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 2.2.1.6 版)

中華民國 113 年 01 月 04 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	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	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	
V2.2.1.5	2022/12/01	1. 程式更新為 v2.2.1.5 2. 文件版號更新同程式版號	
V2.2.1.6	2024/01/04	1. 主程式更新支援 ZuluJDK 2. 相關程序配合進行調整說明	

目錄

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 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：

用戶需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。由於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，其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/downloadArea)下載:

1. **Java JRE 1.8u171 或 ZuluJDK 8.72.0.17 (擇一下載即可)**
2. **憑證安控模組安裝檔(JCICSecurityV2 for 2048 位元)**

作業系統：

本軟體支援 Windows 10-11、 Windows Server 2016 以上 x86 (32 位元)及 x64(64 位元)作業系統，需搭配 Java JRE 1.8u171 或 ZuluJDK 8.72.0.17 軟體(擇一使用)：

※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 JRE1.8u171 或 ZuluJDK 8.72.0.17。

憑證作業:

當進行 「4.2 憑證申請作業」、「4.3 憑證安控模組設定」、「4.7 憑證安控模組功能測試」及「4.8 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 位址需開放 80、443 port)

- 測試
  - ◆ 線上申請憑證網址
    https://cloudrademo.twca.com.tw/JCIC
    (對應 IP 為 60.250.3.144)
  - ◆ 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 219.87.64.186,60.250.3.156)
  - ◆ 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)
- 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，需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)**

可於臺網網頁(https://www.twca.com.tw/downloadArea)下載。

(3) 測試晶片卡

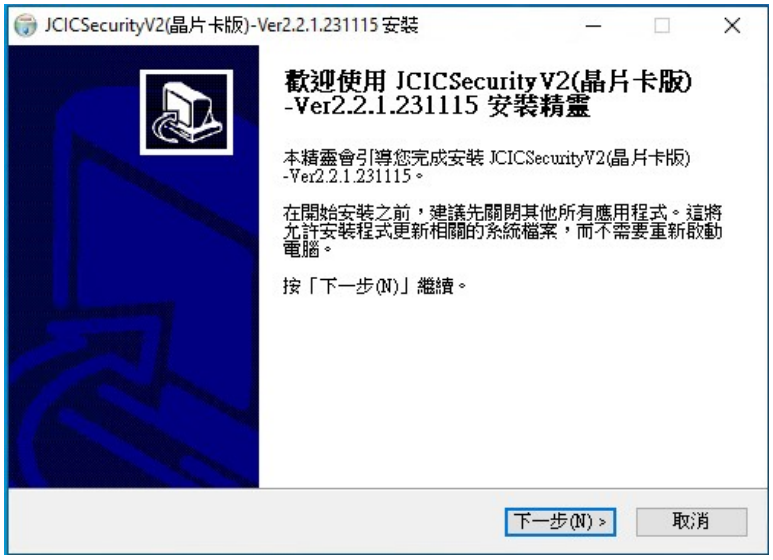
測試晶片卡請至 http://www.twca.com.tw 網站的下載中心中尋找**財團法人金融聯合徵信中心加密檔案傳輸作業**之憑證註冊申請表單，並下載填具後，向「臺灣網路認證股份有限公司」申請取得。相關聯絡資訊請參閱「5.聯絡資訊」章節。

(4) 正式晶片卡

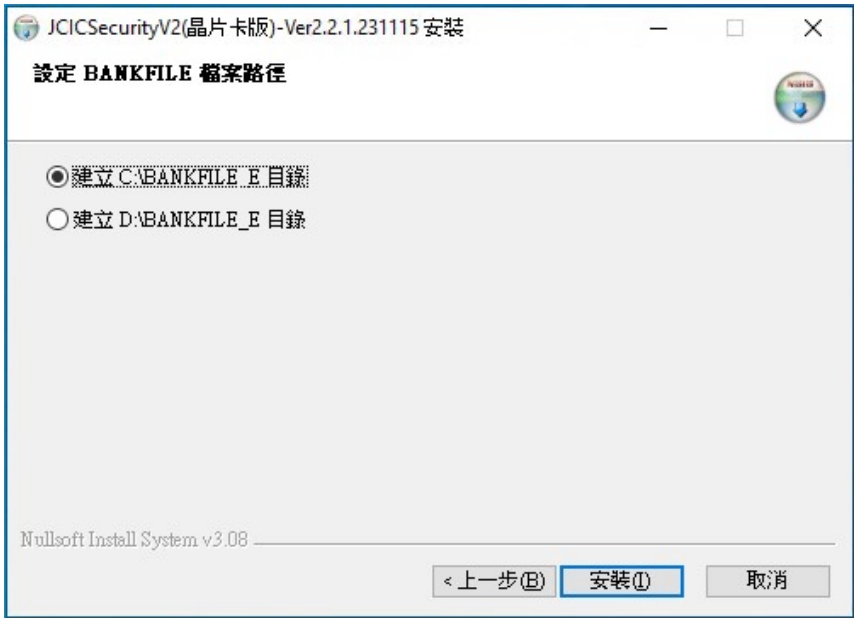
正式晶片卡請至 http://www.twca.com.tw 網站的下載中心中尋找**財團法人金融聯合徵信中心加密檔案傳輸作業**之憑證註冊申請表單，並下載填具後，向「臺灣網路認證股份有限公司」申請取得。相關聯絡資訊請參閱「5.聯絡資訊」章節。

