eSignTrust 加密/解密小工具

入門指南

(Quick Start Manual)

日期: 2025/03/03

版本: 1.7

目錄

1. 簡介

1.1 簡介

本工具為使用 eSignTrust 電子證書進行加密/解密檔案的小工具，包括有命令行版本及圖形用户介面(GUI)版本。

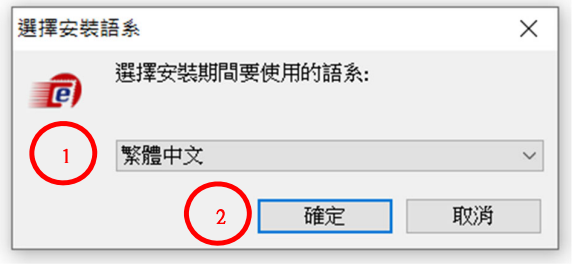
2. 系統要求

作業系統為 Windows 10 或 11，並且需安裝 Microsoft .net framework 3.5 版本或以上

3. 安裝 eSignTrust 加密/解密小工具

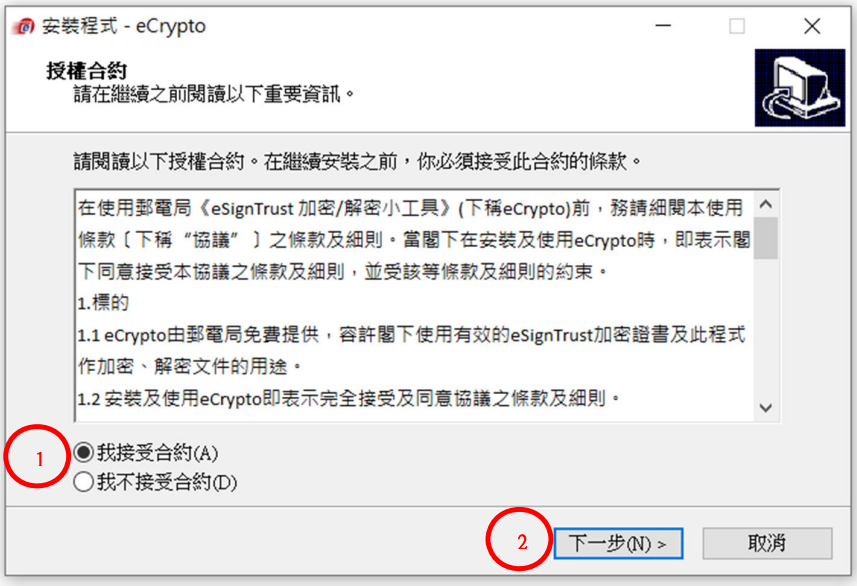
1. 打開 eSignTrust 加密/解密小工具安裝文件；

2. 選擇安裝過程的語言；



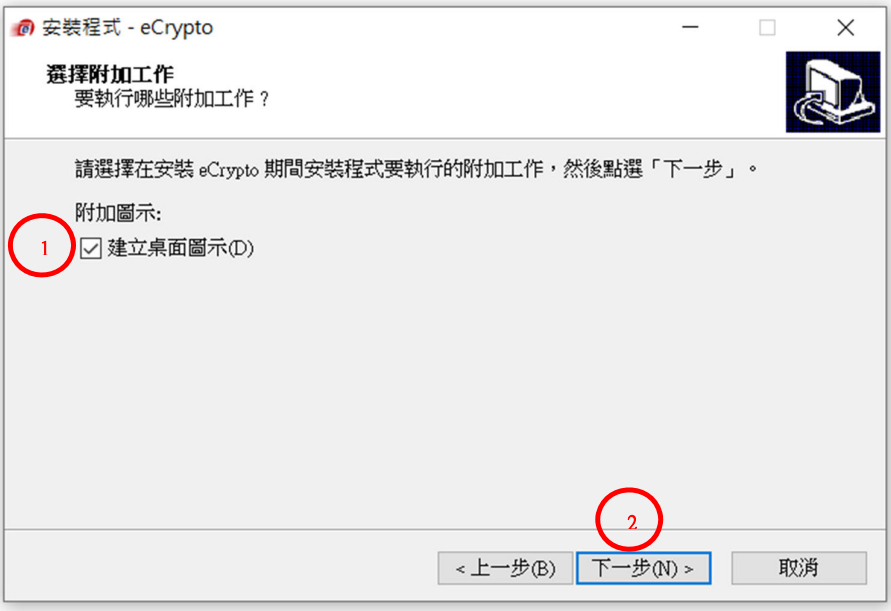
(1). 選擇語言；
(2). 點擊 “確定” 按鈕。

3. 閱讀並接受合約條款；



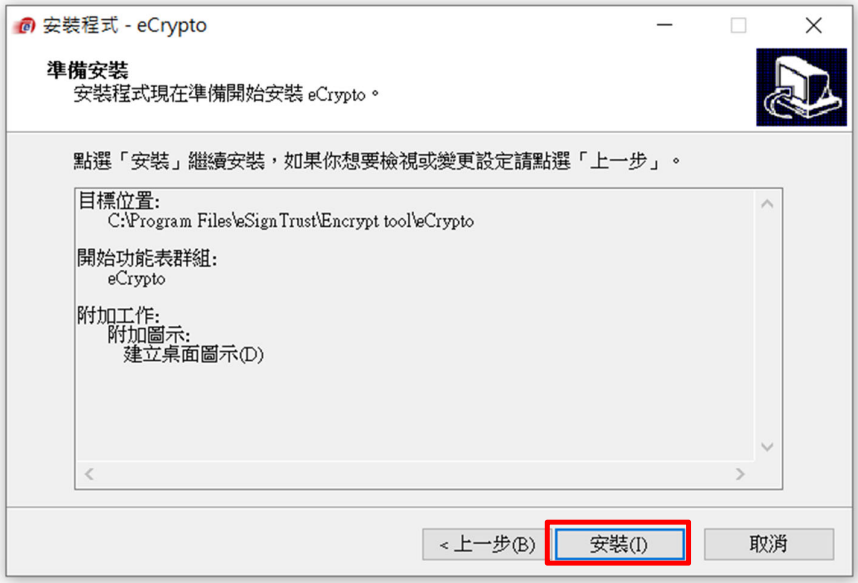
(1). 選擇 “我接受合約” ；
(2). 點擊 “下一步” 按鈕。

4. 選擇 “建立桌面圖示” ；



(1). 勾擇 “建立桌面圖示” ；
(2). 點擊 “下一步” 按鈕。

5. 點擊 “安裝” ，開始安裝 eSignTrust 加密/解密小工具；



