

財團法人金融聯合徵信中心
憑證安控模組(JCICSecurityV2)
安裝使用手冊

(第 2.2.1.2 版)



中華民國 106 年 11 月 21 日

文件修訂履歷

發行/修訂 版次	發行/修訂 生效日期	發行與變更 說明	備 註
V1.0.0	2012/03/13	初版	
V1.0.1	2012/06/11	增加.Net Framework 3.5 安裝	
V1.0.2	2012/9/14	增加環境檢測功能說明	
V1.0.3	2012/12/3	增加 VPN 網路連線設定說明 增加防火牆設定說明	
V1.0.4	2013/4/19	增加憑證申請作業注意事項 增加問題處理內容	
V2.2.1	2014/12/1	程式更新為 v2.2.1.0 更新：安裝說明、設定說明等...	
v2.2.1.2	2015/1/23	修正： 1, VPN 網路連線, 預設可進行偵測 2, 聯徵中心 VPN IP, 改為下拉式選單, 預先設置測試及正式 IP, 或由鍵盤修改 3, 傳送檔案及接收檔案之會員帳號選	



		單, 下拉時自動由小至大排序	
V2.2.1.2	2015/3/9	修正: 1、 正式/測試模式切換時, 憑證挑選 條件一併同時更換。 2、 P7b 檔會在載入或有更新時, 將所 有聯徵憑證放入/cert 中	

目錄

文件修訂履歷.....	2
1. 簡介.....	6
2. 作業環境需求.....	6
2.1. 硬體需求.....	6
2.2. 軟體需求.....	6
2.3. 功能說明.....	10
3. 憑證安控模組安裝及設定步驟.....	10
3.1. 憑證安控模組安裝.....	10
3.2. 憑證申請作業.....	20
3.3. 憑證安控模組設定.....	30
3.4. 憑證安控模組啟動/暫停/繼續/停止服務測試.....	53
3.5. VPN 網路偵測.....	58
3.6. 作業記錄檢視.....	60
3.7. 憑證安控模組功能測試.....	62
3.8. 憑證安控模組上線使用.....	74
4. Q & A.....	75
4.1. 憑證註冊中心網站登入帳號解鎖.....	75

4.2.	晶片卡密碼修改.....	75
4.3.	晶片卡鎖卡解碼.....	76
4.4.	問題處理.....	78
5.	聯絡資訊.....	85

1. 簡介

本文件主要以 Step by Step 方式說明財團法人金融聯合徵信中心憑證安控模組 (JCICSecurityV2) 之安裝、晶片卡與憑證申請以及憑證安控模組設定與操作等相關操作步驟。本操作手冊之各項操作以 Windows 7 作業系統為範例。

2. 作業環境需求(原機升版可略過此步驟)

2.1. 硬體需求

必備硬體需求：

具備晶片卡讀卡機設備。請先自行安裝購買之讀卡機驅動程式，並檢查晶片卡讀卡機是否安裝正常。

註：晶片卡讀卡機之驅動程式涉及不同設備之安裝程序，不在本份文件說明範圍，請自行參考讀卡機說明手冊。晶片讀卡機規格需符合 PC/SC 標準並通過微軟 WHQL 認證。

2.2. 軟體需求

請先至臺網網頁(<https://www.twca.com.tw/Portal/download/Download.aspx#d11>) 下載：

1. Java JRE 1.6u27 軟體

- 檔名為 jre-6u27-windows-i586.exe

2. 憑證安控模組安裝檔(JCICSecurityV2 for 2048 位元)

- 檔名為 JCICSecurityV2 v2.2.1.2.msi

作業系統：

支援 Windows XP、Windows Vista、Windows 7、Windows 2003 Server、Windows 2008 Server 及 Windows 2012 Server 等 x86 (32 位元)及 x64(64 位元)作業平台。

Java JRE 1.6u27 軟體：

Java Runtime Environment 1.6u27 版本(臺網網頁提供 1.6u27(x86) 版安裝載點)

※注意：憑證安控模組只支援 32 位元版本 JRE，若已安裝 64 位元版本 JRE，請先移除後再安裝 Java JRE 1.6u27 軟體。

網頁瀏覽器：

需使用 Windows IE 6.0 (含) 中文版以上版本。

憑證作業：

當進行「3.2 憑證申請作業」、「3.3 憑證安控模組設定」、「3.7 憑證安控模組功能測試」及「3.8 憑證安控模組上線使用」等作業時，需連接「臺灣網路認證股份有限公司」網站。

網路環境：

請先開放防火牆,資訊如下:

(1)臺網 IP 位址(如貴單位有架設防火牆,請告知貴單位管理人員,針對 IP 位址

開放 80、443 port)

- 測試

- ◆ 線上申請憑證網址 <https://cloudrademo.twca.com.tw/JCIC>

(對應 IP 為 219.87.64.176)

- ◆ 憑證安控模組-憑證廢止資訊(CRL)

http://itax.twca.com.tw/testcrl/Test_fuca_revoke_2013.crl

http://itax.twca.com.tw/testcrl/Test_fuca_revoke_Sha2_2013.crl

- ◆ (對應 IP 為 219.87.64.182,60.250.3.152)

- ◆ 憑證安控模組-交易夥伴/憑證鍊

<http://www.twca.com.tw/Portal/download/download.aspx>

(對應 IP 為 219.87.64.178,60.250.3.148)

- 正式

- ◆ 線上申請憑證網址 <https://aspra.twca.com.tw/JCIC>

(對應 IP 為 219.80.58.114 ,210.66.125.114)

- ◆ 憑證安控模組-憑證廢止資訊(CRL)

http://itax.twca.com.tw/FUCA/revoke_2017_sha2.crl

(對應 IP 為 219.87.64.186,60.250.3.156)

◆憑證安控模組-交易夥伴/憑證鍊

<http://www.twca.com.tw/Portal/download/download.aspx>

(對應 IP 為 219.87.64.178,60.250.3.148)

(2)請會員與聯徵設定 VPN 連線，之後，再請依照

以下作業操作：

(A) 加入聯徵 VPN 網路，做法: 請洽聯徵中心進行設定

專屬網路(HiLink VPN)

◆ 測試 IP: 172.31.201.125

◆ 正式 IP: 172.31.200.125

(B) 確認方式: 請使用 telnet 功能確認是否可連結到 10.18.16.41 的 TCP 80 及 443 Port，指令：「telnet 10.18.16.41 80」、「telnet 10.18.16.41 443」

(C) 設定 Hosts:以 Notepad 開啟『C:\Windows\System32\drivers\etc\hosts』檔，並在該文件最後面加上下方三行資訊後儲存。

```
10.18.16.41    ssl_eval.taica.com.tw    # For JCICSecurityV2
10.18.16.41    www.twca.com.tw          # For JCICSecurityV2
10.18.16.41    itax.twca.com.tw        # For JCICSecurityV2
```

(D) 設定完成請確認是否成功，請嘗試開啟下方五個網址，確認是否能夠順利透過 VPN 下載檔案。

http://itax.twca.com.tw/testcrl/Test_fuca_revoke_2013.crl



http://itax.twca.com.tw/testcrl/Test_fuca_revoke_Sha2_2013.crl

http://www.twca.com.tw/picture/file/JCIC_Test.p7b

http://www.twca.com.tw/picture/file/JCIC_Prod.p7b

http://itax.twca.com.tw/FUCA/revoke_2017_sha2.crl

2.3. 功能說明

➤ 憑證載具

- ※ 使用符合銀行公會「金融 XML 憑證載具規格」規範之晶片卡作為憑證載具。
- ※ 需輸入兩組卡片密碼始可運作，建議兩組密碼由不同人員分持。
- ※ 執行中若卡片被移除再插入，需再次輸入兩組卡片密碼。

➤ 憑證安控模組 (JCICSecurityV2)

- ※ 以 Windows 系統服務方式執行。
- ※ 可對檔案進行簽章與加密保護。
- ※ 可對加密檔案進行解密與驗章。

註：本使用手冊之憑證安控模組(JCICSecurityV2)以 v2.2.1.2 版本為範例。實際使用版本以最新版本之安裝檔為主。

3. 憑證安控模組安裝及設定步驟

3.1. 憑證安控模組安裝

3.1.1 取得憑證安控模組安裝程式(JCICSecurityV2 v2.2.1.2.msi)以及晶片卡

※注意：請先確認安裝帳號為 Administrator (帳號即使在管理者群組中，亦有可能安裝失

敗，請確定為 Administrator 帳號)，避免安裝過程發生權限不足，導致安裝失敗或安裝後使用異常！

(1) **憑證安控模組安裝檔(JCICSecurityV2 for 2048 位元)**

- 檔名為 JCICSecurityV2 v2.2.1.2.msi

可於臺網網頁(<https://www.twca.com.tw/Portal/download/Download.aspx#d11>)下載。

(2) 測試晶片卡

測試晶片卡請至 <http://www.twca.com.tw> 網站的下載中心中尋找**財團法人金融聯合徵信中心加密檔案傳輸作業之憑證註冊申請表單**，並下載填具後，向「臺灣網路認證股份有限公司」申請取得。相關聯絡資訊請參閱「5.聯絡資訊」章節。

(3) 正式晶片卡

正式晶片卡請至 <http://www.twca.com.tw> 網站的下載中心中尋找**財團法人金融聯合徵信中心加密檔案傳輸作業之憑證註冊申請表單**，並下載填具後，向「臺灣網路認證股份有限公司」申請取得。相關聯絡資訊請參閱「5.聯絡資訊」章節。

3.1.2 安裝憑證安控模組(JCICSecurityV2 v2.2.1.2.msi)

- (1) 連續點擊『JCICSecurityV2 v2.2.1.2.msi』檔案，開始進行安裝



(2) 安裝時偵測是否已經安裝「Java JRE 軟體」

※注意：憑證安控模組只支援 32 位元版本 JRE，若已安裝 64 位元版本 JRE，請先移除後再安裝 Java JRE 1.6u27 軟體。

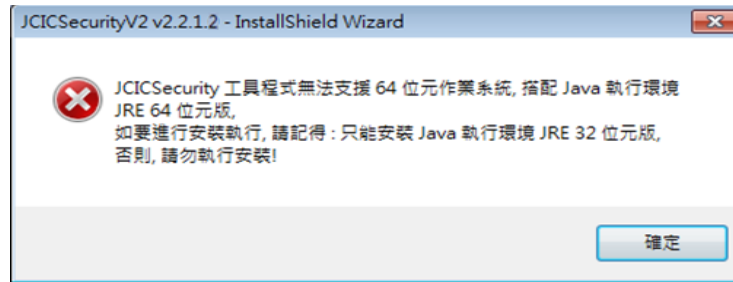
- 1, 首先偵測作業系統，是否已經安裝「Java JRE 軟體」，如果出現畫面：



表示：電腦尚未安裝『Java JRE 軟體』，請先行安裝之後，才能繼續執行安裝。

安裝「Java JRE 軟體」步驟，請參考 [3.1.3] 章節說明。

- 2, 若作業系統，已經安裝「Java JRE 軟體」，仍出現畫面如下：



表示：執行環境電腦為 64 位元，較不建議在此電腦上安裝。若要安裝，也只能安裝 32 位元『Java JRE 軟體』，目前無法支援 64 位元『Java JRE 軟體』。安裝「Java JRE 軟體」步驟，請參考「3.1.3」章節說明。

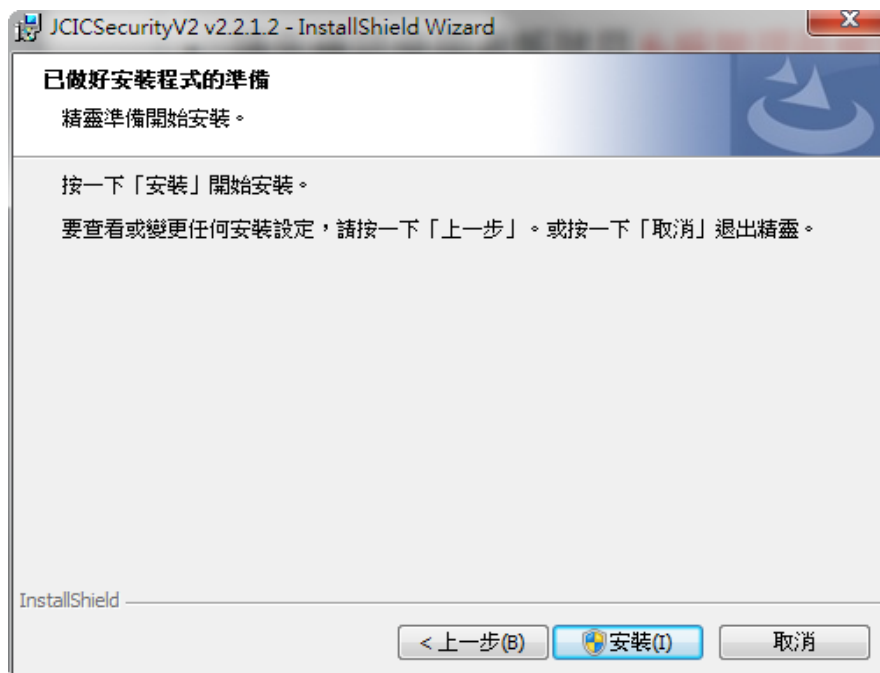
(3) 點擊「下一步」繼續進行安裝



(5) 安裝時，需指定安控模組作業目錄。如系統先前已經安裝過，或目錄已經存在，將略過這個步驟。



(6) 點擊「安裝」繼續進行安裝步驟

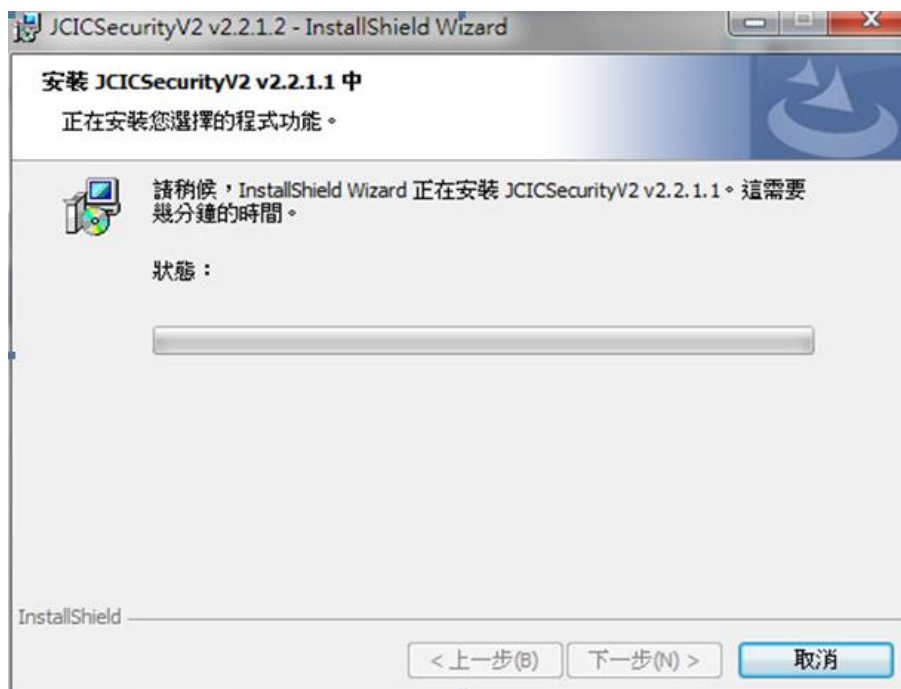


(7) 按「確定」，進行 Windows 服務安裝

這是提示你：當出現使用者控制視窗，程式名稱為 JavaAsService.exe 時，需要取得您的授權。



(8) 開始安裝



(9) 完成安裝檔安裝作業



- (10) 安裝時如果出現此錯誤訊息：『C:\JCICSecurityV2\JavaAsService.exe 無法啟動
這個程式，因為應用程式的設定不正確。重新安裝應用程式應該可以修復這個
問題。』時，請參考 4.4 問題處理。

3.1.3 Java JRE 1.6u27 軟體安裝(原機升版可略過此步驟)

- (1) 請於臺網網頁(<https://www.twca.com.tw/Portal/download/Download.aspx#d11>)下載
並執行『jre-6u27-windows-i586.exe』檔案以進行 Java JRE 1.6u27 軟體安裝
- (2) 點選「執行」，進行 Java JRE 1.6u27 軟體安裝。



(3) 直接點擊「安裝」，繼續進行安裝作業。

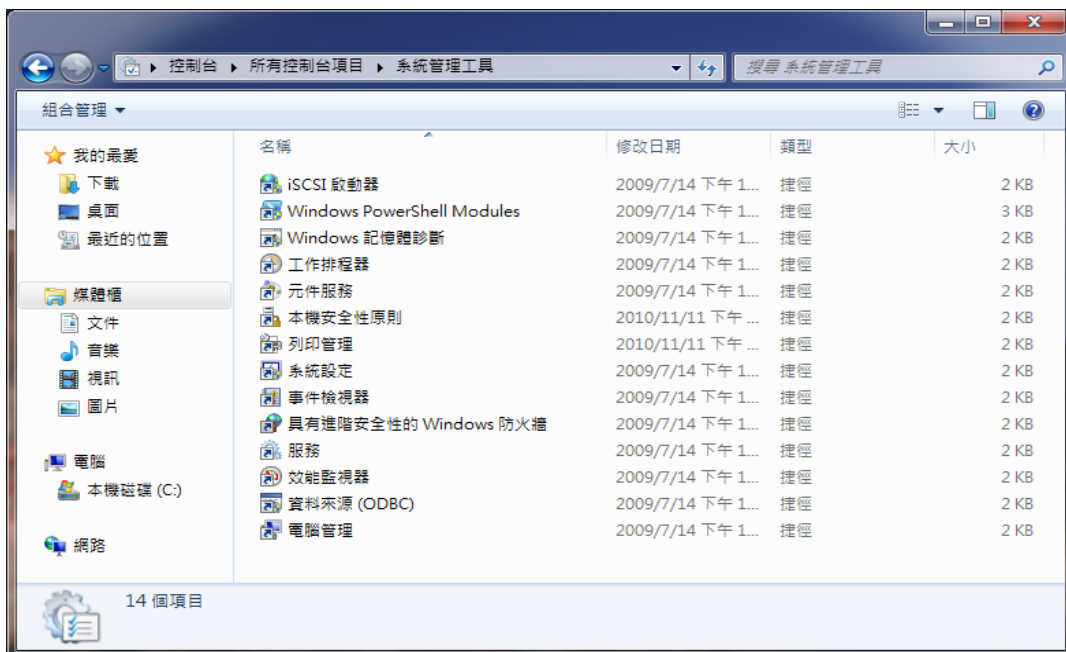


(4) Java JRE 1.6u27 軟體安裝完成



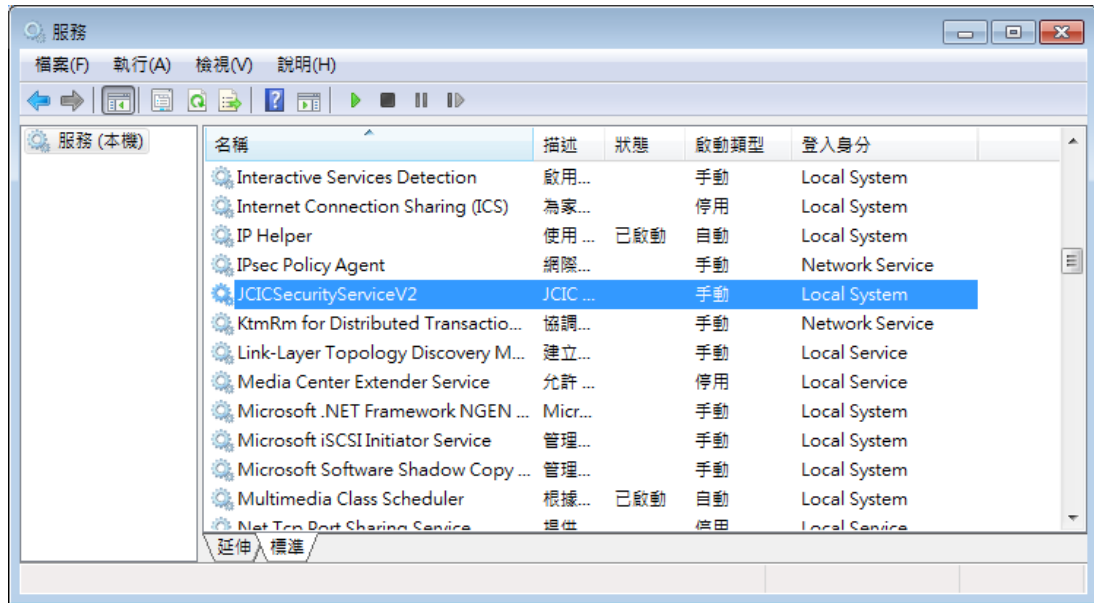
3.1.4 確認憑證安控模組系統服務是否成功安裝

(1) 開啟『控制台\所有控制台項目\系統管理工具』



(2) 點擊『服務』圖示，開啟 Windows 系統服務，找出服務名稱

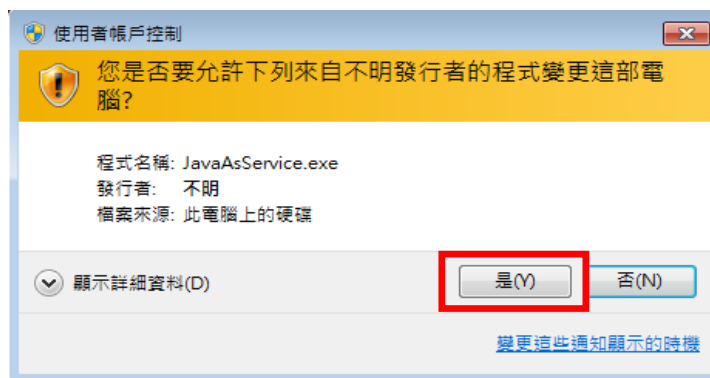
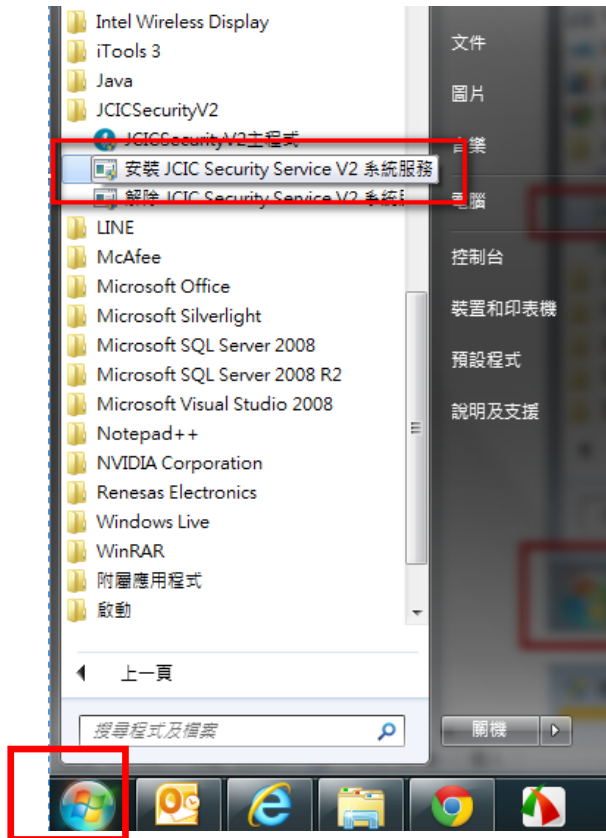
『JCICSecurityServiceV2』，有出現表示已經安裝完成。