3.1.2 安裝憑證安控模組

(1) 點擊『JCICSecurityV2.msi』檔案，開始進行安裝，畫面顯示如下，可點選「下一步」繼續進行安裝



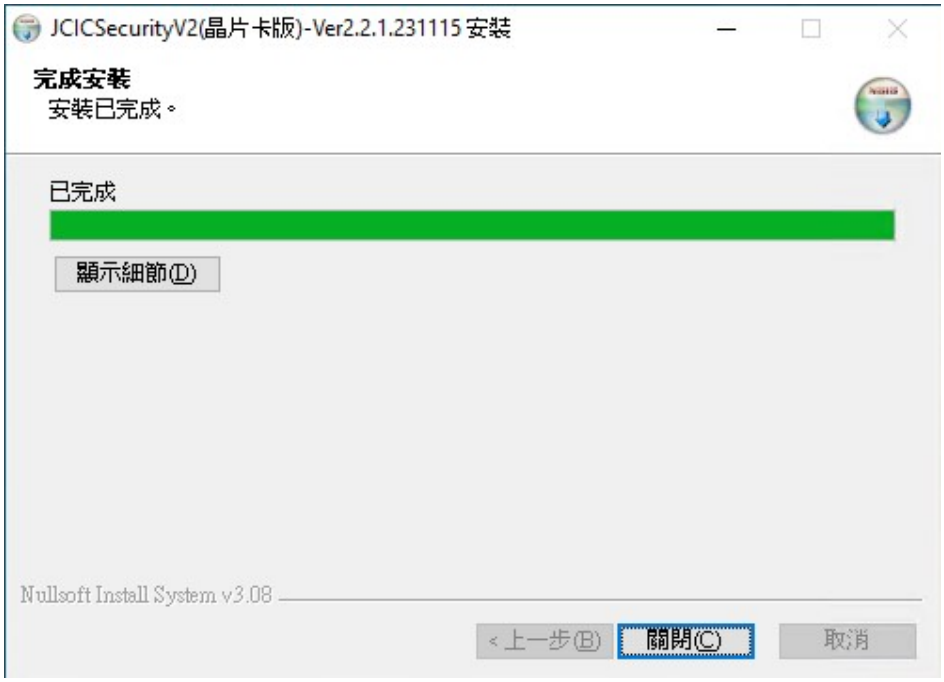
(2) 安裝時，需指定安控模組作業目錄。如系統先前已經安裝過，或目錄已經存在，將略過這個步驟。



(3) 安裝時將偵測是否已經安裝「**Java JRE 軟體**」，如出現以下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 Java JRE 1.8u171 安裝程序**」或「**3.1.4 ZuluJDK 8.72.0.17 安裝程序**」章節說明。

※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 JRE 1.8u171 或 ZuluJDK 8.72.0.17。

(4) 畫面將顯示安裝進度，若完成安裝將顯示如下圖，點選「關閉」即可



將

(5) 確認安裝完成後，開啟 C:\JCICSecurityV2\JavaAsService.ini
將 Java 路徑指向 3.1.3 或 3.1.4 所安裝之路徑