6. 點擊 “完成” ，安裝完成。

7. 如未安裝智能卡驅動程式，請安裝智能卡驅動程式。

4. 命令行版本介紹

4.1 指令用法

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

參數	說明
-E	加密模式
-D	解密模式
[certfile option]	在加密模式下，必需指定加密所使用的 eSignTrust 電子證書 在解密模式下，可選擇是否指定解密所使用的 eSignTrust 電子證書
-c certfile	
-i	加密/解密模式下指定加密/解密單一檔案的參數
-d	加密/解密模式下指定加密/解密一個資料夾的參數 (程式進行加密時，只對該資料夾內副檔名非為.e7e 的所有檔案(不包括子資料夾內的檔案) 進行加密；而解密時，只對該資料夾內副檔名為.e7e 的所有檔案 (不包括子資料夾內的檔案)進行解密
source	指定所讀取的單一檔案/資料夾的路徑
[overwrite file option]	加密/解密模式下，指定是否要覆蓋輸出檔案
-f	若指令含有"**-f**"字串，即表示允許覆蓋檔案；否則不允許覆蓋輸出檔案
[output option]	只適用於加密/解密單一檔案的選項，指定加密/解密檔案的輸出路徑
-o output	
[password option]	只適用於解密模式，指定該 eSignTrust 電子證書的密碼
-p password	