※注意：如未在『服務』中看到 JCICSecurityV2，請按照以下步驟執行(如已有

JCICSecurityV2，請忽略)：

- (1) 點擊『開始』→『所有程式』→『JCICSecurityV2』→捷徑『安裝 JCIC Security Service V2 系統服務』，以『系統管理員身份執行』，開始進行系統服務安裝。



(2) JCIC Security Service V2 系統服務安裝完成

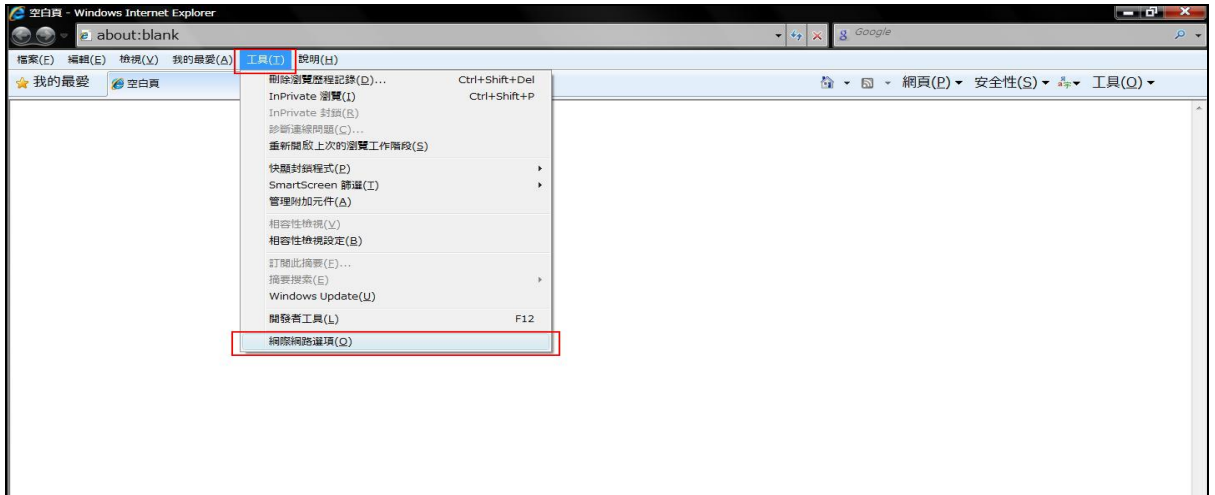
3.2. 憑證申請作業

注意: 執行憑證申請作業必需在網際網路下執行, 若在 VPN 環境下, 請先離開 VPN 環境。

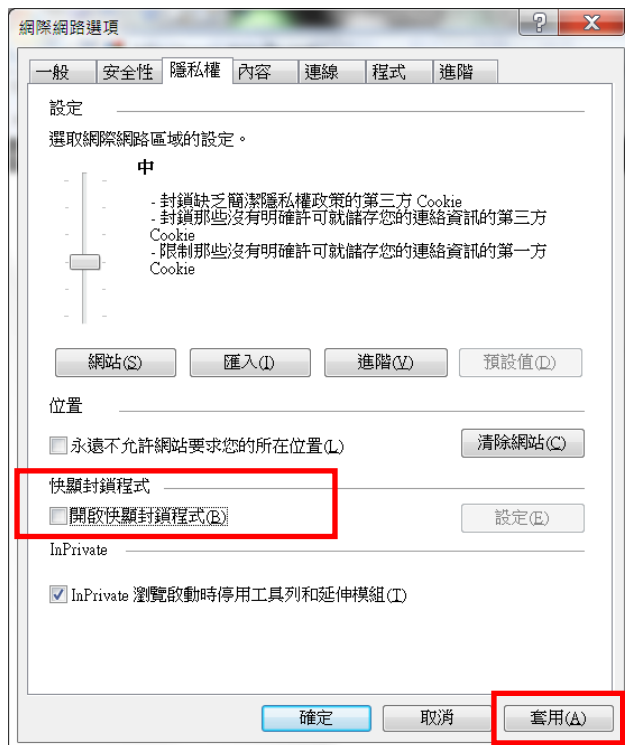
3.2.1 客戶端環境設定

用戶使用前，必需事先調整 IE 安全性設定，設定方式如下：

- (1) 開啟 IE 軟體，於功能選項中選擇「工具」，再於下拉選項中選擇「網際網路選項」設定。

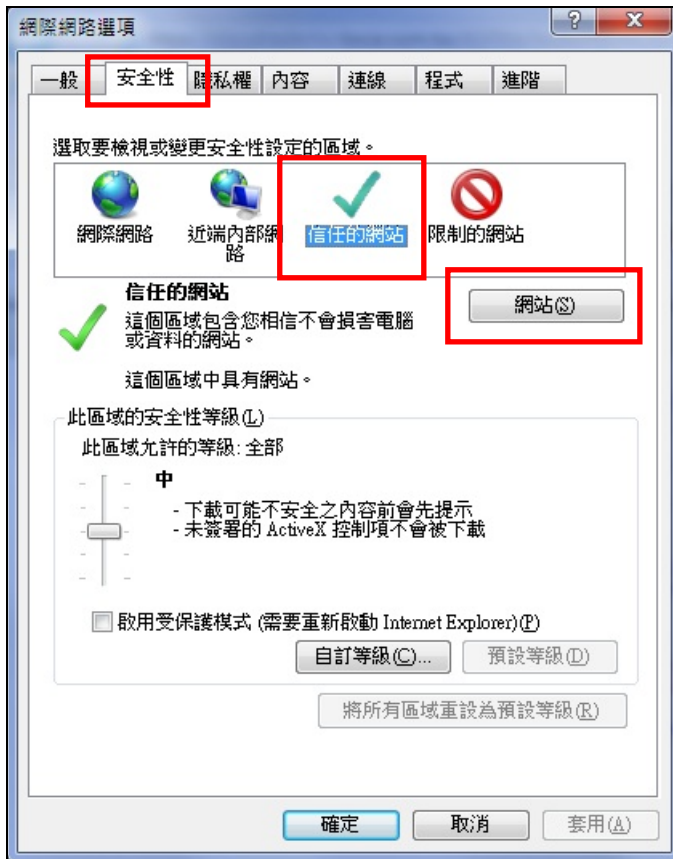


- (2) 於網際網路選項視窗中選擇「隱私權」標籤，並取消勾選「開啟快顯封鎖程式(B)」後，點選「套用」。

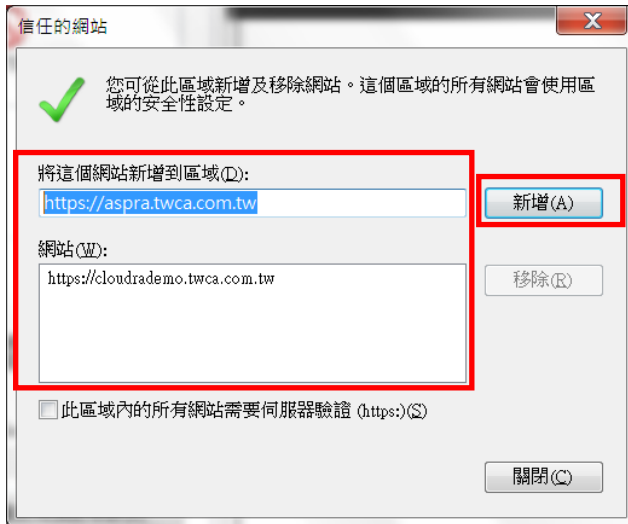


- (3) 於網際網路選項視窗中選擇「安全性」標籤，參考執行(a)、(b)、(c)、(d)將「啟用受保護模式」設定取消，並之加入信任網站步驟後，再按「確定」按鍵完成設定。完成設定後需關閉所有 IE 程式，再重新執行 IE 程式。

- (a) 點選「信任的網站」後，再點選「網站」，



- (b) 請分別輸入「<https://cloudrademo.twca.com.tw>」及「<https://aspra.twca.com.tw>」等兩網址後，點選「新增」

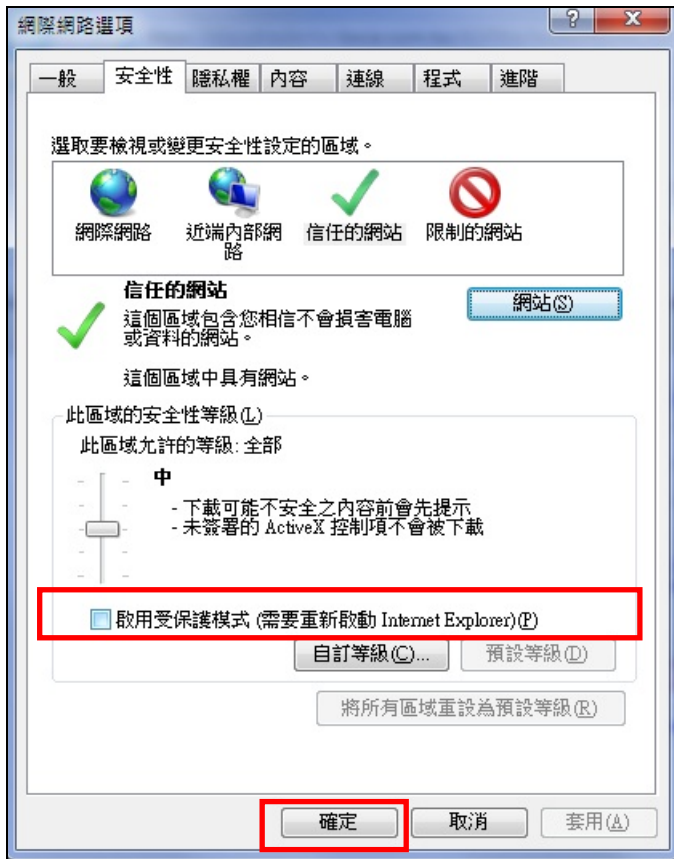


(c) 新增完畢後，點選「關閉」，關閉此對話盒，



(d) 確認「啟用受保護模式」是「取消」的狀態後，請點選「確定」，然後關閉所有
IE 程式，再重新執行 IE 程式。

註：如無啟用受保護模式選項，請忽略此操作項目。



3.2.2 憑證申請作業

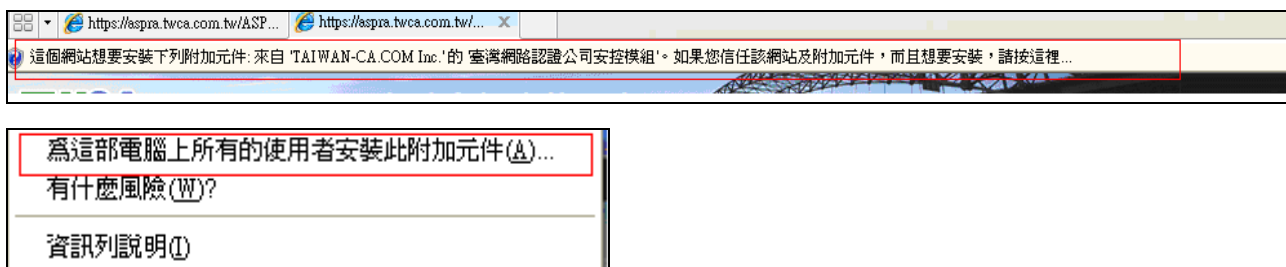
- (1) 使用 IE 連線至「財團法人金融聯合徵信中心加密檔案傳輸作業憑證註冊中心」

測試憑證申請網址：<https://cloudrademo.twca.com.tw/JCIC>

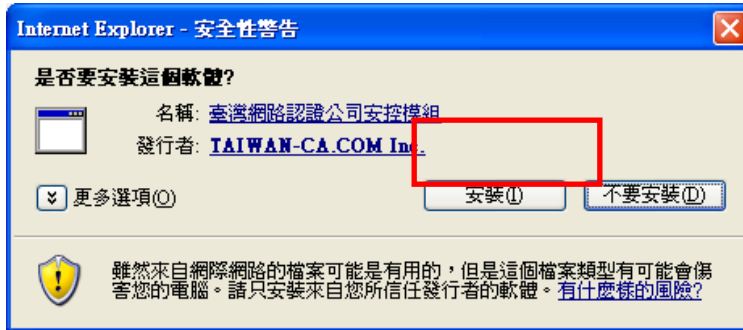
正式憑證申請網址：<https://aspra.twca.com.tw/ASPRA/faces/Home.jsp?RA=JCIC>

- (2) 登入網站須安裝網站元件，其方式下：

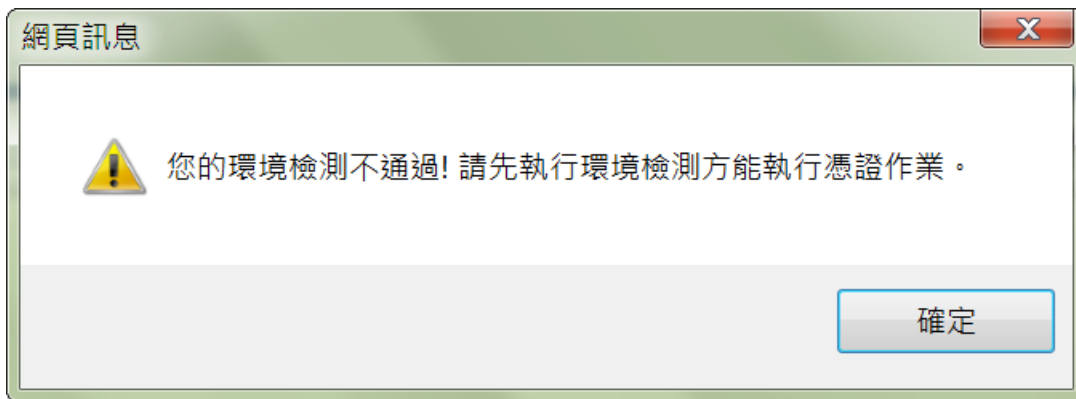
(a)將游標指向網頁中夾帶的訊息（如下圖），按右鍵安裝。



(b) 請依網站顯示之訊息安裝網站元件 (如下圖), 請點選「安裝」。

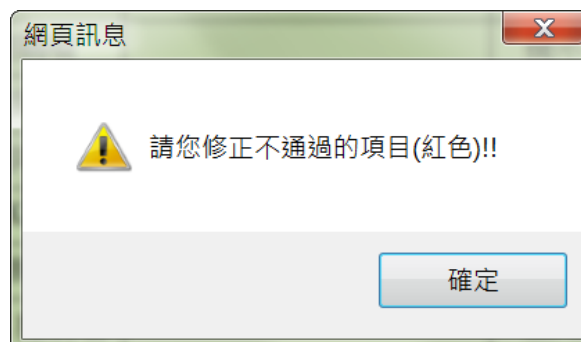


(c) 注意!!若用戶登入系統時跳出以下視窗：



✓ 登入後點選主選單中的「環境檢測」, 畫面將跳出環境檢測結果頁面,

以下圖為例, 未加入信任網站。



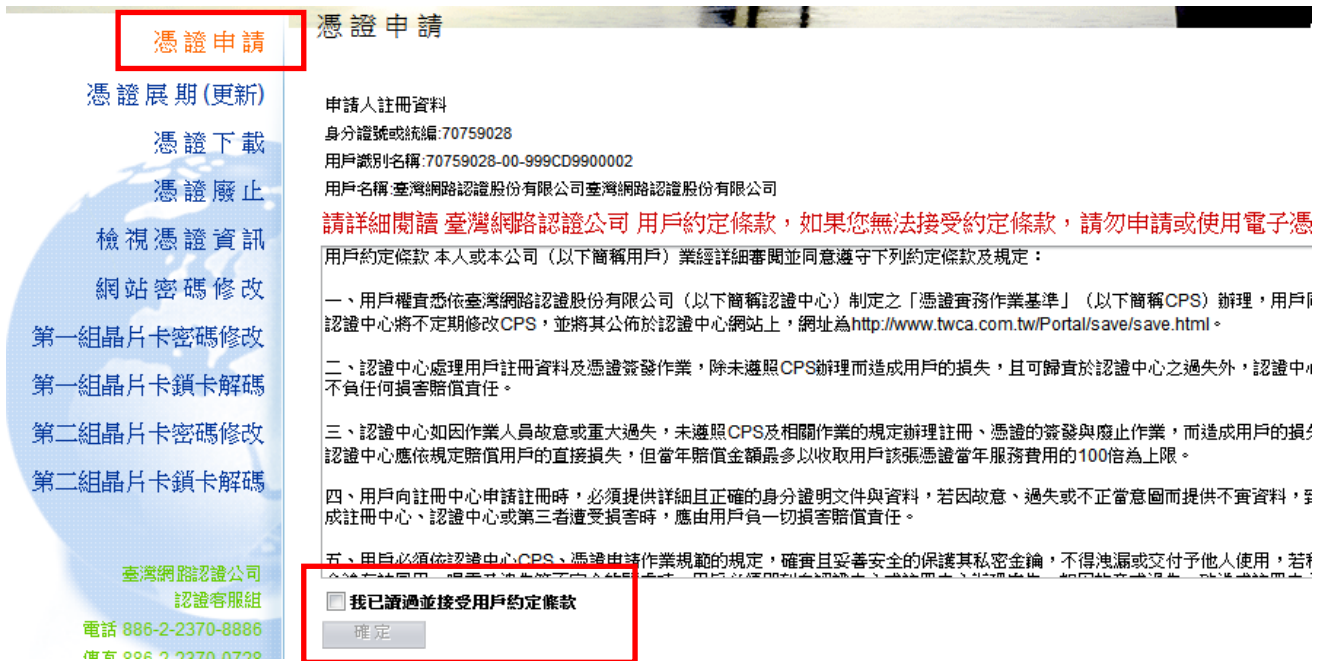
憑證作業環境檢查					
檢查項目			檢查結果		
作業系統版本(OS)			Microsoft Windows 7(x86)		
螢幕解析度(Monitor DPI)			全彩(24 位元)1237 x 696 像素		
瀏覽器版本			Internet Explorer(IE) 9.0		
支援JavaScript			JavaScript 1.3		
ActiveX 版本(Capix)			4.0.1.3		
ActiveX 版本(P11)			1.0.0.1		
系統環境(IE)設定調整項目					
序號	設定調整項目(信任網站區域)	目的	建議設定	您目前的設定	全部變更設定
1	加入信任網站 (*.twca.com.tw)	允許正常使用網路元件	加入	未加入	變更設定
2	下載已簽署的 ActiveX 控制項		提示	提示	變更設定
3	下載未簽署的 ActiveX 控制項		提示	提示	變更設定
4	自動提示 ActiveX 控制項	允許安裝與執行元件	停用	停用	變更設定
5	起始未標示成安全的 ActiveX 控制項		提示	提示	變更設定
6	執行 ActiveX 控制項與外掛程式		啟用	啟用	變更設定
7	執行標示為安全的 ActiveX 控制項		啟用	啟用	變更設定
8	指令碼處理 - Active Scripting	允許網頁程式運作與切換	啟用	啟用	變更設定
9	使用快顯封鎖程式(XP SP2 以上)	避免封鎖造成系統無法使用	停用	停用	變更設定
10	Yahoo 快捷列 - 阻擋跳窗功能		停用	停用	變更設定
11	Google 工具列 - 阻擋跳窗功能		停用	停用	變更設定
12	MSN 工具列 - 阻擋跳窗功能		停用	停用	變更設定

(3) 請輸入「憑證作業網站密碼單」封面上的「網站帳號」及密碼單內的密碼，並依螢幕上顯示的圖形數字輸入驗證碼，輸入完成後按下「登入」。

首次登入網站時，須變更網站密碼，此網站密碼為進入此網站(線上申請憑證及憑證展期)時使用，請牢記您的網站密碼，此網站密碼輸入三次錯誤將會暫停登入網站權限)。如密碼輸入錯誤超過三次後，解除憑證註冊中心網站登入帳號密碼鎖定之過程請參閱 Q&A 中之「4.1 憑證註冊中心網站登入帳號解鎖」章節。



