

# 安全電子郵件憑證 *S/MIME*

Thunderbird 憑證匯入、安裝、應用手冊

版本 1.1

中華電信股份有限公司

中華民國 110 年 02 月 24 日

## 目 錄

|     |                               |    |
|-----|-------------------------------|----|
| 1.  | 前置準備工作 .....                  | 1  |
| 2.  | 初次設定作業 .....                  | 2  |
| 2.1 | 安裝 THUNDERBIRD 軟體.....        | 2  |
| 2.2 | 開啟並設定帳號.....                  | 3  |
| 2.3 | 設定[軟體型] S/MIME 憑證 .....       | 5  |
| 2.4 | 設定[IC 卡片/裝置型] S/MIME 憑證 ..... | 8  |
| 2.5 | 設定帳號之 S/MIME 簽章憑證.....        | 11 |
| 3.  | 郵件簽章/加密應用流程.....              | 15 |
| 3.1 | 郵件簽章.....                     | 15 |
| 3.2 | 郵件加密.....                     | 15 |
| 3.3 | 檢視郵件簽章.....                   | 17 |

### 修訂歷程表

| 版次  | 發佈日期      | 修訂內容摘要                   | 修訂者 |
|-----|-----------|--------------------------|-----|
| 1.0 | 109/11/20 | 初版。                      | 黃柏舜 |
| 1.1 | 110/2/24  | 新增：<br>1. IC 卡憑證匯入與使用指引。 | 黃柏舜 |
|     |           |                          |     |
|     |           |                          |     |

# 1. 前置準備工作

## [軟體型] S/MIME 憑證

(一) 已前往 <https://hikey.hinet.net/gra/>

申請取得軟體型 S/MIME 憑證 pfx 檔案

## [IC 卡片/裝置型] S/MIME 憑證

請先備妥以下軟硬體環境：

(一) 已申請取得內含 S/MIME 憑證 IC 卡。

(二) IC 卡讀卡機一台。

(三) 安裝 HiCOS 卡片管理工具。

(官網連結下載: [http://moica.nat.gov.tw/download\\_1.html](http://moica.nat.gov.tw/download_1.html))

