Submit" button is visible below the CSR text area.

6. **Company Information:** Tax Identification Number (TIN) and Business Registration Number (BRN) also can be update. Ensure the TIN and BRN is matched and registered with LHDN. If not, the message is displayed on the screen (as in the picture below).



The screenshot shows the TRUSTGATE web application interface. A message box at the top right states: "Company not found! Please make sure your Tax Identification Number and Business Registration Number are valid." Below this, the 'Certificate Signing Request (CSR)' form is visible. The form includes fields for 'Personal Information' (Name, Full Name, Address, Email, Phone, City, State, Country) and 'Company Information' (Company Name, Company ID, Registration No., Address, Phone, City, State, Country). The 'Personal Information' section is partially filled with data.

7. **Completion:** After done update the CSR information, click 'Submit'



The screenshot shows the TRUSTGATE web application interface. The 'Certificate Signing Request (CSR)' form is visible. The form includes fields for 'Personal Information' (Name, Full Name, Address, Email, Phone, City, State, Country) and 'Company Information' (Company Name, Company ID, Registration No., Address, Phone, City, State, Country). The 'Personal Information' section is partially filled with data. The 'Submit' button is highlighted at the bottom right of the form.

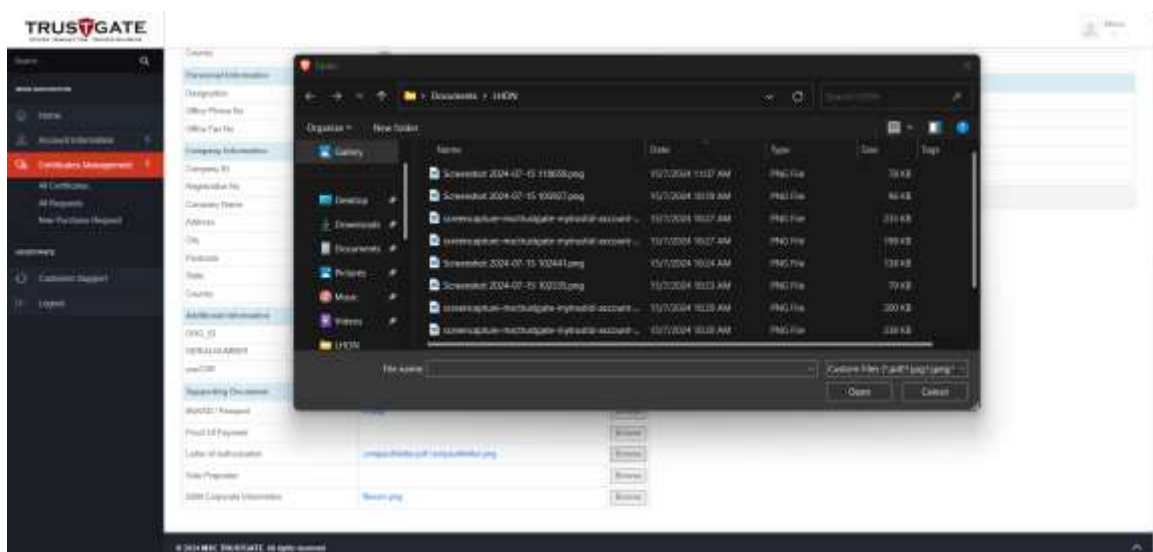
8. CSR has been updated: The screen below show after the CSR has been updated.

The screenshot displays the 'CERTIFICATE MANAGEMENT' page in the TRUSTGATE system. The page is divided into several sections for managing certificates. The left sidebar contains navigation links for 'Home', 'Account Information', 'Certificate Management', 'All Certificates', 'All Requests', 'New Certificate Request', 'Customer Support', and 'Logout'. The main content area is titled 'CERTIFICATE MANAGEMENT' and includes a 'Download Certificate Request' button. The page is organized into three main columns: 'Request Information', 'Personal Information', and 'Company Information'. The 'Request Information' section shows details like 'Index', 'Date Submitted', and 'Status'. The 'Personal Information' section includes fields for 'Name', 'MyID No.', 'Full Name', 'Email', 'Mobile No.', 'Address', 'City', 'Postcode', 'State', and 'Country'. The 'Company Information' section includes 'Company ID', 'Registration No.', 'Company Name', 'Address', 'City', 'Postcode', 'State', and 'Country'. The 'Additional Information' section includes 'MVA ID', 'JERAMIA MVAID', and 'Last CSR'. The 'Supporting Documents' section includes 'MVA ID Request', 'Proof of Payment', 'Letter of Authorization', 'Tax Payer', and 'SME Corporate Information'. The 'Certificate Signing Request Information' section shows the 'Certificate Signing Request' and its 'Status'. The 'Payment Information' section shows 'Amount', 'Date', 'Type', and 'Balance'. The 'Status' section shows 'Status' and 'Action' buttons. The page is dated '10/01/2021 10:01:01 AM'.

9. Update Supporting Document: Click 'Browse' button to update the supporting document.

This screenshot shows the same 'CERTIFICATE MANAGEMENT' page as the previous one, but with a red rectangular box highlighting the 'Supporting Documents' section. This section contains five rows of information, each with a 'Browse' button for updating the document: 'MVA ID Request', 'Proof of Payment', 'Letter of Authorization', 'Tax Payer', and 'SME Corporate Information'. The 'Browse' buttons are located to the right of each document name. The rest of the page layout, including the sidebar and other sections, remains the same.

- 10. Choose File:** Choose the updated file from your device. Click 'Open' button to proceed. Updating supporting document is done.



7.3 Reissue Certificate

If the private key is missing, or you need to deploy the same certificate on multiple servers while retaining the same subject Distinguished Name (DN), you can reissue the certificate. To do this, generate a new key pair and create a Certificate Signing Request (CSR) using the existing subject DN. This process ensures that the new certificate retains the original identity, even though the private key has been regenerated. Follow the steps below to reissue the certificate:

- 1. Reissue certificate:** To issue certificate, navigate the 'Certificate Management' in the left side bar and click 'All Certificates' option. On this page, you will see a list of all issued certificates. To start reissue process, select the certificate you wish to reissue and click the 'Reissue' button.



2. **Soft Certificate Option:** Then, select the Soft Certificate Option either PKCS#12 or PEM format.



3. **Certificate information:** Fill in the certificate details in the respective fields, ensure the information matches your existing certificate exactly. After that, enter and re-enter the Soft Certificate Activation PIN. Then, click 'Reissue' button to proceed.

Reissue Soft Certificate

Soft Certificate Options

PKCS#12 format (P12)

Certificate Information

Common Name (CN): The company or organization name*

Example: MSC TRUSTGATE SDN BHD

Organization Name (O): The company or organization name*

Example: MSC TRUSTGATE SDN BHD

Country (C): The country of the organization – 2-letter ISO code*

Select Country

Serial Number (SN): The Business Registration Number (BRN)*

Example: 199801012345

Organization Identifier (ORG_ID): The Tax Identification Number (TIN)*

Example: C10569812345

Soft Certificate Activation

PIN *

PIN

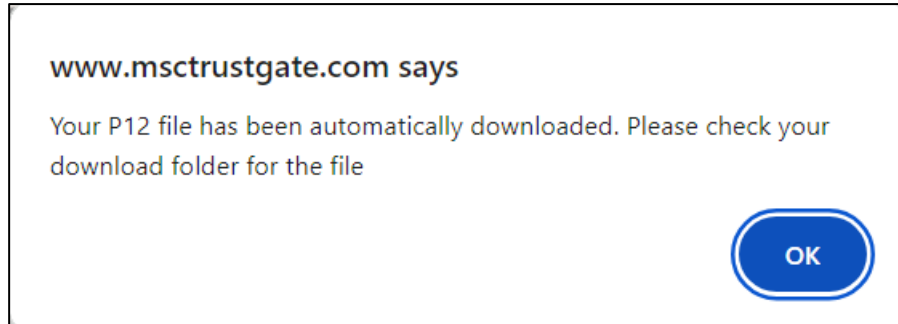
Reenter PIN*

Reenter PIN

Cancel

Reissue

4. **Certificate Reissue Successful:** A dialog box will appear confirming that your P12 file has been automatically downloaded. Please check your downloads folder to retrieve the file.



8 Certificate Revocation

Certificate revocation is a process in Public Key Infrastructure (PKI) that invalidates a digital certificate before its scheduled expiration date. Reasons for certificate revocation include a compromised private key, a lost or stolen private key or changes to the information contained in the certificate.

Below are the steps to revoke a certificate:

1. **Revocation Form:** Download the revocation form [HERE](#).
2. **Fill out the form:** After downloading the form, please fill it out completely.
3. **Submit the form:** Submit the completed form by sending an email to revoke@msctrustgate.com.
4. **Notification Revocation:** The CA will notify you that the certificate has been successfully revoked. The notification will be sent to your email.
5. **CRL Generation:** The CRL will be generated within 24 hours.

9 Support and Resources

You may request support related to digital certificate by sending an email to support@msctrustgate.com with the subject: [LHDN eInvoice] <Brief description on the problem>. You may also call our support team at 03-83181800 during MSC Trustgate Business Hour (Monday – Friday: 9am – 6pm; Lunch Time: 1pm – 2pm (Friday: 12.15pm – 2.45pm). For other eInvoice inquiries, please contact LHDN directly.

10 Appendices

Appendix A: Generating Certificate Signing Request (CSR)

This section applies solely to purchase for Soft Certificate.

You are solely responsible for managing your key pair and certificate. The key pair must be securely generated and stored. Any data signed using your private key, whether with or without your consent, is your responsibility.