(4) 請點選「憑證申請」功能，視窗右邊會顯示您所要申請的憑證資訊，請確認憑證註冊資料是否正確，並詳讀約定條款。若接受約定條款請確認無誤後請勾選「我已讀過並接受用戶約定條款」，並按下「確定」。

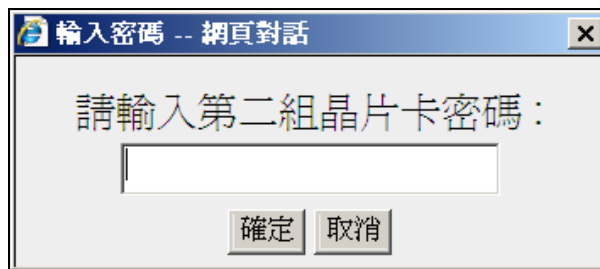
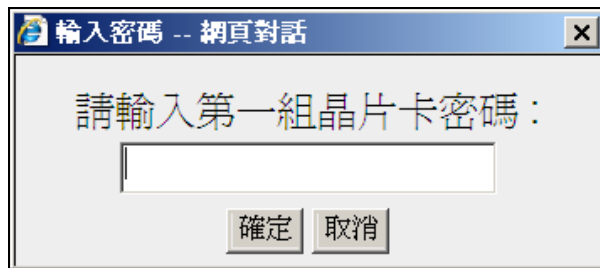


(5) 請確認將晶片卡插入讀卡機中，然後輸入兩組晶片卡密碼（請注意：**若輸入之密碼**

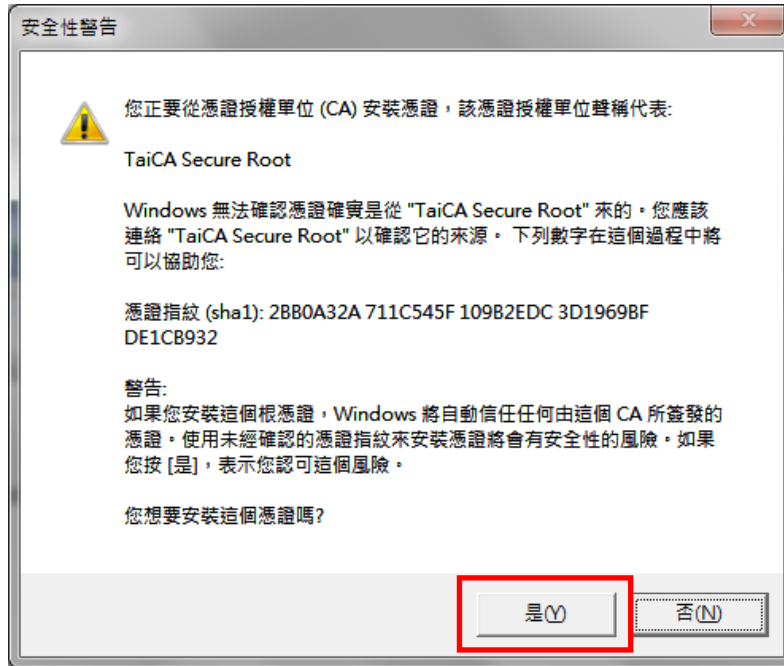
錯誤超過三次時，將被鎖卡無法使用。欲解除鎖卡狀態請參閱 Q&A 中之「4.3 憑

證晶片卡鎖卡解碼」之章節)，輸入完成後，請按下「確定」。

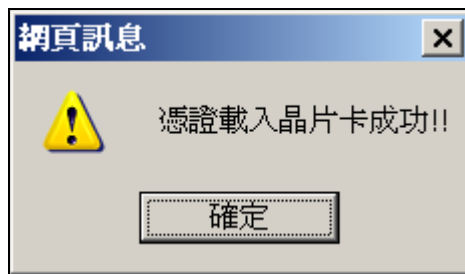
註：晶片卡密碼兩組預設皆為六個 0。請自行依公司政策規範修改晶片卡密碼並妥善保管。晶片卡密碼修改方式請參閱 Q&A 中之「4.2 晶片卡密碼修改」。



- (6) 晶片卡將開始產製金鑰並進行憑證申請，憑證申請作業過程約需 1~3 分鐘，請耐心等待，切勿離開此畫面，也不要將晶片卡自讀卡機中拔除。
- (7) 若螢幕顯示「您正要從憑證授權單位 (CA) 安裝憑證，該憑證授權單位聲稱代表」視窗，請按下「是」。



(8) 憑證申請完成，請按下「確定」。



(9) 完成憑證申請作業



3.2.3 提供加密憑證序號予聯徵中心

- (1) 請點選「檢視憑證資訊」功能，視窗右邊會顯示您所有的憑證資訊。
- (2) 請找出並記下有效起始日為最新且憑證用途為加密憑證之「憑證序號」後，

通知聯徵中心，以利測試或上線作業。

註：聯絡資訊請參閱「5.聯絡資訊」章節。

財團法人金融聯合徵信中心加密檔案傳輸作業憑證註冊中心
 Trust. Warranty. Cooperation. Action

檢視憑證資訊

憑證申請
 憑證展期(更新)
 憑證下載
 憑證廢止
 檢視憑證資訊
 網站密碼修改
 第一組晶片卡密碼修改
 第一組晶片卡鎖卡解碼
 第二組晶片卡密碼修改
 第二組晶片卡鎖卡解碼

臺灣網路認證公司
 認證客服組
 電話 886-2-2370-8886
 傳真 886-2-2370-0728

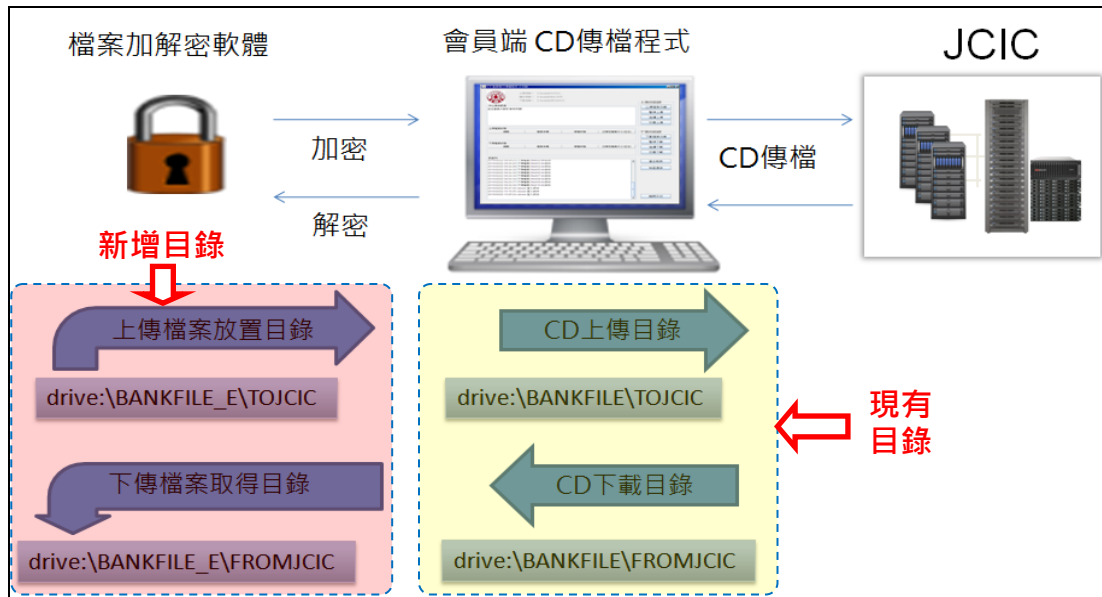
若欲執行"存檔"作業，請依下列說明辦理：
 1. 您必須分別對簽章憑證及加密憑證執行存檔動作。
 2. 上述簽章憑證及加密憑證之有效截止日必需相同。
 3. 存檔之憑證通常是最近申請(更新)的憑證。
 4. 存檔過程中，請自行指定儲存檔案的目錄名稱，完成後，請檢查上述目錄內是否有您執行"存檔"的相對應檔案(副檔名為.cer)產生，且檔案的修改日期與作業時間相同。

憑證編號	用戶識別名稱	憑證序號	憑證狀態	憑證用途	有效起始日	有效截止日	申請人主旨	簽發者主旨	憑證檔
395	70759028-00-999CD9900002	4D81B340	有效	加密憑證	Thu Feb 23 19:49:33 CST 2012	Sun Feb 23 23:59:59 CST 2014	CN=70759028-00-999CD9900002,OU=Joint Credit Information Center,OU=9980000-RA-JCIC,OU=TaiCA Test FXML CA,O=Finance,C=TW	CN=TaiCA Test FXML CA,OU=Evaluation Only,O=TAWAN-CA.COM Inc.,C=TW	存檔
394	70759028-00-999CD9900002	4D81B33D	有效	簽章憑證	Thu Feb 23 19:49:27 CST 2012	Sun Feb 23 23:59:59 CST 2014	CN=70759028-00-999CD9900002,OU=Joint Credit Information Center,OU=9980000-RA-JCIC,OU=TaiCA Test FXML CA,O=Finance,C=TW	CN=TaiCA Test FXML CA,OU=Evaluation Only,O=TAWAN-CA.COM Inc.,C=TW	存檔

3.3. 憑證安控模組設定

3.3.1 建立憑證安控模組使用目錄(原機升版可略過此步驟)

- (1) 憑證安控模組使用目錄建立作業，已在程式安裝時完成，在此不再另外說明。
- (2) 下圖為增加憑證安控模組後，使用單位端系統之目錄運作之說明。



(5) 請確認下列之目錄已存在。

drive:\BANKFILE_E\TOJCIC
 drive:\BANKFILE_E\FROMJCIC
 drive:\BANKFILE_E\FROMBAK
 drive:\BANKFILE_E\TOBAK

註 1: 「drive:」代表原 BANKFILE 目錄所在之磁碟，如「C:」或「D:」

註 2: 『drive:\BANKFILE_E\TOJCIC』：放置欲上傳至聯徵中心的原始檔之目錄

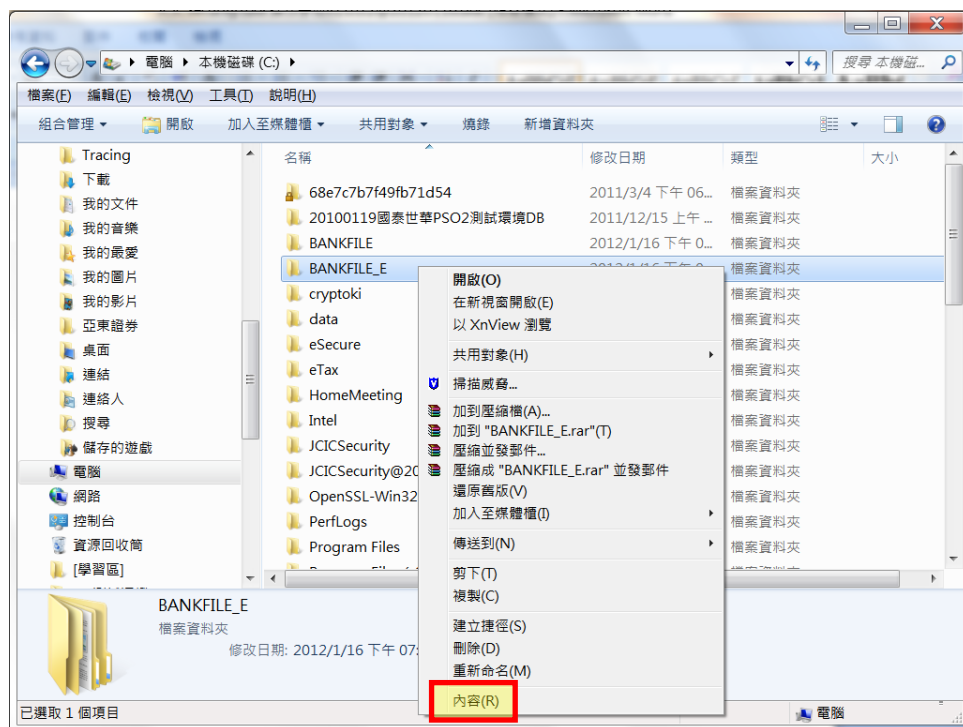
『drive:\BANKFILE_E\FROMJCIC』：該目錄存放聯徵中心傳送過來，完成解密驗章之明文檔案。

『drive:\BANKFILE_E\FROMBAK』：該目錄存放聯徵中心加密過後傳送過來之加密檔案備份。可做為當雙方其中一方對傳輸過後之內容有疑慮之舉證資料。請各使用單位依需求執行備份及清除檔案等作業。

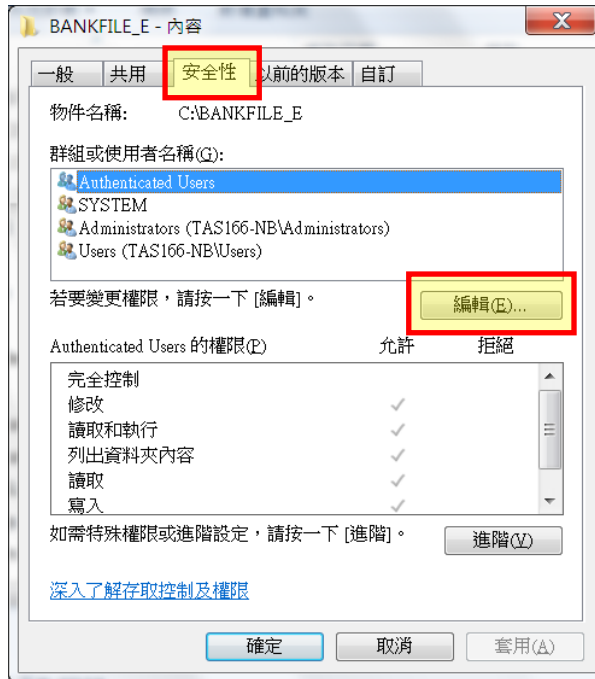
『drive:\BANKFILE_E\TOBAK』：該目錄存放使用單位端傳送至聯徵中心之原始未加密的檔案備份。請各使用單位依需求執行備份及清除檔案等作業。

(6) 完成目錄確認後，設定 BANKFILE_E 權限為 cduser 帳號具備完全控制權限

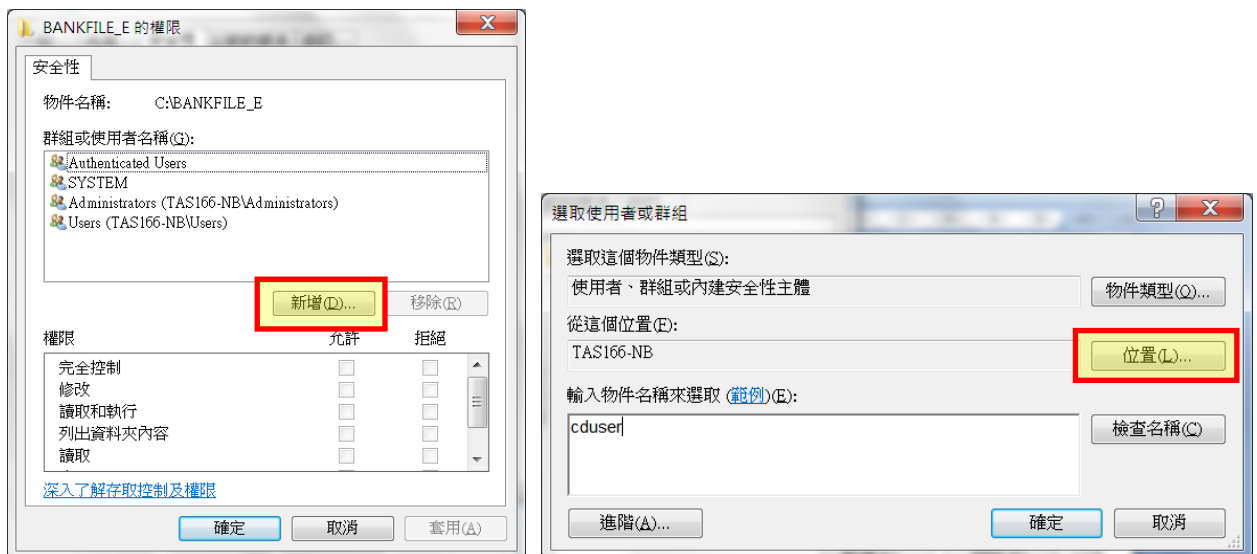
(a) 於 BANKFILE_E 目錄點擊右鍵後，選取「內容」



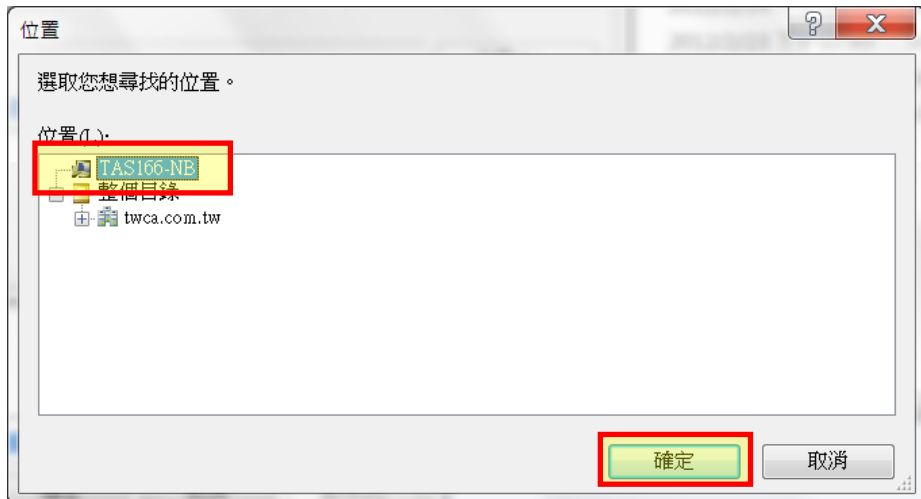
(b) 切換主選單為「安全性後」，點擊「編輯」鈕。



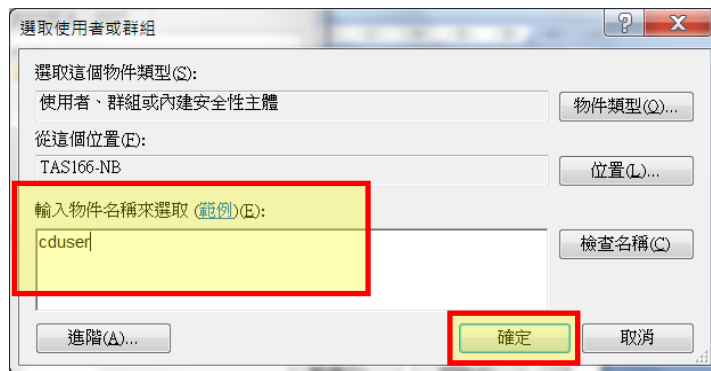
(c) 點擊「新增」鈕後，系統出現選取使用者或群組的視窗，請點擊該視窗之「位置」鍵。



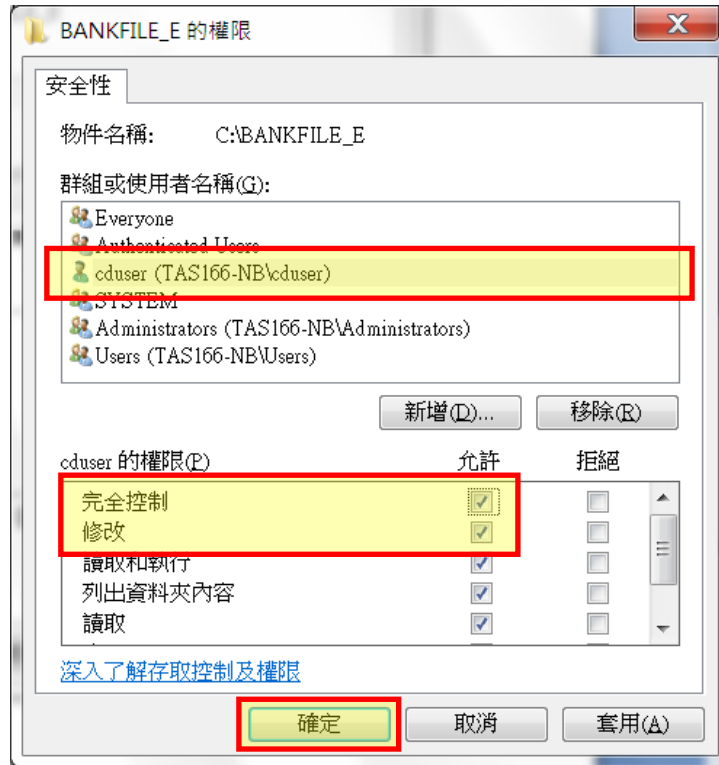
(d) 於位置視窗中選取目前使用之本機名稱後，按「確定」鈕。以下圖為例，本機名稱為「TAS166-NB」。