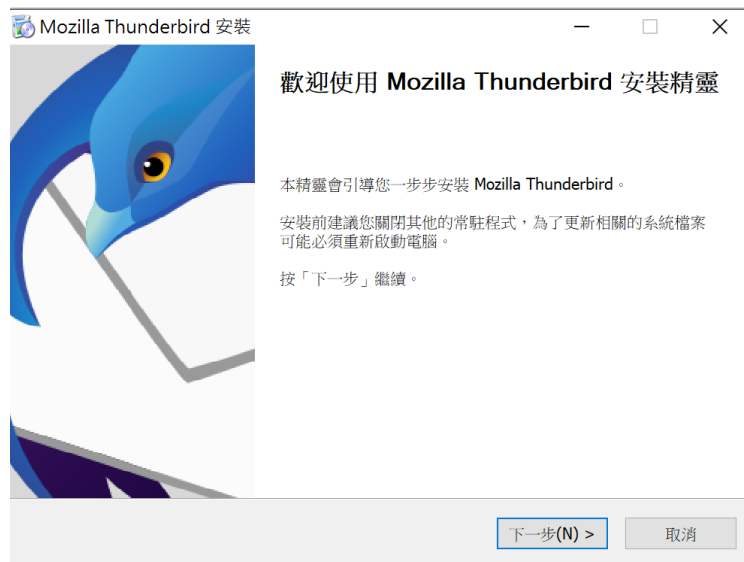
## 2. 初次設定作業

### 2.1 安裝 Thunderbird 軟體

(一) 前往[下載 Thunderbird 軟體](http://moztw.org/thunderbird/)。



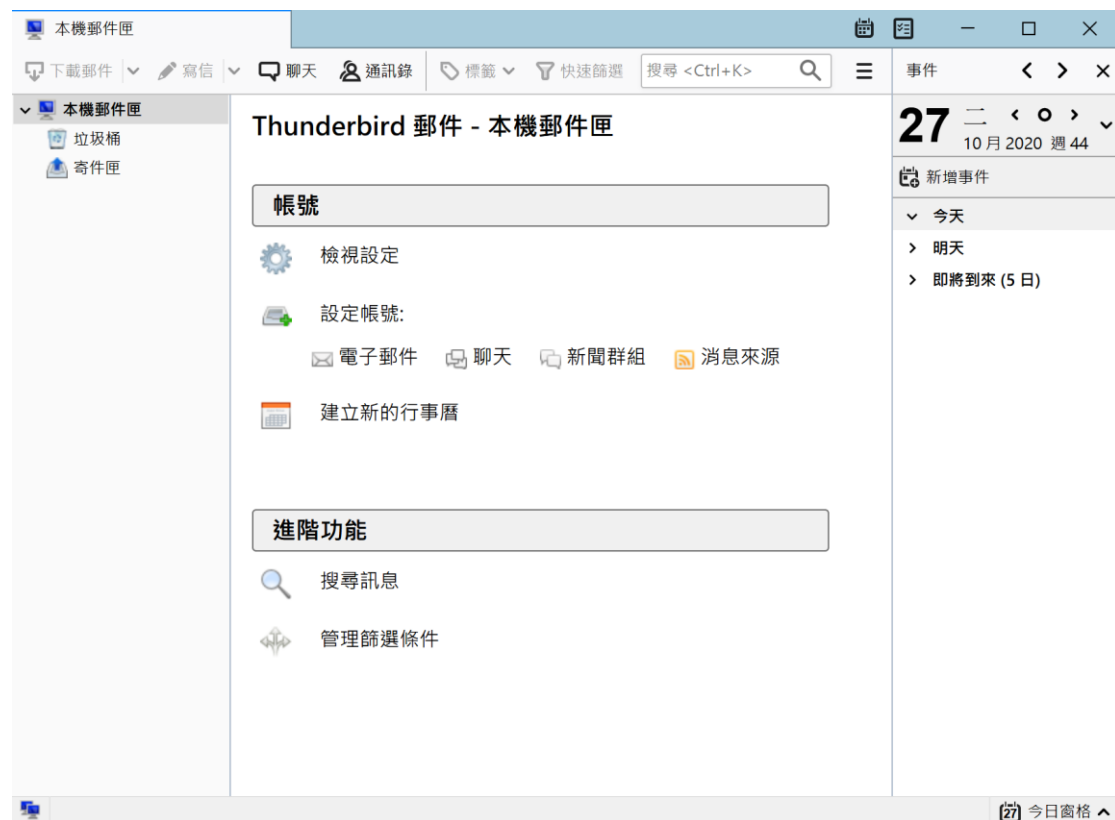
(二) 進行安裝。





## 2.2 開啟並設定帳號

### 1. 開啟軟體



## 2. 設定郵件帳號 (以 Gmail / G-Suite 為例)

加入現有郵件帳號

您的大名 (N): 黃小橋 您的名字，用於顯示在您的郵件上

電子郵件地址 (L): gmpp@csie.io 您目前的電子郵件地址

密碼 (P): ●●●●●●●●●●

記住密碼 (M)

從 Mozilla ISP 資料庫找到以下設定

IMAP (遠端資料夾)  POP3 (將郵件保留在您的電腦上)

收件: POP3 pop.gmail.com SSL  
寄件: SMTP smtp.gmail.com SSL  
使用者名稱: gmpp@csie.io

手動設定 (M) 完成 (D) 取消 (A)

## 3. 如出現 Gmail 如出現無法登入到伺服器且您確認您的帳號密碼資訊無誤，請依照附錄一說明，進行應用程式存取權設定

加入現有郵件帳號

您的大名 (N): 黃小橋 您的名字，用於顯示在您的郵件上

電子郵件地址 (L): gmpp@csie.io 您目前的電子郵件地址

密碼 (P): ●●●●●●●●●●

記住密碼 (M)

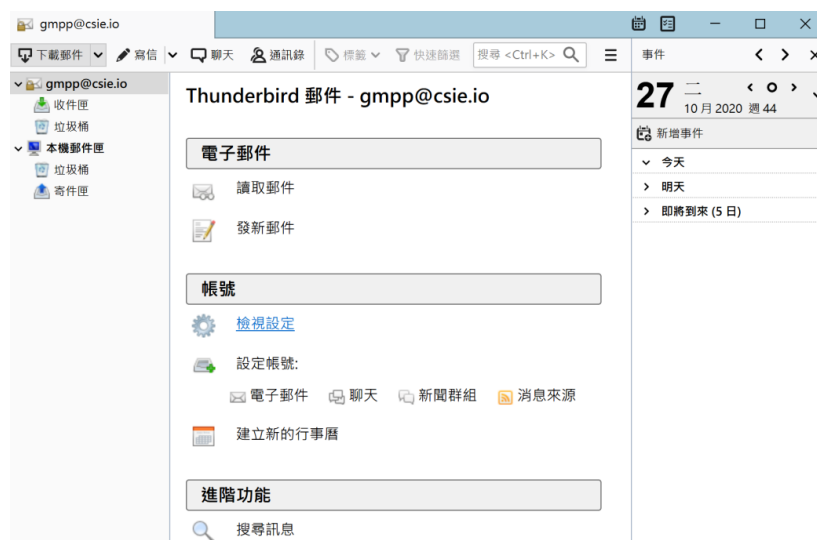
⚠ 無法登入到伺服器。也許是帳號、密碼或設定錯誤。

IMAP (遠端資料夾)  POP3 (將郵件保留在您的電腦上)

收件: POP3 pop.gmail.com SSL  
寄件: SMTP smtp.gmail.com SSL  
使用者名稱: gmpp@csie.io

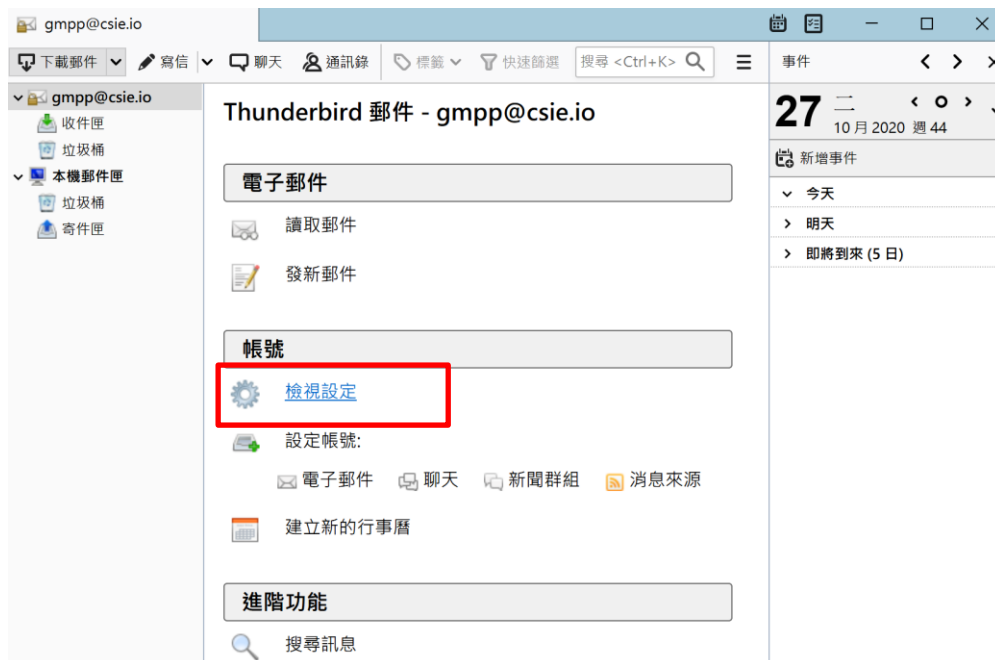
手動設定 (M) 完成 (D) 取消 (A)