4.2 指令範例

4.2.1 加密

1) 單一檔案

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

指定 eSignTrust.cer 電子證書，並對 test.txt 進行加密，加密後的檔案會自動放在同一資料夾內，而檔案名稱會根據原檔案名稱後加上"_encrypted"的字串，而副檔名會改為.e7e。上述範例執行後，所生成加密的檔案會存放於"c:\test\test_encrypted.txt.e7e"。

2) 單一檔案及指定輸出檔案路徑

```
eCrypto.exe -E -c "c:\cert\eSignTrust.cer" -i "c:\test\test.txt" -o
"c:\test\test_after_encrypted.txt.e7e"
```

同 1)指令情況差不多，而不同的是 2) 的指令多加了指定輸出檔案路徑的參數。

3) 資料夾

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

指定 eSignTrust.cer 電子證書，並對資料夾" c:\test "內副檔案非為.e7e 的所有檔案進行加密，加密後的檔案會自動存放於原路徑下的 output 資料夾，而所有加密後的檔案名稱後會加上"_encrypted"的字串，副檔名並會改為.e7e。上述範例執行後，加密的檔案會存放於"c:\test\output"裡。

4.2.2 解密

1) 單一檔案

- 沒有指定證書

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

- 指定證書

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

對 test_encrypted.txt.e7e 進行解密，解密後的檔案會自動放在同一資料夾內，而檔案名稱會根據原檔案名稱後加上"_decrypted"的字串，並移除副檔名.e7e。上述範例執行後，所生成解密的檔案會存放於"c:\test\test_encrypted_decrypted.txt"。

2) 單一檔案及指定輸出檔案路徑

- 沒有指定證書

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

- 指定證書

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

同 1)指令情況差不多，而不同的是 2) 的指令多加了指定輸出檔案路徑的參數。

3) 資料夾

- 沒有指定證書

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

- 指定證書

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

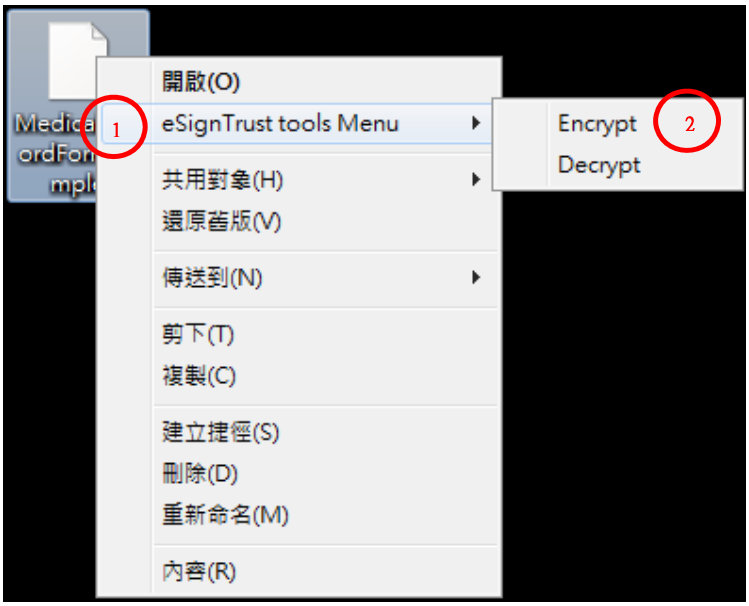
對資料夾" c:\test\decrypted "內副檔案為.e7e 的所有檔案進行解密，解密後的檔案會自動存放於原路徑下的 output 資料夾，而所有解密後的檔案名稱後會加上"_decrypted"的字串，並會移除副檔名.e7e。上述範例執行後，解密的檔案會存放於"c:\test\encrypted\output"裡。

