

# eSignTrust 加密/解密小工具 入門指南

# (Quick Start Manual)

日期: 2025/03/03

版本: 1.7

本文件之版權乃屬於澳門特別行政區郵電局電子認證服務,任何未經本機構同意對本文或本文內容之複製、儲存、傳送 及其他未提及的侵權行為,將視為對本文件版權的侵犯,本機構保留對此等行為採取法律追究的權利。本文件內容的擁 有權乃屬於澳門特別行政區郵電局電子認證服務,其內容為機密並只向文件接收者透露。

# 目錄

1.	簡	節介…	
	1.1	f	簡介3
2.	系	統要	要求
3.	安	<del>Z</del> 裝 E	ESIGNTRUST 加密/解密小工具4
4.	命	命令行	行版本介紹
	4.1	ł	指令用法7
	4.2	ł	指令範例7
	4.	.2.1	加密7
	4.	.2.2	解密8
5.	G	SUI 版	反本介紹9
	5.1	t	加密文件9
	5.2	<u>ا</u>	解密已加密的文件10
6.	匯	重出 E	ESIGNTRUST 證書操作步驟12
7.	注	E意事	事項 (限命令行版本)15
8.	常	常見的	的錯誤提示 (限命令行版本)
	8.1	t	加密16
	8.2	角	解密16

# 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;

選擇安裝	語系	×
ē	選擇安裝期間要使用的語系:	
	繁體中文	~
	2 確定 取》	肖

(1). 選擇語言;

(2). 點擊"確定"按鈕。

3. 閱讀並接受合約條款;

⑦ 安裝程式 - eCrypto	_		×
授權合約 請在繼續之前閱讀以下重要資訊。			J.
請閱讀以下授權合約。在繼續安裝之前,你必須接受此合約的條款。			
在使用郵電局《eSignTrust 加密/解密小工具》(下稱eCrypto)前,務請 條款〔下稱"協議"〕之條款及細則。當閣下在安裝及使用eCrypto時 下同意接受本協議之條款及細則,並受該等條款及細則的約束。 1.標的 1.1 eCrypto由郵電局免費提供,容許閣下使用有效的eSignTrust加密證 作加密、解密文件的用途。 1.2 完裝及使用oCounton表示完全接受及同意接送之條款及細則。	///	用 ^ 、 閣	
1 ●我接受合約(A) ①我不接受合約(D)	>	~ 取消	Ĵ

- (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";

⑦ 安裝程式 - eCrypto     ◎	_		×
<b>選擇附加工作</b> 要執行哪些附加工作?			
請選擇在安裝 eCrypto 期間安裝程式要執行的附加工作,然後點選「 附加圖示:  1 ☑ 建立桌面圖示(D)	下一步」	•	
<上一步(B) 下一步(	< (N	取	消

- (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;

🔊 安裝程式 - eCrypto -		×
<b>準備安裝</b> 安裝程式現在準備開始安裝 eCrypto。	c	
點選「安裝」繼續安裝,如果你想要檢視或變更設定請點選「上一步」。		
目標位置: C:\Program Files\eSignTrust\Encrypt tool\eCrypto	^	,
開始功能表群組: eCrypto		
附加工作: 附加圖示: 建立桌面圖示(D)		
<	>	,
<上一步(B) 安裝(I) 安裝(I)	取	消

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
-Е	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)指令情况差不多,而不同的是 2)的指令多加了指定輸出檔案路 徑的參數。 eSignTrust 加密/解密小工具--入門指南(Quick Start Manual)

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;

	開啟(O)	_	
Medica 1	eSignTrust tools Menu	•	Encrypt 2
mpk	共用對象(H)	•	Decrypt
	還原舊版(V)		
	傳送到(N)	•	
	剪下(T)		
	複製(C)		
	建立捷徑(S)		
	刪除(D)		
	重新命名(M)		
	內容(R)		

(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;



4. 選擇加密證書;

	Windows 安全性
	Select Certificate Select a certificate from the following list to get information on that certificate
1	登録者: eSignTrust Government C 有效期自: 20/2/2017 到 21/2/2020 按一下此處,檢視憑證內容
	2 確定 取満