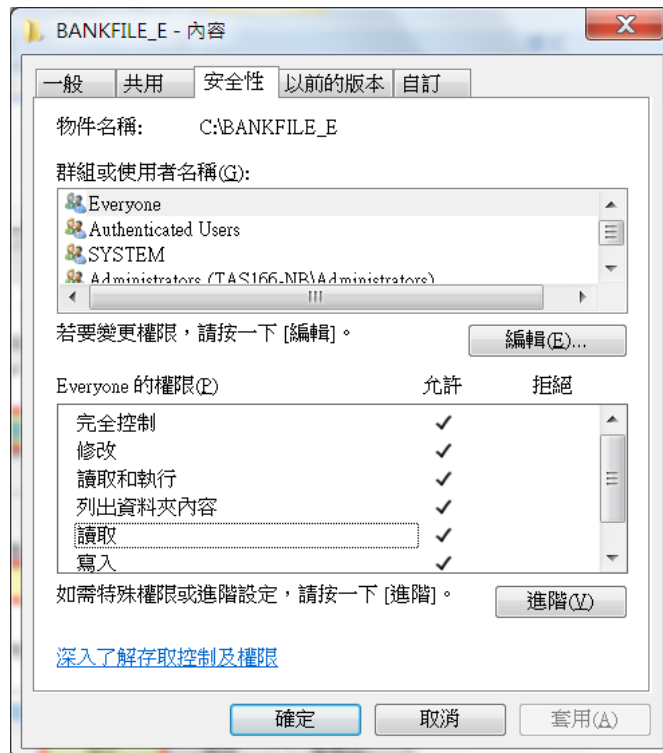
(e) 於輸入物件名稱來選取欄位中，輸入「cduser」後點選「確定」。



(f) 選取「cduser」後，於 cduser 權限之完全控制項目中勾選「允許」。完成後點選「確定」。

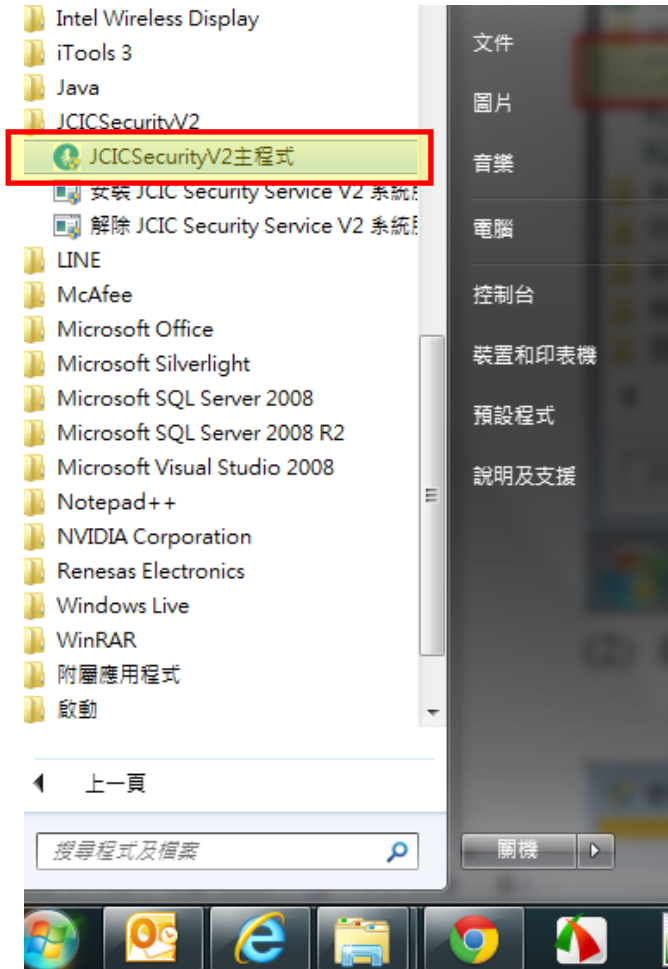


(g) 點擊「確定」完成目錄權限調整作業。

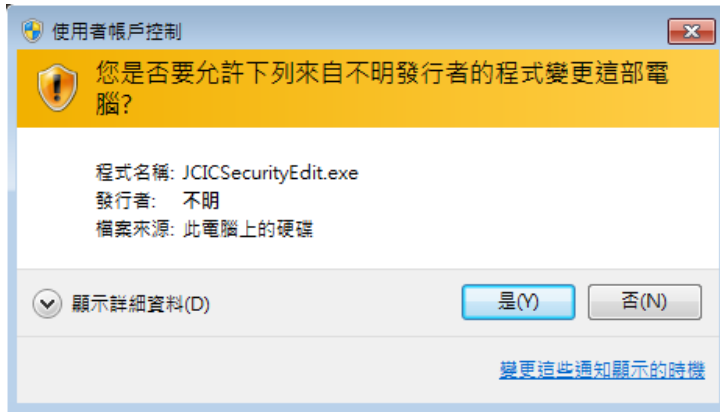


3.3.2 啟動憑證安控模組，並讀取晶片卡憑證資料

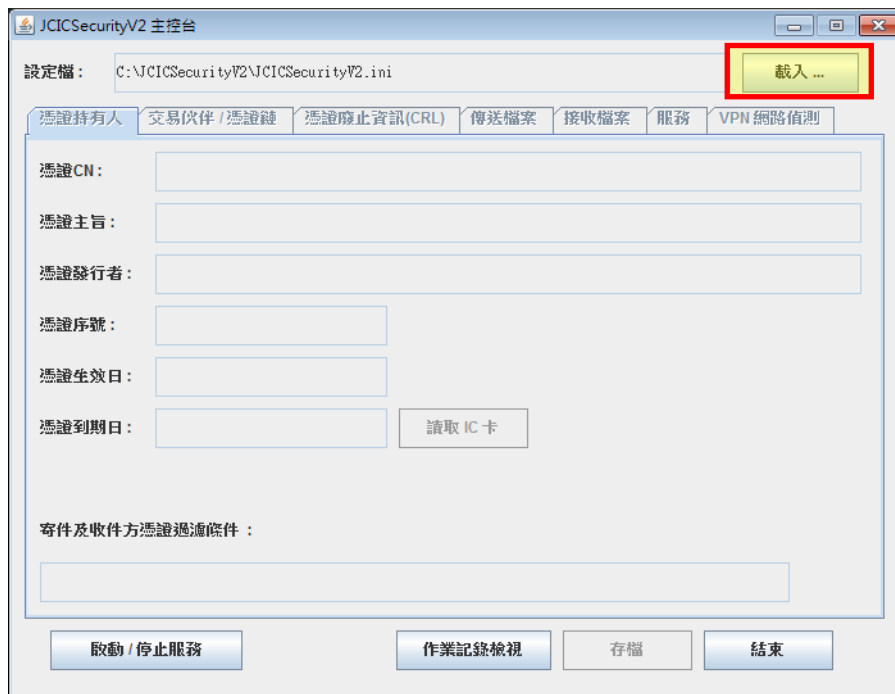
- (1) 點擊『開始』→『所有程式』→『JCICSecurityV2』→捷徑『JCICSecurity V2 主控台』（為聯徵中心圖示），以『系統管理員身份執行』。



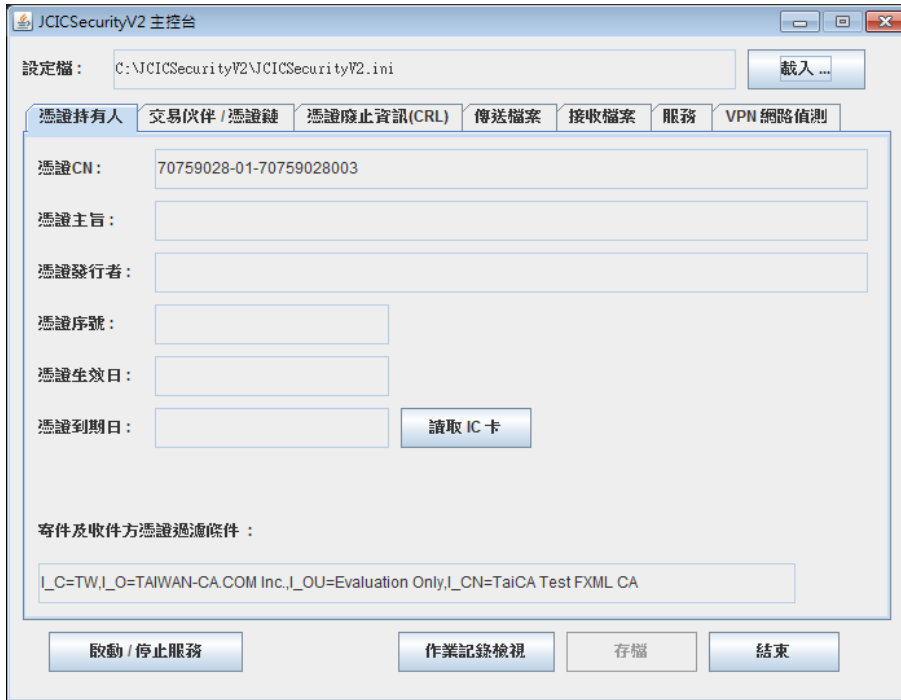
- (2) 執行後，出現如下畫面，請點選『是』，必要時需輸入系統管理員密碼，以繼續執行，若點選『否』將立即返回作業系統。



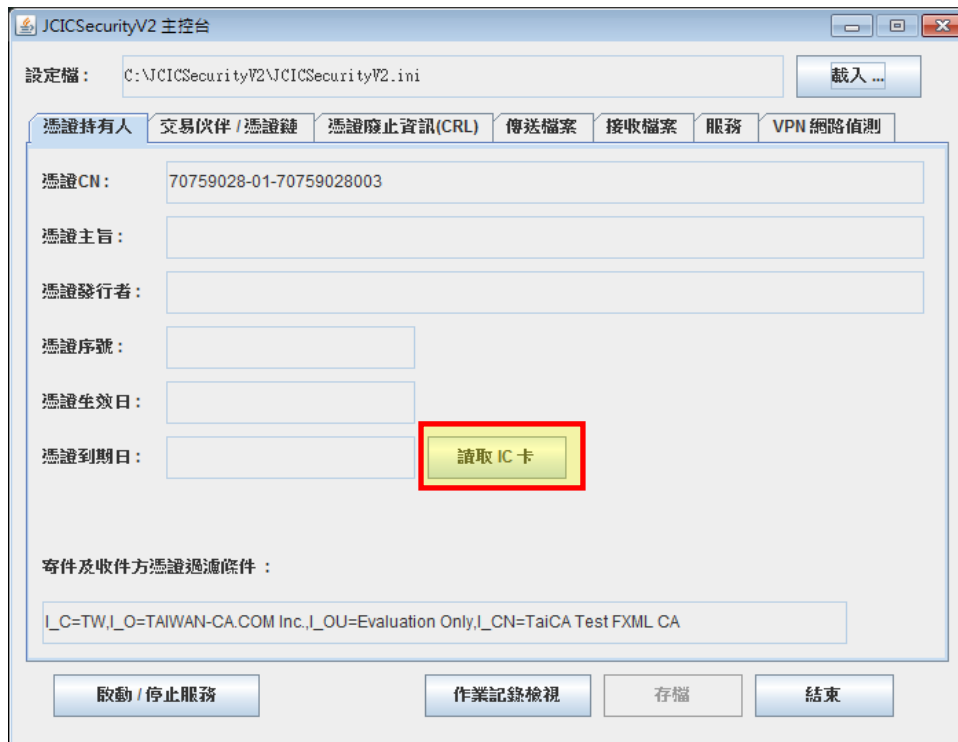
(3) 成功開啟 JCICSecurityV2 主控台。點擊「載入」讀取加解密軟體目前之設定值。



(4) 當點選載入之後，『JCIC Security V2 主程式』會將加解密軟體目前之『憑證持有人』設定載入。畫面如下：



(5) 點選『讀取 IC 卡』以取得晶片卡中之憑證資訊。



(6) 點選『讀取 IC 卡』之後，請輸入兩組晶片卡密碼



(8) 完成『讀取 IC 卡』之後，出現下圖。完成後，請點選「存檔」。

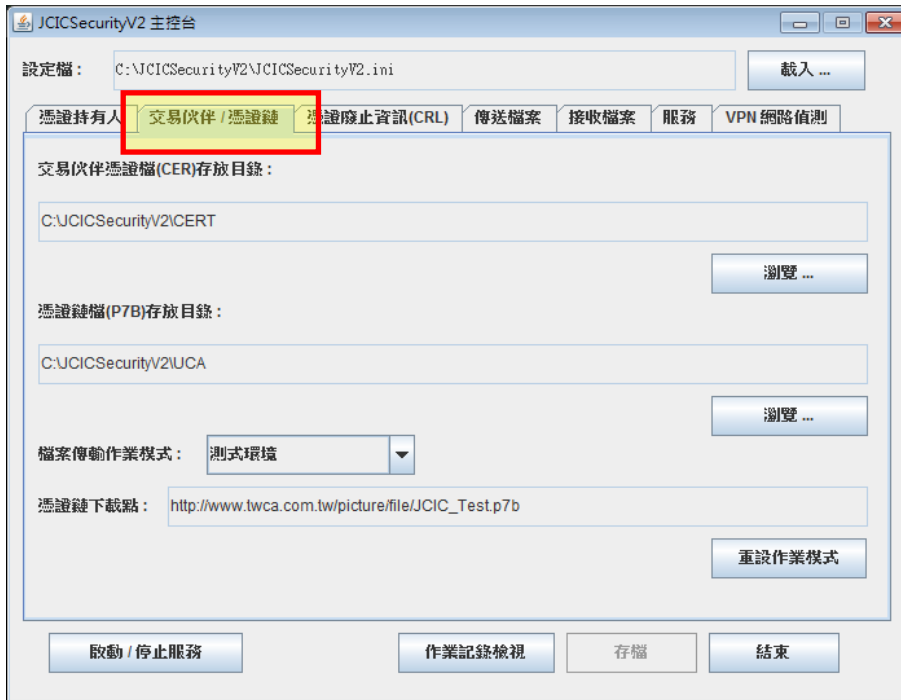


(9) 設定檔存檔成功。

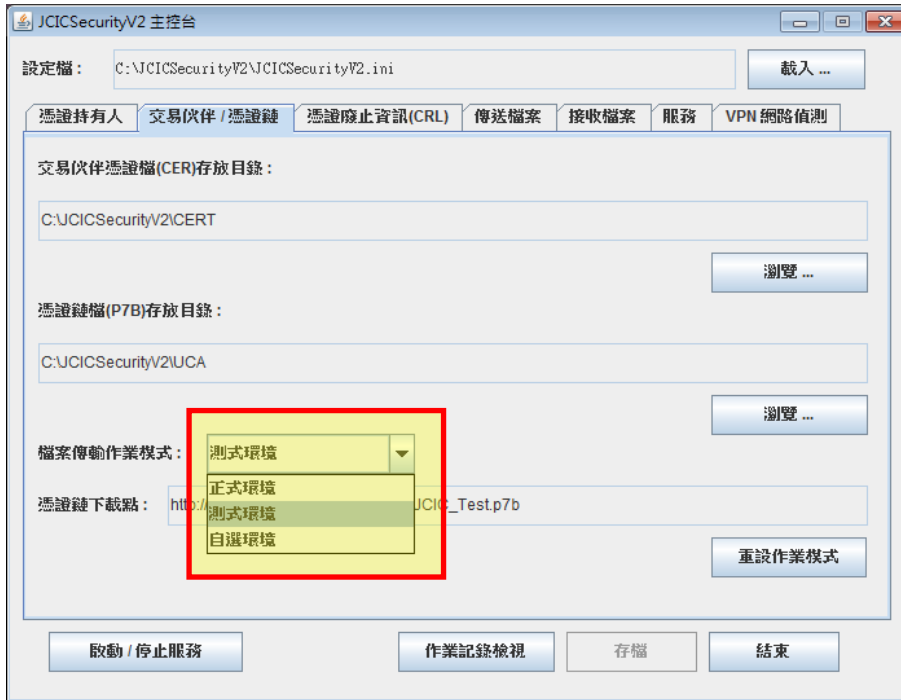


3.3.3 設定交易夥伴/憑證鏈

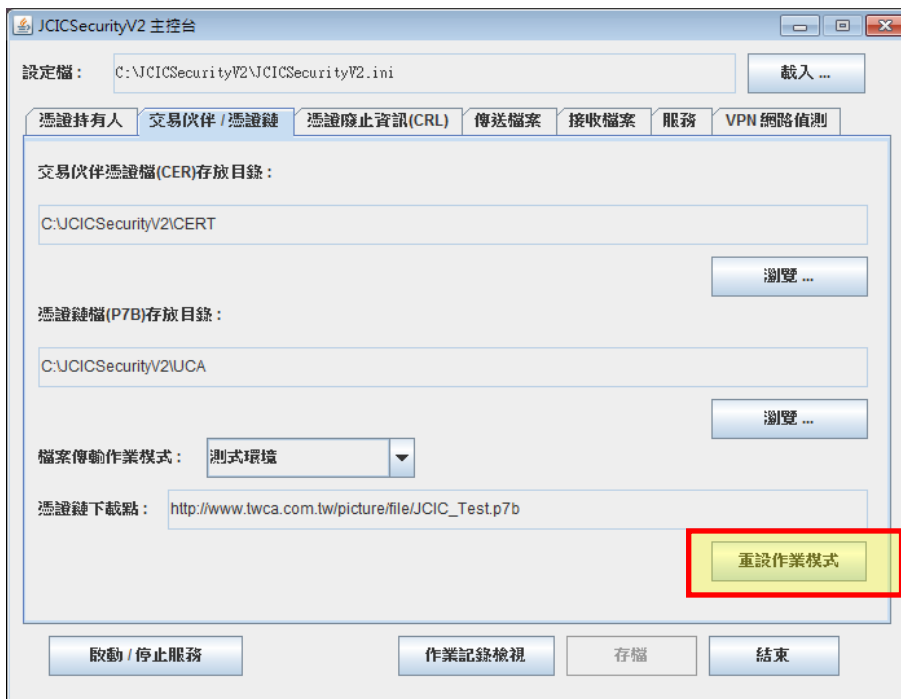
(1) 於 JCICSecurityV2 控制台上方功能選單中點擊『交易伙伴/憑證鏈』。



