



以安全元件作為IoT裝置安全防護 -以HiKey 為例

- HiKey 簡介

- HiKey在Raspberry Pi之設置

- IoT憑證匯入到HiKey方法



Introductin of HiKey

❖ HiKey是一種智慧型PKI載具，整合「安全晶片」與「多功能讀卡機」。提供使用者多種增值應用服務，透過存取控制與加解密技術，可避免機密資料外洩，是一種安全方便又好用的資安產品。

❖ 規格

- 介面: USB2.0 ，支援PC/SC V2.0
- 加解密運算支援:
 - RSA演算法：1024/2048位元長度公開金鑰(Public key)及私密金鑰(Private key)
 - Triple-DES 演算法：112 位元長度之金鑰（用於External / Internal Authentication命令及安全訊息命令加密及驗證功能）
 - SHA-1 /SHA2 Hash演算法。
- 資安認證: FIPS140-2 Level 2+



Introductin of HiKey



中華電信
Chunghwa Telecom

❖ 應用

- 企業內VPN安控
- 各上線系統PKI認證應用
- Computer Secure Logon功能
- 檔案加解密
- 電子資料數位簽章
- 安全電子郵件
- 提供電子交易身分認證
- IoT裝置安全認證與安全傳輸



HiKey 在Raspberry Pi之設置

❖ HiKey在樹莓派的驅動程式安裝

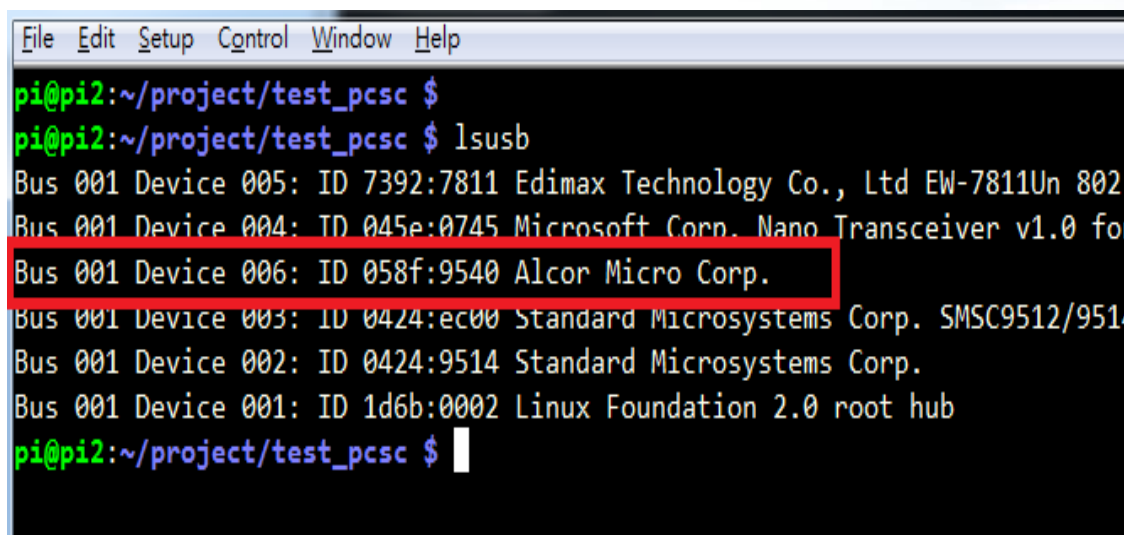
■ Step1:

將HiKey 插入樹莓派USB Port，HiKey 上面的紅燈會亮起，



- Step2:

在樹莓派的console上輸入 lsusb，可看HiKey列入USB裝置上。



```
File Edit Setup Control Window Help
pi@pi2:~/project/test_pcsc $
pi@pi2:~/project/test_pcsc $ lsusb
Bus 001 Device 005: ID 7392:7811 Edimax Technology Co., Ltd EW-7811Un 802
Bus 001 Device 004: ID 045e:0745 Microsoft Corp. Nano Transceiver v1.0 fo
Bus 001 Device 006: ID 058f:9540 Alcor Micro Corp.
Bus 001 Device 003: ID 0424:ec00 Standard Microsystems Corp. SMSC9512/951
Bus 001 Device 002: ID 0424:9514 Standard Microsystems Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
pi@pi2:~/project/test_pcsc $
```