Three frequently tools used for managing Key Pairs are:

- KeyStore Explorer
- OpenSSL
- Java Key Store (JKS)

The Certificate Signing Request (CSR) and certificate must contain the following information:

Certificate Field	OID	Expected Content	Value Example
commonName (CN)	2.5.4.3	The company or organization name.	Company Name Sdn Bhd
serialNumber	2.5.4.5	The business registration number (BRN) of the organization that is linked to the TIN provided above.	202005123456
organizationName (O)	2.5.4.10	The company or organization name.	Company Name Sdn Bhd
organizationIdentifier	2.5.4.97	The Tax Identification Number of the organization (TIN).	C20830570210
countryName (C)	2.5.4.6	The country of the organization - 2-letter ISO code.	MY

Only the following algorithm is supported for LHDN e-Invoice Organization Certificate:

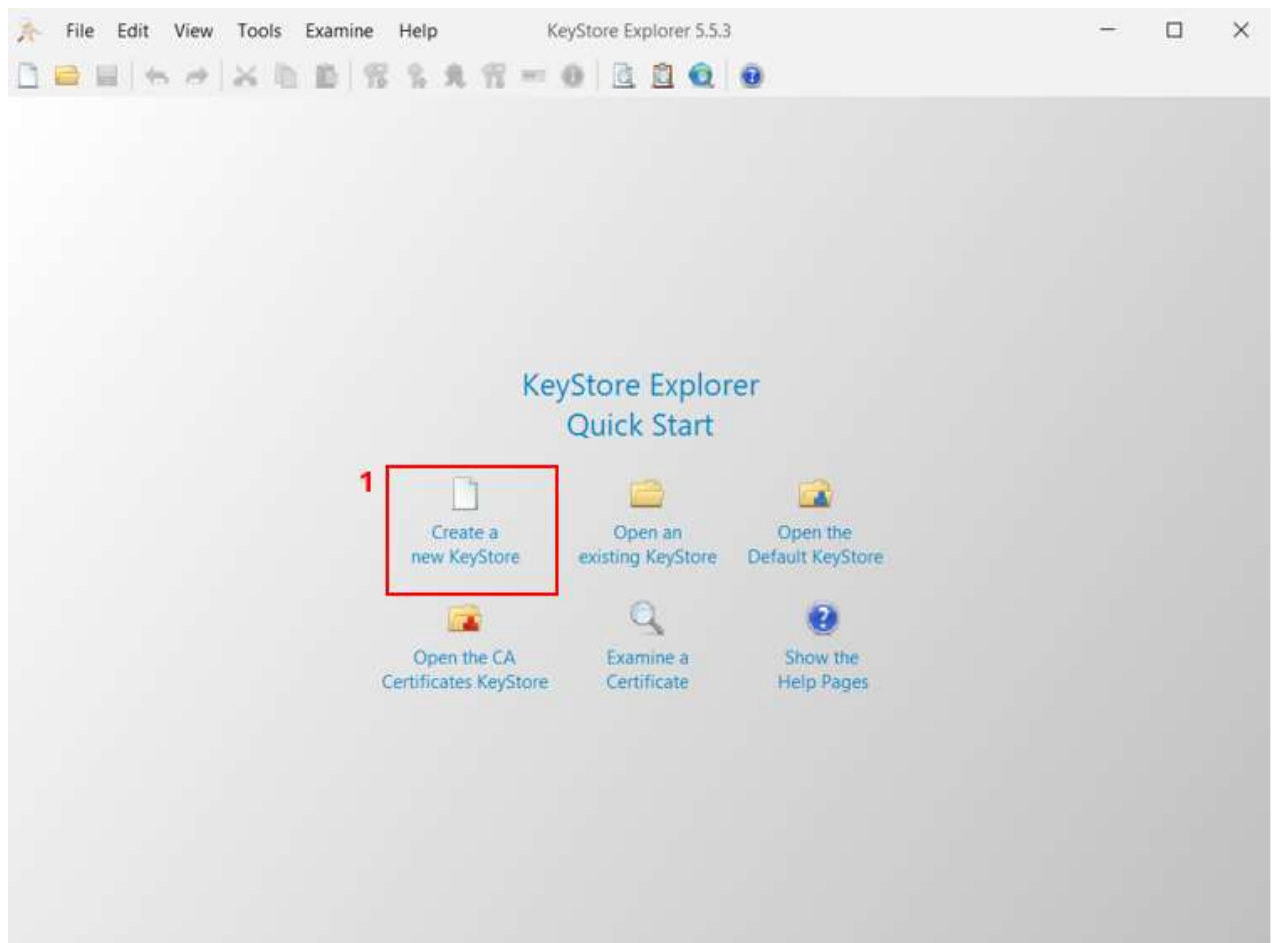
CSR Format:	PKCS#10
Key Type:	RSA
Key Size:	2048
Signature Algorithm:	sha256WithRSAEncryption
Exponent	65537 (0x10001)

a) KeyStore Explorer

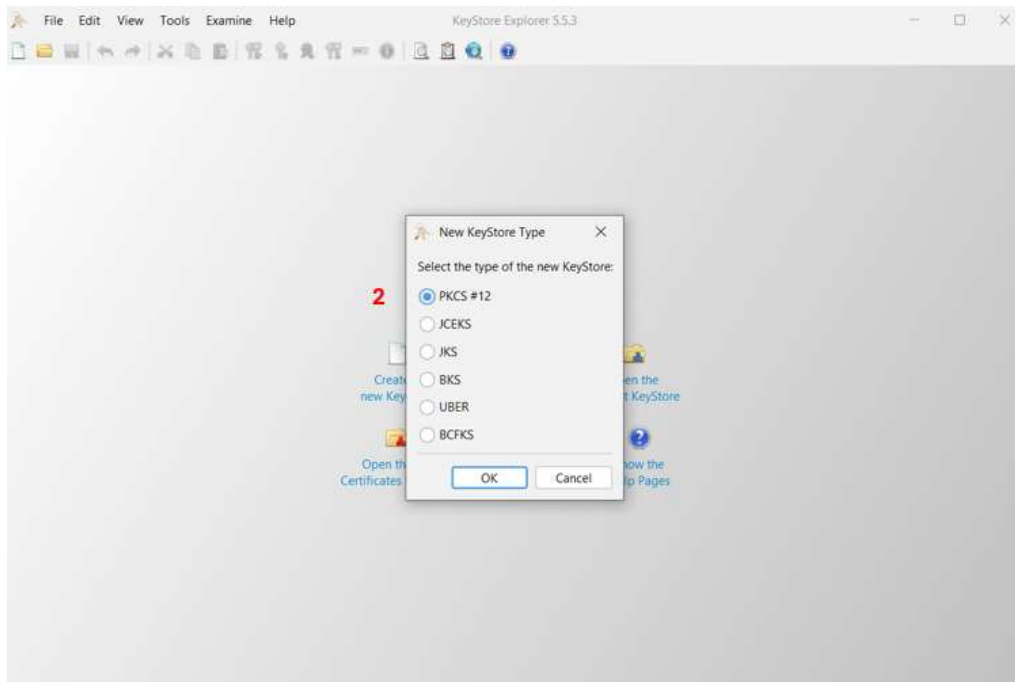
KeyStore Explorer is an open GUI replacement for the Java command-line utilities keytool and jarsigner. KeyStore Explorer can be used to create, edit and save KeyStore files. When using KeyStore Explorer, the typical order of operations is to generate CSR first, followed by exporting private key. Below is the explanation of generating CSR and export private key:

i. Generate CSR

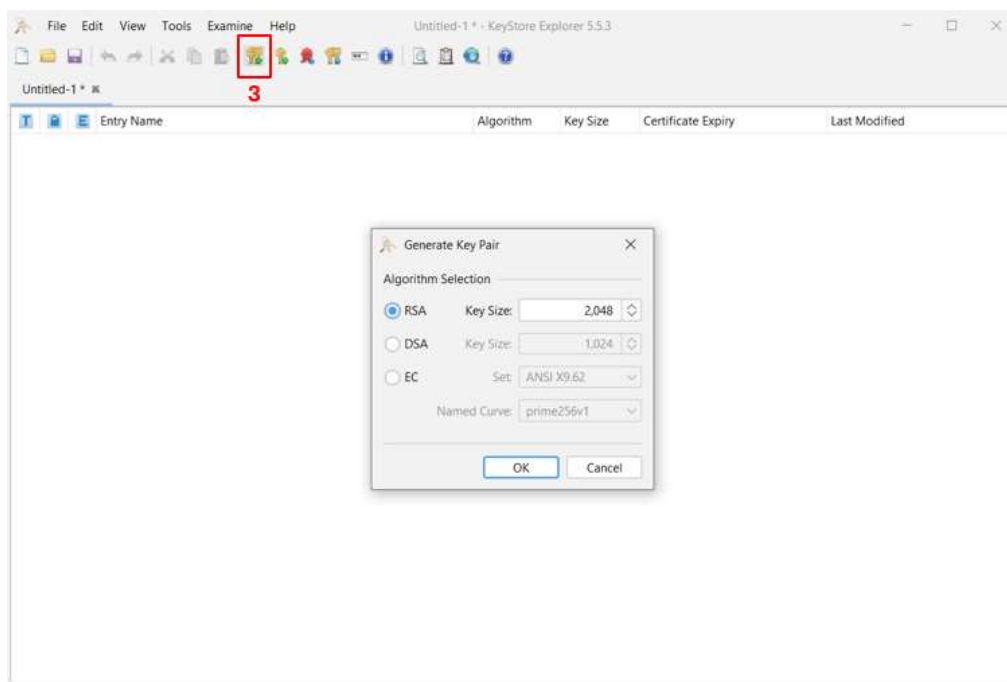
1. **Download and install KeyStore Explorer:** Visit KeyStore Explorer page (<https://keystore-explorer.org/>) to download and get more information on the program. Install and run the program accordingly.
2. **Create a new KeyStore:** Run KeyStore Explorer and create a new keystore.



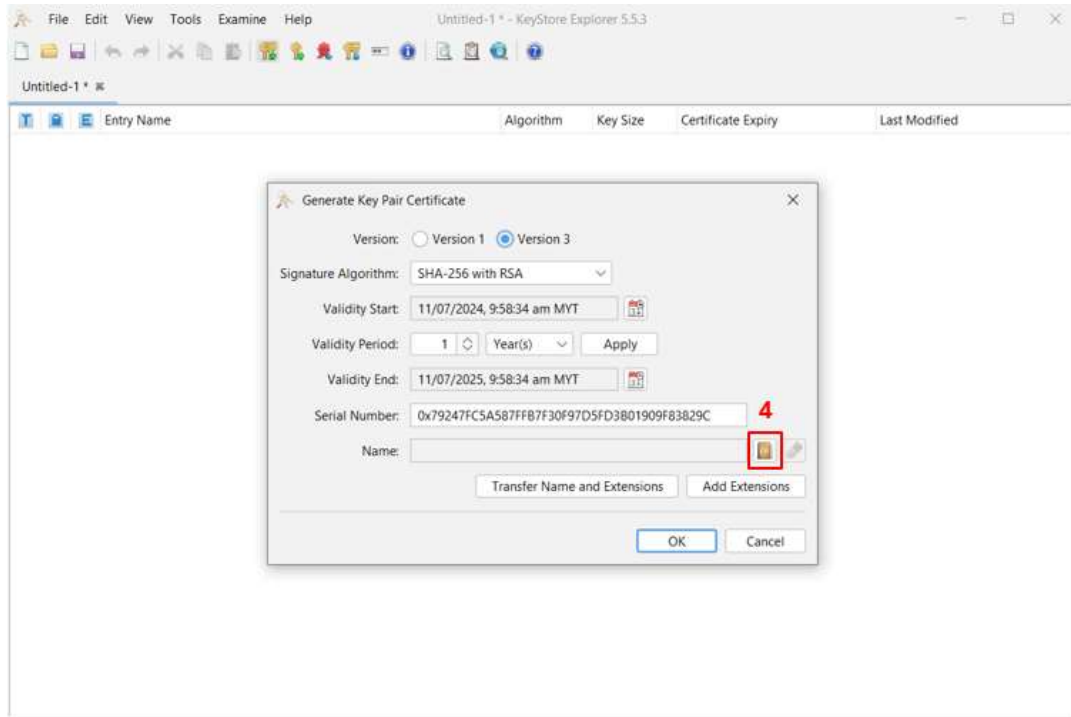
3. **Select New KeyStore type:** You can select the type of the new KeyStore (PKCS#12) as shown in the picture below. Then click 'OK' button to proceed.