(2) 依用途於「檔案傳輸作業模式」之下拉選單中選取適合之選項。如果使用測試晶片卡時，請選取「測試環境」；於上線使用正式晶片卡時，請選取「正式環境」選項。



(3) 點擊『重設作業模式』。



(4) 自動完成憑證鏈檔案下載及儲存。



(5) 自動完成中心端加密憑證檔案下載及儲存。

註:請記住該 EE 憑證檔之檔案名稱, 該檔案將於 3.3.4 章節之步驟(6)及 3.3.5 章節之步驟(3)使用之。



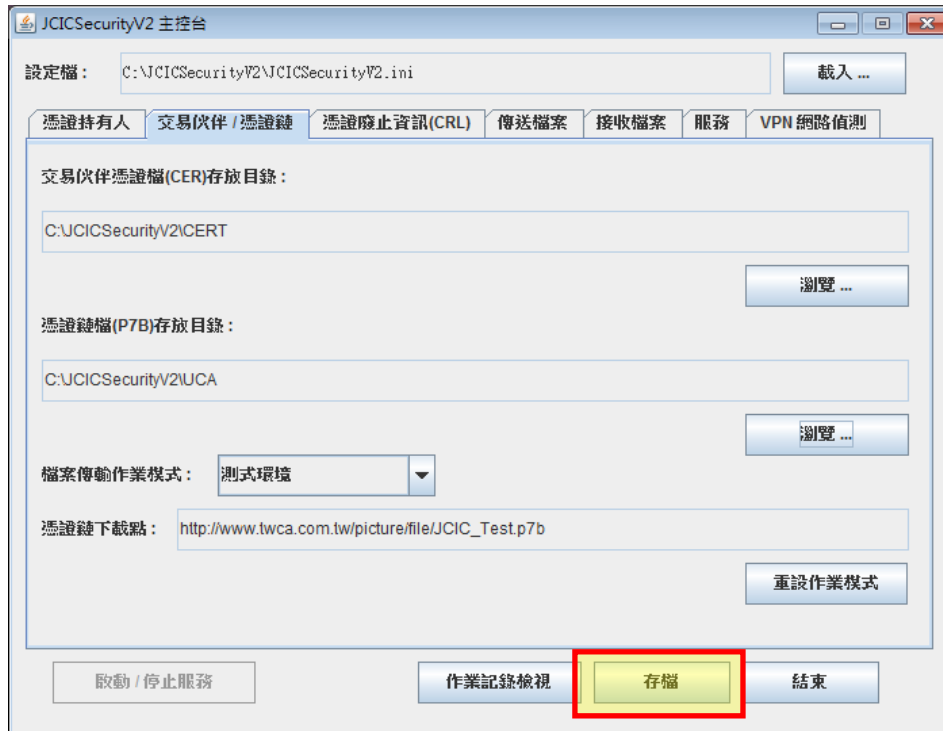
(6) 自動完成寄件及收件方憑證過濾條件設定。



(7) 自動完成 CRL 下載點 URL 設定。



(8) 點擊『存檔』，儲存目前設定值。



(9) 設定檔存檔成功。



3.3.4 傳送檔案設定

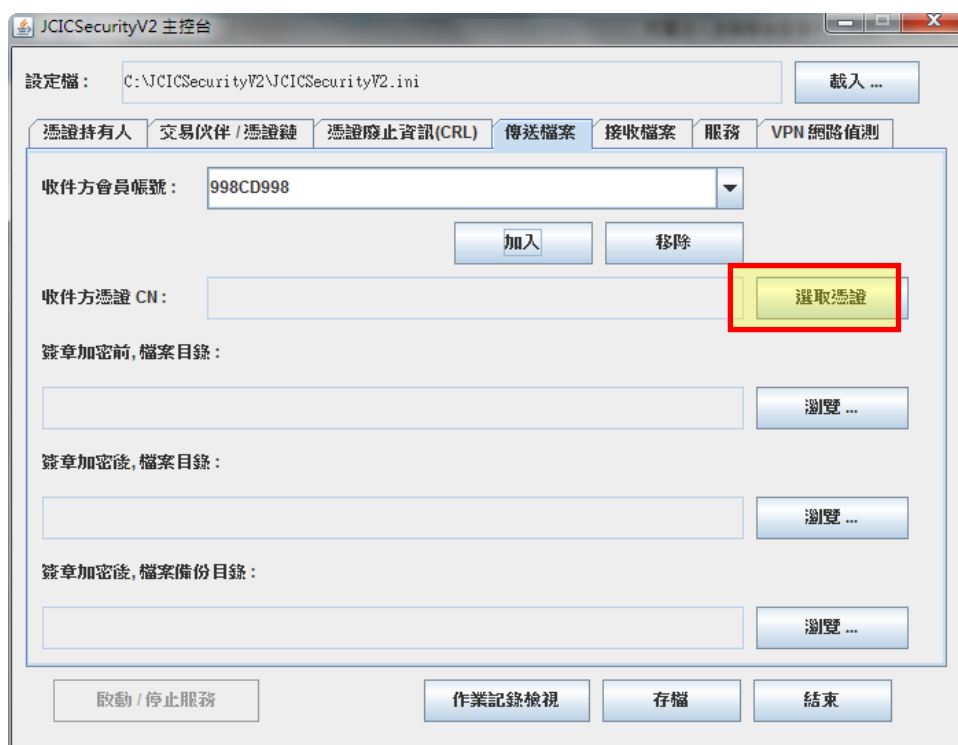
(1) 於 JCICSecurityV2 控制台上功能選單中點擊『傳送檔案』。



(2)於「收件方會員帳號:」欄位輸入「998CD998」後,點選「加入」鍵。



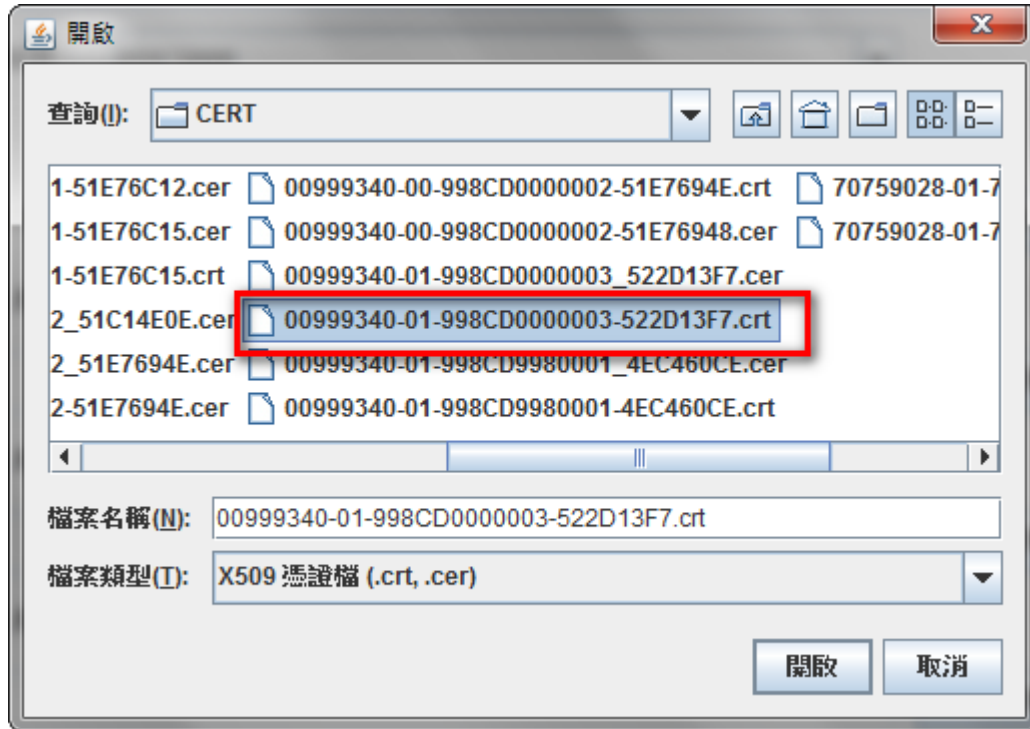
(3) 點擊「選取憑證」鈕。



(4) 選取 3.3.3 節之步驟(5)所顯示之憑證檔，並點擊「開啟」。

注意: 正式環境收送件方憑證 CN 的選取為

00999340-01-998CD0000003-522D13F7 !



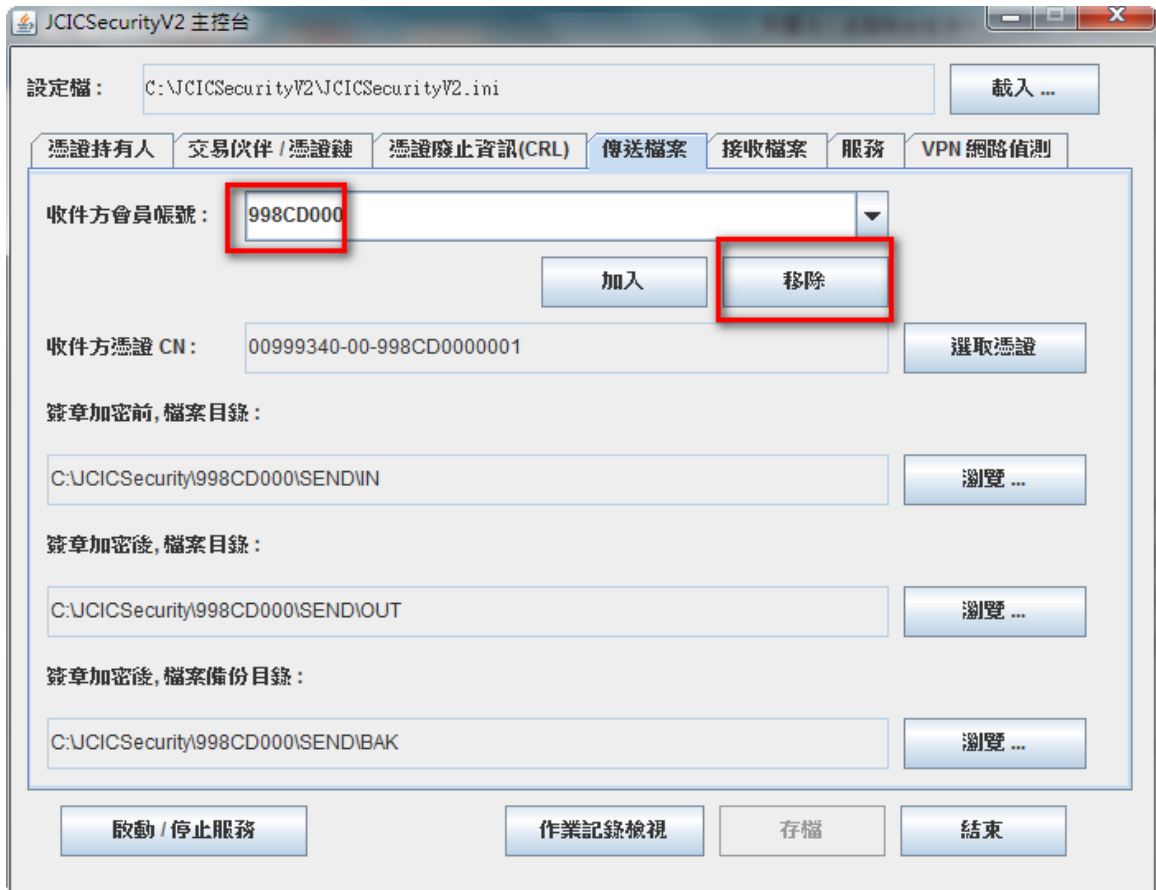
(5) 選取簽章加密前，檔案目錄:之「瀏覽」鍵，並選取「C:\BANKFILE_E\TOJCIC」

選取簽章加密後，檔案目錄:之「瀏覽」鍵，並選取「C:\BANKFILE\TOJCIC」

選取簽章加密後，檔案備份目錄:之「瀏覽」鍵，並選取「C:\BANKFILE_E\TOBAK」

註: 依「3.3.1 建立憑證安控模組使用目錄」章節之目錄建置調整 C 或 D。

(6) 移除 998CD000 帳號



(7) 點擊『存檔』，儲存目前設定值。

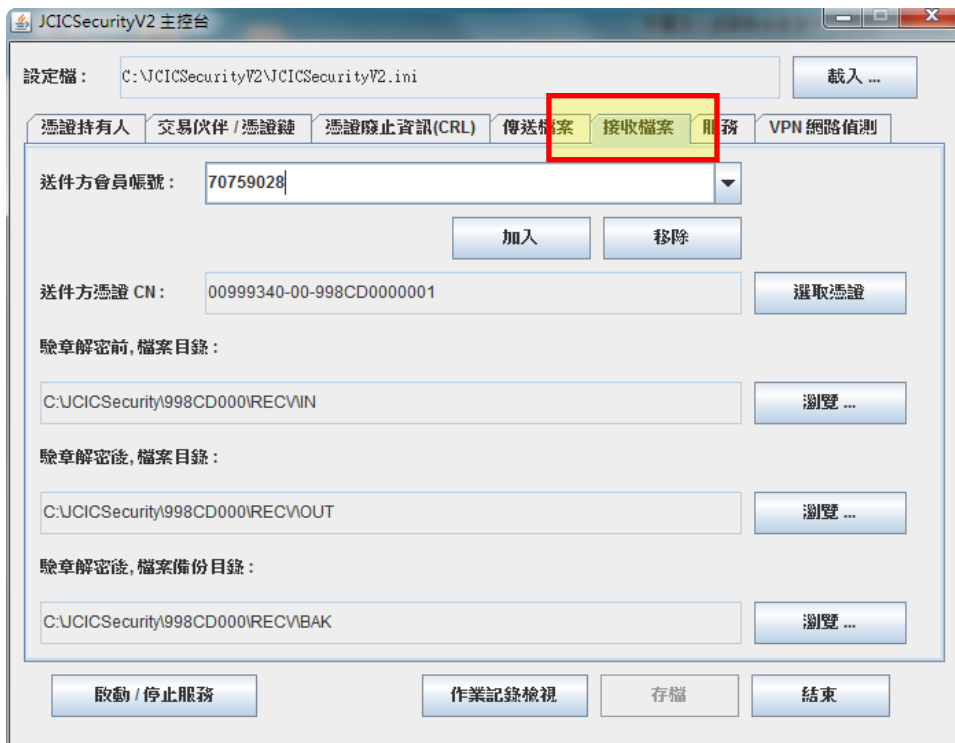


(8) 設定檔存檔成功。



3.3.5 接受檔案設定

(1) 於 JCICSecurityV2 控制台上方功能選單中點擊『接收檔案』。



(2) 於「送件方會員帳號:」欄位輸入「998CD998」後，點選「加入」鍵。



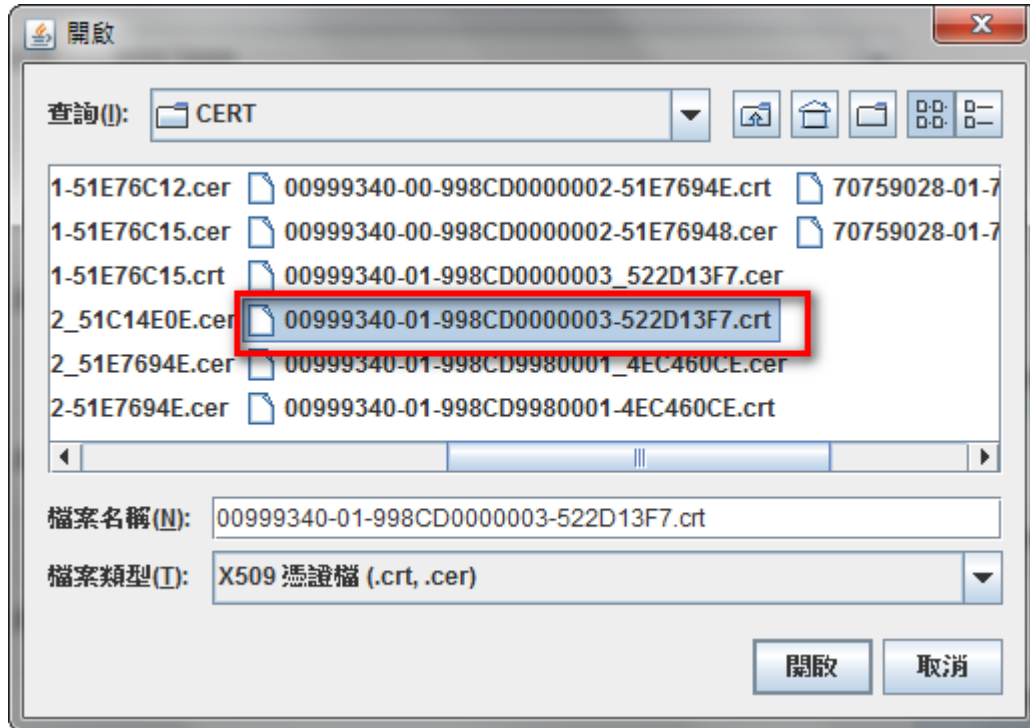
(3) 點擊「選取憑證」鈕。



(4) 選取 3.3.3 節之步驟(5)所顯示之憑證檔，並點擊「開啟」。

注意: 正式環境收送件方憑證 CN 的選取為

00999340-01-998CD0000003-522D13F7 !



(5) 選取驗章解密前，檔案目錄:之「瀏覽」鍵，並選取「C:\BANKFILE\FROMJIC」

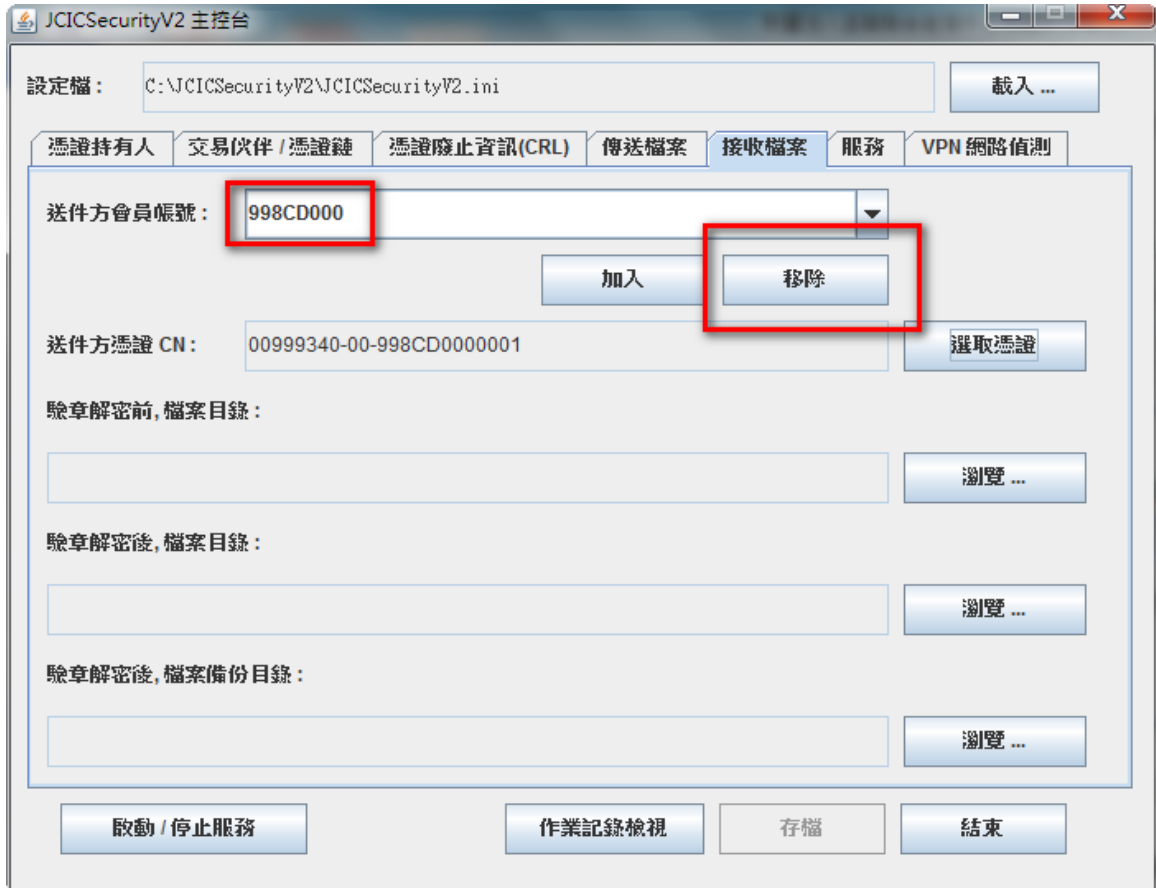
選取驗章解密後，檔案目錄:之「瀏覽」鍵，並選取「C:\BANKFILE_E\FROMJIC」

選取驗章解密後，檔案備份目錄:之「瀏覽」鍵，並選取「C:\BANKFILE_E\FROMBAK」

註: 依「3.3.1 建立憑證安控模組使用目錄」章節之目錄建置調整 C 或 D。



(6) 移除 998CD000 帳號



(7) 點擊『存檔』，儲存目前設定值。



(8) 設定檔存檔成功。

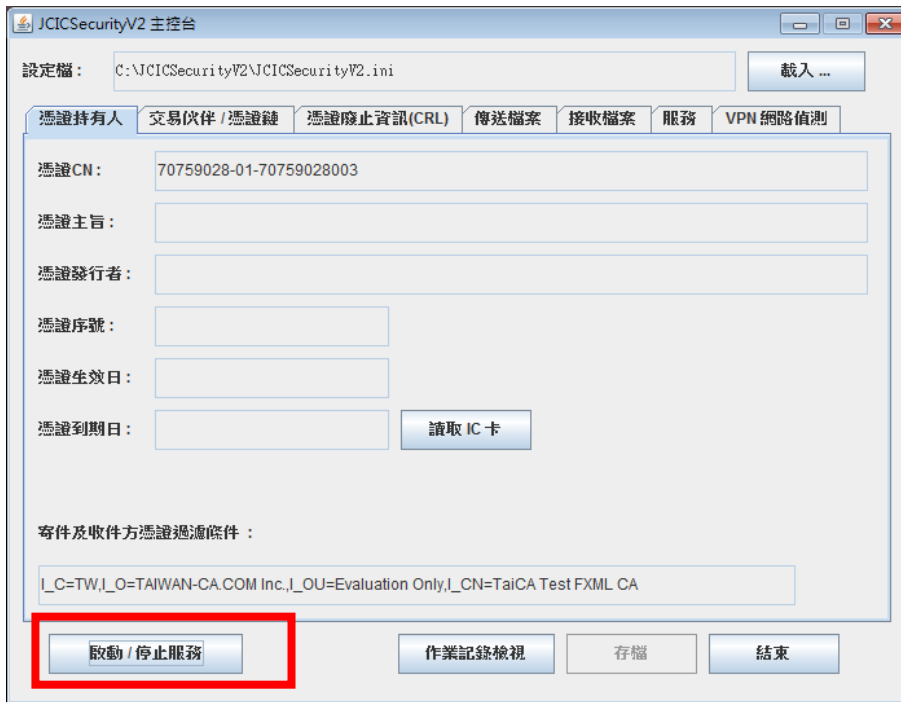


3.4. 憑證安控模組啟動/暫停/繼續/停止服務測試

***注意:如使用單位之測試機與正式機為同一部電腦時, 請注意進行憑證安控模組啟動測試時, 切勿執行正式環境之檔案傳輸作業(包含傳送及接收檔案)。**

3.4.1 憑證安控模組啟動服務

(1) 下圖為『JCIC Security V2 主程式』執行畫面, 請點擊『啟動/停止服務』按鈕。



(2) 點選『啟動/停止服務』後，畫面如下：



(3) 啟動服務前，請確定讀卡機驅動程式，已經安裝完成，且晶片卡已經插入讀卡機。

點選『啟動服務』，依序輸入 2 組 IC 卡密碼。



如點選『取消』將取消讀取 IC 卡作業，返回畫面繼續操作。

等待十數秒之後，顯示服務啟動成功。



3.4.2 憑證安控模組暫停服務

(1) 當服務已經啟動執行中，如下畫面



(2) 點選『暫停服務』，即可將服務暫停，如下畫面

等待十數秒之後，顯示服務暫停成功。

註:當系統正在進行大檔案加解密傳輸時，請勿進行停止或暫停服務作業。



3.4.3 憑證安控模組繼續服務

(1) 當服務已經暫停執行中，如下畫面



(2) 點選『繼續服務』，即可將服務繼續，如下畫面

等待十數秒之後，顯示服務繼續成功。



3.4.4 憑證安控模組停止

(1) 當服務已經啟動執行中，如下畫面



(2) 點選『停止服務』，即可將服務停止，如下畫面

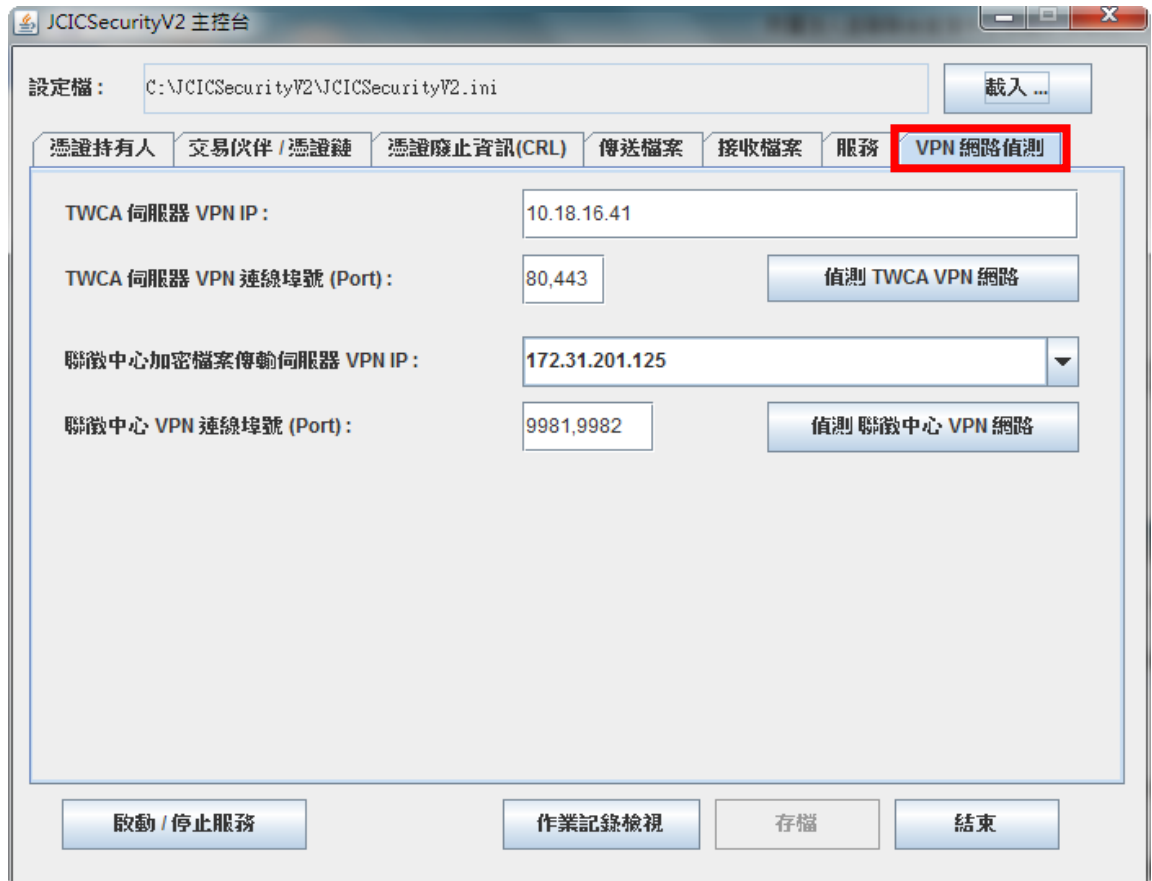
等待十數秒之後，顯示服務停止成功。

註:當系統正在進行大檔案加解密傳輸時，請勿進行停止或暫停服務作業。



3.5. VPN 網路偵測

下圖為『JCIC Security V2 主程式』執行畫面，點選『VPN 網路偵測』：



3.5.1 TWCA 伺服器 VPN IP

3.5.2 TWCA 伺服器 VPN 連線埠號(Port)

TWCA 伺服器 VPN 設定，請參考 [3.1.4] 章節(5)及(6)之設定

3.5.3 聯徵中心加密檔案傳輸伺服器 VPN IP

3.5.4 聯徵中心 VPN 連線埠號(Port)