## 4. 如通過驗證，即可看到信箱已設定完成



## 2.3 設定[軟體型] S/MIME 憑證

### 1. 點選下圖之 [檢視設定]

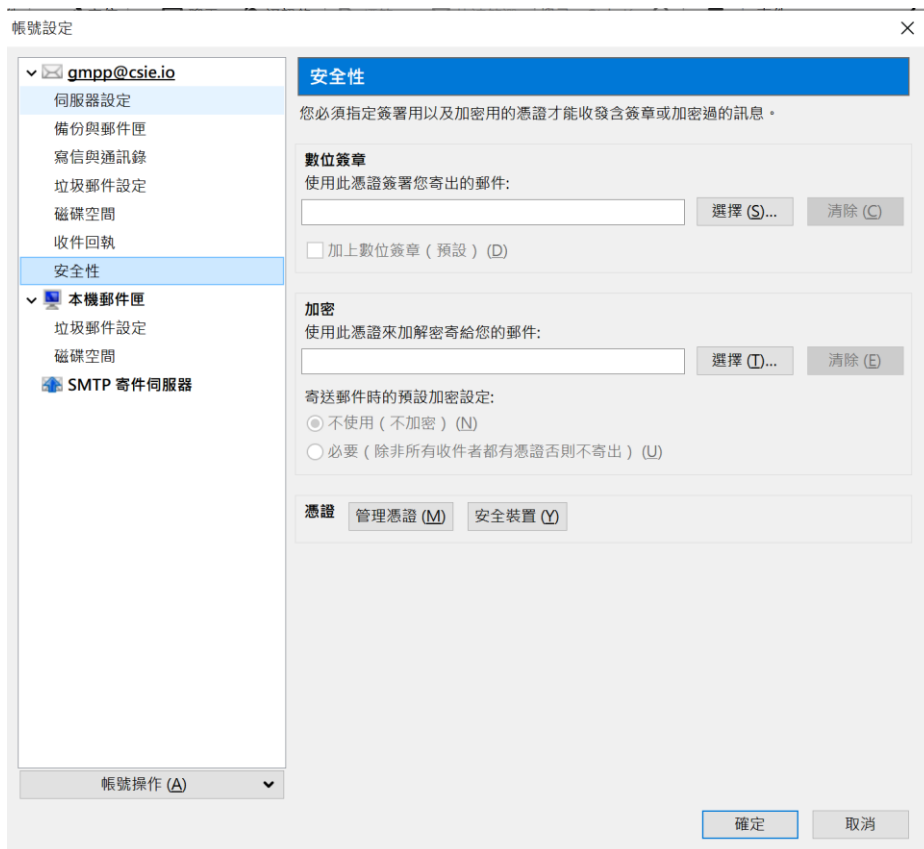


### 2. 在設定選項中，尋找 [端對端加密] 選項



在某些較先前版本的 Thunderbird 可能顯示為 [安全性] 的選項





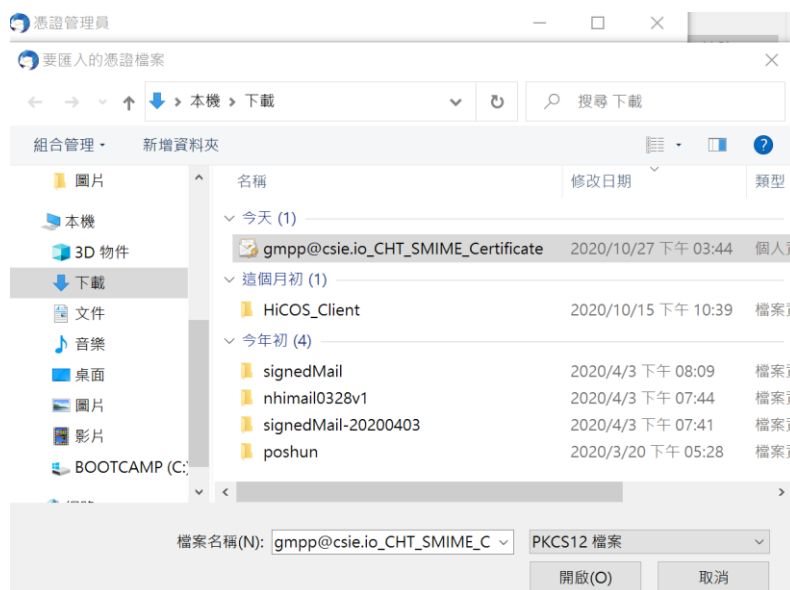
3. 點選 **[管理 S/MIME 憑證]** 或 **[管理憑證]** (較舊版, 如上圖), 進行憑證匯入/更新