4. **Click Generate Key Pair:** Locate Generate Key Pair icon, labelled with the number 3 in the picture below, and click on it. A new dialog box will appear. From the available options, select the cryptographic algorithm "RSA" with Key Size 2,048, as shown in the picture below. Click "OK" to confirm your selection.

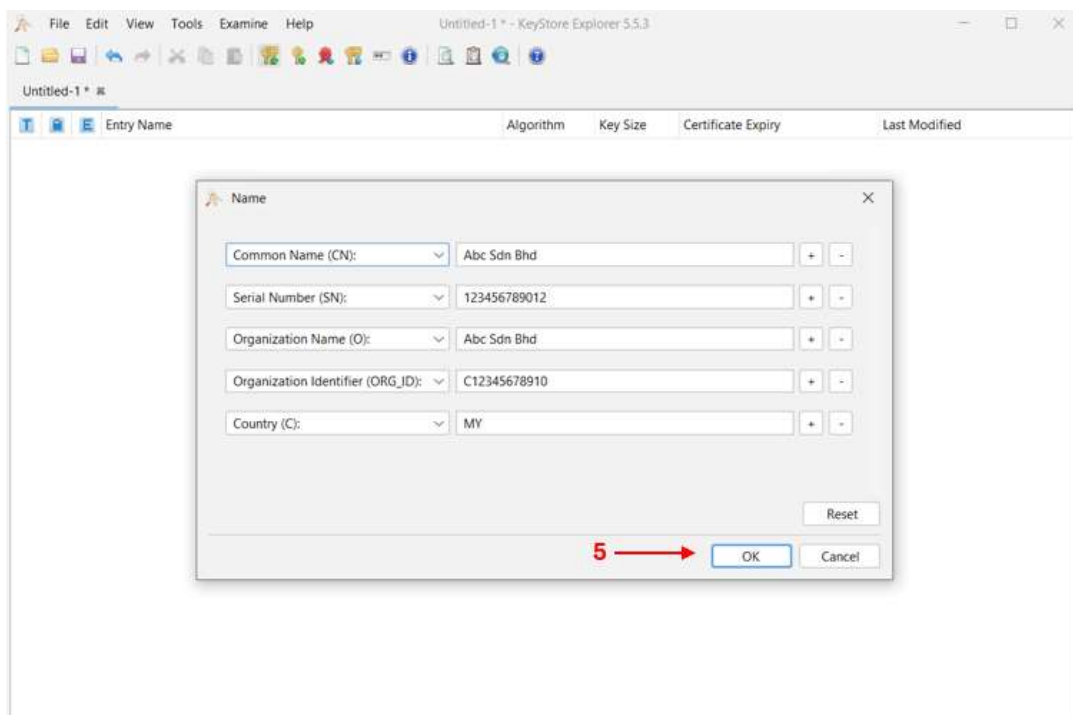


5. **Confirm self-signed certificate parameter:** A new dialog box will appear. Leave all the default value as shown in the picture below. This value will be used to generate self-signed certificate. Locate the icon labelled with the number 4 in the picture below and click on it.

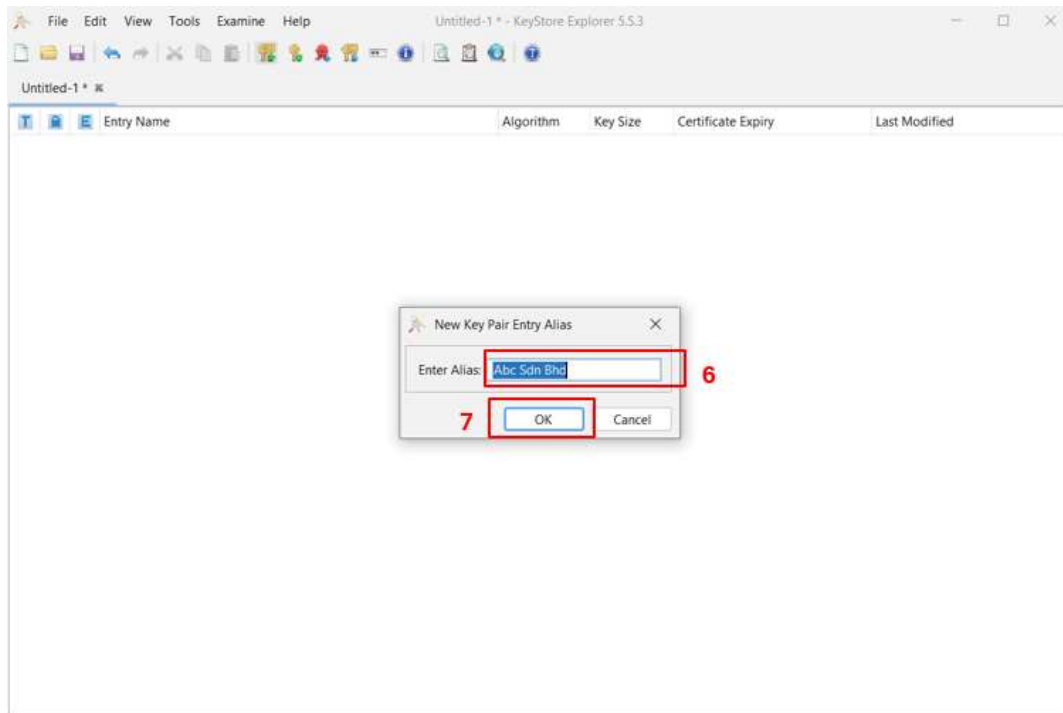


6. **Fill in Certificate Details:** A new dialog box will appear. Enter the required details for the certificate in the corresponding fields as follows, and then click OK button:

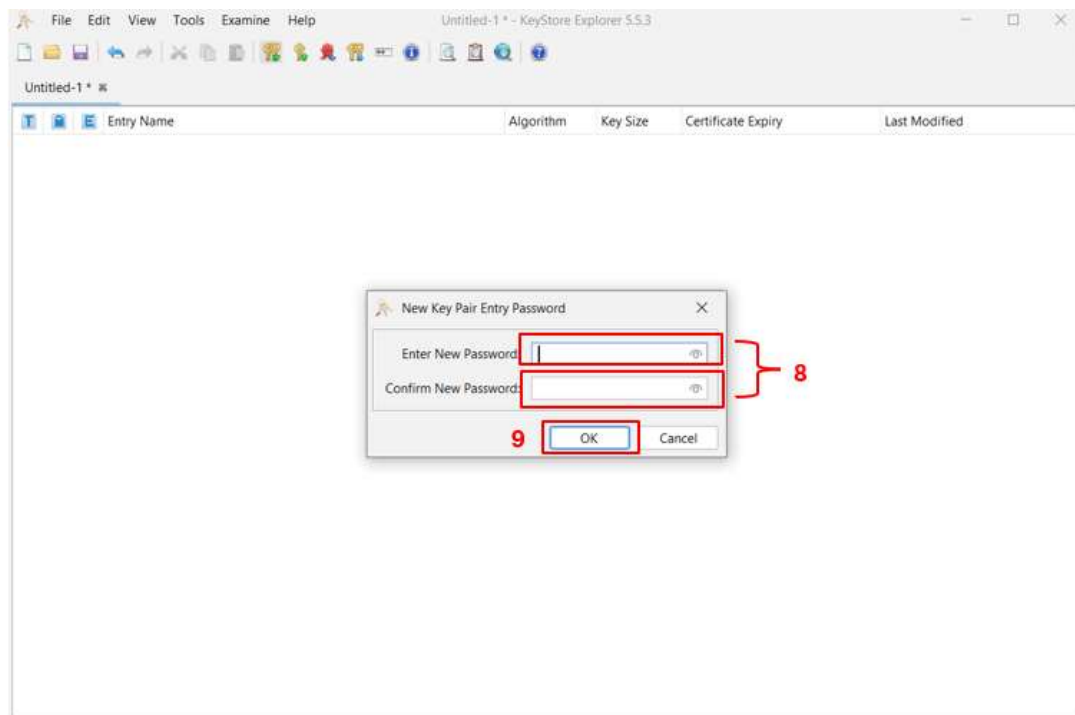
- Common Name (CN): The company or organization name.
- Serial Number (SN): The Business Registration Number (BRN) of the organization that is linked to the TIN provided above.
- Organization Name (O): The company or organization name.
- Organization Identifier (ORG_ID): The Tax Identification Number (TIN) of the organization.
- Country (C): The country of the organization – 2-letter ISO code



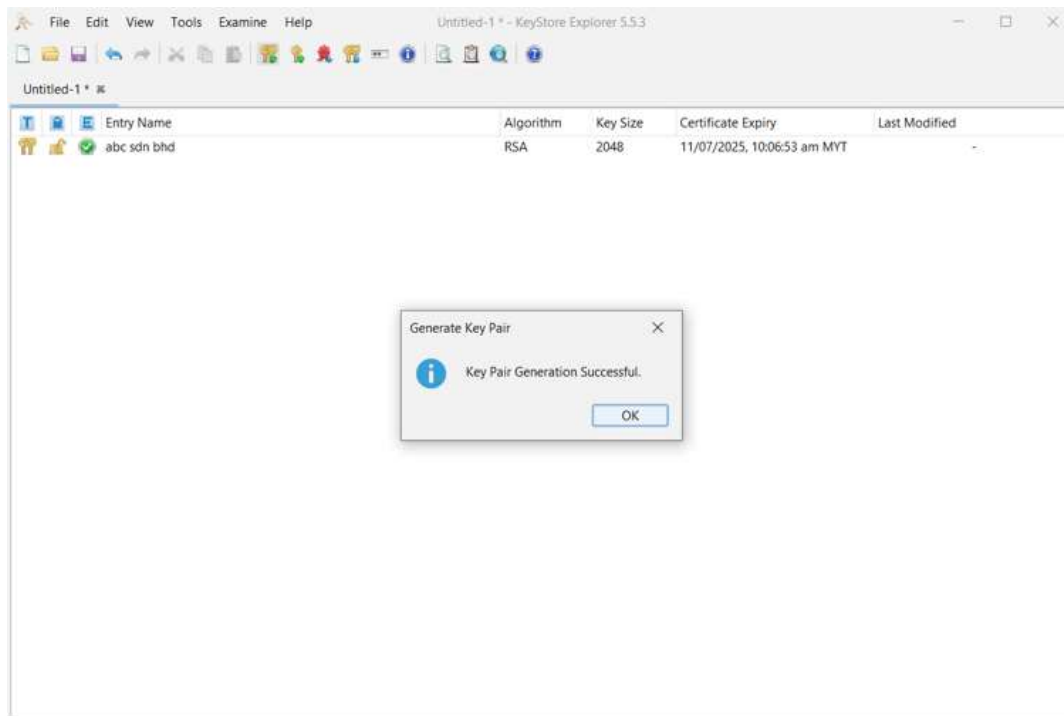
7. **Set the Alias:** Assign an alias to the key pair. Enter the Alias name in the respective field (labelled with no 6) and then click 'OK' button to proceed.



