eSignTrust Encrypt / Decrypt tool

(Quick Start Manual)

Date: 2017/09/08

Version: 1.6

Contents

1. Introduction

1.1 Description

The tool includes command line and GUI versions, which uses an eSignTrust certificate to encrypt/decrypt a file or a folder.

2. System requirements
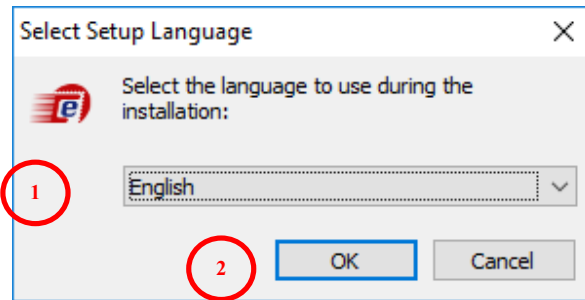
- OS: Windows 7
- Microsoft .net framework: 3.5 or later version.

3. Install eSignTrust Encrypt / Decrypt tool

1. Open eSignTrust Encrypt/Decrypt tool installation file；

2. Select the language during installation；

(1). Select the language；

(2). Press "OK" Button

3. Read and agree the license agreement；
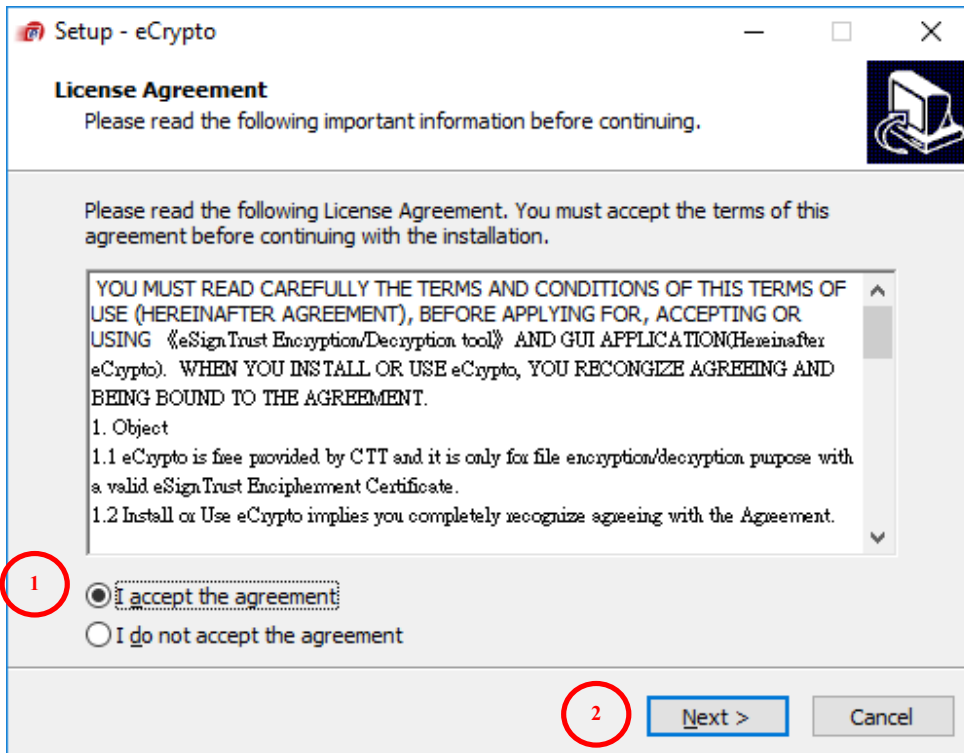
(1). Select "I accept the agreement"；

(2). Click "Next >" Button

4. Select "Create a desktop shortcut"；
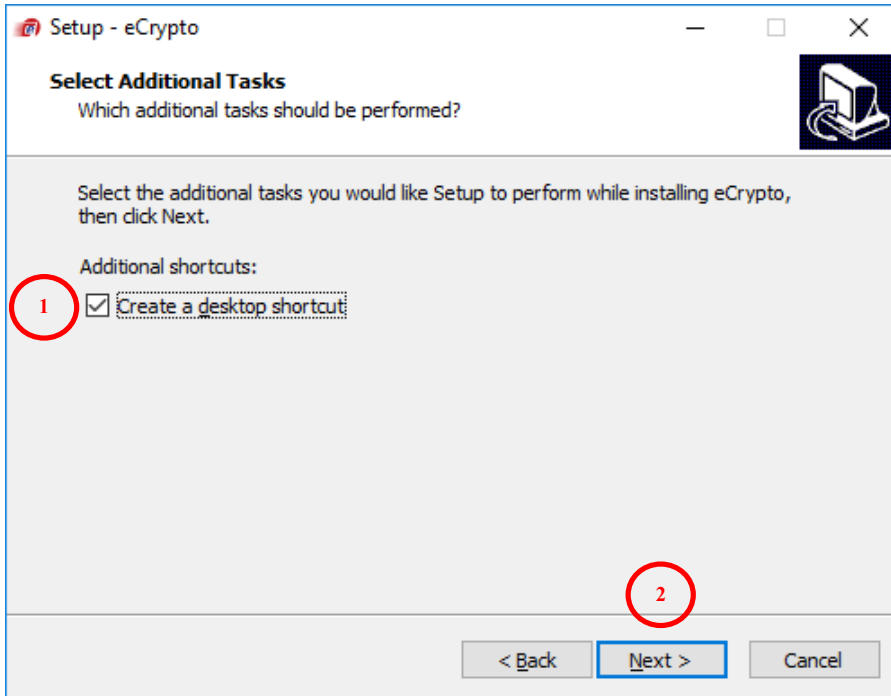
      (1). Select "Create a desktop shortcut"；
      (2). Click "Next >" Button。

5. Click "Install", then will install the eSignTrust Encrypt/Decrypt tool；

6. Click "Finish", to exit the Setup

7. * Please install the smart cart driver if the driver is not installed

4. Command line version

4.1 Command line usage

eCrypto.exe [-E|-D] [certfile option] [-i|-d] source [overwrite file option] [output option] [password option]