※注意:若本步驟未設定，本服務可能無法啟動。

3.1.3 Java JRE 1.8u171 安裝程序（原機升版可略過此步驟）

(1) 請於臺網網頁下載並執行軟體安裝

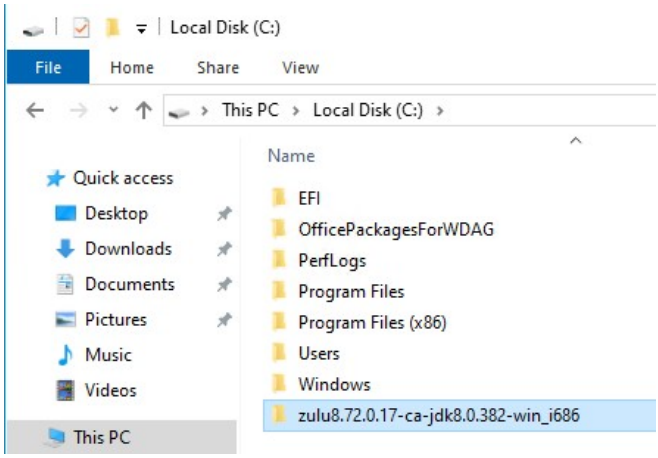
(2) 點選「執行」，進行軟體安裝。

(3) 直接點擊「安裝」，繼續進行安裝作業。

(4) Java 軟體安裝完成

3.1.4 ZuluJDK 8.72.0.17 安裝程序（原機升版可略過此步驟）

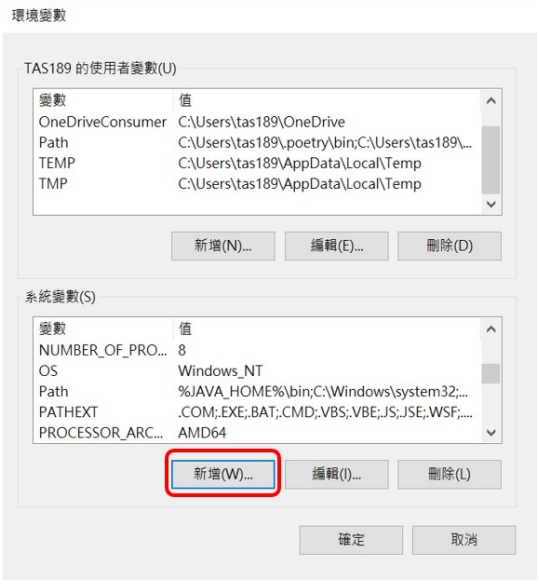
(1) 將下載之 ZuluJDK 目錄放置於 C:\根目錄下



(2) 開啟 windows「編輯系統環境變數」功能

(3) 點選「進階」分頁，點選「環境變數」按鈕

(4) 點選系統變數區塊下方的「新增按鈕」