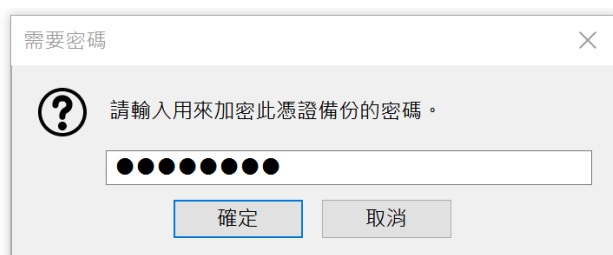
#### 4. 在[你的憑證]頁籤，點選 [匯入] 按鈕



#### 5. 選取憑證所在位置後，按下[開啟]



#### 6. 輸入憑證自訂密碼後，按下確定



## 7. 如匯入成功，即可看到憑證已匯入 Thunderbird



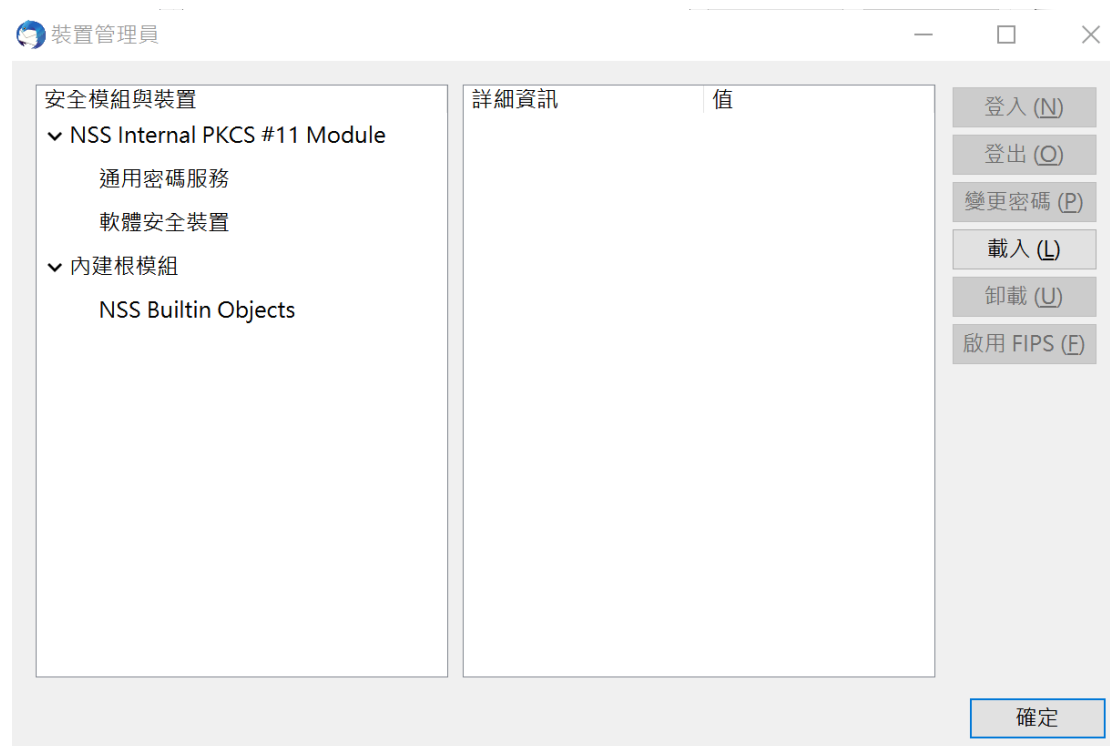
## 2.4 設定[IC 卡片/裝置型] S/MIME 憑證

**(!!! --- 請確定已安裝 [HiCOS 卡片管理工具](#) ---!!!)**

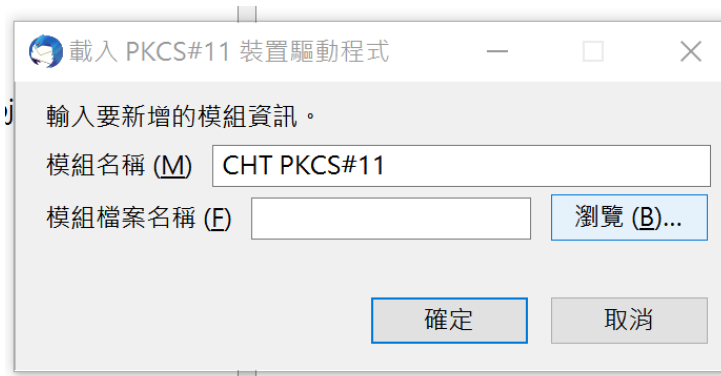
1. 在設定選項中 → 找到 [端對端加密] / [安全性] 功能中，  
點選 [S/MIME 安全裝置] / [安全裝置] 按鈕