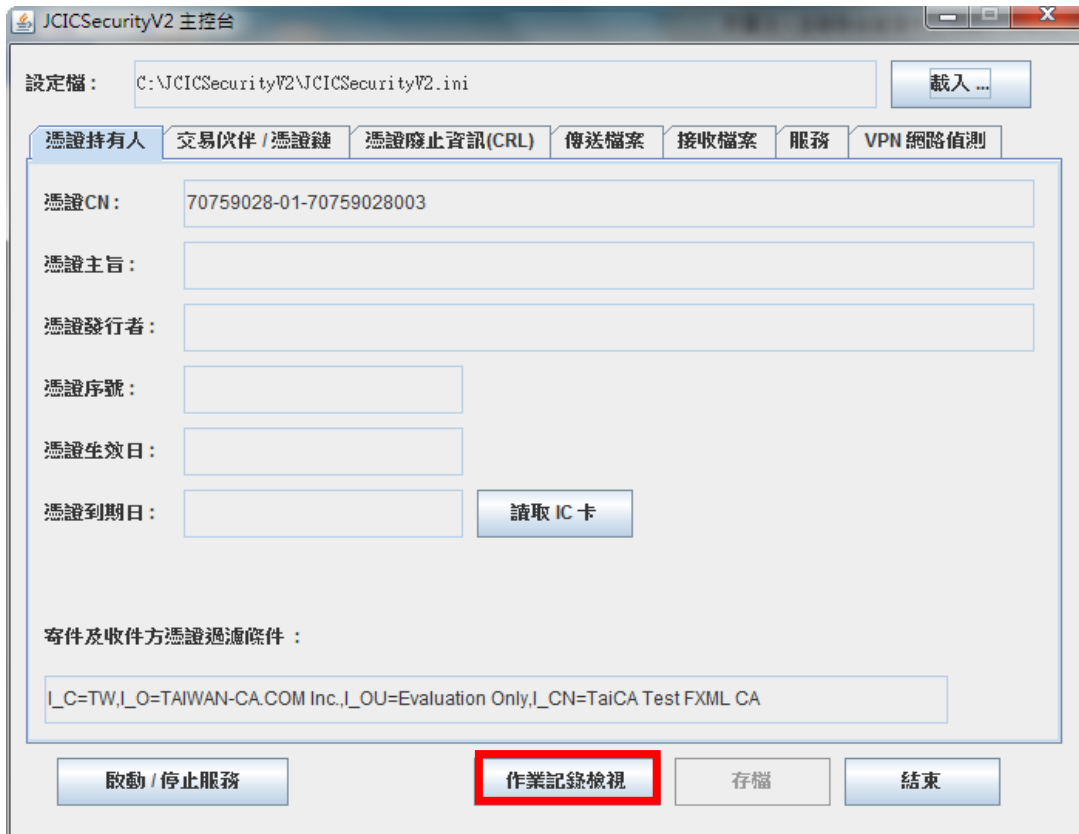
聯徵中心 VPN 設定，請參考 [3.1.4] 章節(5)及(6)之設定

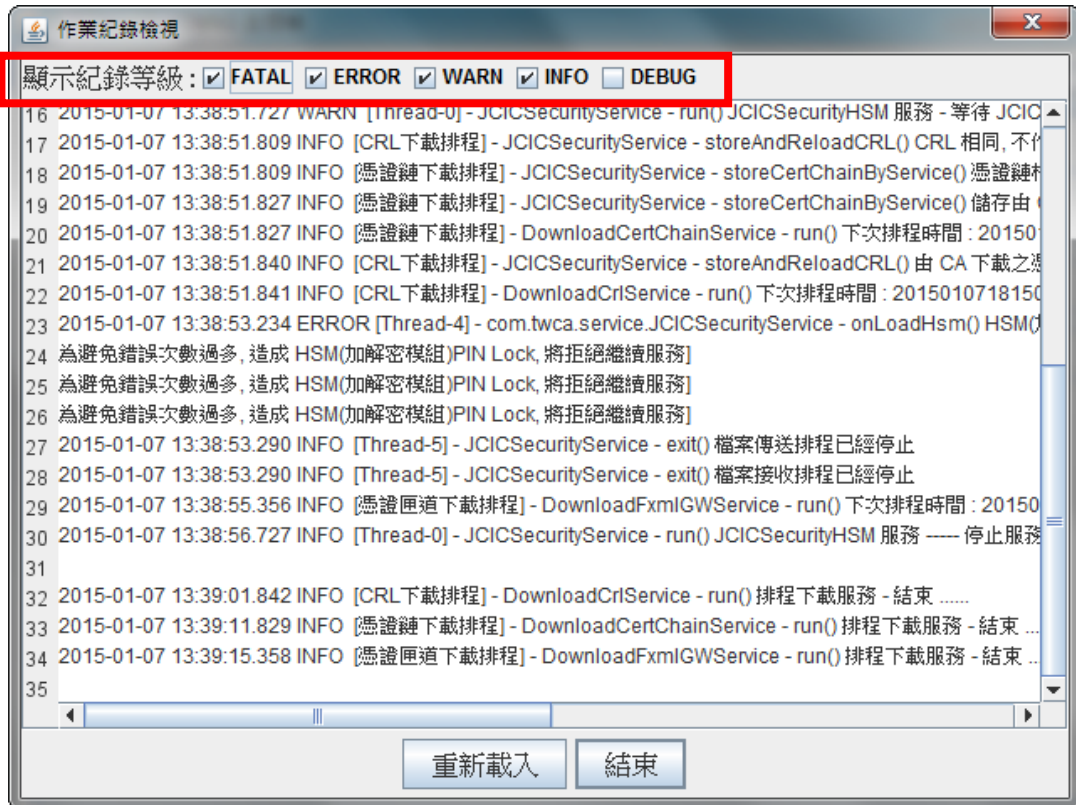
設定完成後，點擊「偵測 TWCA VPN 網路」或「偵測聯徵中心 VPN 網路」，以偵測設定

是否正確

3.6. 作業記錄檢視

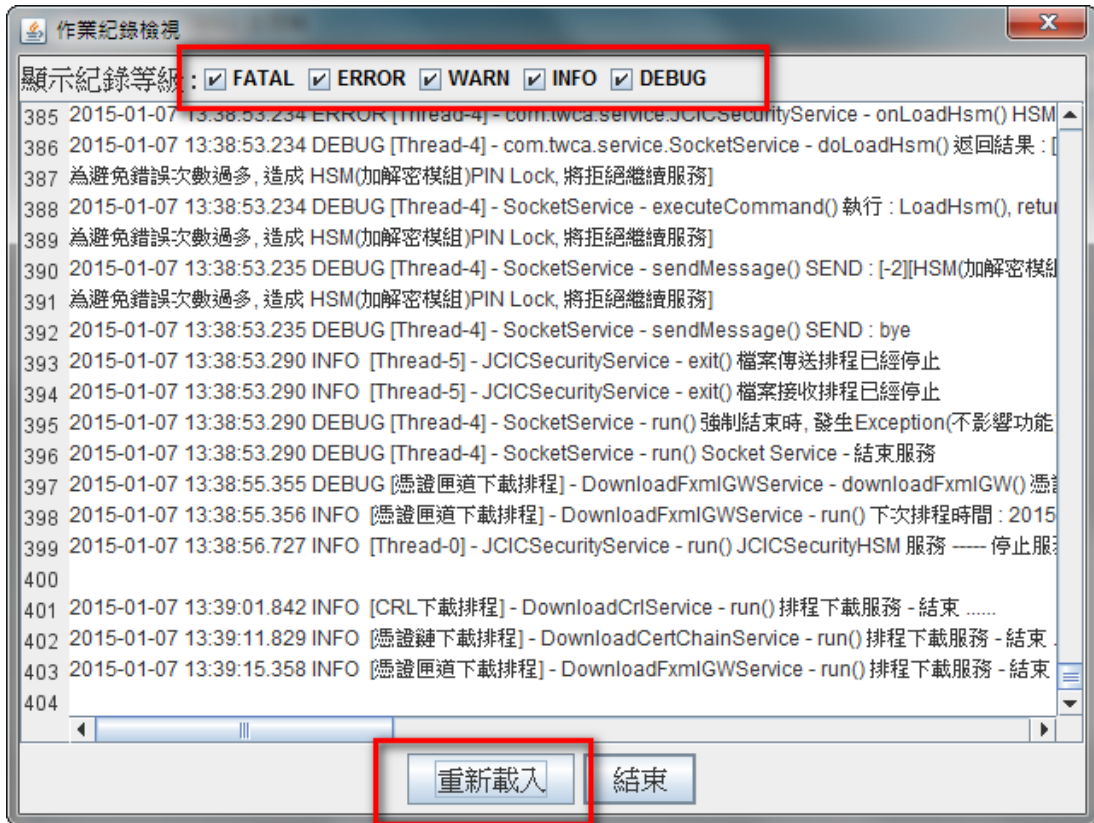
當點選「作業記錄檢視」之後，『JCICSecurityV2 控制台』畫面如下：





顯示紀錄等級分為: FATAL, ERROR, WARN, INFO, DEBUG 共 5 種, 可依需求點選

後, 按下「重新載入」查看紀錄。



3.7. 憑證安控模組功能測試

3.7.1 聯徵中心加密檔案傳輸軟體(CD 傳檔程式)測試環境連線設定

聯徵中心加密檔案傳輸伺服器 IP:

測試: 172.31.201.125

正式: 172.31.200.125

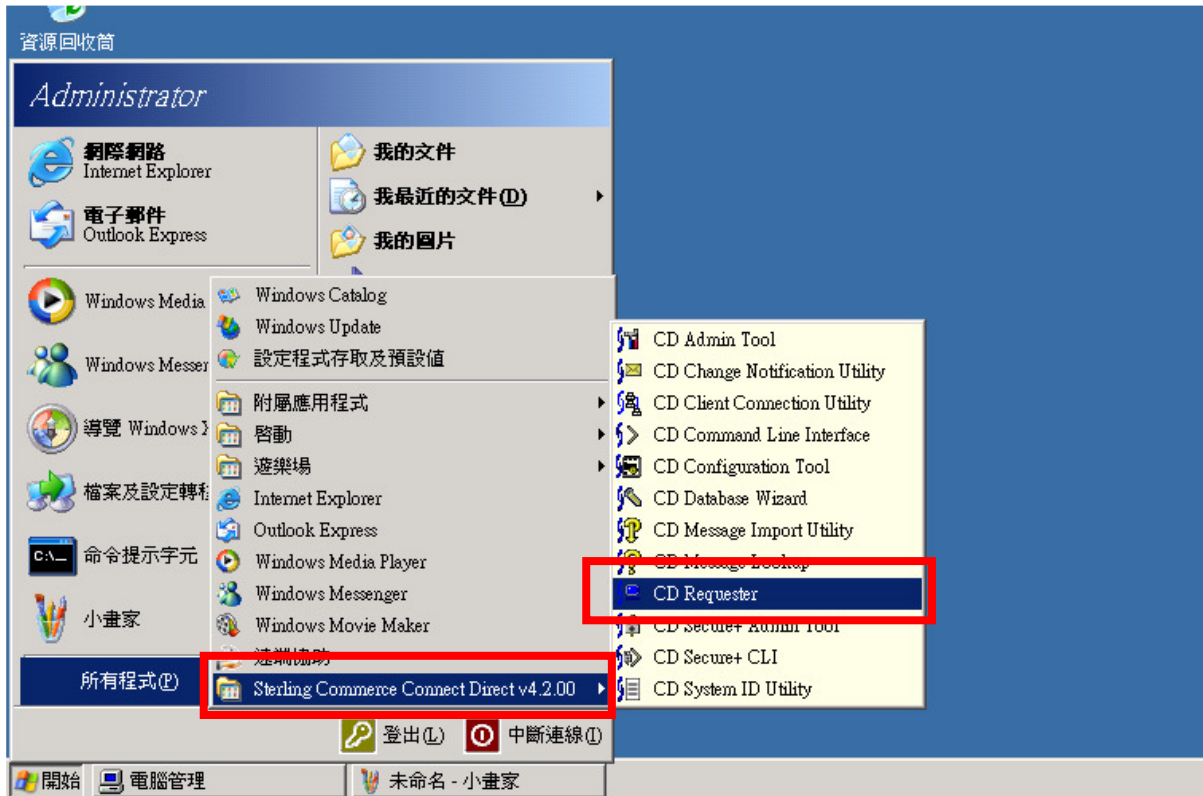
註: 如貴單位有架設防火牆, 請告知貴單位管理人員, 針對聯徵中心加密檔案傳輸伺

服器 IP172.31.200.125 及 172.31.201.125 開啟雙向 9981、9982 port。

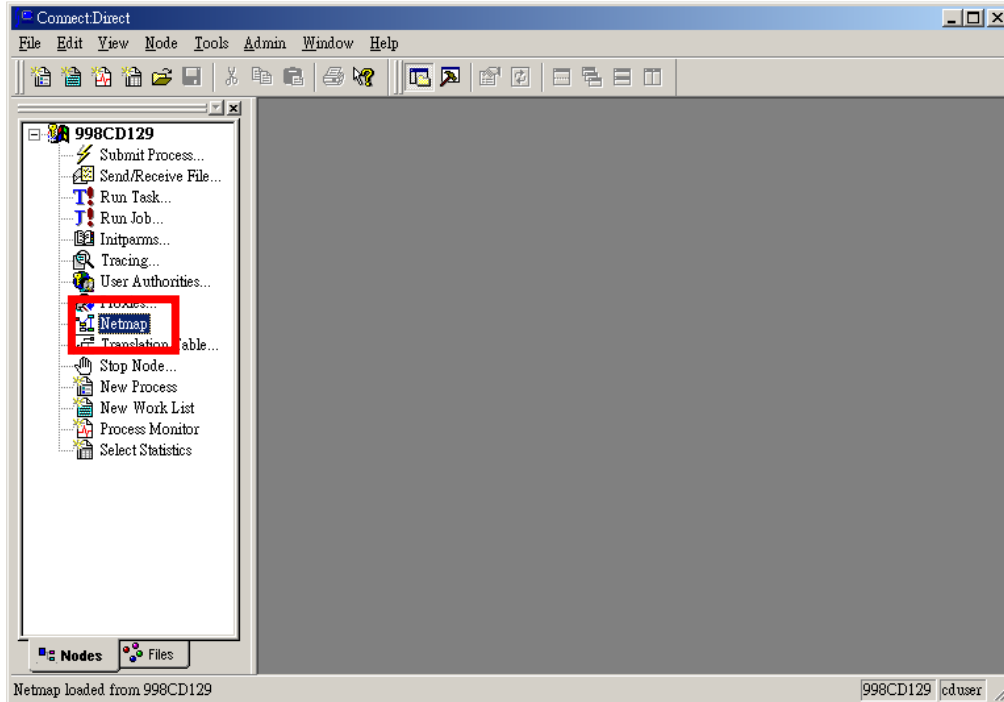
設定 CD Server IP 請參考以下步驟:

Step 01.更改 CD netmap 設定:

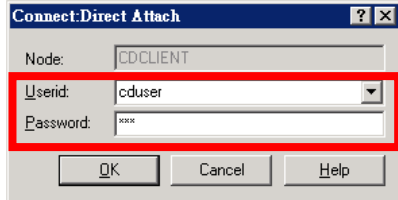
- (1) 開始』 - 『程式集』 - 『Sterling Commerce Connect Direct v4.2.00』
- 『CD Requester』。