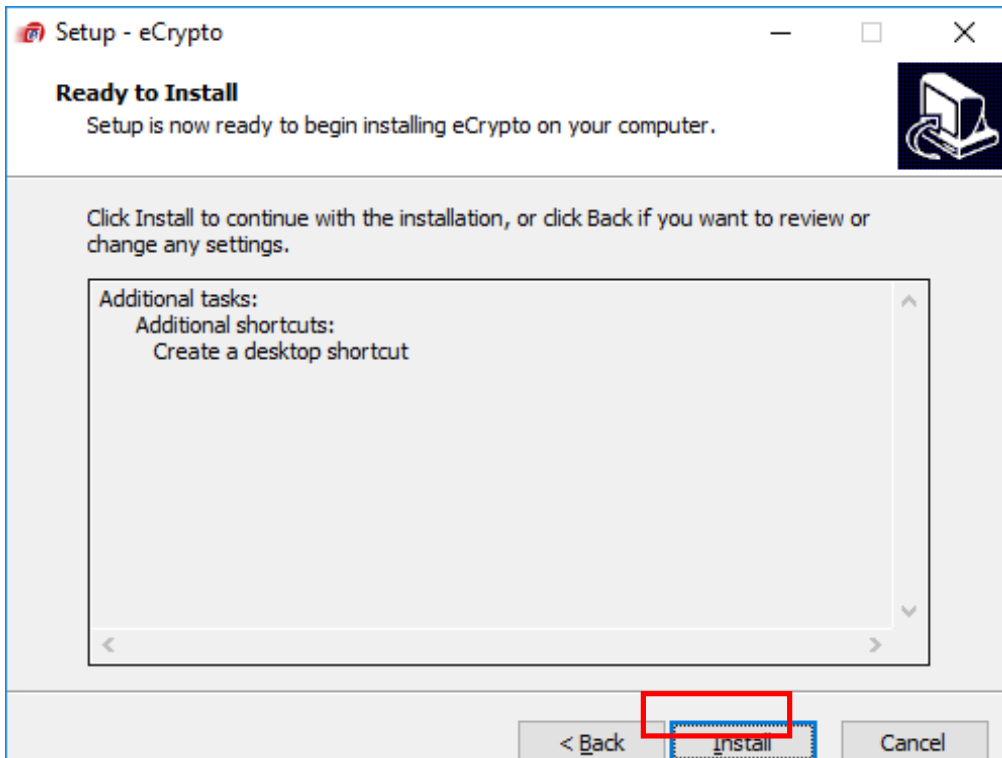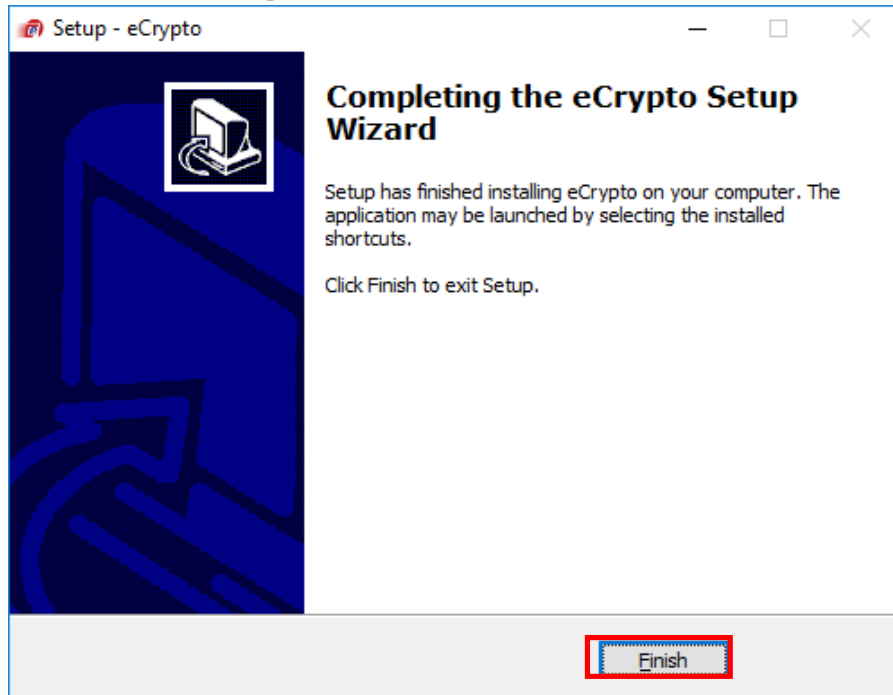| Parameters	Description
-E	Encrypt Mode
-D	Decrypt Mode
[certfile option]	In Encrypt Mode: Should specify the eSignTrust certificate file In Decrypt Mode: It's optional to specify the eSignTrust certificate file
-c certfile	
-i	In Encrypt/Decrypt Mode: A single file parameter
-d	In Encrypt/Decrypt Mode: A folder parameter. (*please see Important notes 3. 4. 5. for details*)
Source	Specify the input path: A single file or a folder
[overwrite file option]	In Encrypt/Decrypt Mode: Optional function for overwriting the output file
-f	If "–f" specifies in the command, then will apply the overwrite file function
[output option]	Only use in a single file syntax: Specify the output path after encryption/decryption
-o output	
[password option]	Only use in Decrypt Mode: Specify eSignTrust certificate password
-p password	

4.2 Command line sample

4.2.1 Encryiption
1) A single file
eCrypto.exe -E -c "c:\cert\eSignTrust.cer" -i "c:\test\test.txt"
The command requires to specify the eSignTrust certificate file to do an encryption process. This tool will add the string "_encrypted" to the end of the filename and also add the .e7e file extension. After encryption, the encrypted file will save in the same directory. In the above command sample, it will encrypt the file and save it in "c:\test\test_encrypted.txt.e7e".

2) A single file with a specified output path
eCrypto.exe -E -c "c:\cert\eSignTrust.cer" -i "c:\test\test.txt" -o "c:\test\test_after_encrypted.txt.e7e"
It is almost same as 1), but it is a little difference that it contains a specified output path in 2) command syntax.

3) A folder

`eCrypto.exe -E -c "c:\cert\eSignTrust.cer" -d "c:\test"`

The command requires to specify the eSignTrust certificate file to do an encryption process. This tool will create a subfolder "output" and the encrypted files will save in the subfolder. The tool only encrypts non .e7e format file. For each encrypted file, it will add the string "_encrypted" to the end of every filename and also add the .e7e file extension.