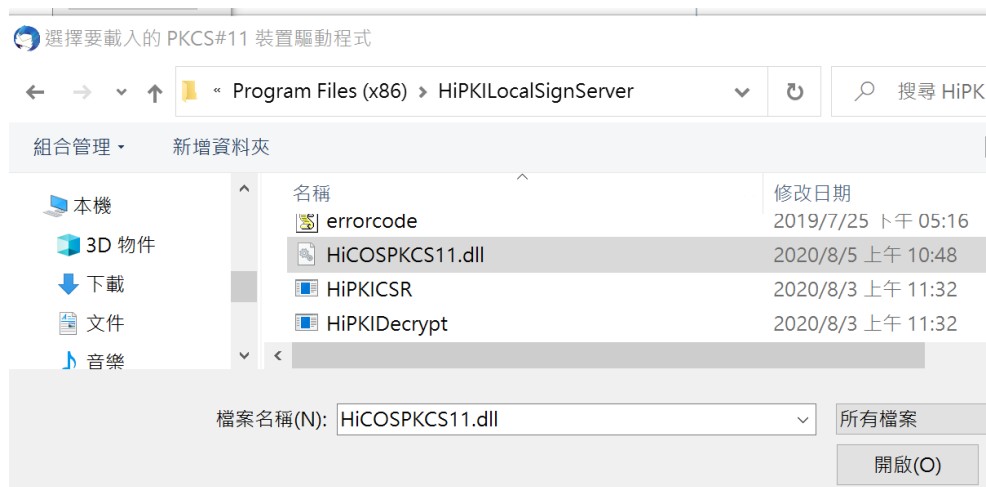
## 2. 點擊右方 [載入] 之按鈕



3. 提示您輸入新的模組資訊，請在模組名稱輸入 **CHT PKCS#11** 或其他自訂名稱，並按下 **[瀏覽]** 按鈕，指定模組檔案所在位置。



4. 選取檔案位置，該檔案位於 C:\Program Files (x86)\HiPKILocalSignServer\ 目錄中 HiCOSPCKCS11.dll 檔案