(2) 點選『Netmap』兩下。

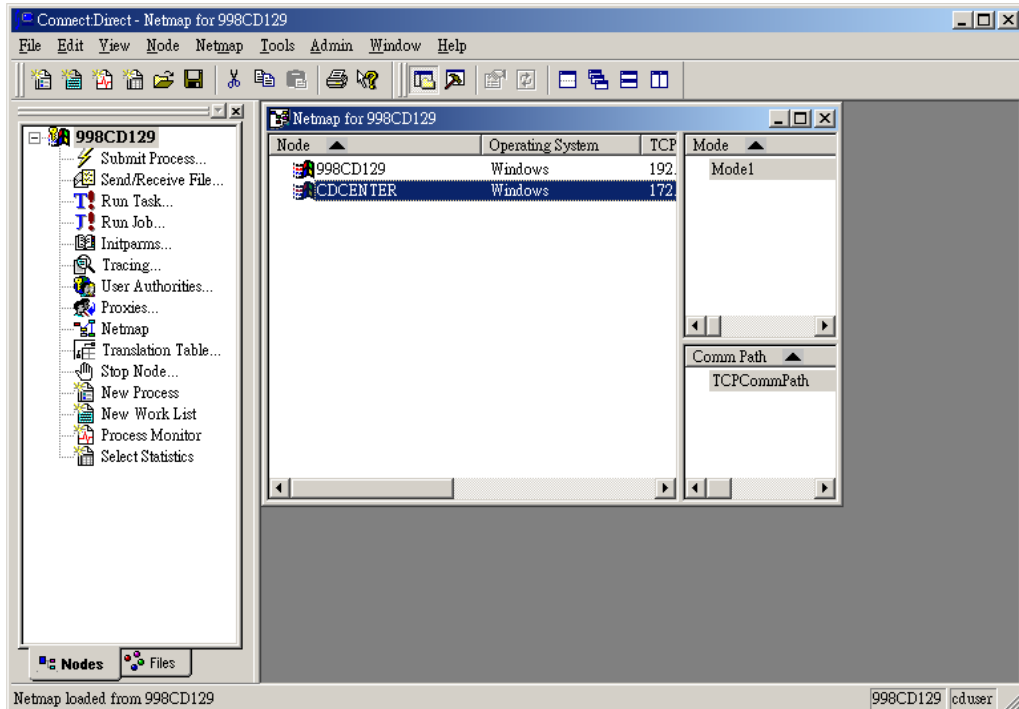


(3) 請輸入 cduser 及密碼，並注意大小寫。

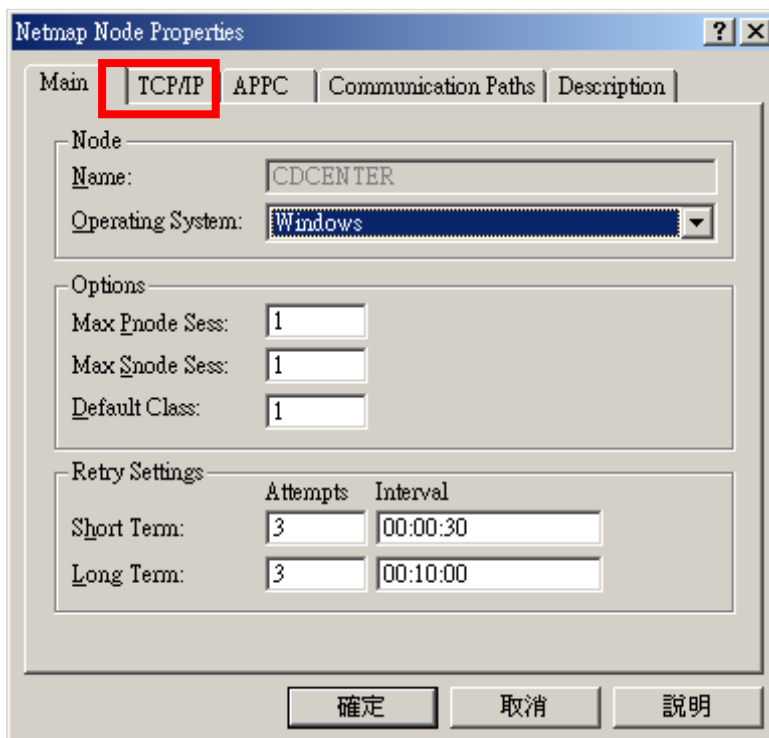


(4) 點選『CDCENTER』。





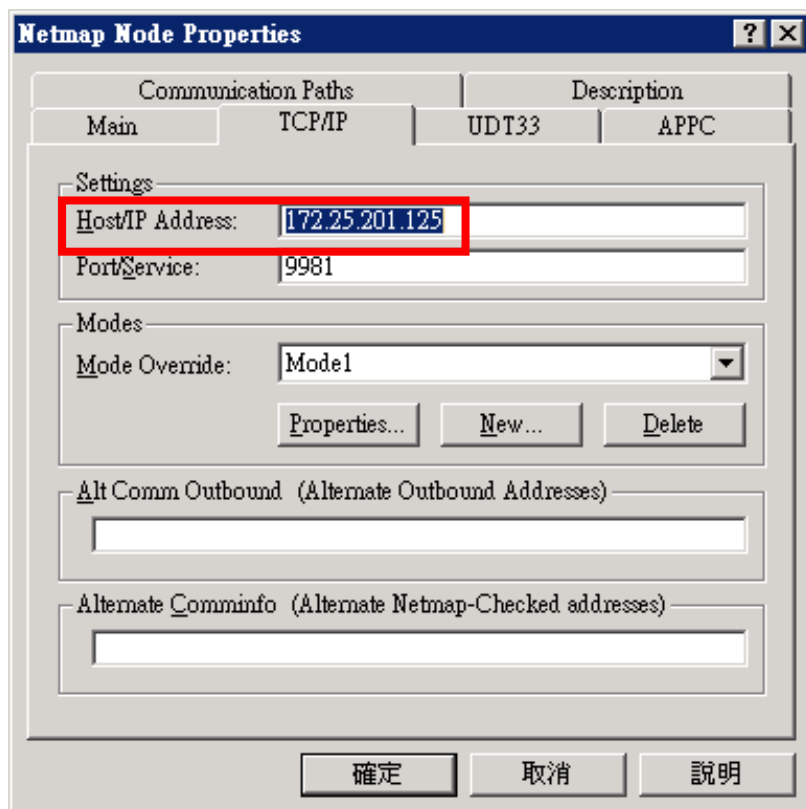
(5) 點選『TCP/IP』。



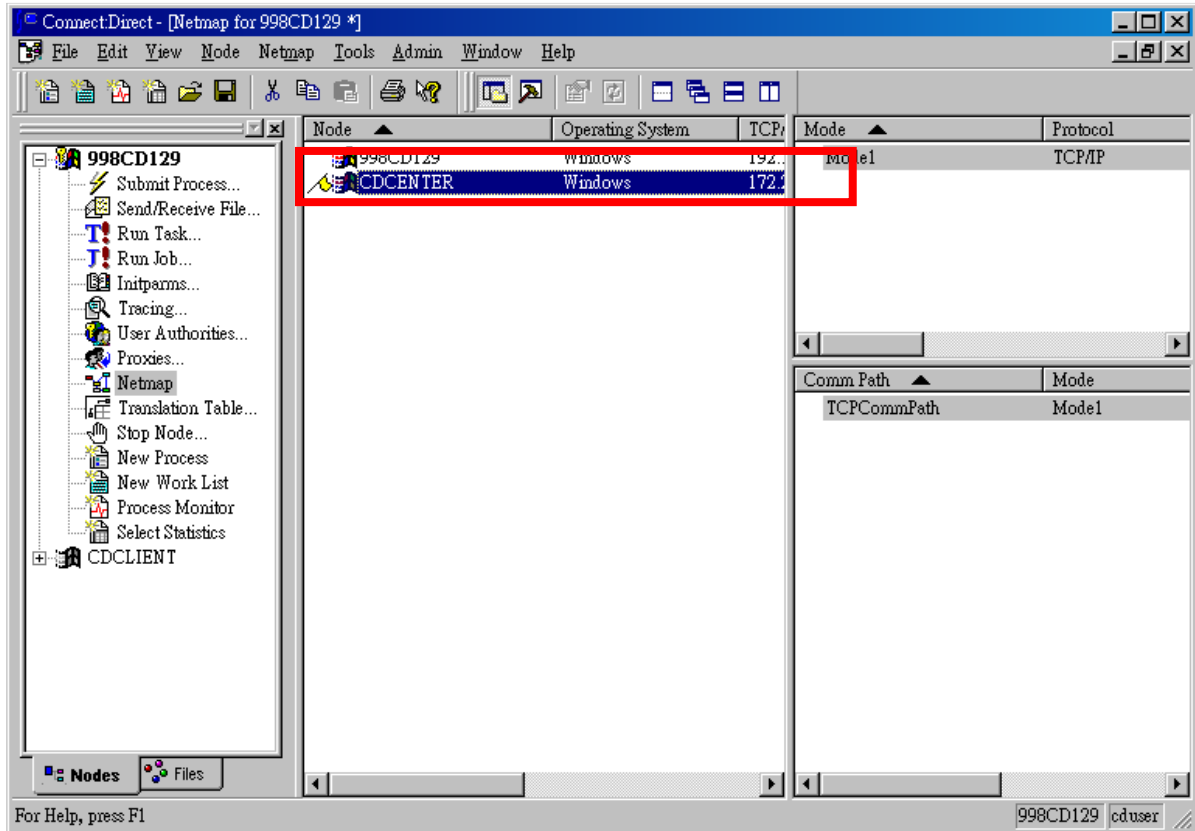
(6) 依需求更改 Host/IP，並按『確定』。

註：欲進行測試時，請將 Host/IP 指定為「172.31.201.125」

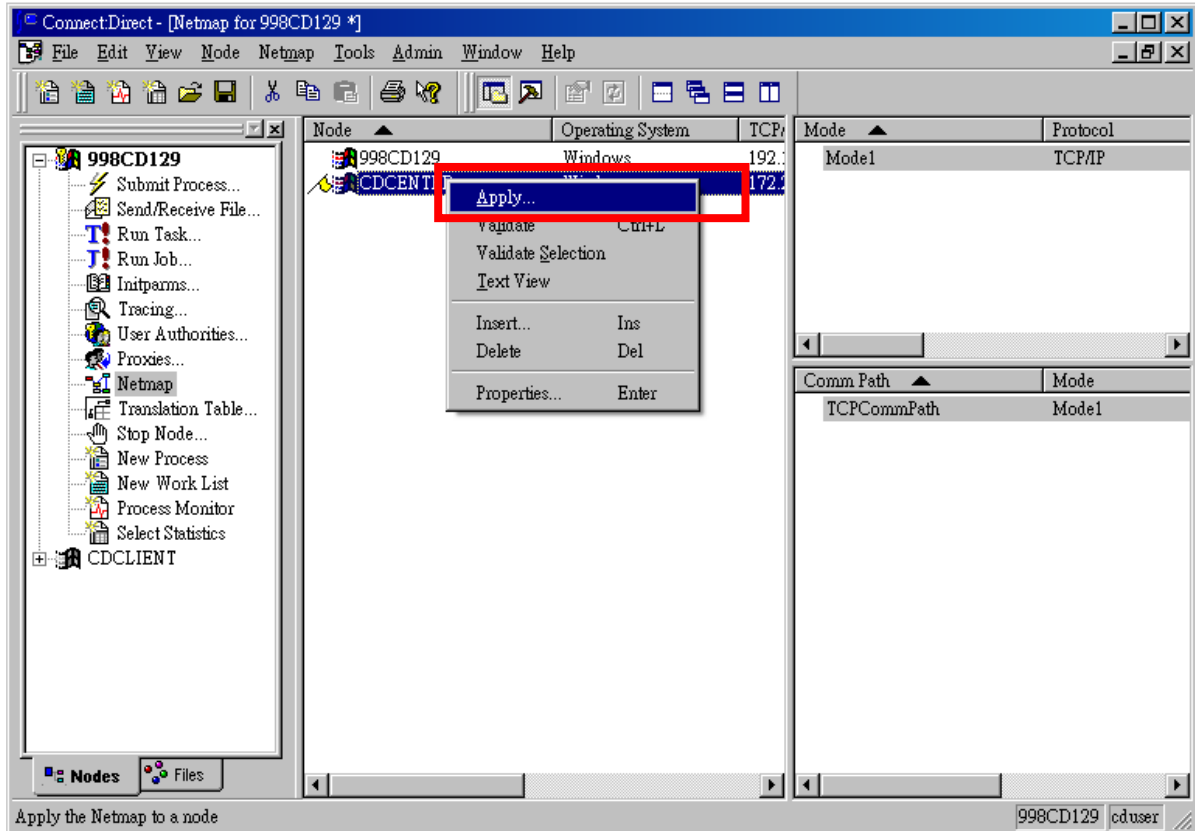
正式環境請將 Host/IP 指定為「172.31.200.125」



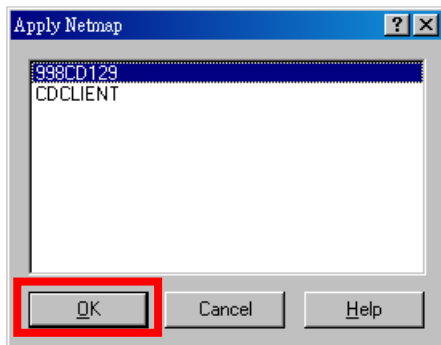
(7) 『CDCENTER』 前方出現黃色旗幟，將游標移至『CDCENTER』 前按右鍵。



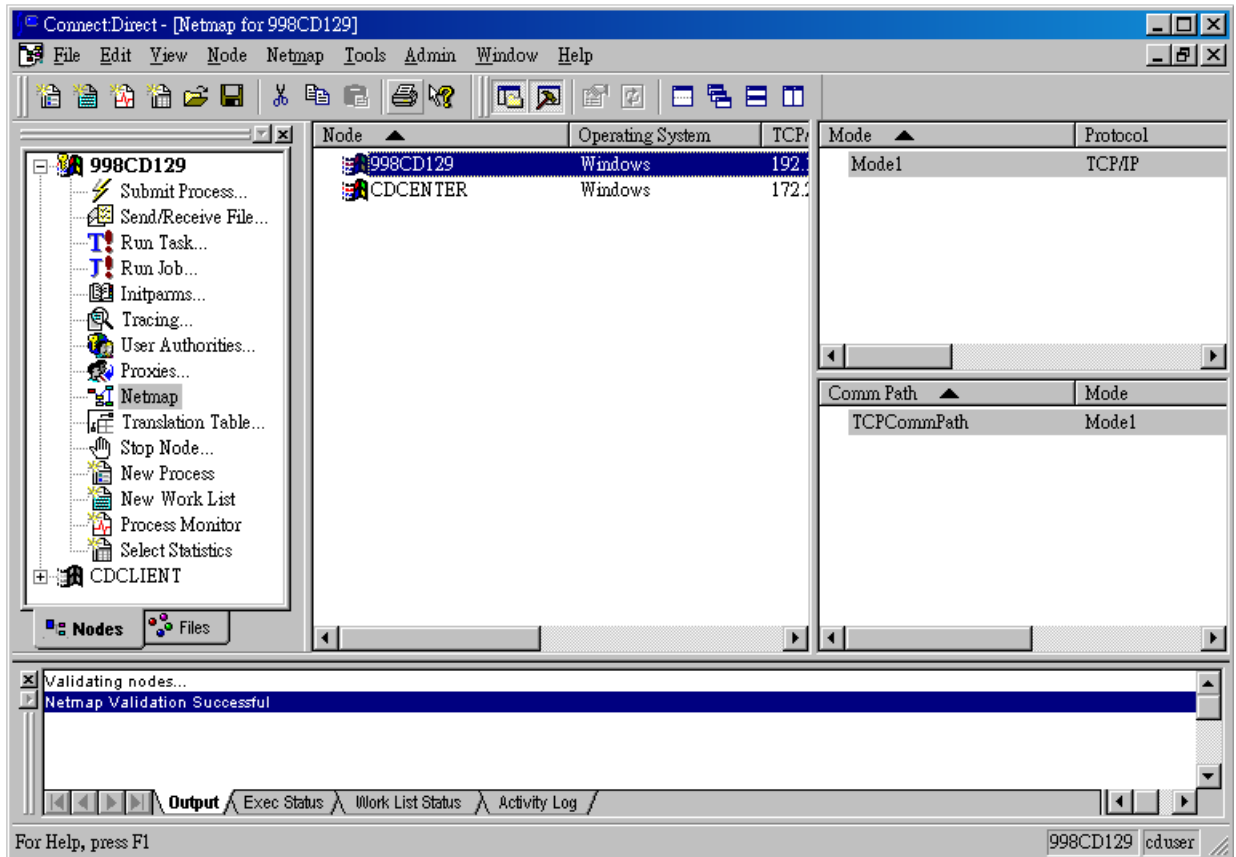
(8) 點選『Apply』。



(9) 點選『OK』鍵。



(10) 『CDCENTER』前方黃色旗幟消失，更改完成。



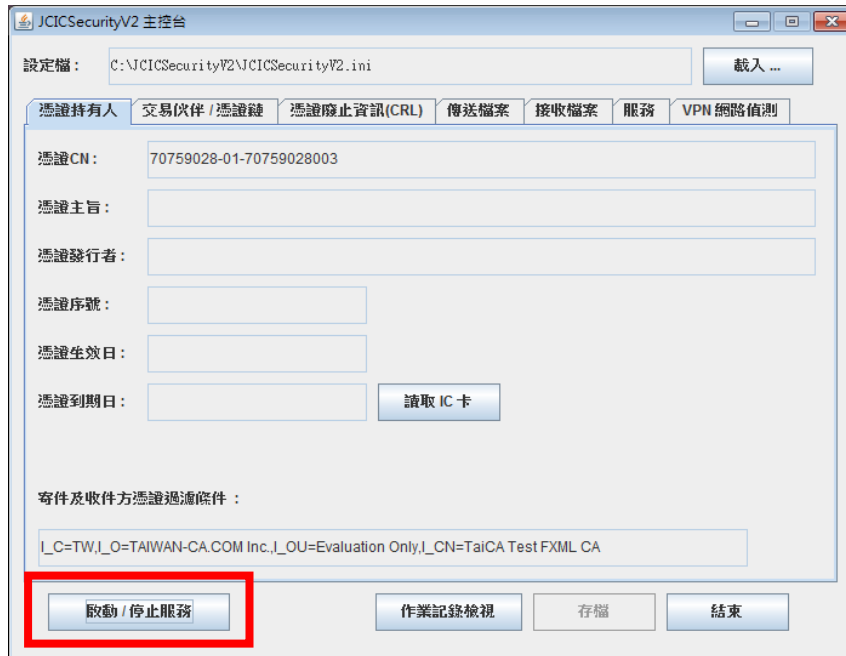
Step 02. 更改 C:\JCIC\UI\config\sip.txt 內容。

註：測試環境請更改為「172.31.201.125」

正式環境請更改為「172.31.200.125」

3.7.2 憑證安控模組啟動

(1) 下圖為『JCIC Security V2 主程式』執行畫面，請點擊『啟動/停止服務』按鈕。



(2) 點選『啟動/停止服務』後，畫面如下：



(3) 啟動服務前，請確定讀卡機驅動程式，已經安裝完成，且 IC 卡已經插入讀卡機。

點選『啟動服務』，依序輸入 2 組 IC 卡密碼。



如點選『取消』將取消讀取 IC 卡作業，返回畫面繼續操作。

等待十數秒之後，顯示服務啟動成功。

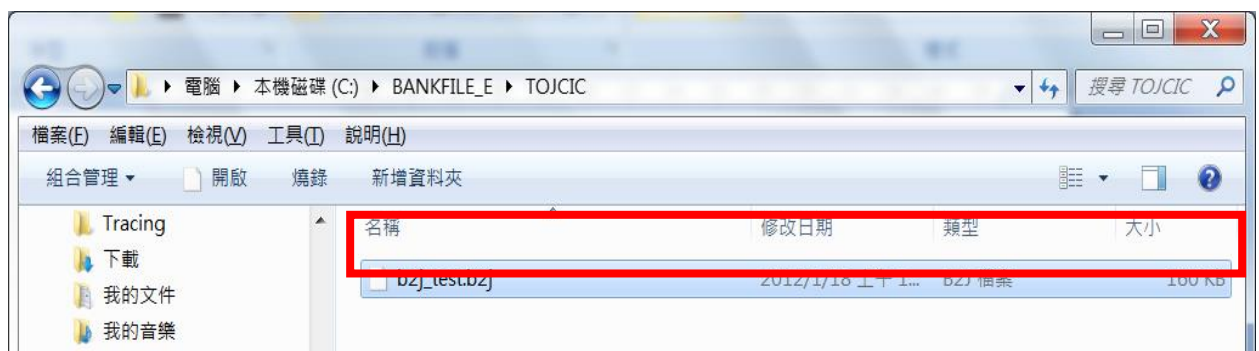


3.7.3 與聯徵中心測試小組聯繫

請與聯徵中心測試小組進行聯繫，並進行後續加解密軟體測試作業流程。相關聯絡資訊請參閱「5.聯絡資訊」章節。

3.7.4 加密簽章測試用檔案，並上傳至聯徵中心

(1) 複製測試個案『b2j_test.b2j』檔案至「drive:\BANKFILE_E\TOJCIC」目錄。

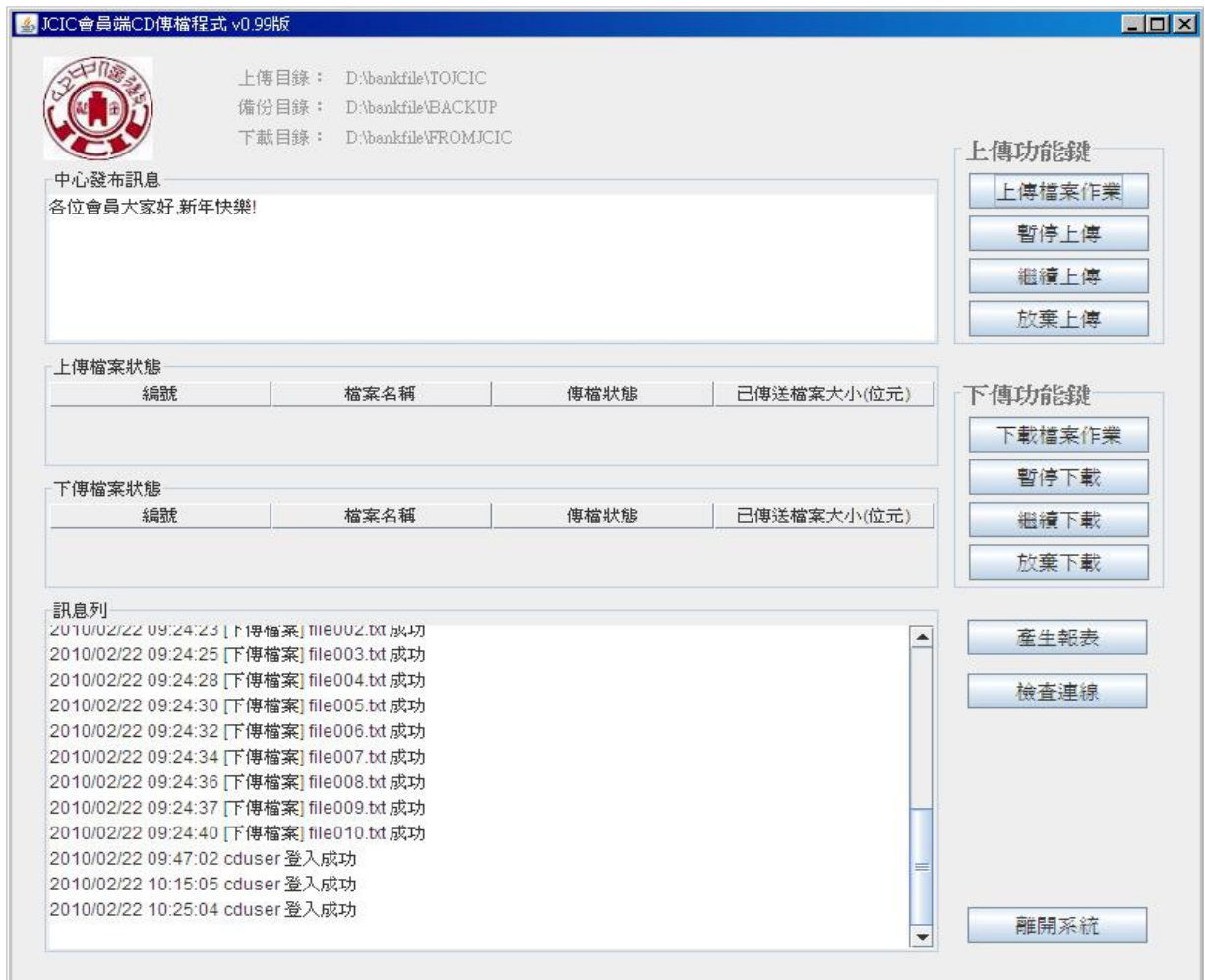


(2) 經過約 10 秒鐘後，觀察「drive:\BANKFILE \TOJCIC」目錄，此時該目錄應新增

— 「b2j_test.b2j.p7」檔案。



(3) 使用聯徵中心加密檔案傳輸軟體(CD 傳檔程式)之操作介面將該檔案上傳至聯徵中心。



3.7.5 接收聯徵中心之測試用檔案，並測試解密驗章功能

(1) 使用**聯徵中心加密檔案傳輸軟體**(CD 傳檔程式)之操作介面下載檔案至使用單位端。

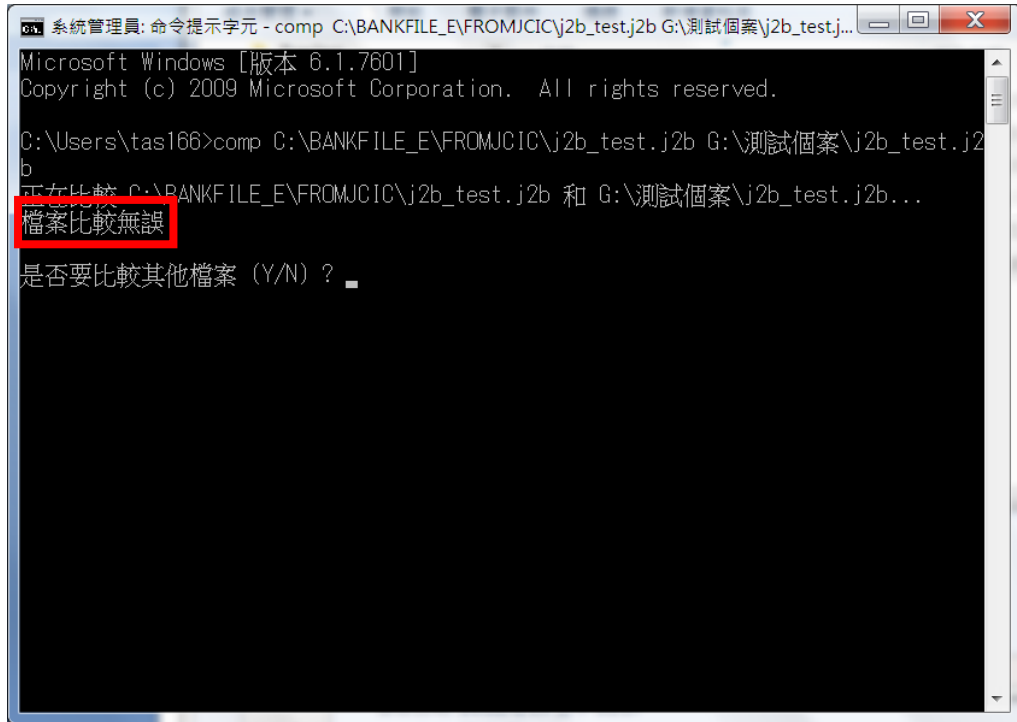
(2) 完成檔案下載後，請等待經過約 10 秒鐘時間，觀察

[drive:\BANKFILE_E \FROMJCIC] 目錄，是否新增 [j2b_test.j2b] 檔案。若有，代表所接受的聯徵中心加密簽章保護之檔案已經順利解密成功。