5. GUI 版本介紹

5.1 加密文件

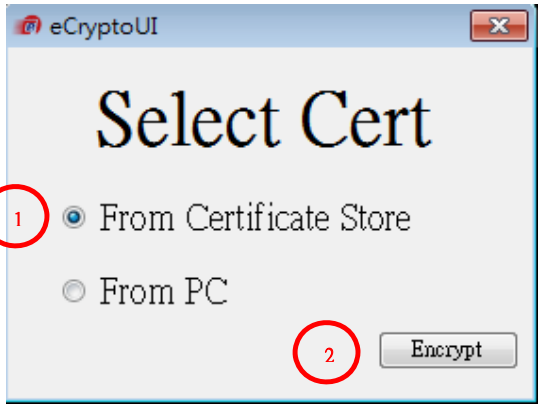
1. 插入具有加密證書的智能卡；

2. 打開加密功能選單；



(1). 在需要加密文件，點擊右鍵，點擊 “eSignTrust tools Menu” ；
(2). 點擊 “Encrypt” 。

3. 選擇證書來源；

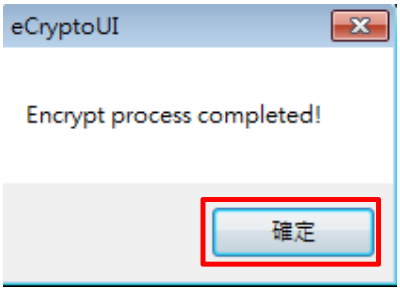


(1). 選擇 “From Certificate Store” ；
(2). 點擊 “Encrypt” 。

4. 選擇加密證書；

(1). 選擇加密證書；
(2). 點擊 “確認” 。

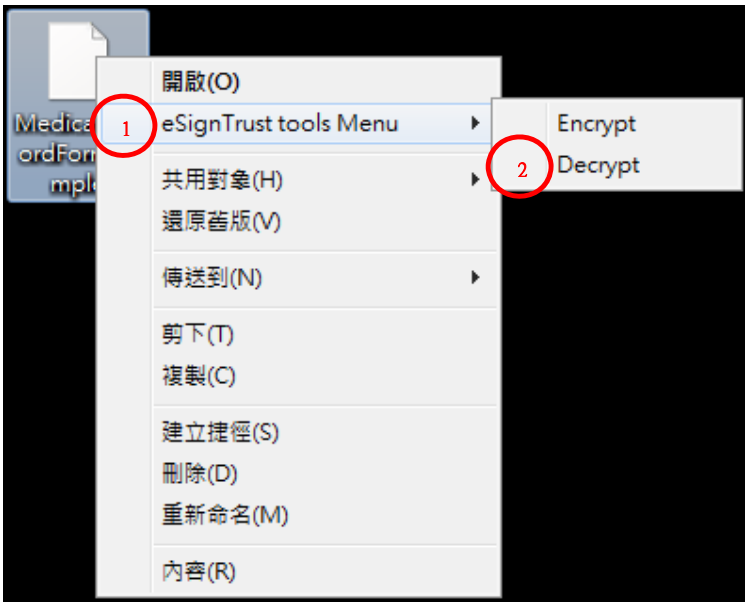
5. 產生一個後綴為 “e7e” 的加密文件，提示加密成功，點擊 “確定” 完成加密。



5.2 解密已加密的文件

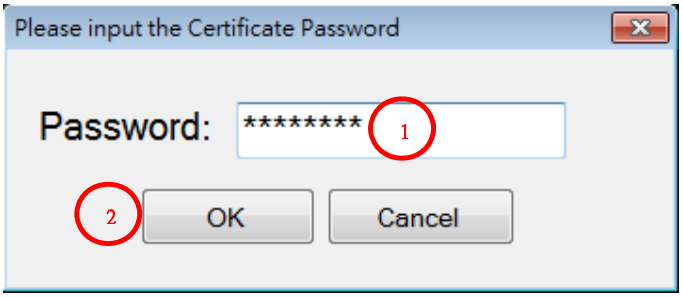
1. 插入具有對應解密證書的智能卡；

2. 打開解密功能選單；



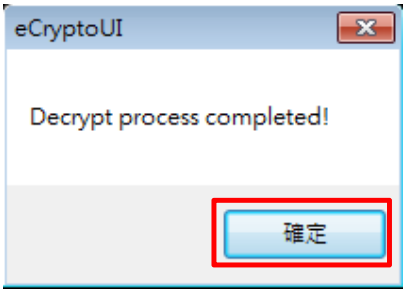
(1). 在後綴為 “e7e” 的加密文件，點擊右鍵，點擊 “eSignTrust tools Menu” ；
(2). 點擊 “Decrypt” 。