- Step3: 安裝pcscd 和pcsc-tools

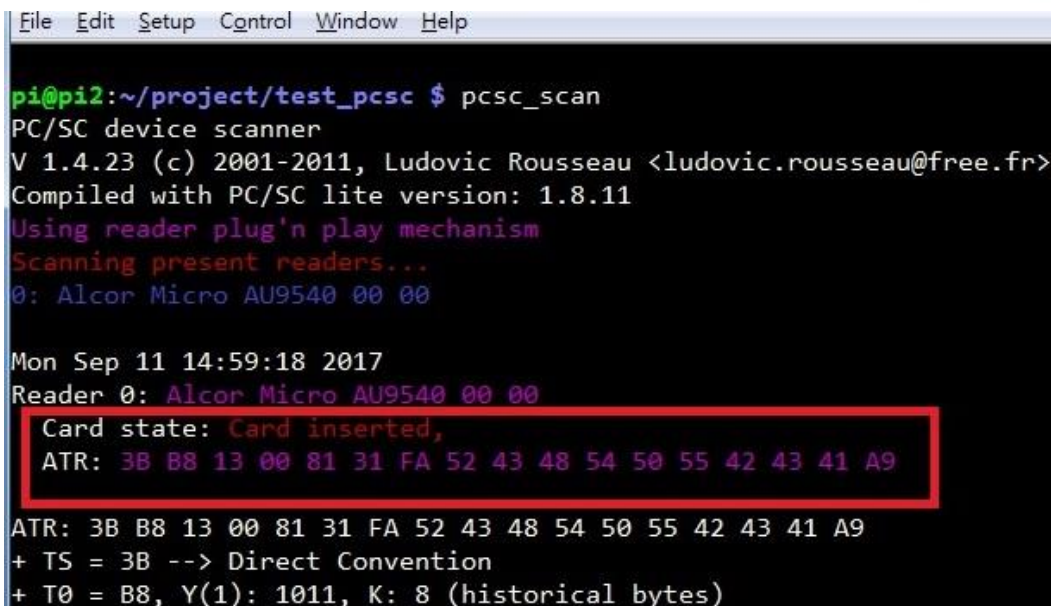
```
$ sudo apt-get install pcscd pcsc-tools
```

- Step4: 安裝 pcsclite library

```
$ sudo apt-get install libpcsclite-dev
```

- Step5: 測試HiKey若是有產生ATR，表示 HiKey驅動程式正常運作。

```
$ pcsc_scan
```



```
File Edit Setup Control Window Help
pi@pi2:~/project/test_pcsc $ pcsc_scan
PC/SC device scanner
V 1.4.23 (c) 2001-2011, Ludovic Rousseau <ludovic.rousseau@free.fr>
Compiled with PC/SC lite version: 1.8.11
Using reader plug'n play mechanism
Scanning present readers...
0: Alcor Micro AU9540 00 00

Mon Sep 11 14:59:18 2017
Reader 0: Alcor Micro AU9540 00 00
Card state: Card inserted,
ATR: 3B B8 13 00 81 31 FA 52 43 48 54 50 55 42 43 41 A9

ATR: 3B B8 13 00 81 31 FA 52 43 48 54 50 55 42 43 41 A9
+ TS = 3B --> Direct Convention
+ T0 = B8, Y(1): 1011, K: 8 (historical bytes)
```

- Step6: 測試pcsc-lite lib是否安裝成功

- 下載與執行 HiKey 測試程式:

\$ git clone <https://github.com/wujansin/HiKey-Test.git>

\$ cd HiKey-Test

\$ make : 產生執行檔 test_pcsc

\$./test_pcsc : 執行 test_pcsc , HiKey接受GenKey APDU命令 ,
回應一組8 bytes亂數和狀態碼 90 00 。

```
File Edit Setup Control Window Help
pi@pi2:~/project/test_pcsc $ ls
Makefile test_pcsc.c
pi@pi2:~/project/test_pcsc $ make
cc -pthread -I/usr/include/PCSC test_pcsc.c -lpcsc-lite -o test_pcsc
pi@pi2:~/project/test_pcsc $ ./test_pcsc
Reader name: Alcor Micro AU9540 00 00
Send command: 80 84 00 00 08
Response data: 22 12 7B D4 D0 F9 81 0C
Status code: 90 00
pi@pi2:~/project/test_pcsc $
```



下載IoT憑證

- ❖ 在CHT IoT平台的設備管理的網頁上點取憑證，可以把此裝置的憑證下載到個人電腦上



智慧聯網平台
SMART PLATFORM

首頁 開發者中心 專案管理 帳號資訊 聯絡我們 登出

首頁 / 專案管理 / 設備管理

設備管理

專案名稱: 環境品質監測

+ 增加感測器 + 增加設備 → 返回

快速搜尋:

設備編號	設備名稱	設備描述	設備類型	功能
4427354416	環境品質監控系統	監控溫度、濕度和空氣品質之系統	general	    

顯示第 1 至 1 項結果，共 1 項

設備: 環境品質監控系統 (編號:4427354416) 感測項目

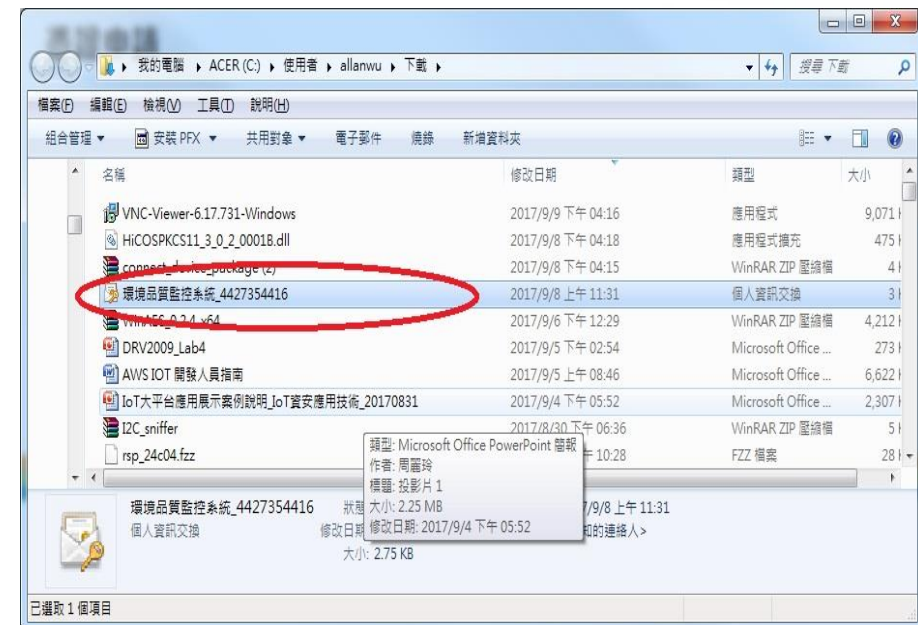
上頁 1 下頁



- ❖ 點選憑證後，進入到憑證申請的頁面，按下送出，即可把憑證存在個人電腦內。
- ❖ 存入在電腦內的檔案為 PKCS12 格式之 pfx檔

憑證申請

設備名稱	環境品質監控系統
設備描述	監控溫度、濕度和空氣品質之系統
設備編號	4427354416
憑證名稱	環境品質監控系統_4427354416
<input type="button" value="送出"/>	