(3) 於程式集中之附屬應用程式中開啟「命令提示字元」，並輸入

[comp drive:\BANKFILE_E\FROMJCIC\j2b_test.j2b drive:\測試個案\j2b_test.j2b] 指令，
如出現「檔案比較無誤」之字樣，代表檔案正確無誤，測試完成。



3.7.6 回報聯徵中心測試作業完成

- (1) 完成測試後，請回報予聯徵中心測試小組。

3.8. 憑證安控模組上線使用

3.8.1 請依據「3.2 憑證申請作業」章節進行正式晶片卡以及憑證之申請。完成憑證申請安裝、下載本中心憑證，並依「3.2.3 提供加密憑證序號予聯徵中心」章節說明，將憑證序號告知聯徵中心。

3.8.2 聯徵中心將與使用單位聯繫安排上線時程。

4. Q & A (原機升版可略過此步驟)

4.1. 憑證註冊中心網站登入帳號解鎖

4.1.1 作業時機

用戶於登入憑證註冊中心網站時，連續輸入密碼錯誤三次將造成暫停登入網站權限，此時可遵循此說明進行網站權限重新開放及登入密碼重新設定之作業。

4.1.2 作業程序

(1) 用戶憑證作業網站密碼輸入錯誤連續三次，安全性管控將會鎖定用戶登入帳號及密碼，將會無法登入。

(2) 如已輸入錯誤達三次以上，請至臺灣網路認證公司網站(<http://www.twca.com.tw>)

下載中心內的『財團法人金融聯合徵信中心加密檔案傳輸作業專區』下載『用戶憑證作業網站密碼重新設定申請單』填寫後用印原留存之印鑑，郵寄至臺灣網路認證公司辦理用戶憑證作業網站密碼重設作業。

註：郵寄地址及收件人為『台北市延平南路 85 號 10 樓 張淑貞小姐收』

4.2. 晶片卡密碼修改

4.2.1 作業時機

變更「晶片卡密碼」。

注意：本晶片卡有兩組密碼，可分別設定。

4.2.2 作業程序

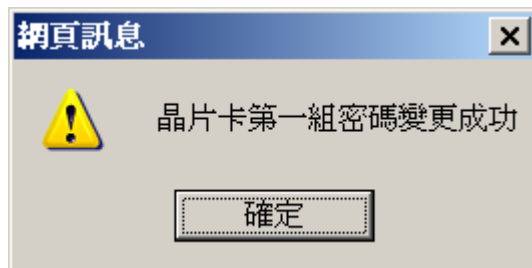
- (1) 登入註冊中心系統。
- (2) 請依據您要變更的哪一組晶片卡密碼，點選視窗左邊「第一組晶片卡密碼修改」或「第二組晶片卡密碼修改」功能，視窗右邊會顯示密碼修改步驟。
- (3) 請先輸入「舊密碼」（目前使用的晶片卡密碼）。
- (4) 於「新密碼」欄位輸入欲設定的新晶片卡密碼，並於「再確認」欄位重新輸入欲設定之新晶片卡密碼，最後按下「確認變更」。

The screenshot shows the TWCA website's password change interface. The header includes the TWCA logo and the text "財團法人金融聯合徵信中心加密檔案傳輸作業憑證註冊中心" and "Trust. Warranty. Cooperation. Action". The main content area is titled "第一組晶片卡密碼修改". On the left, there is a navigation menu with options like "憑證申請", "憑證展期(更新)", "憑證下載", "憑證廢止", "檢視憑證資訊", "網站密碼修改", "第一組晶片卡密碼修改" (highlighted), "第一組晶片卡鎖卡解碼", "第二組晶片卡密碼修改", and "第二組晶片卡鎖卡解碼". The main form area contains the following fields and instructions:

- 請輸入晶片卡目前使用之密碼
- 舊密碼
- 請設定晶片卡新密碼，密碼長度6~16個字
- 新密碼
- 再確認
- 確認變更

At the top right of the form area, there are links for "回首頁" and "登出".

- (5) 畫面顯示「晶片卡密碼變更完成」訊息視窗，請按「確定」按鍵。



4.3. 晶片卡鎖卡解碼

4.3.1 作業時機

用戶於連續輸入錯誤密碼三次造成晶片卡鎖卡，可使用此功能解開晶片卡鎖卡狀態並重新設定晶片卡密碼。

注意：本晶片卡有兩組密碼，依據您被鎖卡的第一組晶片卡密碼或第二組晶片卡密碼分別進行解碼。

4.3.2 作業程序

- (1) 登入註冊中心系統。
- (2) 請依據您要解碼的哪一組晶片卡密碼，點選視窗左邊「第一組晶片卡鎖卡解碼」或「第二組晶片卡鎖卡解碼」功能，視窗右邊會顯示鎖卡解碼步驟。

財團法人金融聯合徵信中心加密檔案傳輸作業憑證註冊中心
Trust. Warranty. Cooperation. Action

第一組晶片卡鎖卡解碼 [回首頁](#) [登出](#)

憑證申請
憑證展期(更新)
憑證下載
憑證廢止
檢視憑證資訊
網站密碼修改
第一組晶片卡密碼修改
第一組晶片卡鎖卡解碼
第二組晶片卡密碼修改
第二組晶片卡鎖卡解碼

步驟1. 請插入您的晶片卡，並輸入網站登入密碼，執行卡片驗證

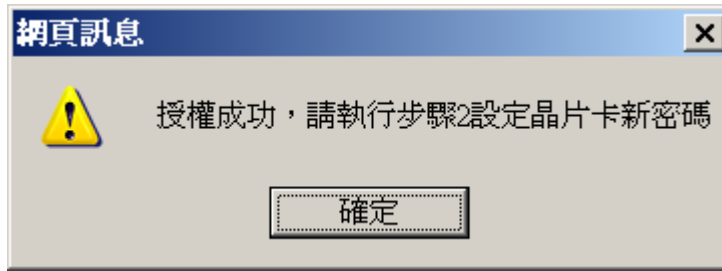
網站密碼

步驟2. 請設定晶片卡新密碼，密碼長度6~16個字

新密碼

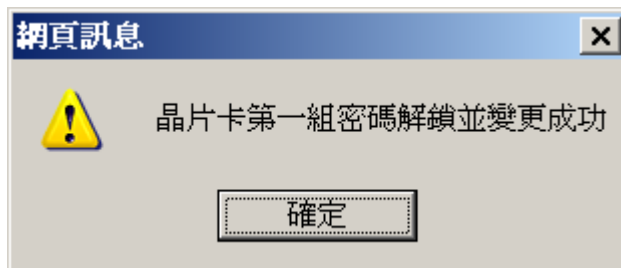
再確認

- (3) 請先將晶片卡插入讀卡機中，在「網站密碼」欄位輸入您的網站密碼，輸入完後，按下「卡片驗證」按鍵。
- (4) 若驗證成功，視窗顯視「卡片驗證成功」訊息。



<p>憑證申請</p> <p>憑證展期(更新)</p> <p>憑證下載</p> <p>憑證廢止</p> <p>檢視憑證資訊</p> <p>網站密碼修改</p> <p>第一組晶片卡密碼修改</p> <p>第一組晶片卡鎖卡解碼</p> <p>第二組晶片卡密碼修改</p> <p>第二組晶片卡鎖卡解碼</p>	<h3>第一組晶片卡鎖卡解碼</h3> <p>卡片驗證成功</p> <p>步驟1. 請插入您的晶片卡，並輸入網站登入密碼，執行卡片驗證</p> <p>網站密碼 <input type="text"/></p> <p><input type="button" value="卡片驗證"/></p> <p>步驟2. 請設定晶片卡新密碼，密碼長度6~16個字</p> <p>新密碼 <input type="text"/></p> <p>再確認 <input type="text"/></p> <p><input type="button" value="確認重置"/></p>
---	--

- (5) 再於「新密碼」欄位輸入欲設定的新晶片卡密碼，並於「再確認」欄位重新輸入欲設定之新晶片卡密碼，最後按下「確認變更」按鍵。
- (6) 作業成功，螢幕顯示「晶片卡第一組密碼解鎖並變更成功」或「晶片卡第二組密碼解鎖並變更成功」訊息。



4.4. 問題處理

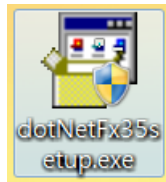
4.4.1 問題描述: 出現系統訊息「C:\JICISecurityV2\JavaAsService.exe 無法啟動這個程式, 因為應用程式的設定不正確。重新安裝應用程式應該可以修復這個問題。」

問題處理方式:

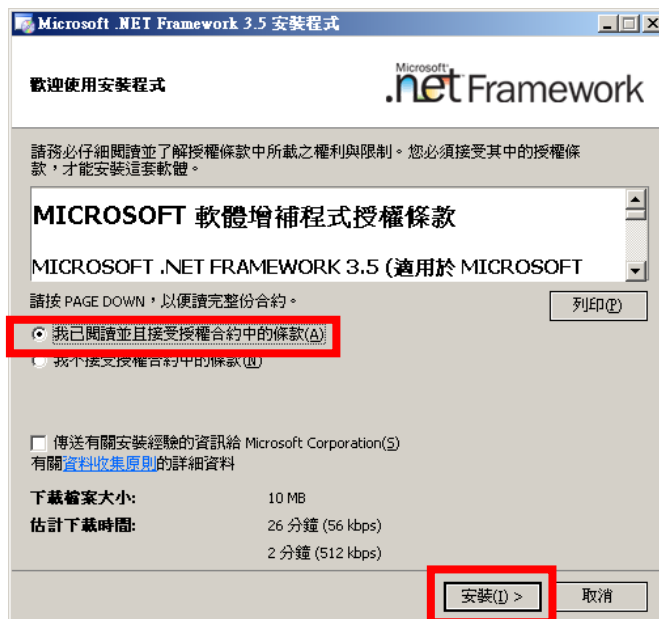
(1) 請開啟 IE Browser , 並輸入下方 URL , 進行 .Net Framework 3.5 安裝程式下載。

<http://download.microsoft.com/download/7/0/3/703455ee-a747-4cc8-bd3e-98a615c3aedb/dotNetFx35setup.exe>

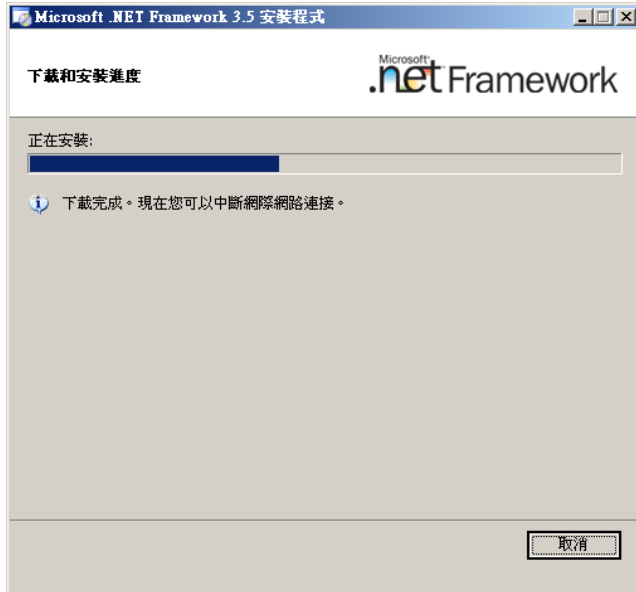
(2) 點擊 .Net Framework 3.5 安裝程式 (dotNetFx35setup.exe) 進行安裝。



(3) 選取「我已閱讀並且接受授權合約中的條款」後, 點擊「安裝」。



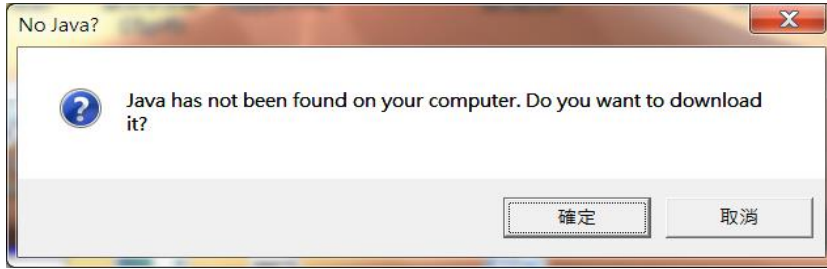
(4) .Net Framework 3.5 安裝中。



(5) 完成 .Net Framework 3.5 安裝。



4.4.2 問題描述: 憑證安控模組無法正確啟動並出現下方圖示:



問題處理方式:

請參考「財團法人金融聯合徵信中心憑證安控模組(JCICSecurityV2)安裝使用手冊.doc」 3.1.3 章節完成 Java JRE 1.6u27 軟體安裝後，再重新啟動憑證安控模組。

4.4.3 問題描述: 憑證安控模組無法正確開啟 JCICSecurityService 服務管理，並

出現下方訊息:



問題處理方式:

請參考「財團法人金融聯合徵信中心憑證安控模組(JCICSecurityV2)安裝使用手冊.doc」 3.1.4 章節完成安裝 憑證安控模組系統服務 後，再重新啟動憑證安控模組。

4.4.4 問題描述: Win7/Vista 環境下在啟動憑證安控模組時，出現「JCICSecurityService

啟動失敗 OpenService 無法 5: 存取被拒」 訊息。

問題處理方式:

請於啟動「JCIC Security V2 主程式」時，點擊捷徑『JCICSecurity 控制台』右鍵，以『系統管理員身份執行』。

4.4.5 問題描述: 啟動憑證安控模組時，出現「Windows 服務: JCICSecurityService 啟動失敗，請檢視 LOG 內容」之訊息。

問題處理方式:

- (1) 請確認插入正確卡片後，重新啟動服務，並且輸入兩組正確之密碼。
- (2) 如果仍然無法成功啟動，請開啟

「C:\JCICSecurityV2\LOG\JCICSecurity.Service.LOG」Log 檔案，並以「執行失敗」為關鍵字，查看最新之錯誤訊息，並依以下 Log 問題原因及處理表格建議進行問題排除。



錯誤訊息	問題原因	建議處理方式
執行失敗, IC 卡返回錯誤訊息 : error:800050A2:Vendor defined:PKCS11_login:Invalid PIN length	輸入之密碼長度錯誤 (至少為6碼)	請輸入正確密碼
執行失敗, IC 卡返回錯誤訊息 : error:80004005:Vendor defined:PKCS11_open_session:General Error	讀卡機驅動程式錯誤	請重新安裝正確之讀卡機驅動程式
執行失敗, IC 卡返回錯誤訊息 : C7 PINCode Error!!	第一組憑講密碼錯誤	請輸入正確密碼
執行失敗, IC 卡返回錯誤訊息 : C7 PINCode Lock!!	第一組憑講密碼已鎖住	請依手冊4.3章節解鎖卡後, 再重新啟動
執行失敗, IC 卡返回錯誤訊息 : C9 PINCode Error!!	第二組憑講密碼錯誤	請輸入正確密碼
執行失敗, IC 卡返回錯誤訊息 : C9 PINCode Lock!!	第二組憑講密碼已鎖住	請依手冊4.3章節解鎖卡後, 再重新啟動
執行失敗, IC 卡憑證 CN 不符, 取消作業	使用錯誤的卡片	請使用正確卡片
執行失敗, IC 卡返回錯誤訊息 : No Token!	卡片錯誤、卡片沒插、讀卡機驅動程式未安裝	請檢查讀卡機已正確接上電腦、讀卡機的驅動程式已經安裝, 並且正確卡片是否已經插入讀卡機。

4.4.6 問題描述: 啟動憑證安控模組成功後, 卻無自動進行檔案簽章加密及解密驗章等作業。

問題處理方式:

請開啟 [C:\JCICSecurityV2\LOG\JCICSecurity.Info.LOG] Log 檔, 並依

JCICSecurity.Edit.LOG 檔案錯誤處理說明之錯誤訊息說明內容建議進行問題排除。

以下為各 Log 說明及錯誤訊息之建議處理方式:



檔案名稱	說明
JCICSecurity.Edit.LOG	記錄『JCICSecurity 控制台』編輯及服務啟動/停止作業之執行過程。
JCICSecurity.Info.LOG	記錄『JCICSecurity 服務』啟動/停止作業期間之執行過程及憑證廢止清單CRL下載過程。
JCICSecurity.Service.LOG	記錄『JCICSecurity 服務』服務作業期間之關於檔案加解密及簽驗章執行過程。

- **Log 名稱:** JCICSecurity.Edit.LOG

記錄『JCICSecurity 控制台』編輯及服務啟動/停止作業之執行過程。

註: 該 Log 檔無相關錯誤訊息及對應處理建議表。

- **Log 名稱:** JCICSecurity.Info.LOG

錯誤訊息	問題原因	建議處理方式
onReloadProperty() 沒有憑證廢止清單(CRL)檔, 服務無法啟動	無CRL或 CRL無法正確載入	請關閉憑證安控模組, 再重新開啟憑證安控模組, 系統將會自動重新下載CRL。 如仍無法解決時, 請確認網路是否異常。
onReloadProperty() 沒有載入 CA 憑證鏈檔, 服務無法啟動	無正確之憑證鏈	請依照手冊中之3.3.3 設定交易夥伴/憑證鏈步驟, 下載正確之憑證鏈檔及伙伴憑證檔後, 重新開啟憑證安控模組。
onReloadProperty() 設定檔缺少 PartnerFolder 或 沒有交易伙伴憑證檔, 服務無法啟動	無正確之伙伴憑證	請依照手冊中之3.3.3 設定交易夥伴/憑證鏈步驟, 下載正確之憑證鏈檔及伙伴憑證檔後, 重新開啟憑證安控模組。

- **Log 名稱:** JCICSecurity.Service.LOG

錯誤訊息	問題原因	建議處理方式
執行失敗, IC 卡返回錯誤訊息 : error:800050A2:Vendor defined:PKCS11_login:Invalid PIN length	輸入之密碼長度錯誤 (至少為6碼)	請輸入正確密碼
執行失敗, IC 卡返回錯誤訊息 : error:80004005:Vendor defined:PKCS11_open_session:General Error	讀卡機驅動程式錯誤	請重新安裝正確之讀卡機驅動程式
執行失敗, IC 卡返回錯誤訊息 : C7 PINCode Error!!	第一組憑講密碼錯誤	請輸入正確密碼
執行失敗, IC 卡返回錯誤訊息 : C7 PINCode Lock!!	第一組憑講密碼已鎖住	請依手冊4.3章節解鎖卡後, 再重新啟動
執行失敗, IC 卡返回錯誤訊息 : C9 PINCode Error!!	第二組憑講密碼錯誤	請輸入正確密碼
執行失敗, IC 卡返回錯誤訊息 : C9 PINCode Lock!!	第二組憑講密碼已鎖住	請依手冊4.3章節解鎖卡後, 再重新啟動
執行失敗, IC 卡憑證 CN 不符, 取消作業	使用錯誤的卡片	請使用正確卡片
執行失敗, IC 卡返回錯誤訊息 : No Token!	卡片錯誤、卡片沒插、讀卡機驅動程式未安裝	請檢查讀卡機已正確接上電腦、讀卡機的驅動程式已經安裝, 並且正確卡片是否已經插入讀卡機。

5. 聯絡資訊

財團法人金融聯合徵信中心:

電話: (02)23813939