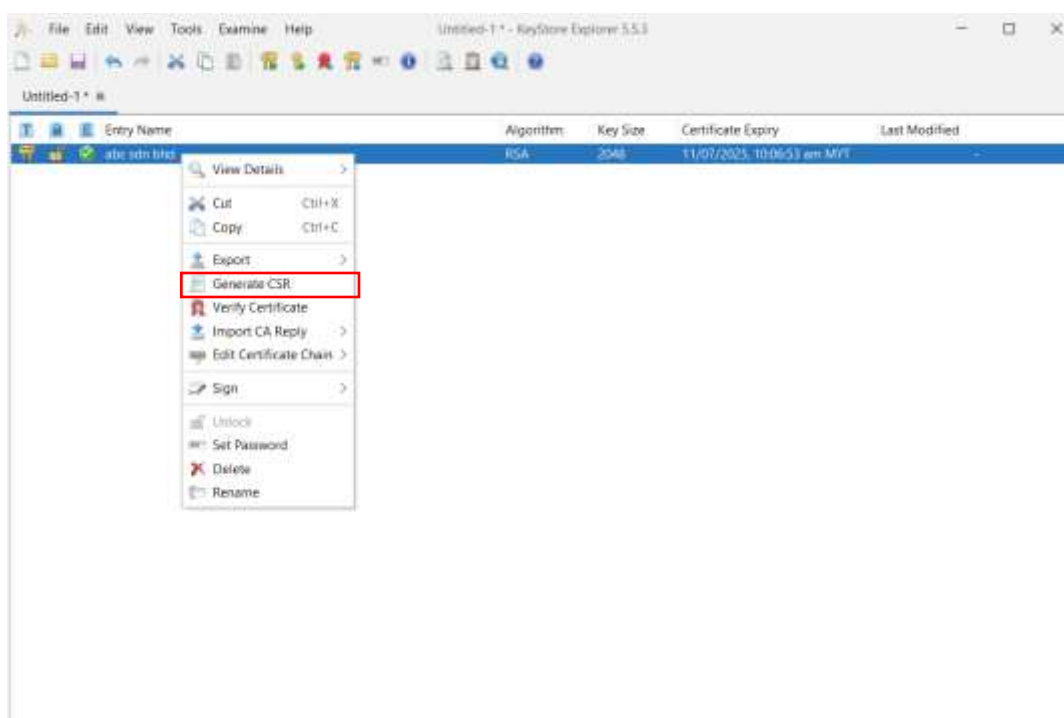
8. **Set the password:** You will be prompted to set and confirm new password for the private key. After setting up the password, click 'OK' button to proceed.



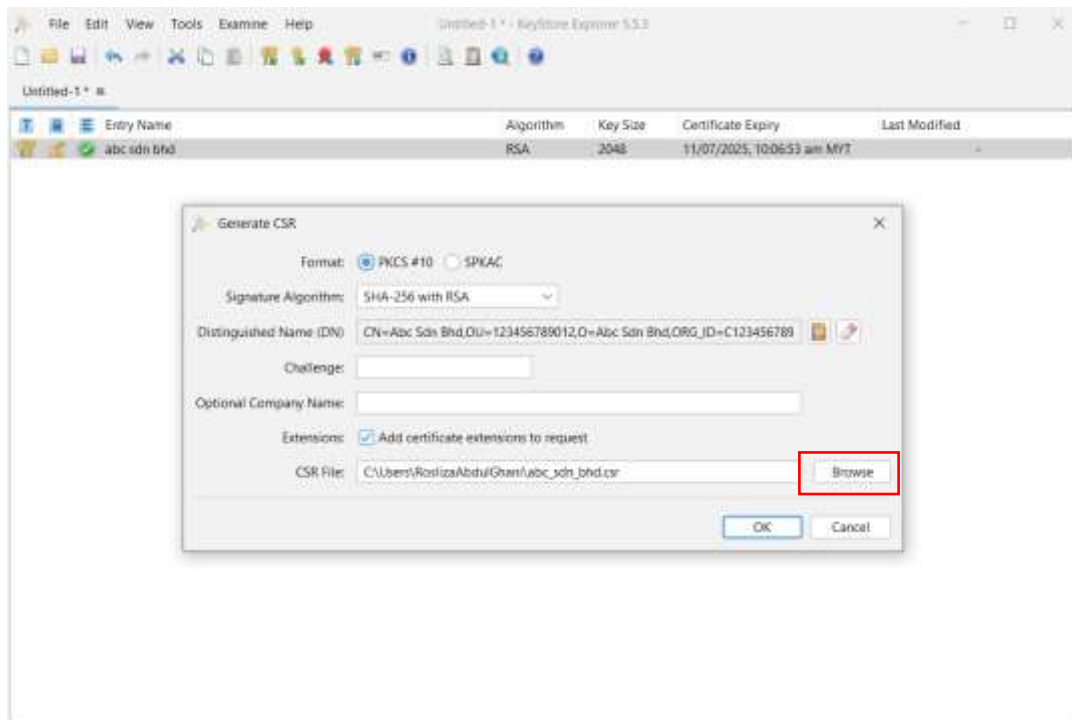
9. **Key Pair is generated:** A message will appear on the screen: 'Private Key Generation Successful'. Click the OK button to acknowledge the message. You will now see the alias for the private key you set in Step 7 displayed in the list of keys.



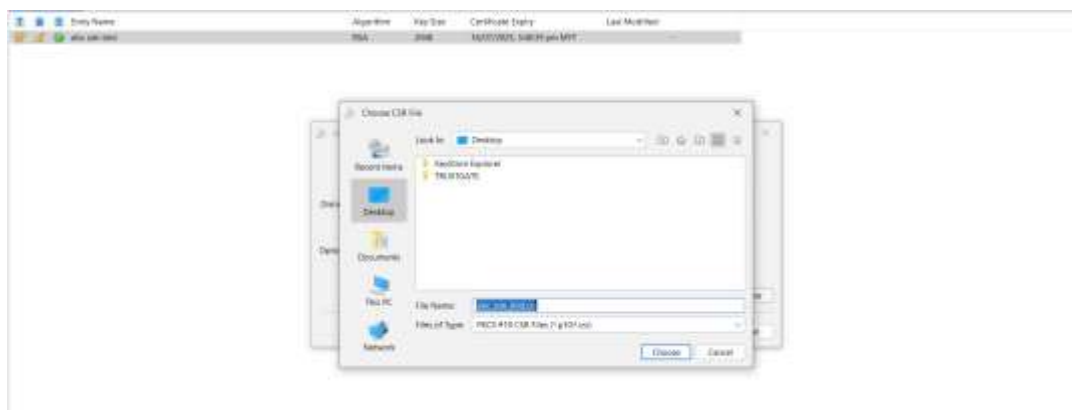
10. **Initiate Generate CSR:** To generate a Certificate Signing Request (CSR) for the new key created in the previous step, find the Entry Name corresponding to the private key alias you set in the previous step. Right-click on the private key alias (Entry Name). From the context menu that appears, select the option 'Generate CSR'.



11. **Confirm CSR parameters:** A new dialog box will appear. Leave all the default value as shown in the picture below. This value will be used to generate CSR. And then click on 'Browse' button to locate the location and file name to save your CSR.



12. **Save the CSR file:** Browse and confirm file name and its location on your computer to save the exported CSR file. Then, click 'Choose' button to save the CSR file.



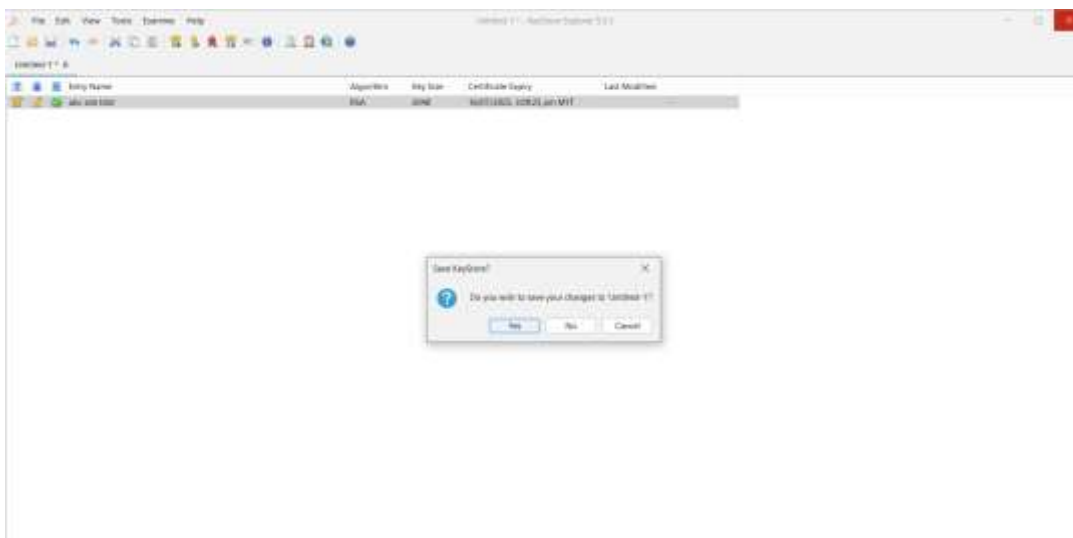
13. **Review Exported CSR File:** You can open CSR file using a notepad to view and copy the contents.