4.2.2 Decryption

1) A single file

- Without a certificate

`eCrypto.exe -D -i "c:\test\test_encrypted.txt.e7e" -p password`

- With a certificate

`eCrypto.exe -D -c "c:\cert\eSignTrustDecrypt.pfx" -i "c:\test\test_encrypted.txt.e7e" -p password`

This tool will add the string "_decrypted" to the end of the filename and also remove the .e7e file extension. After decryption, the decrypted file will save in the same directory. In the above command sample, it will decrypt the file and save it in "c:\test\test_encrypted_decrypted.txt".

2) A single file with a specified output path

- Without a certificate

`eCrypto.exe -D -i "c:\test\test_encrypted.txt.e7e" -o "c:\test\test_decrypted.txt" -p password`

- With a certificate

`eCrypto.exe -D -c "c:\cert\eSignTrustDecrypt.pfx" -i "c:\test\test_encrypted.txt.e7e" -o "c:\test\test_decrypted.txt" -p password`

It is almost same as 1), but it is a little difference that it contains a specified output path in 2) command syntax.

3) A folder

- Without a certificate

`eCrypto.exe -D -d "c:\test\encrypted" -p password`

- With a certificate

`eCrypto.exe -D -c "c:\cert\eSignTrustDecrypt.pfx" -d "c:\test\encrypted" -p password`

The tool will decrypt all the .e7e format files in the specified folder and all the decrypted files save in the "output" subfolder. For each decrypted file, it will add the string "_decrypted" to the end of every filename and also remove the .e7e file extension. In the above command sample, it will save in "c:\test\encrypted\output"
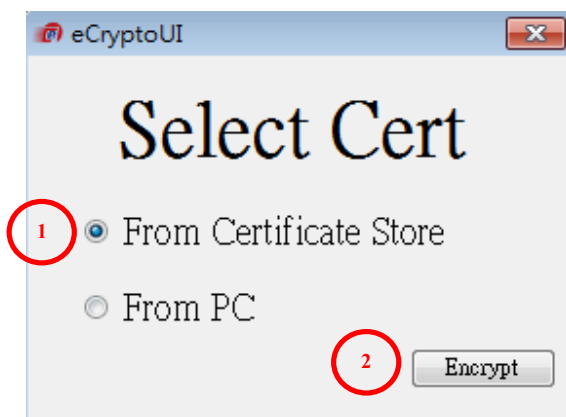
5. GUI version
5.1 Encryption
1. Insert a smart card with an encryption certificate；
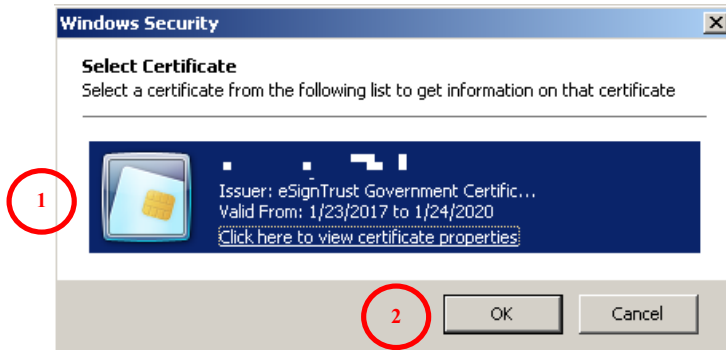
2. Open eSignTrust tools Menu；
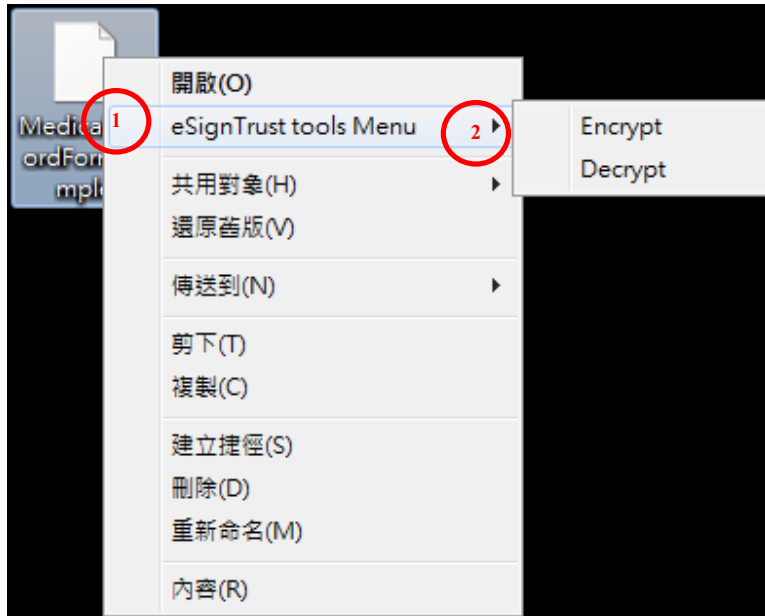
(1). For the Encrypt file, please right click a mouse and select "eSignTrust tools Menu"；
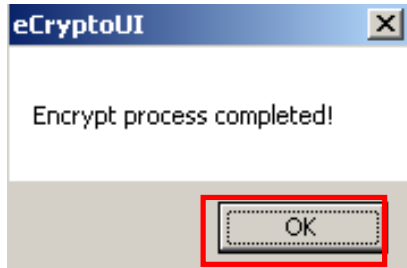(2). Click "Encrypt"