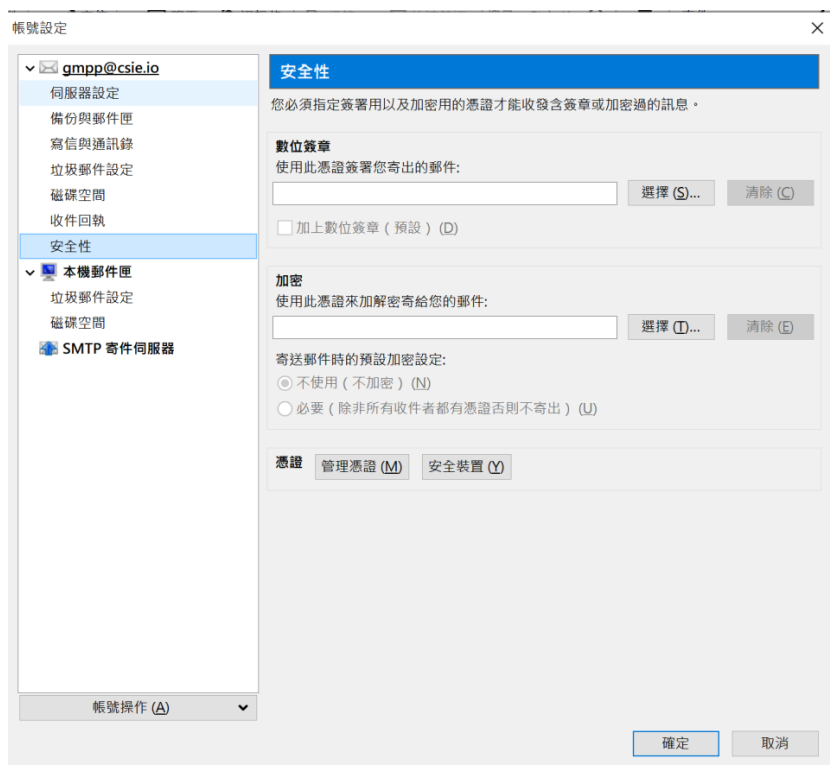
如未能發現該檔案，請確認有安裝 HiCOS 卡片管理小工具、與跨平台元件

5. 安裝成功後，您會發現安全模組與裝置中，新增了一個 CHT PKCS#11 裝置，如點選其中的讀卡機介面，可看到相關版本資訊。



## 2.5 設定帳號之 S/MIME 簽章憑證

1. 在[安全性] 選項中，找到**數位簽章**區域，

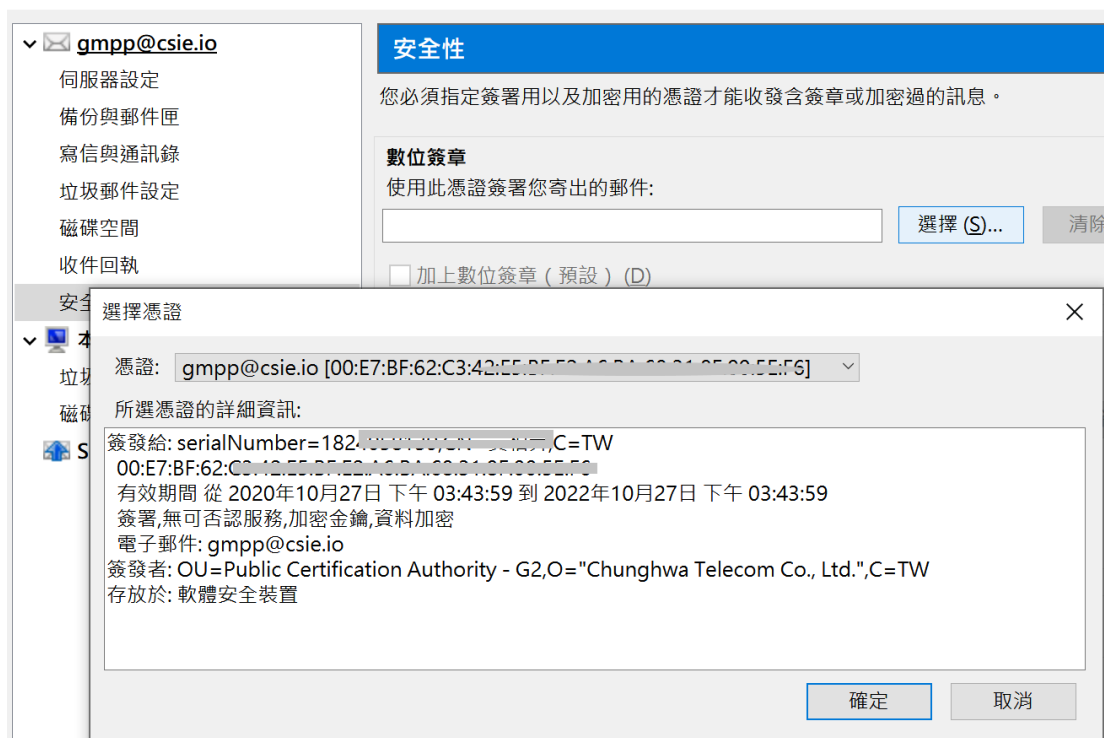


或在 [端對端加密] 選項中，S/MIME 區域中，點選 [選擇] 按鈕，來指定郵件的簽章憑證。



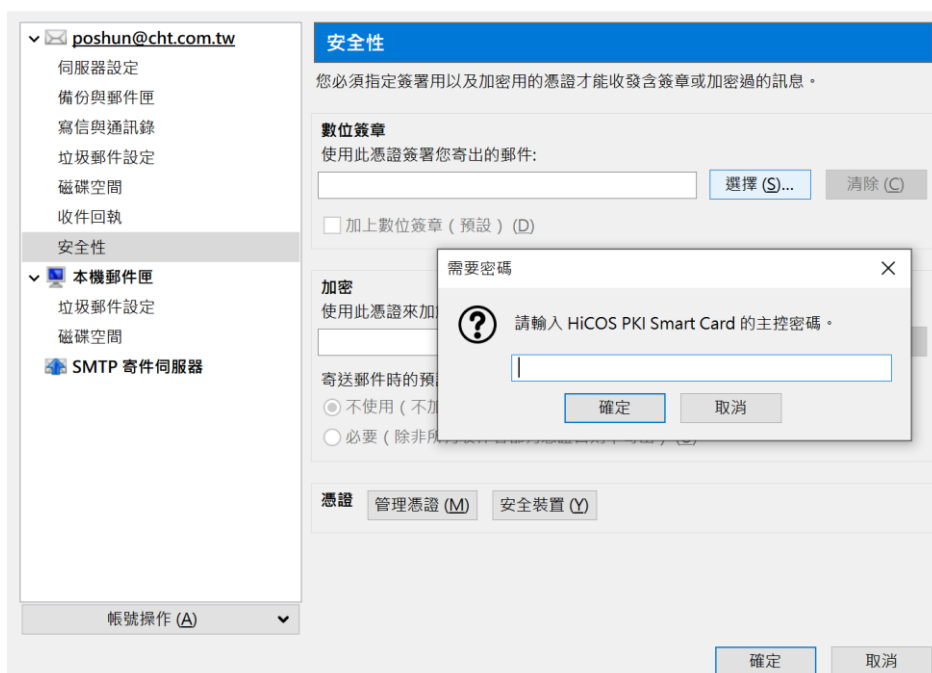
2. 如您是軟體型的 S/MIME 憑證，在此時會跳出對話框，要求你選擇先前已匯入之軟體憑證，來當成日後郵件簽章之預設憑證。

帳號設定



- 如您是 IC 卡片/裝置型 S/MIME 憑證，在點選後會出現 [需要密碼的對話框]，此時請輸入卡片密碼。(請先確認已將卡片插入 IC 讀卡機中，再執行此步驟)