匯入IoT憑證到HiKey



中華電信
Chunghwa Telecom

❖ 安裝 Firefox 和PKCS#11元件

- 下載憑證到個人電腦主機後，請先下載Firefox瀏覽器 和 HiCOSPCKS11_XXX.dll檔案，
- 目前Firefox適用的版本為**50.xx.xx X86版本(32bits)**，Firefox 下載網址

<https://ftp.mozilla.org/pub/firefox/releases/50.0.2/win32/en-US/>

- HiCOSPCKS11_XXX.dll檔案 下載網址
<https://github.com/wujansin/HiKey-IoT>



- ❖ Step1:安裝Firefox完成後，請點選瀏覽器的右上角，進入選項頁面：



❖ Step2:進入到選項頁面後，依序點選 進階 → 憑證 → 安全裝置

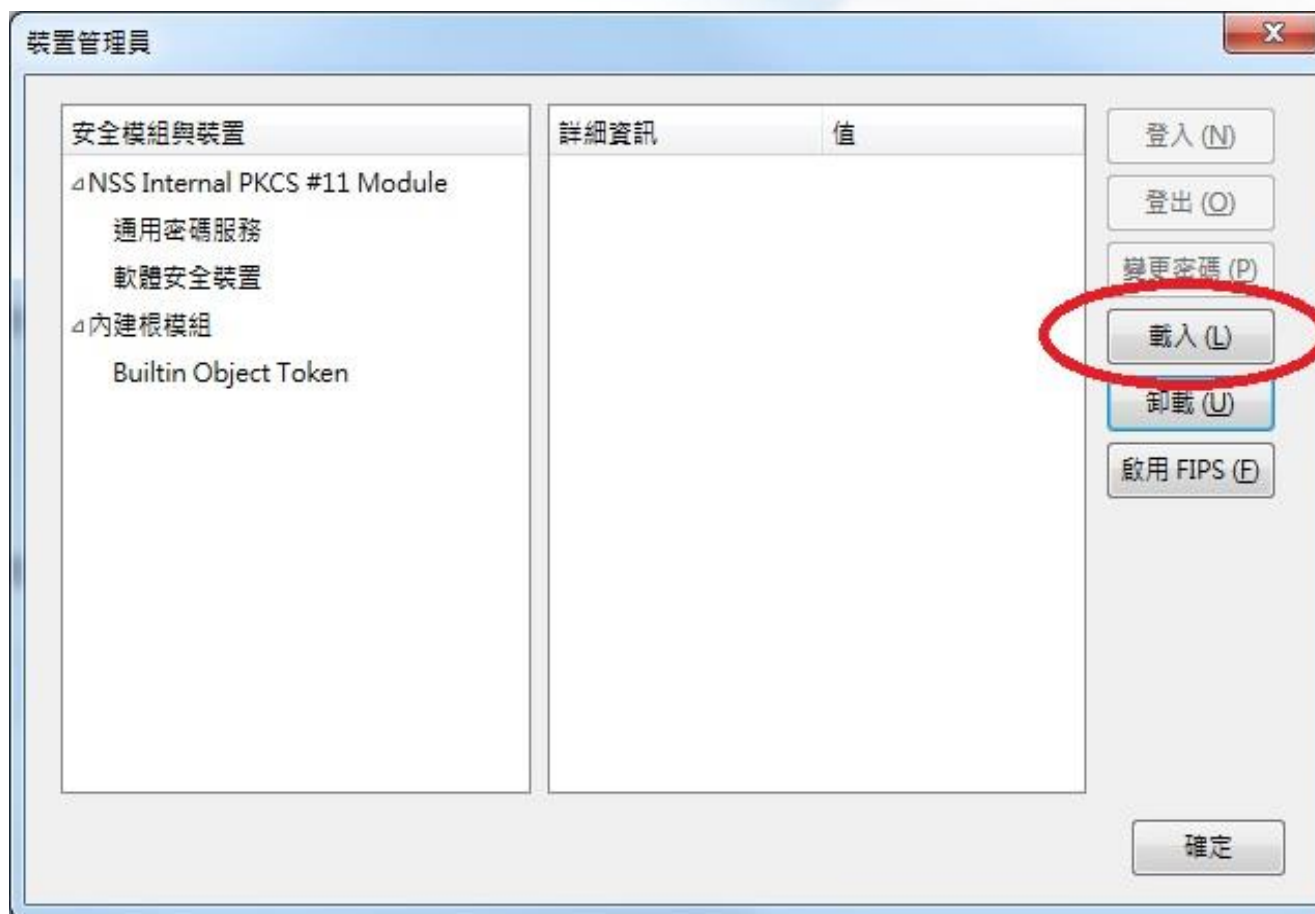


ALWAYS AHEAD 為您

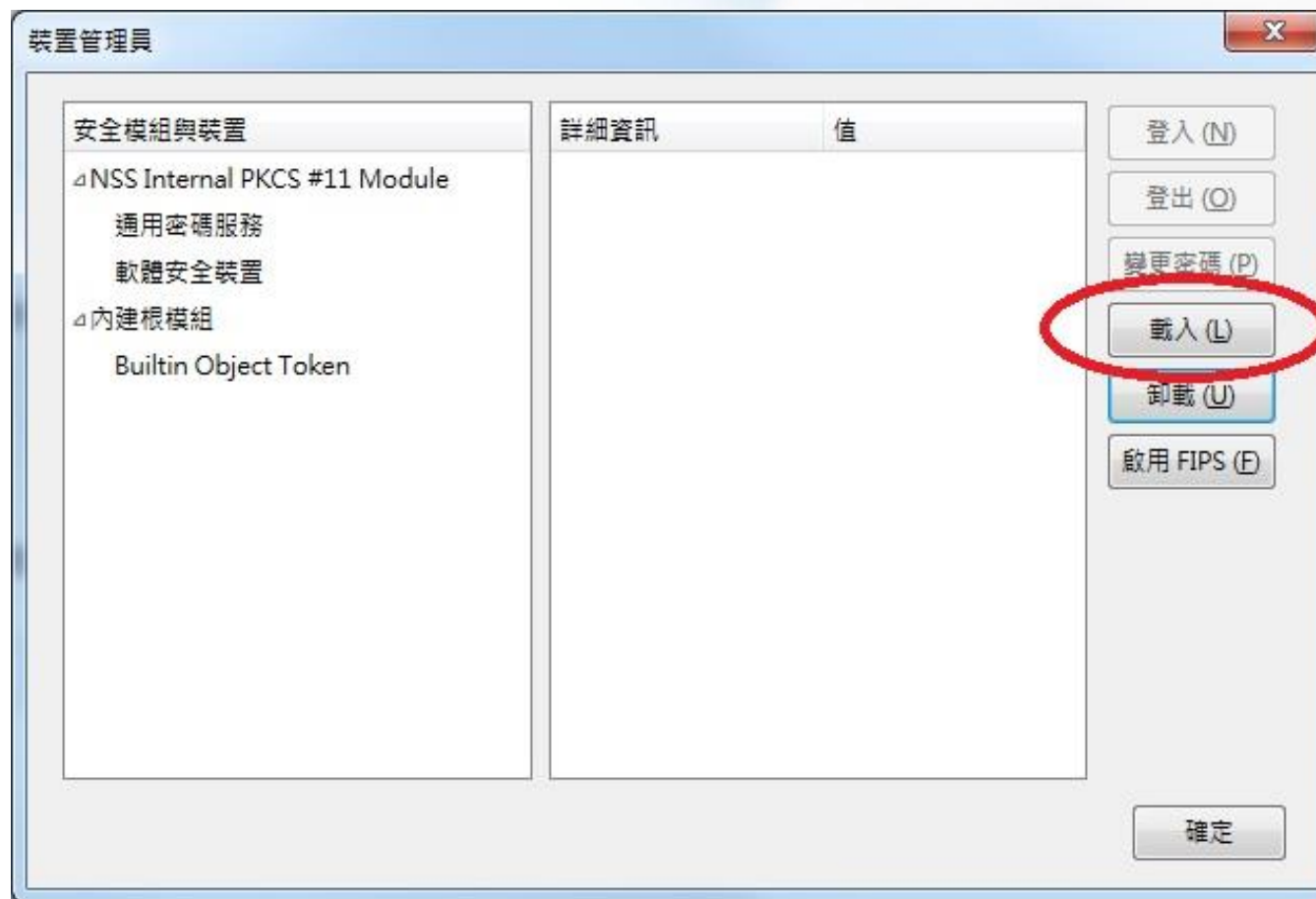


Refresh your life