3. 填寫智能卡密碼；



(1). 填寫智能卡密碼；
(2). 點擊 “OK” 。

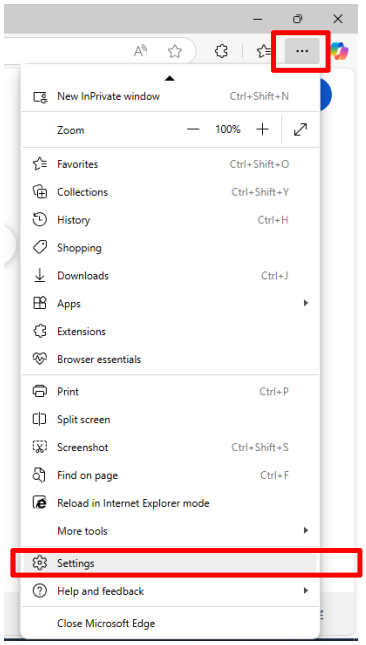
4. 產生解密後的原文件，提示解密成功，點擊 “確定” 完成解密。

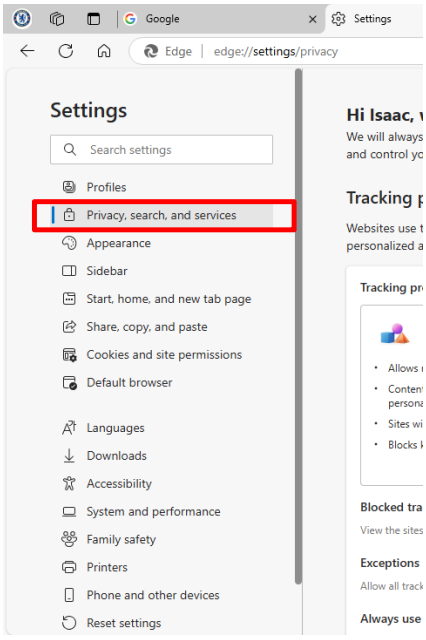


6. 匯出 eSignTrust 證書操作步驟

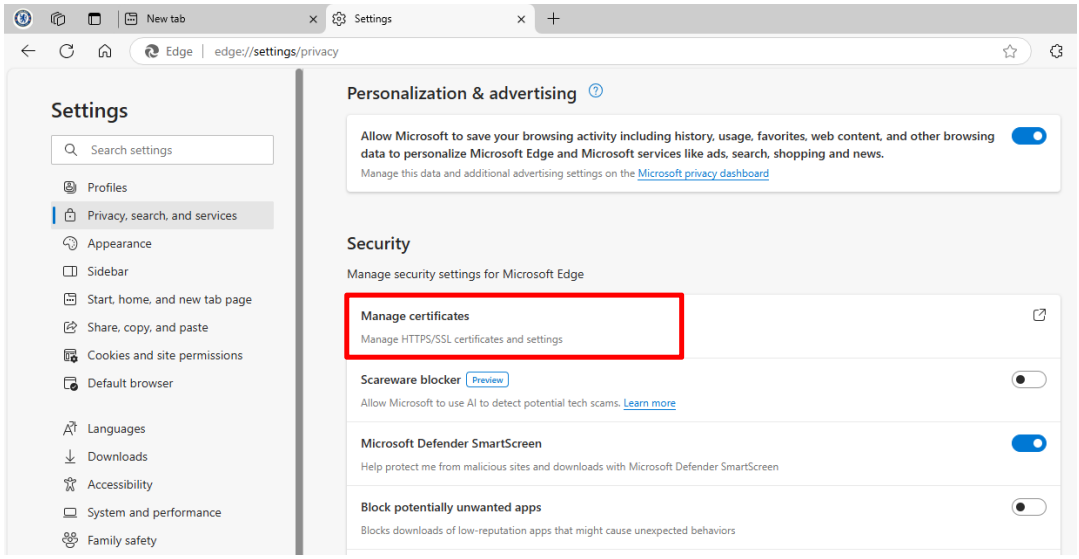
1. 開啟 Microsoft Edge 瀏覽器

2. 在 Menu 選項選擇 “設定” -> “私隱權、搜尋與服務”

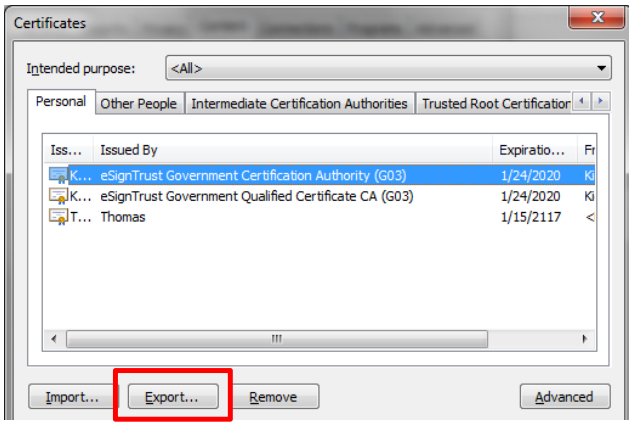




3. 在 “安全性” 項目內，選擇 “管理證書”