3. Select a source for the certificate；

(1). Select "From Certificate Store"；
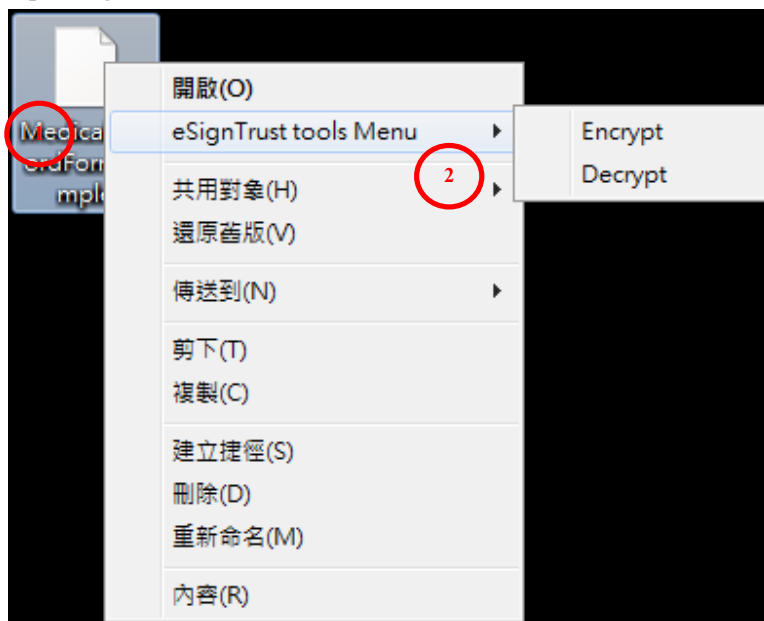(2). Click "Encrypt"

4. Select a certificate for encryption；

(1). Select a certificate；
(2). Click "OK"

5. The program will generate an encrypted file (ext. e7e). Please click "OK" to finish the encrypt process.
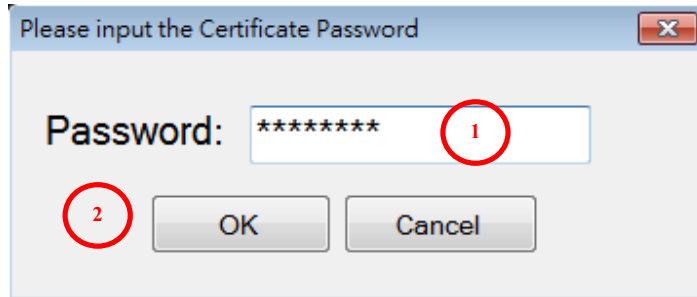

5.2 Decryption

1. Insert a smart card with a corresponding certificate for the encrypted file；
2. Open SignTrust tools Menu；

(1). For the Encrypted file, please right click a mouse and select "eSignTrust tools Menu；
(2). Click "Decrypt"