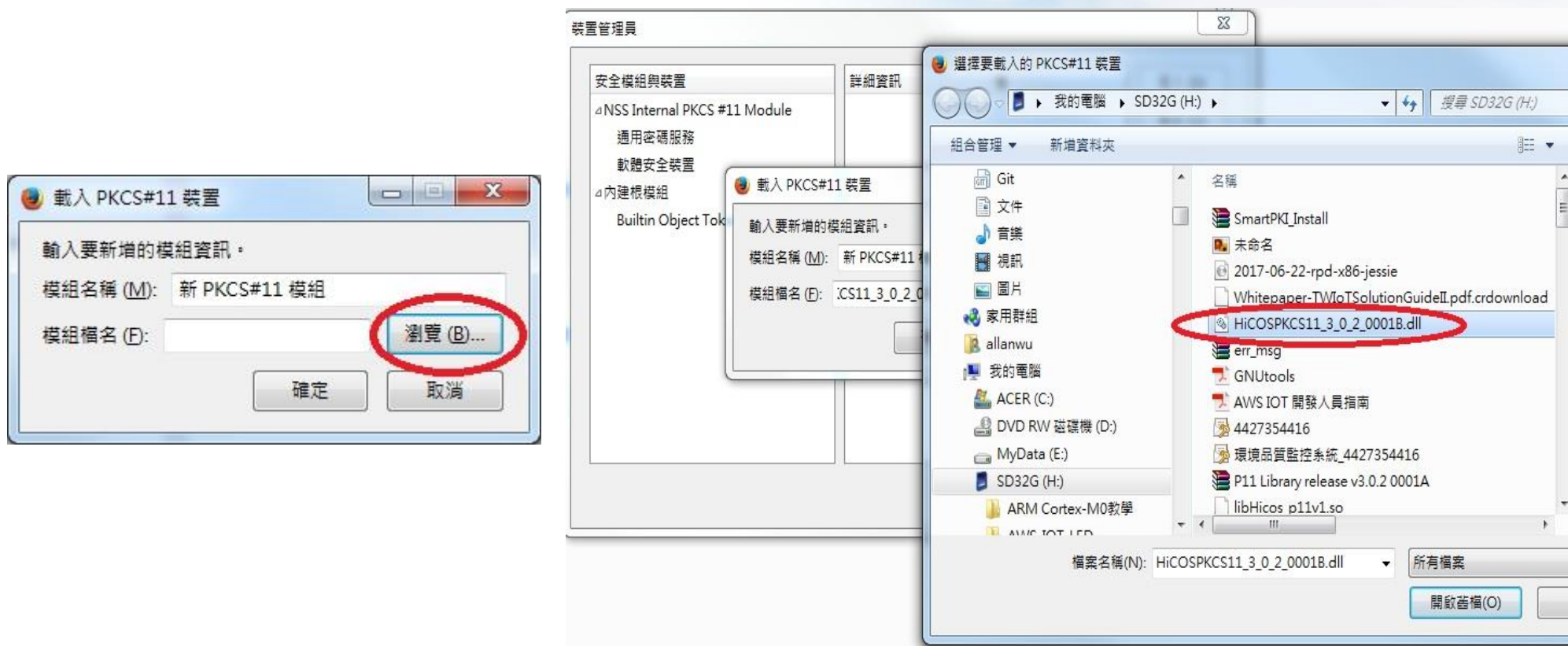
❖ Step3:跳出裝置管理員頁面，點選右邊欄位的載入



❖ Step 4: 跳出裝置管理員頁面，點選右邊欄位的載入



❖ Step 5:跳出載入PKCS#11裝置的頁面，點選瀏覽，把HiCOSPCKCS11_XXX.dll檔案載入



- ❖ Step 6: 此時已經載入HiCOSPCKS11的dll檔案，若HiKey已經插在個人電腦上，點選左邊欄位的新PKCS#11 模組，會出現HiCOS PKI Smart Card已經載入，按下確定離開。