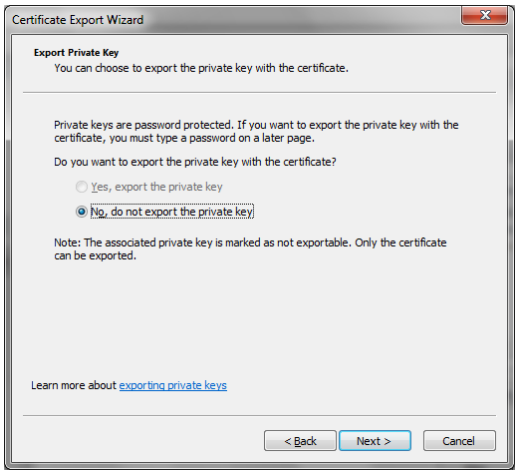


4. 選取欲要匯出的 eSignTrust 證書，並按 Export 按鈕

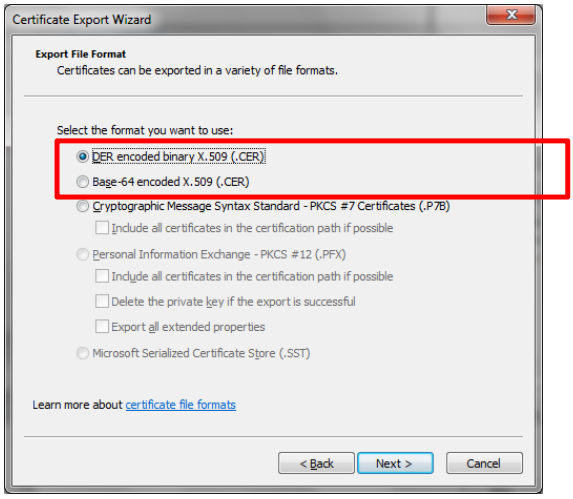


5. IE 彈出 Certificate Export Wizard 視窗，按下 Next 按鈕

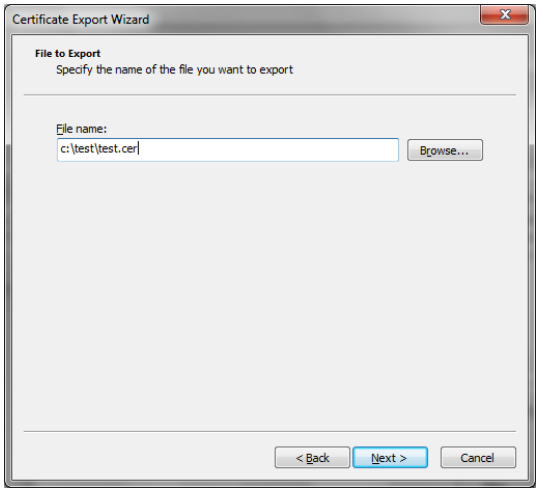
6. 按下 Next 按鈕



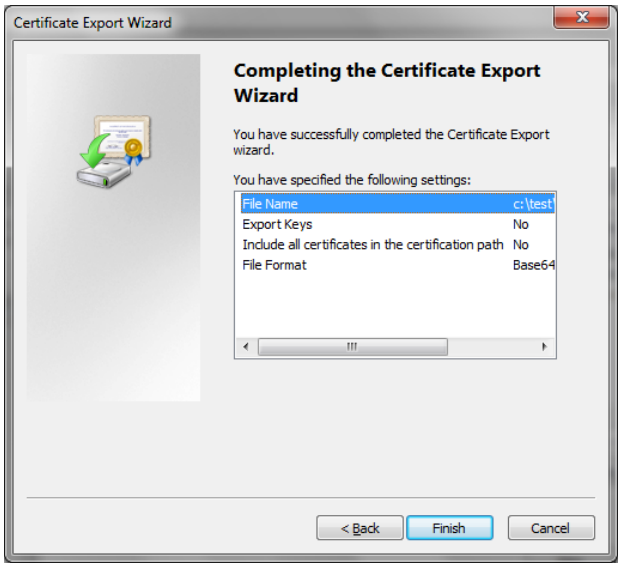
7. 可任一選擇 DER encoded binary X.509 (.CER) 或 Base-64 encoded X.509 (.CER)的選項，然後按下 Next 按鈕



8. 指定該電子證書的輸出路徑，如輸出路徑為 c:\test\test.cer



9. 按下 Finish 按鈕，完成匯出電子證書的操作



7. 注意事項 (限命令行版本)

1. 加密所使用的證書只能為非過期的 eSignTrust 電子證書，其他任何電子證書均無法使用。
2. 在使用本工具輸入加密/解密指令時，所指定的證書、檔案的路徑的字串前後需分別加上引號"，如路徑為 c:\test\test.txt，則輸入該路徑為"c:\test\test.txt"。
3. 本工具只會對非為.e7e 檔案進行加密，而解密時只對.e7e 的檔案進行解密。
4. 加密/解密資料夾的功能只對該資料夾下的所有檔案進行加密/解密的程序，而該資料下其他子資夾內的任何資料夾或檔案並不會處理。
5. 加密/解密資料夾的輸出路徑會自動存放於該資料夾下的 output 資料夾。
6. 加密指令需輸入 eSignTrust 電子證書的檔案路徑。
7. 解密指令需輸入被加密檔案所用到的 eSignTrust 電子證書的密碼。

8. 常見的錯誤提示 (限命令行版本)

8.1 加密

1. Error: It is not a valid eSignTrust Certificate

   請使用非過期的 eSignTrust 電子證書。

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

   該電子證書並不是有效的電子證書檔案，或該檔案並不存在

8.2 解密

1. Error: Cannot load any cert!

   請檢查是否有插入智能卡，及安裝智能卡及讀卡器的驅動程式。

2. Error: The encrypted file is not valid!

   請檢查該檔案是否曾使用 eSignTrust 電子證書進行加密的程序。

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

   請檢查是否有插入智能卡，及安裝智能卡及讀卡器的驅動程式。

4. Error: Cannot access the certificate

   請檢查是否已輸入正確的智能卡密碼，並插入正確的智能卡。

----------結束----------