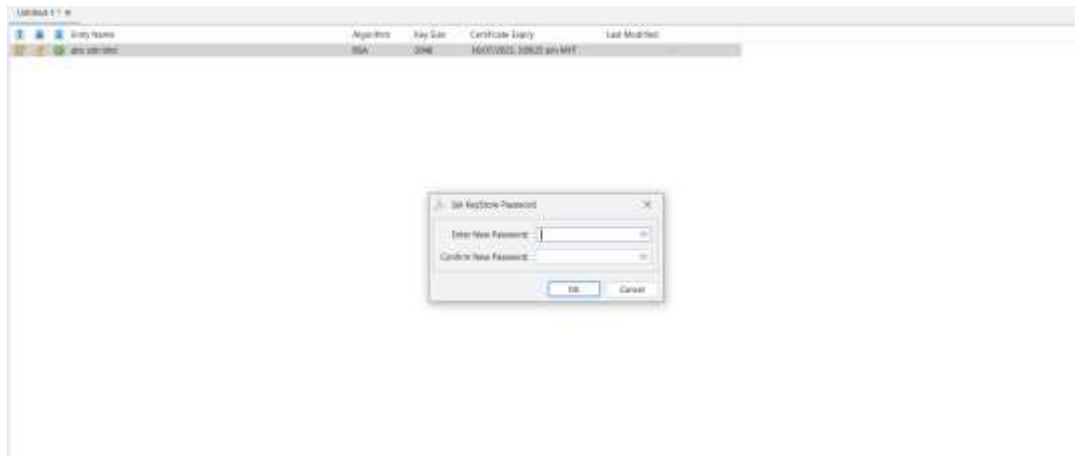
```

abc_sdn_bhd - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE REQUEST-----
MIICrDCCAQCAQAwZzELMAkGA1UEBhMCTVxFTATBgNVBGEtMDEuMjM0NTY3ODkxMDEUMBIGA1UE
CgwLQWJjIFNkbjBCaGQxFTATBgNVBAsMDDEyMzQ1Njc4OTAxMjEUMBIGA1UEAwWLQWJjIFNkbjBC
aGQwgGgEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCkUwtFxGdGdPRZ7T0bwutp3E0GZ7jz
GxViSKSkfFuwdc0H2PzrZp/uPnHjXn2AuC6Aza1wQ87Pb5gWZaXZBWZ0VVWbp9lespV6f7yeu3ws
x0jeToF6bpYU67g7vGdEK16CL+jWNZkABA2D6Pracuq9iwFkz4g+MtrfYAW7Wlp909ya9W66n+r0
KI5DKZRKxklji+IAWB6zzSnDi45KnTZXYJMXKJSVRHGLXBYxRXNMxC/FmND1gE5Xofz97/fNMLC7v
btDa4Q4c48J/puL85m9/komsdVujLAZIEz8BfBRNbkkB601i22wTCdo41JyTjnbwfgvF3PyFdnCq
KrmClnXhAgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEACF0L4J9gKYzarzSvvx+girwDtGXJw9+/
LR1uiUH6/LkG0RTV2QE12ZKusa15L9QBMQAwj389RlAFFAW2mG++fSbCvTXUdE3lUSpDobawU0L2
mE4Gv1XmkfVhHhXGh9Yb1yq0ld884JFt4zC6w6BrZJ8PvvndrjTNE0wTASZGLVtHjxPsf7sGCr6Q
/2CS1fsdzCJehYsYZXju5+kA02YewzdkuJMtDq3VZSve3mvDQ99lDo/Hg1V49Y+IgJNYuR7E6BDS
dMWEDYPM33MIu9R07jPTDvFp0P41k9czyxy4U8D7coVvt2kiTDDPF2LP+cZLn6gchVXWCWRNZoyh
z694Yg==
-----END CERTIFICATE REQUEST-----
  
```

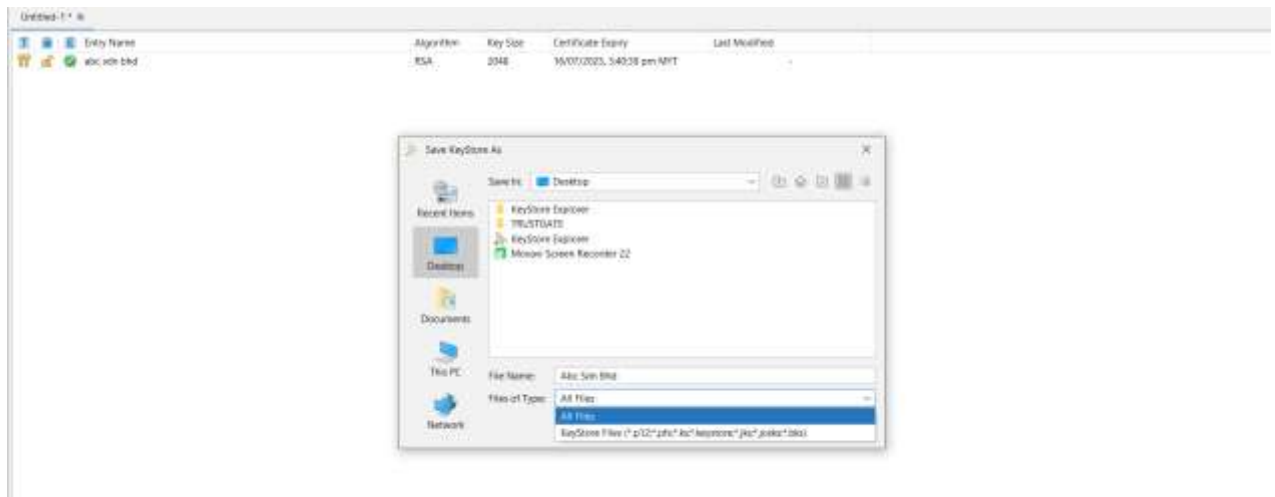
14. **Save KeyStore file:** To ensure your key is available for future use, the KeyStore file need to be saved. When you are ready to close the KeyStore Explorer program, proceed to close the application as usual. A prompt will appear asking if you want to save the KeyStore file. Click the 'Yes' button to save the KeyStore file. This ensures that the key you created remains available for digitally signing an e-Invoice.



15. **Set Password:** Enter and confirm the password for this KeyStore file. Then, click 'OK' to proceed.

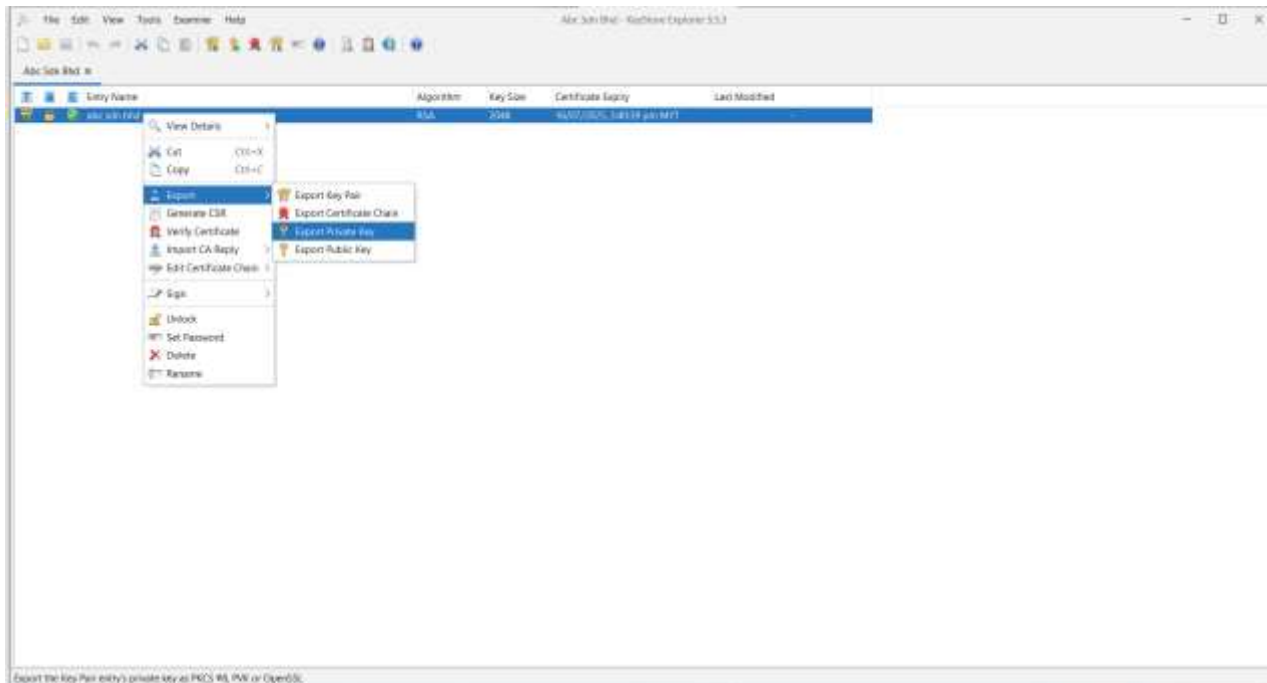


16. **File Location:** Choose location to save the file in your laptop. For Files of Type choose 'All Files'. Then, click 'Save' button to proceed.