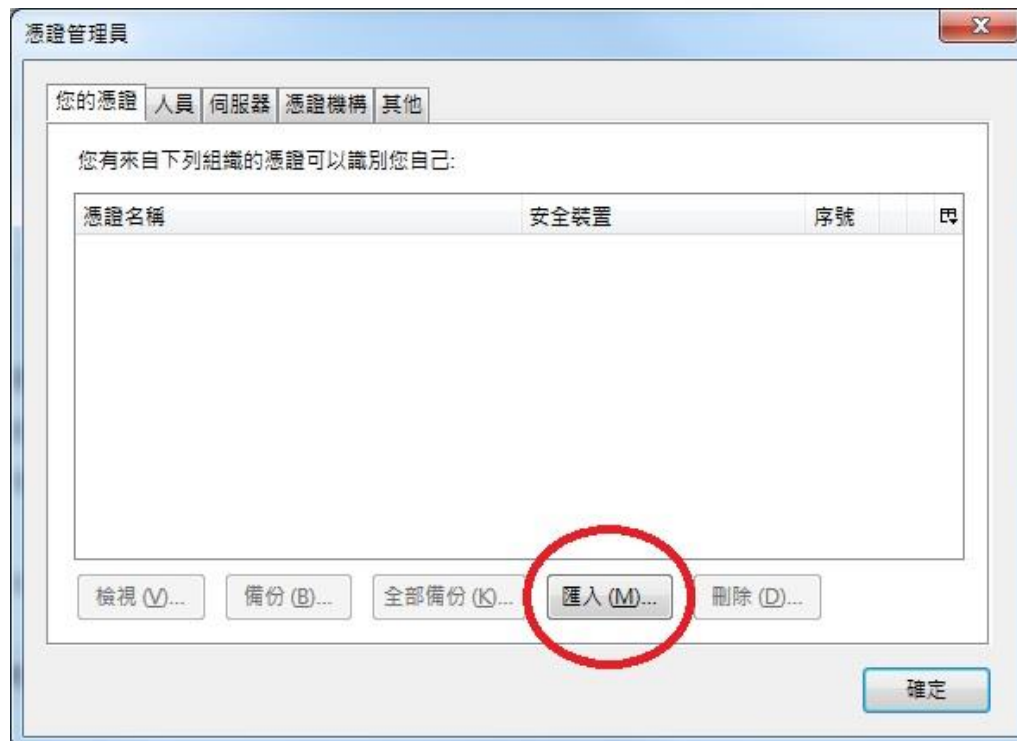
❖ Step 7:回到進階頁面，點選檢視憑證清單，



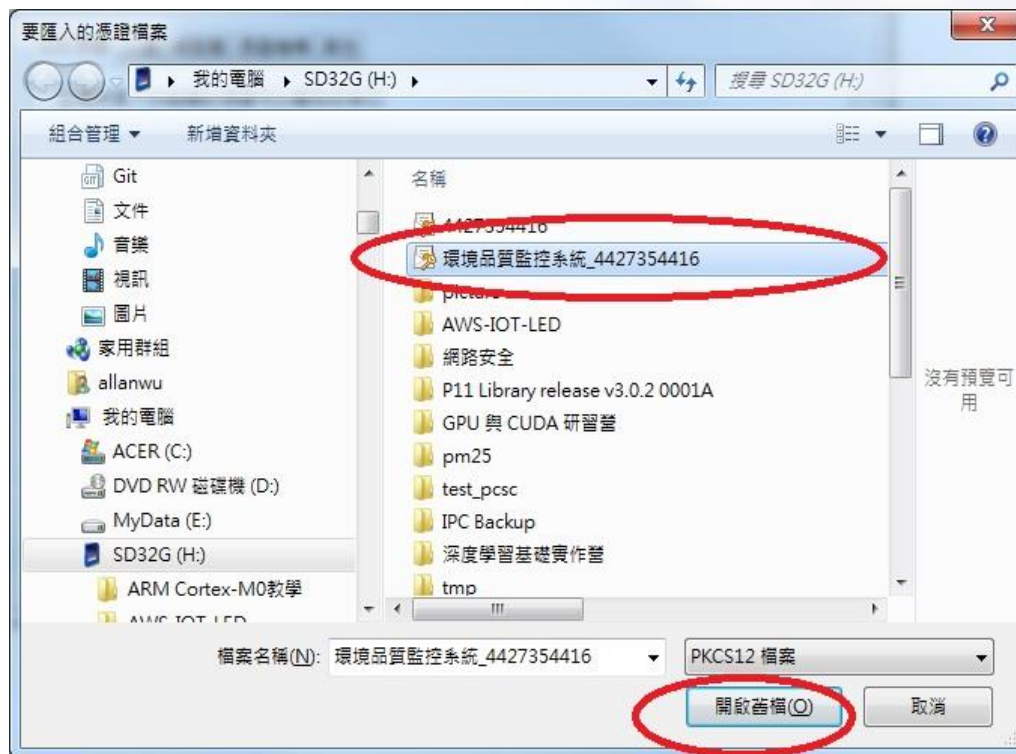
- ❖ **Step 8:**跳出請輸入 HiCOS PKI Smart Card 的主控密碼，此時輸入密碼後按確定



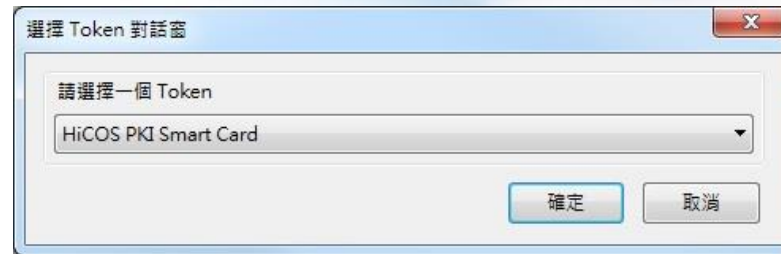
- ❖ **Step 9:**跳出請輸入 HiCOS PKI Smart Card 的主控密碼，此時輸入密碼後按確定



❖ Step 10: 把要匯入的憑證檔案開啟，按下開啟舊檔，



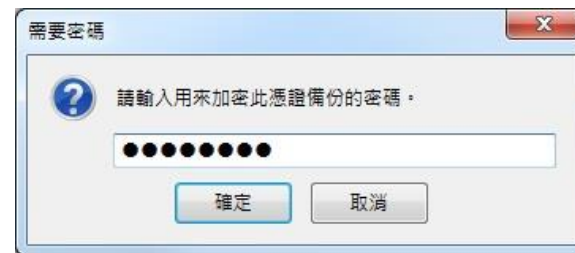
- ❖ Step 11: 出現選擇Token對話窗，選擇 HiCOS PKI Smart Card，按確定



- ❖ Step 12: 輸入HiCOS PKI Smart Card的密碼



- ❖ Step 13: 再輸入用來加密此憑證備份的密碼



- ❖ Step 14: 稍等數秒等憑證匯入到HiKey後，憑證管理員會出現剛剛匯入到HiKey的憑證，安全裝置顯示為 HiCOS PKI Smart Card，表示憑證匯入HiKey成功。