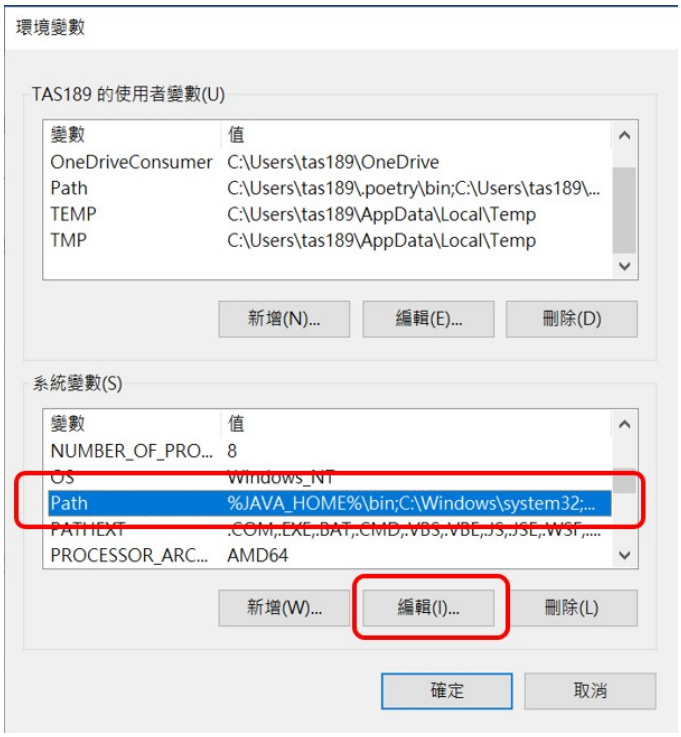
(5) 輸入以下資訊並點選「確定」新增系統變數

變數名稱：JAVA_HOME

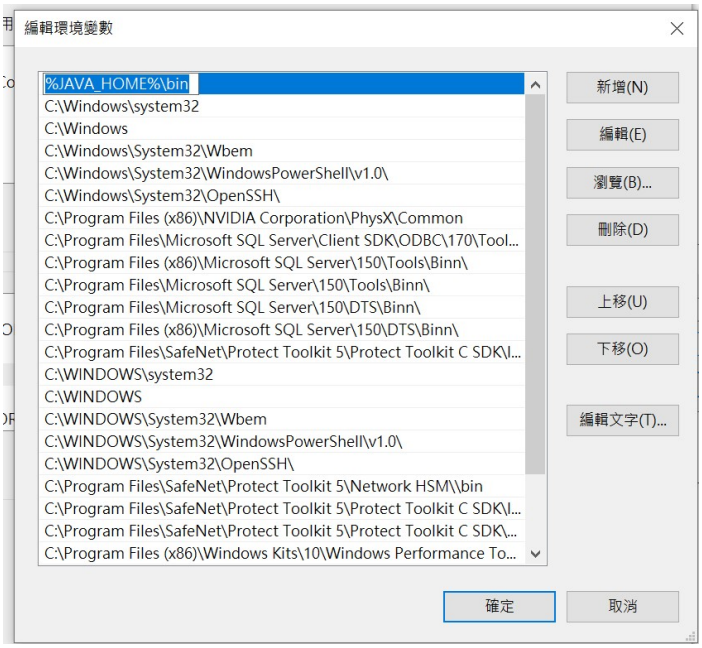
變數值：C:\zulu8.72.0.17-ca-jdk8.0.382-win_i686

※需指定至對應正確路徑，本系統才可正常運作

(6) 選擇系統變數區塊中的 Path 變數使其變為藍底，並點選「編輯」按鈕進行設定。



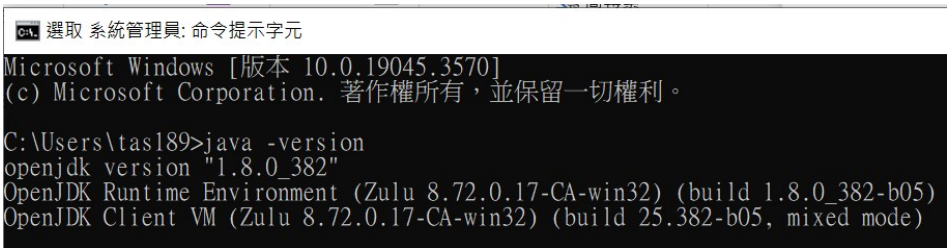
(7) 點選「新增」按鈕新增環境變數
變數值為：%JAVA_HOME%\bin
由於此環境變數有執行順序的差異，故需將其上移至第一行
可參閱下圖所示，設定完成後點選「確定」即可儲存。