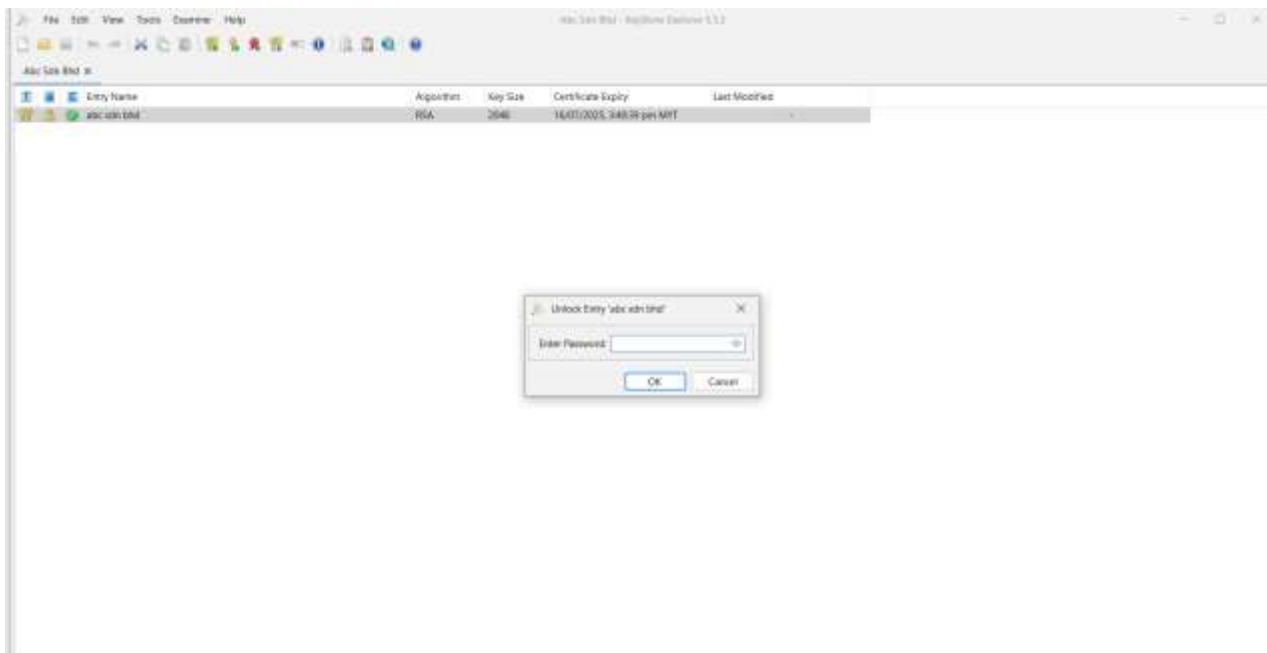


ii. To export private key

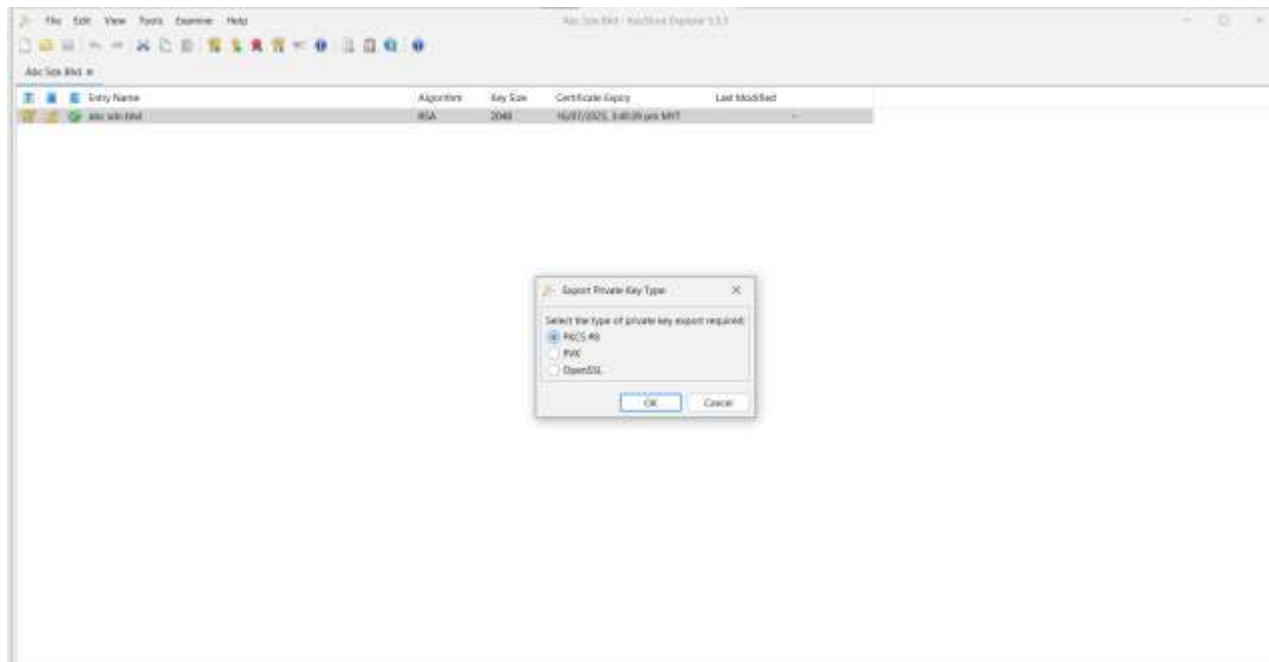
1. **Select Private Key:** Right click on the key pair and select 'Export > Export Private Key'.



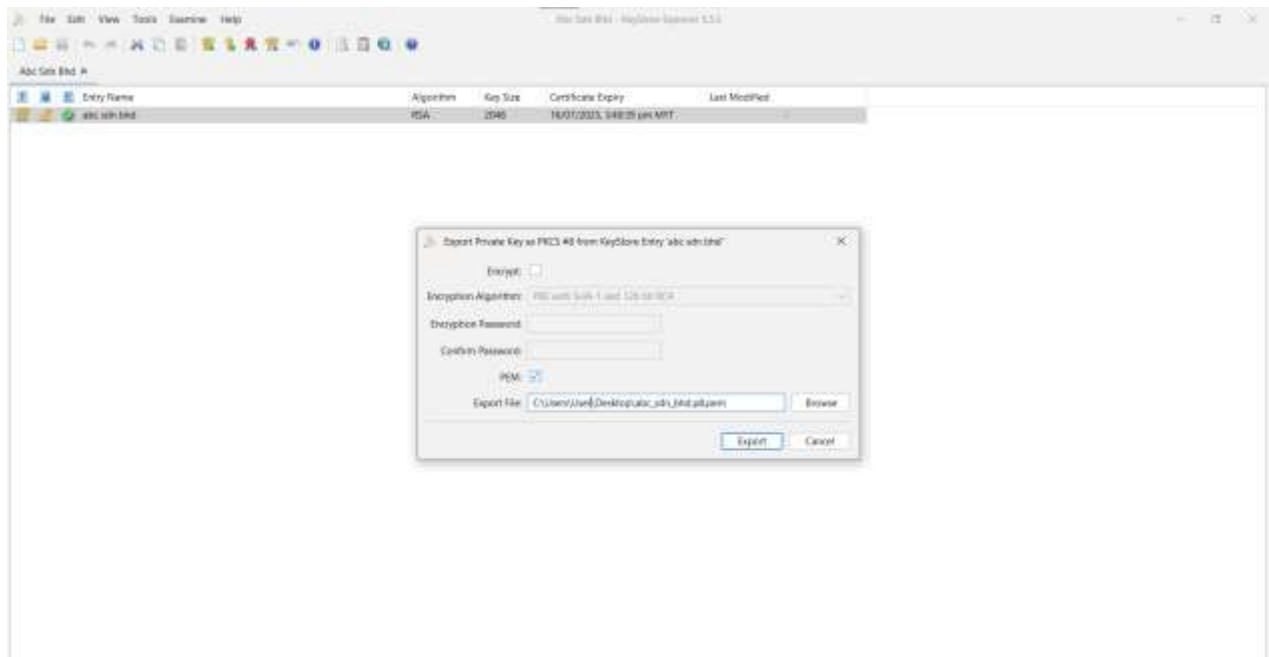
2. **Enter password:** Enter password to unlock the Entry Name.



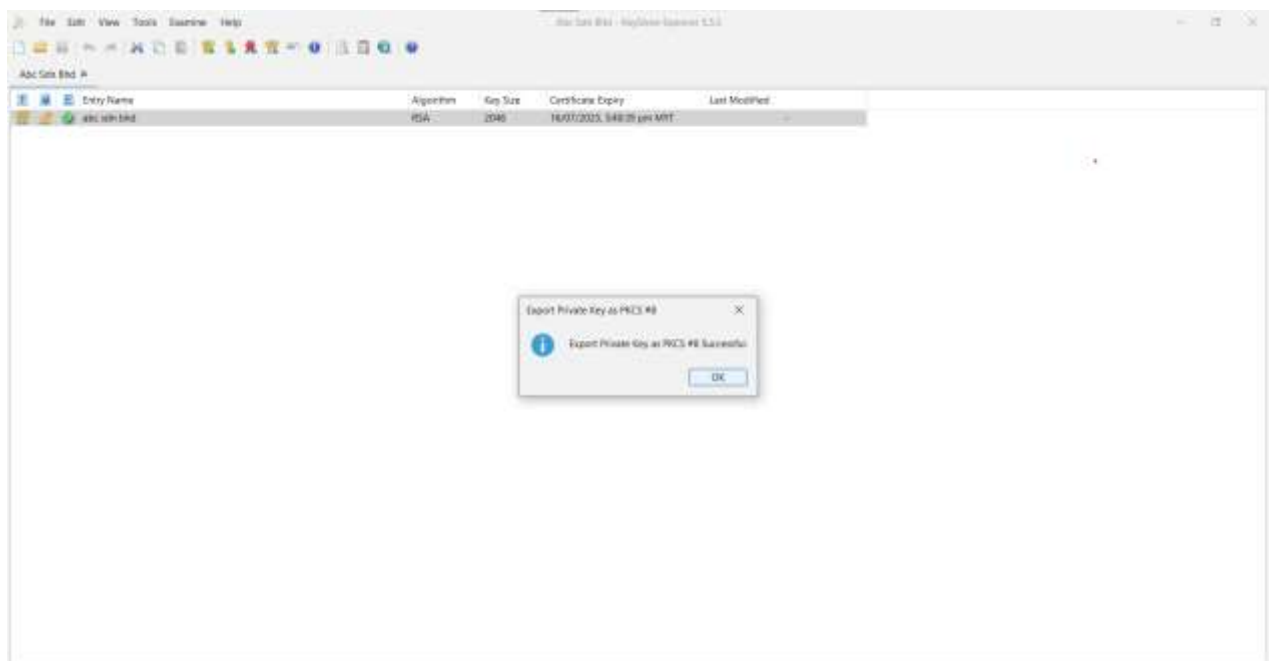
3. **Choose Private Key Type:** You will be presented with options for exporting the private key in different formats. Choose the PKCS #8 type as shown in the picture below. Then, click 'OK' button to proceed.



4. **Export Private Key:** A new dialog box will appear as shown in the picture below. Please **ensure** you:
 - Untick the 'Encrypt' box
 - Tick the 'PEM' box
 - Click 'Browse' button to locate the location and save the export file. Then, click 'Export' button to proceed.



- 5. Successfully Exported:** The private key is successfully exported on your PC. Click 'OK' button to proceed.



b) OpenSSL

To generate a key pair and CSR (please replace the organization information accordingly):

```
openssl req -new -newkey rsa:2048 -nodes -keyout eInvoice.key -out  
eInvoice.csr -subj  
"/C=MY/organizationIdentifier=C20830570210/O=Company Name Sdn  
Bhd/serialNumber=202005123456/CN=Company Name Sdn Bhd"
```

Output:

CSR: eInvoice.csr (This needs to be submitted to MSC Trustgate)

Private Key: eInvoice.key (This needs to be securely stored)

To check the CSR contents:

```
openssl req -text -noout -in eInvoice.csr
```

c) Java Key Store (JKS)

To generate key pair (kindly replace your organization information accordingly)

```
keytool -genkey -keyalg RSA -keysize 2048 -alias eInvoice -keystore  
eInvoice.jks -dname "CN=Company Name Sdn Bhd,  
serialNumber=202005123456, O=Company Name Sdn Bhd,  
2.5.4.97=C20830570210, C=MY"
```

You may be prompted to set or create your keystore password. Please remember this password.