(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。

eCryptoUI	×
Encrypt process complete	d!
確況	È

#### 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;

	開啟(O)	
Medica 1	eSignTrust tools Menu	Encrypt
mpk	共用對象(H)	2 Decrypt
	還原舊版(V)	
	傳送到(N)	•
	剪下(T)	
	複製(C)	
	建立捷徑(S)	
	刪除(D)	
	重新命名(M)	
	內容(R)	

(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;

Please input the Certificate Password	×
Password:	
2 OK Cancel	

(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。

eCryptoUI	×
Decrypt process complete	ed!
T	定

Hi Isaac, v

We will always

and control yo

Tracking F

Websites use t

personalized a

Tracking pr

Allows i

Content
 persona

Sites wi

Blocks I

Blocked tra

View the sites

Exceptions

Allow all track

Always use

### 6. 匯出 eSignTrust 證書操作步驟

- 開啟 Microsoft Edge 瀏覽器 1.
- 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"

۲	Ô	New tab	× 🕄 Settings × +	
$\leftarrow$	С	C Edge   edge://settings	/privacy	☆ <b>3</b>
	Set	tings	Personalization & advertising <sup>©</sup>	
	٩	Search settings	Allow Microsoft to save your browsing activity including history, usage, favorites, web content, and other browsing data to personalize Microsoft Edge and Microsoft services like ads, search, shopping and news.	
	8	Profiles	Manage this data and additional advertising settings on the Microsoft privacy dashboard	
	Ô	Privacy, search, and services		
	6	Appearance	Security	
		Sidebar	Manage security settings for Microsoft Edge	
	Ē	Start, home, and new tab page		c7
	e	Share, copy, and paste	Manage ertificates Manage HTTPS/SL certificates and settings	9
	<b>•</b>	Cookies and site permissions	manage in in opour countace and seconds	
	G	Default browser	Scareware blocker Preview Allow Microsoft to use Al to detect potential tech scams. Learn more	
	A¶,	Languages	Missaade Defender SmartGreen	
	$\underline{\downarrow}$	Downloads	Help protect me from malicious sites and downloads with Microsoft Defender SmartScreen	-
	Ŷ	Accessibility		
		System and performance	Block potentially unwanted apps	$\bullet$
	썅	Family safety	Blocks downloads of low-reputation apps that might cause unexpected behaviors	

4. 選取欲要匯出的 eSignTrust 證書,並按 Export 按鈕

Certificates									
Intended p	tended purpose: <a>l&gt;</a>								
Personal	Other People Intermediate Certification Authorities Trusted Ro	ot Certification	4						
Iss	Issued By	Expiratio	Fr						
К	eSignTrust Government Certification Authority (G03)	1/24/2020	Ki						
БК	eSignTrust Government Qualified Certificate CA (G03)	1/24/2020	Кі						
🛛 🛱 т	Thomas	1/15/2117	<						
•	III		•						
Import	. Export Remove	<u>A</u> dvan	iced						

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

Certificate Export Wizard	
Export File Format Certificates can be exported in a variety of file formats.	
DEE encoded binary X, 509 (CEB)	
Base-64 encoded X.509 (.CER)	
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P78)     Include all certificates in the certification path if possible     Personal Information Exchange - PKCS #12 (.PFX)     Include all certificates in the certification path if possible     Delete the private key if the export is successful     Export all extended properties     Microsoft Sensilized Certificate Store (.SST)	
Learn more about <u>certificate file formats</u>	
< Back Next > Cancel	

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

Certificate Export Wizard		×		
Completing the Certificate Export Wizard				
	You have successfully completed the Certificate Export wizard.			
	You have specified the following settings:			
	File Name	c:\test		
	Export Keys	No		
	Include all certificates in the certification path	No		
	File Format	Base64		
	<	4		
	< Back Finish	Cancel		

第14頁,共16頁

### 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。
- 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。
- 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

- 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

- 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。
- 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。

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。