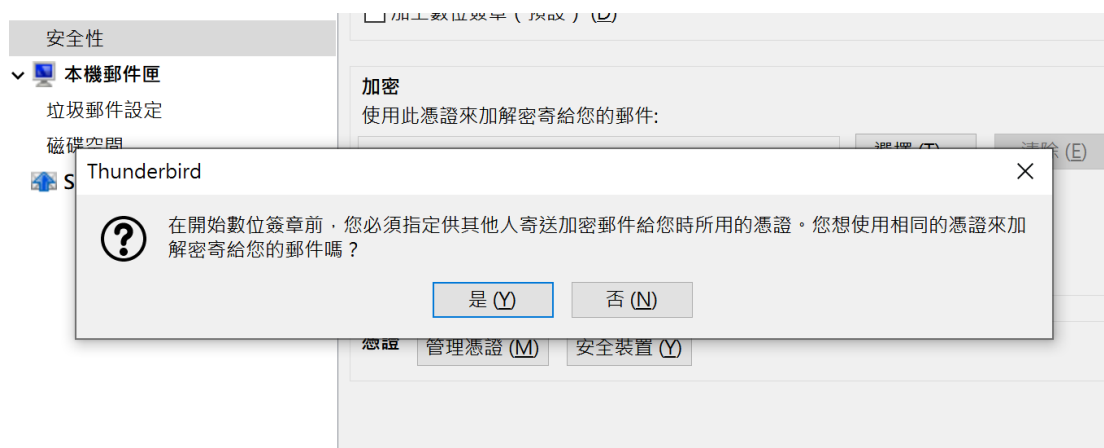
帳號設定



- 如密碼正確，且卡片中擁有有效憑證，則會列出可選擇的憑證。

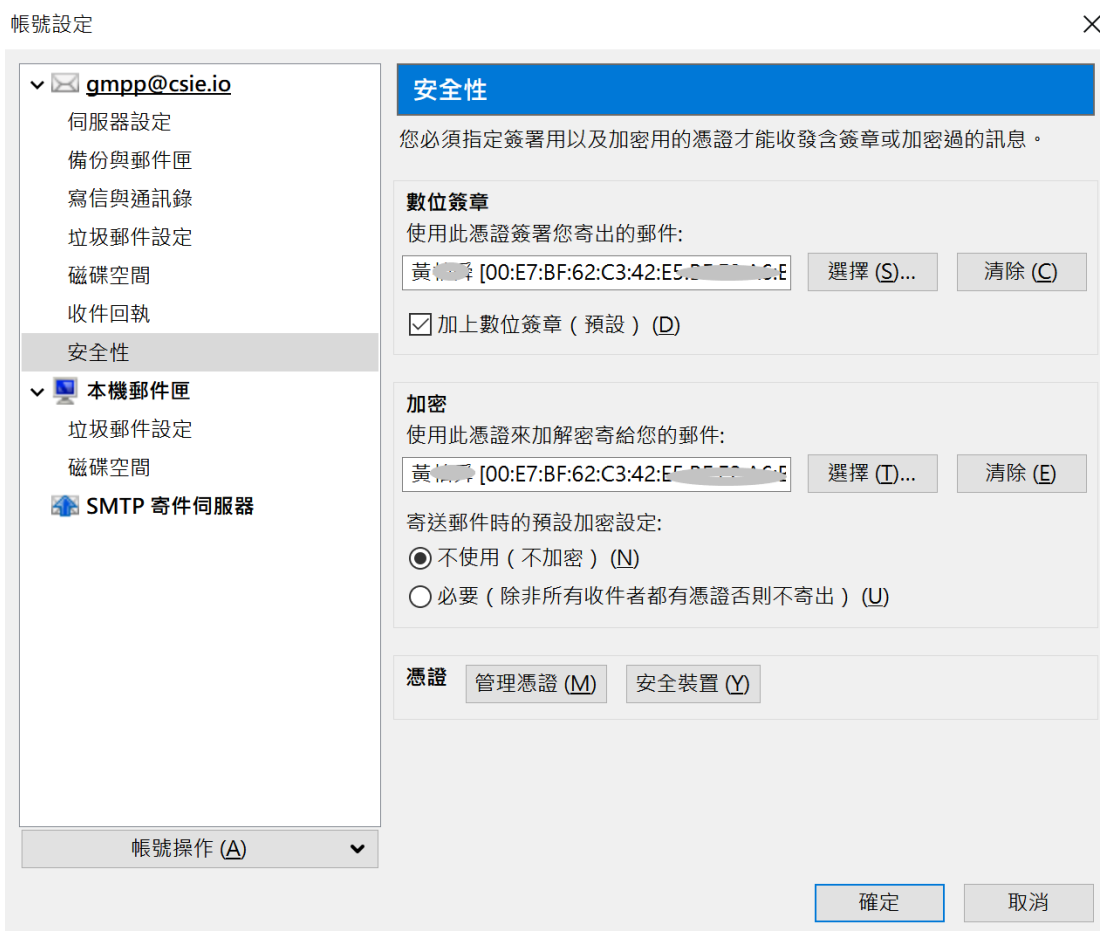


3. 選取正確之簽章憑證後，您可選擇 [是] 按鈕，用相同憑證進行郵件加密應用





4. 調整 [寄送郵件前，是否預設加上數位簽章]  
並依情況，選擇是否需樣預設加密郵件，完成後按下確認

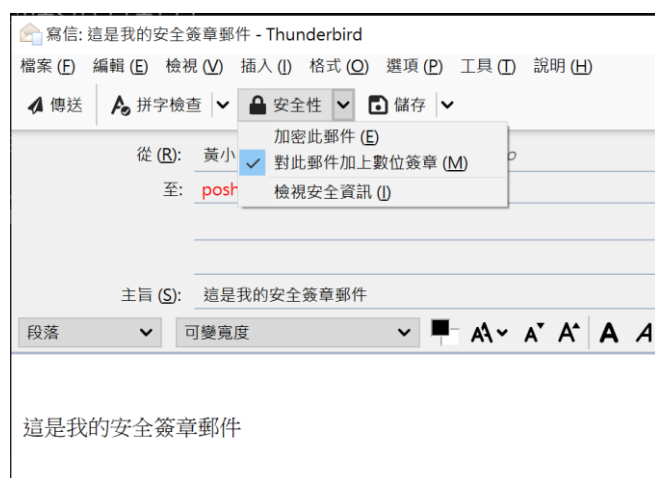


5. 恭喜！到這裡您已完成憑證匯入與設定

## 3. 郵件簽章/加密應用流程

### 3.1 郵件簽章

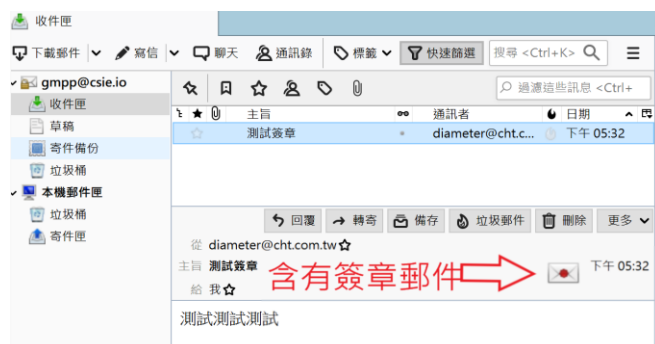
1. 編寫新郵件，填入對方郵件位置，確認[安全性]選項中，對此 [郵件加上數位簽章] 功能有被打勾選取後，即可送信件