To generate CSR:

```
keytool -certreq -keyalg RSA -alias eInvoice -keystore eInvoice.jks -  
file eInvoice.csr
```

Output:

CSR: eInvoice.csr (This needs to be submitted to MSC Trustgate)

Key Store: eInvoice.jks (This needs to be securely stored)

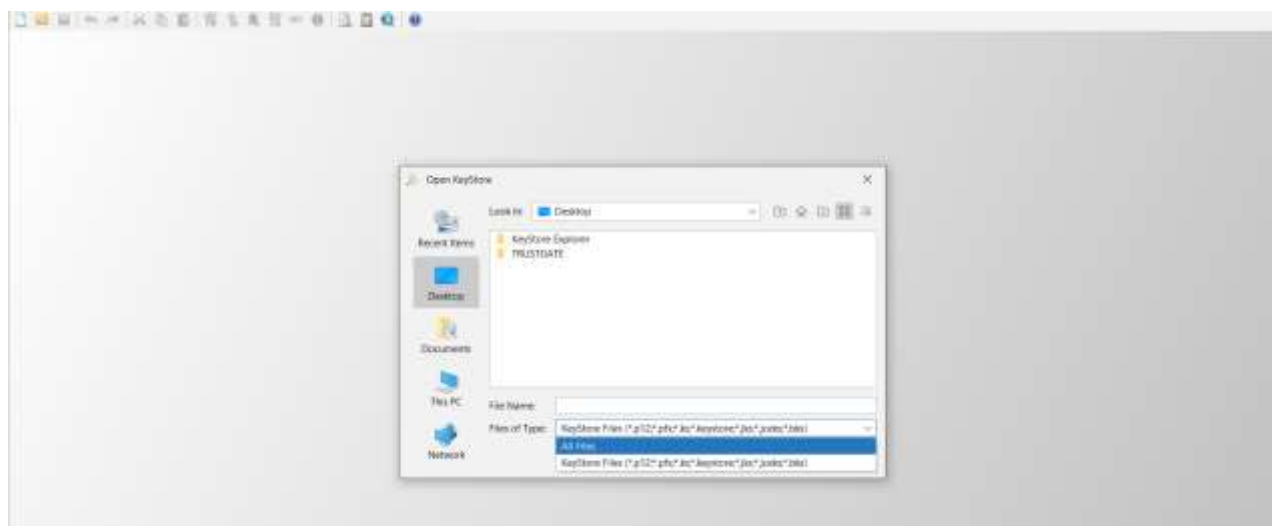
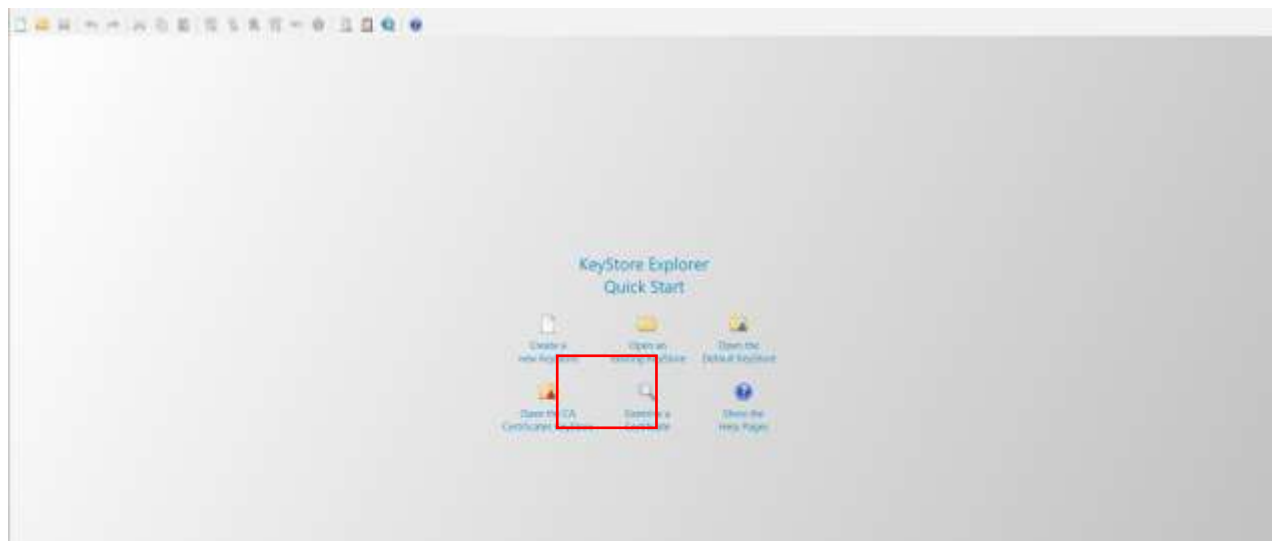
Appendix B: Import PEM file into Key Store

a) KeyStore Explorer

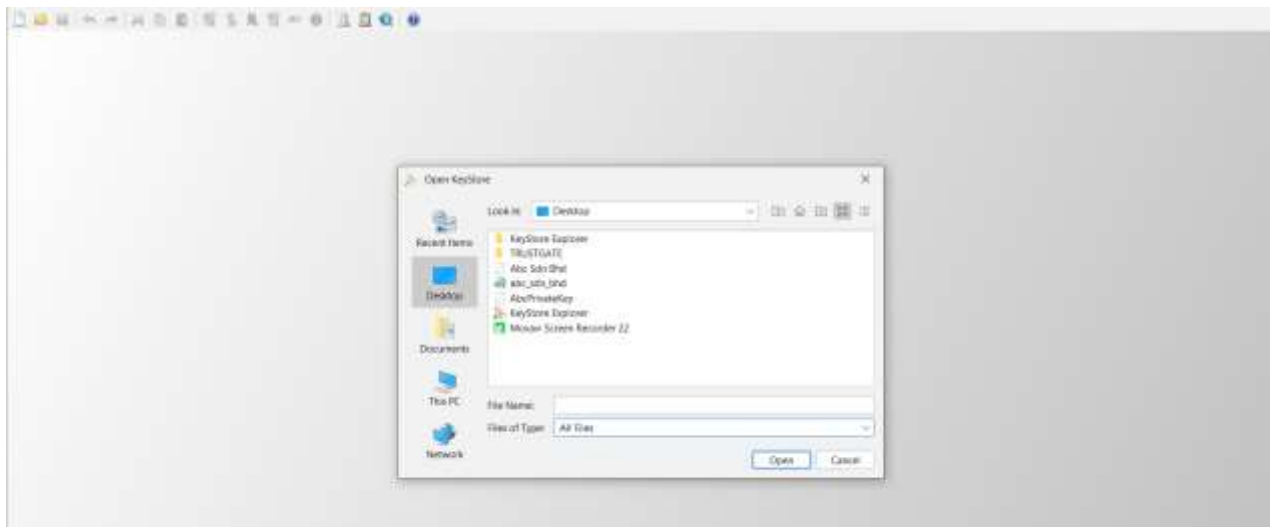
If you already receive a certificate from CA, then you can import the certificate into KeyStore Explorer.

Below are the steps to import the certificate:

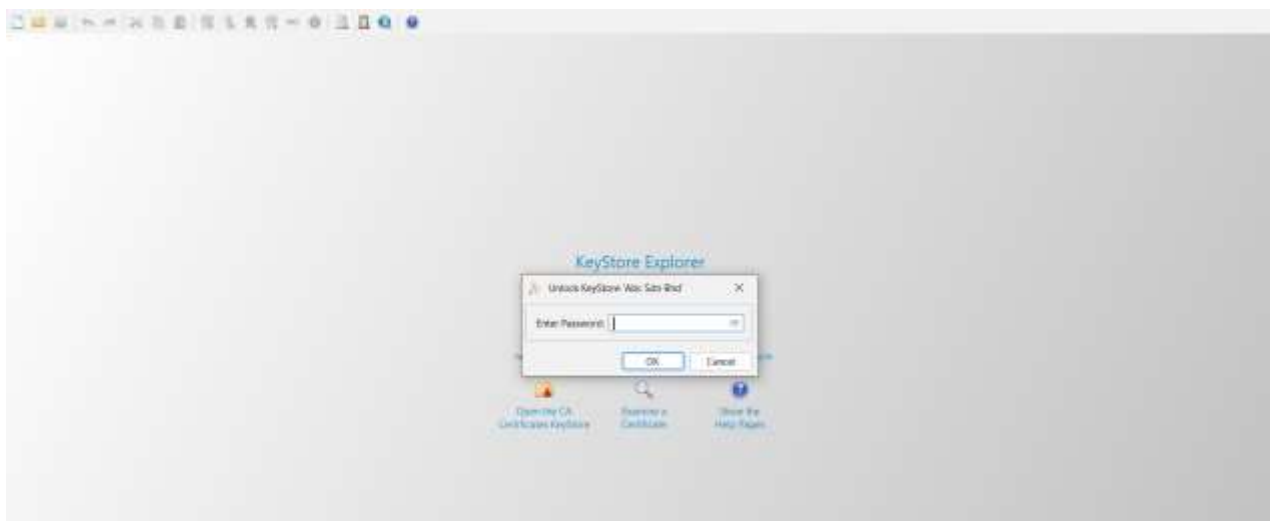
1. **Open Existing File:** Click 'Open an existing KeyStore' in KeyStore Explorer. Click the location that you save the KeyStore file. For 'Files of Type', you can choose All Files.



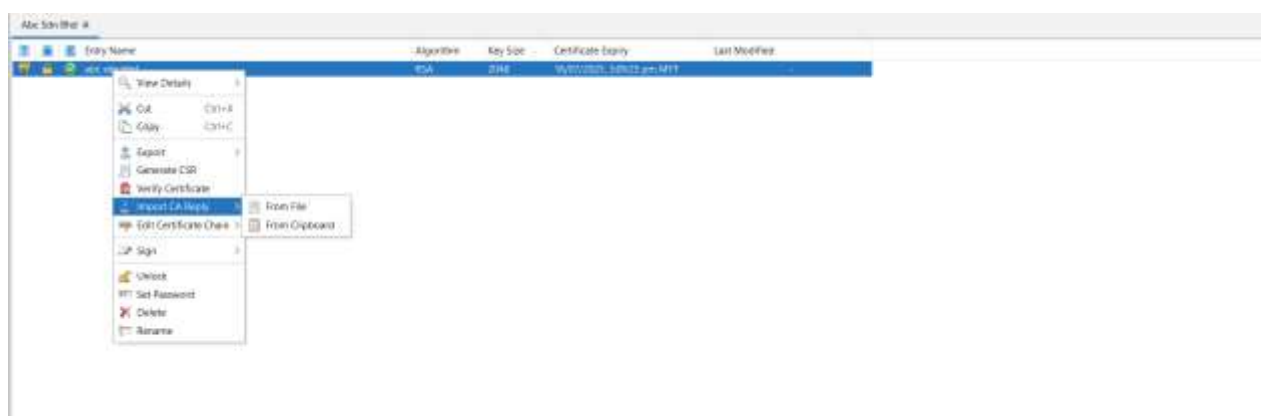
2. **Choose file:** Choose the saved file to open.