3. Input the smart card's password；
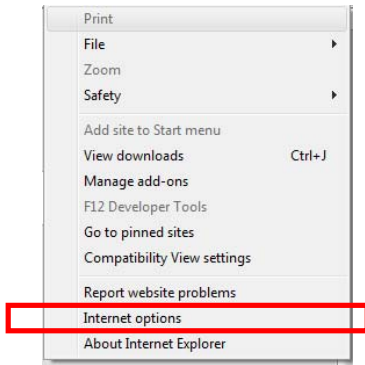

(1). Input the smart card's password；
(2). Click "OK"

4. The program will generate a decrypted file. Please click "OK" to finish the decrypt process.
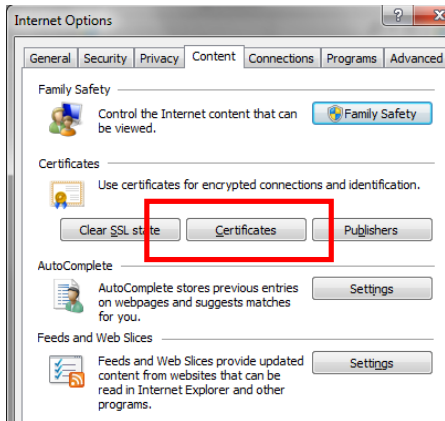
6. Export eSignTrust certificate from IE
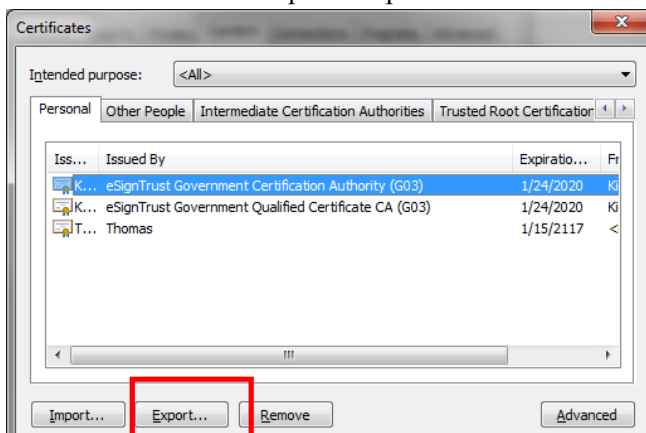
1. Open IE

2. In IE menu, choose "Internet options"

3. In Content page, choose "Certificates"

4. Choose a certificate and press Export button
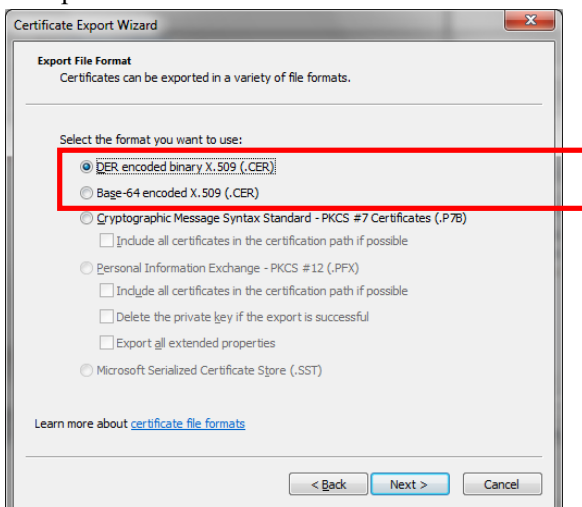
5. IE will prompt a "Certificate Export Wizard window", then press Next button
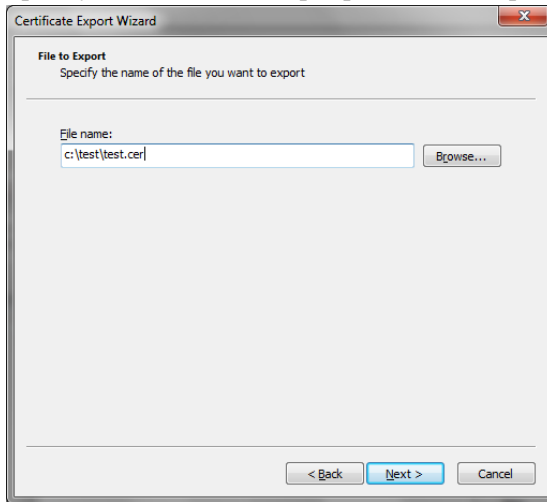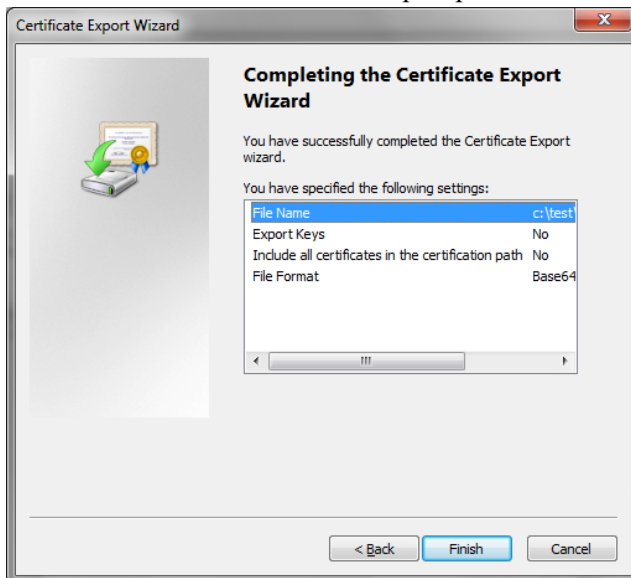