### 3.2 郵件加密

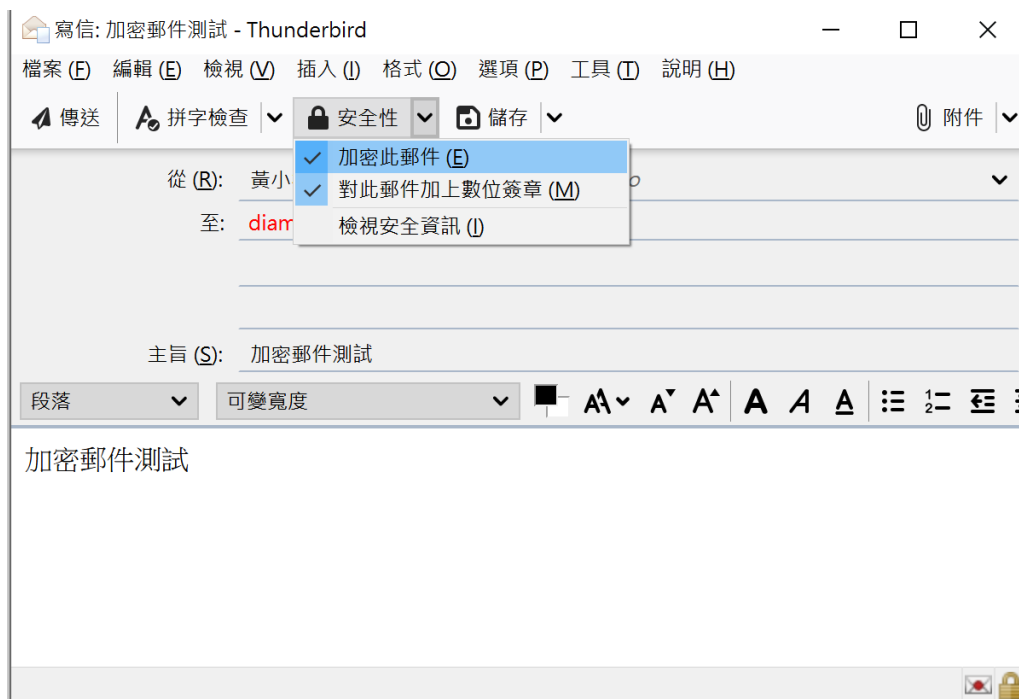
如要請對方發送加密郵件給您，您需要先發送一封簽章郵件給對方，以讓對方可以取得您的公開金鑰資訊。

反之，如您要發送加密郵件給對方，您要請對方先發送一封簽章郵件給您。取得對方公開金鑰後，即可以發送加密郵件對方。

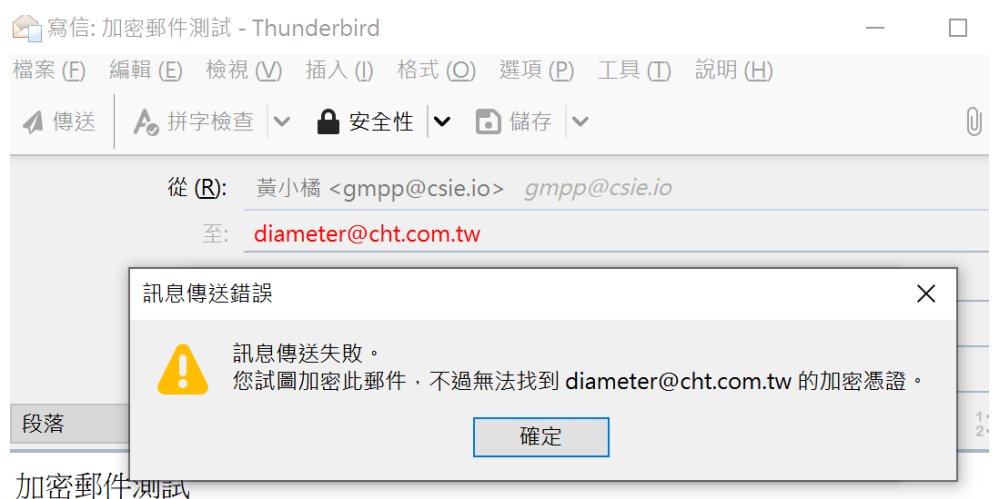


完成上述公鑰交換後，

1. 編輯一封郵件，並選取 [安全性] 按鈕，確認已勾選 [加密此郵件] 與 [對此郵件加上數位簽章]。  
編輯完成後，按下 [傳送] 按鈕即可送出加密郵件



2. 如出現下列對話框，表示暫時無法發送加密郵件。  
須請對方發送一封簽章郵件給您，待您開啟信件後才可發送加密郵件。



## 3.3 檢視郵件簽章

如您想檢查郵件來自何方，是否有被修改過。也可點擊郵件簽章圖示，查看簽署資訊。



亦可點擊 [檢視簽章憑證]，來確認由誰所建立、發送的