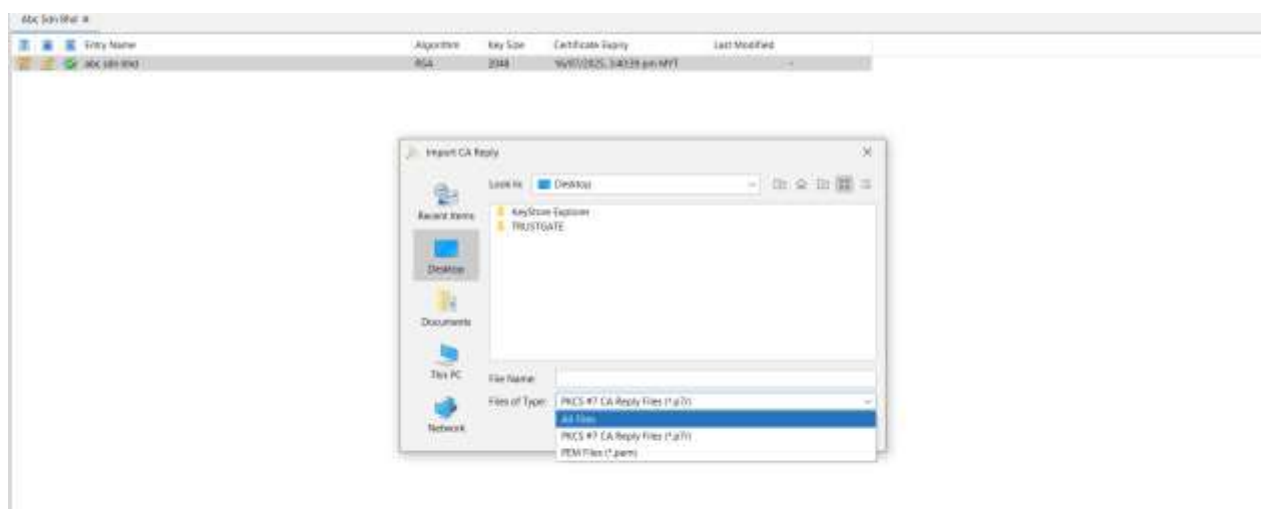
3. **Enter password:** Enter the password to unlock the KeyStore. Then, click 'OK' to proceed.



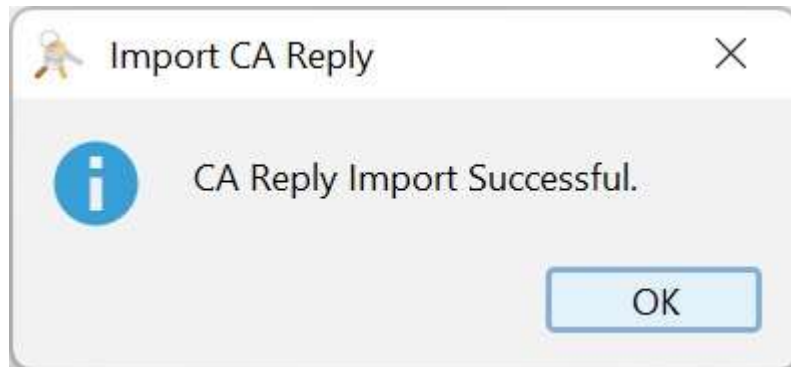
4. **Import certificate:** Right click the key pair entry and select “Import CA Reply” and choose “From File”.



5. **Enter password:** You need to enter password to import the certificate and choose 'All Files' for Type of File. Then, browse and choose the certificate file you received from the CA. Click 'Import' button to proceed.



6. **Successfully Imported:** The certificate from CA is successfully imported in KeyStore Explorer. Click 'OK' button to proceed.



b) OpenSSL

To import certificate (kindly replace your certificate information accordingly)

```
openssl pkcs12 -export -inkey privatekey.pem -in certificate.pem -  
certfile intermediate_certificate.pem -out output.p12
```

c) Java Key Store (JKS)

To import certificate (kindly replace your certificate information accordingly)

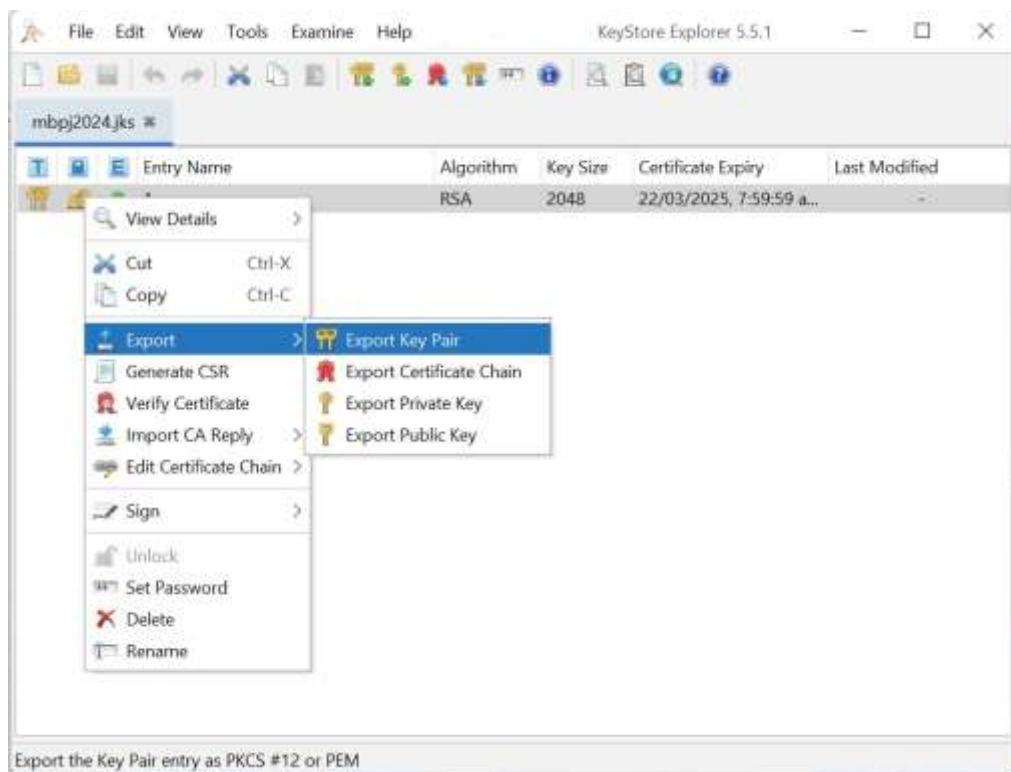
```
keytool -import -alias mycert -file mycertificate.crt -keystore  
mykeystore.jks
```

Appendix C: Export Key from Key Store to P12

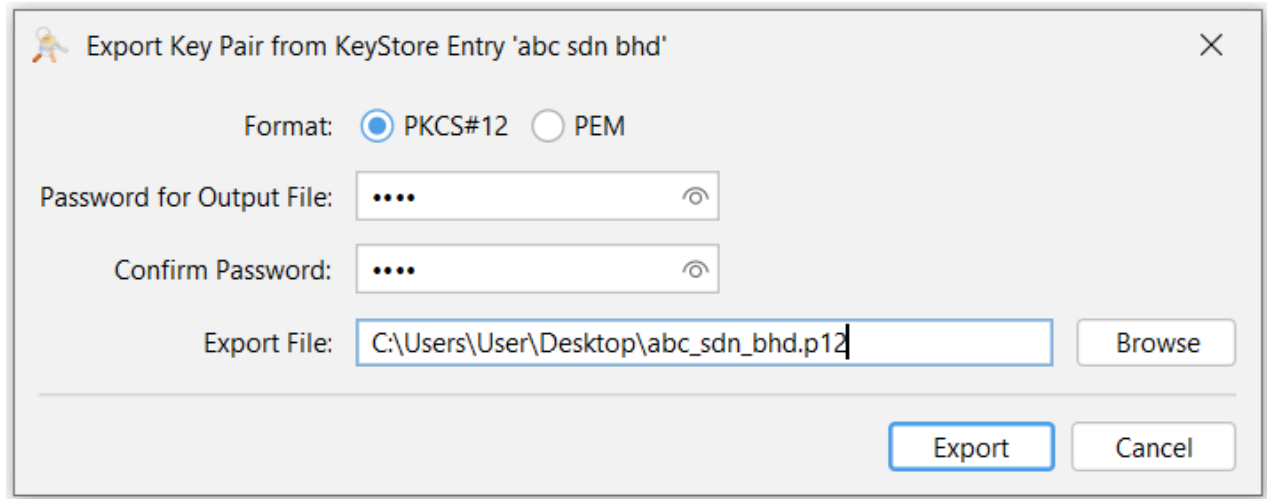
a) KeyStore Explorer

To export key pair to PKCS#12 format.

1. **Select Key Pair:** In the KeyStore Explorer window, locate the key pair you want to export. Right click on the key pair and select 'Export > Export Key Pair'.



2. **Choose Export Format:** A new dialog box will appear asking you to choose the format for exporting the key pair. Leave all the default value as shown in the picture below.
3. **Set a Password:** You need to enter the 'Password for Output File' and 'Confirm Password' in the dialog box appeared. This password will be required to import the certificate and private key from the PKCS#12 file later.
4. **Choose a File Location:** Click the 'Browse' button to locate the location and file name to export your key pair.



5. **Successfully Exported:** The key pair is successfully exported on your PC. Click **OK** button to proceed.



Important Notes:

- **Security:** The PKCS#12 file contains sensitive information (both the private key and certificate), so it's crucial to keep the file secure and protect it with a strong password.
- **Usage:** The exported PKCS#12 file can be used in various applications or systems that require both certificate and the private key.
- **Portability:** PKCS#12 is a widely supported format, so the file can be easily imported into many different environments.

b) OpenSSL

To export key pair in PKCS #12 format.

```
openssl pkcs12 -export -inkey server.key -in server.cer -certfile
intermediate.cer -out server.p12
```

c) Java Key Store (JKS)

To export key pair in PKCS#12 format.

```
keytool -importkeystore -srckeystore keystore.jks -destkeystore  
keystore.p12 -srcstoretype JKS -deststoretype PKCS12 -srcalias  
mykeyalias -deststorepass yourp12password -srcstorepass
```

Kindly replace with your information accordingly:

- 'keystore.jks' with the name of your Java KeyStore file.
- 'keystore.p12' with the desired name of your PKCS#12 file.
- 'mykeyalias' with the alias of the key in your '.jks'.
- 'yourp12password' with the password you want to set for the '.p12' file.
- 'yourjkspassword' with the password of your '.jks'.