6. Press next button
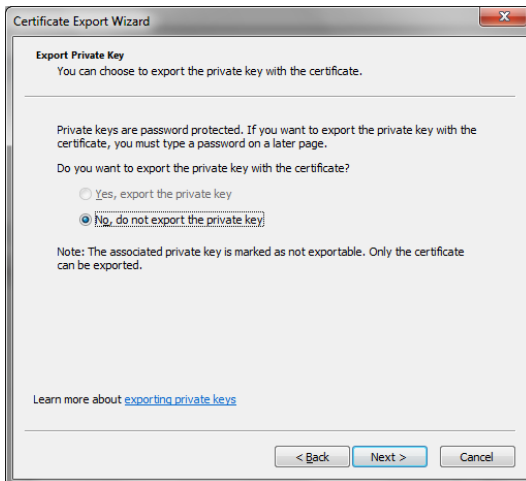
7. Choose either one of DER encoded binary X.509 (.CER) and Base-64 encoded X.509 (.CER) option, then press Next button

8. Specify the certificate output path, for example: c:\test\test.cer

9. Press Finish button to finish the export process

7. Important notes (for command line)

1. Only use any non-expired eSignTrust certificate during encryption.

2. Please add the double quotation marks (") around the file path of a certificate / file / folder in encryption / decryption syntax. For example: if the file is c:\test\test.txt, then input the syntax "c:\test\test.txt".

3. In Encrypt mode, this tool will only encrypt Non .e7e format file. In decrypt mode, the tool will only decrypt .e7e file extension file.

4. This tool only encrypts/decrypts all the files under the folder, but it will exclude any files in each subfolder.

5. In a folder mode, the tool will auto generate a subfolder "output" and the encrypted/decrypted files will save in the subfolder.

6. It is required to input an eSignTrust certificate path in encryption command syntax.

7. It is required to input an eSignTrust certificate password in decryption command syntax.

8. Common Error messages (for command line)
8.1 Encryption

1. Error: It is not a valid eSignTrust Certificate

   Please use a non-expired eSignTurst certificate.

2. Error: This is not a valid certificate or the certificate file does not exist

   The certificate is not a valid certificate format or the file does not exist.

8.2 Decryption

1. Error: Cannot load any cert!

   Please make sure the smart card is inserted on the card reader and check the smart card whether contains the right certificate for the encrypted file. Also, please install the correct drivers of the smartcard and the smartcard reader.

2. Error: The encrypted file is not valid!

   Please check the encrypted file whether it was encrypted by the tool.

3. Error: System cannot find a valid smart card, or the drivers of the smartcard and its reader are not installed

   Please make sure the smart card is inserted on the card reader and check the smartcard whether contains the right certificate for the encrypted file. Also, please install the correct drivers of the smartcard and the smartcard reader.

4. Error: Cannot access the certificate

   Please input the correct smartcard's certificate password and insert the correct smartcard.

--End--