(8) 透過 CMD 指定查看現有 Windows 預設 Java

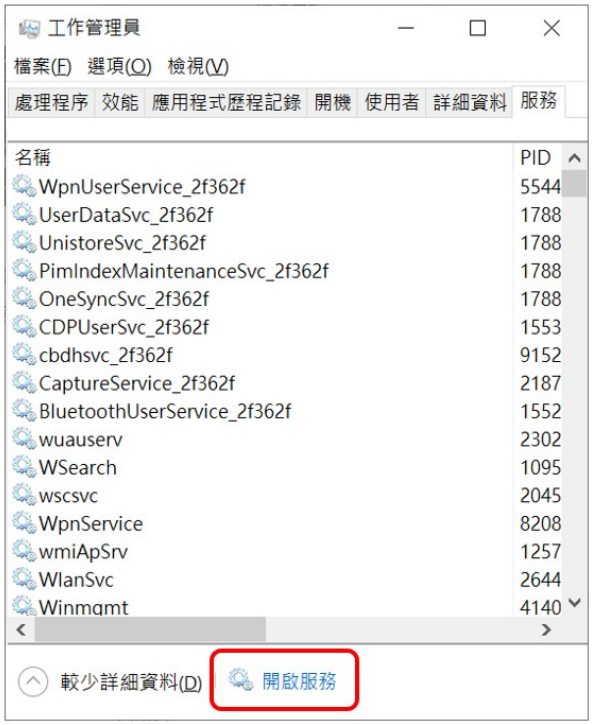
執行指令「java -version」即可看到該環境之預設 Java 版本

正確應顯示如下路徑與 JDK 資訊

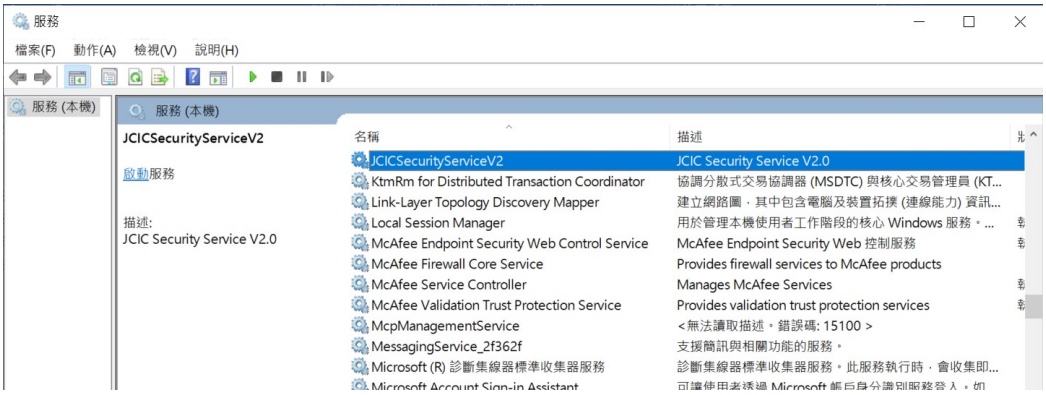


3.1.5 確認憑證安控模組系統服務是否成功安裝

(1) 開啟「工作管理員」點選下方「開啟服務」



(2) 找出服務名稱『JCICSecurityServiceV2』，若有出現表示已經安裝完成。



3.2. 憑證申請作業

執行憑證作業前需事先與**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」申請取得後才可進行以下流程，相關說明以憑證小幫手系統流程為主，不在此章節進行說明。

(1) 憑證小幫手下載點可至臺網網頁(https://www.twca.com.tw/downloadArea)進行下載與安裝。

(2) 若安裝完成，憑證小幫手開啟畫面如下，以系統實際畫面為主，不在此章節進行說明。**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) 若憑證申請完成，需提供加密憑證序號予聯徵中心

a. **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」**

b. **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**

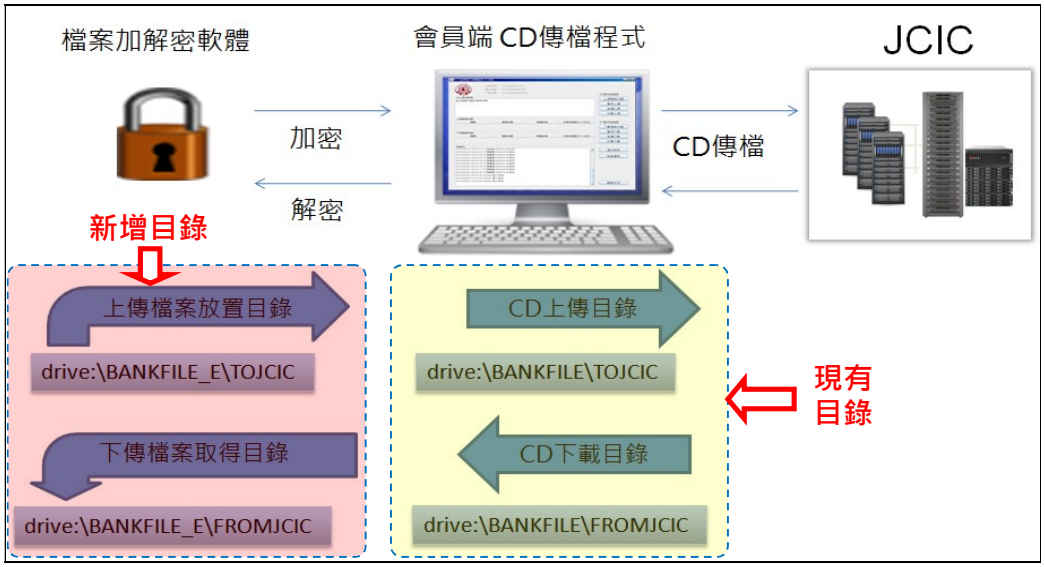
註:聯絡資訊請參閱「5.聯絡資訊」章節。

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。

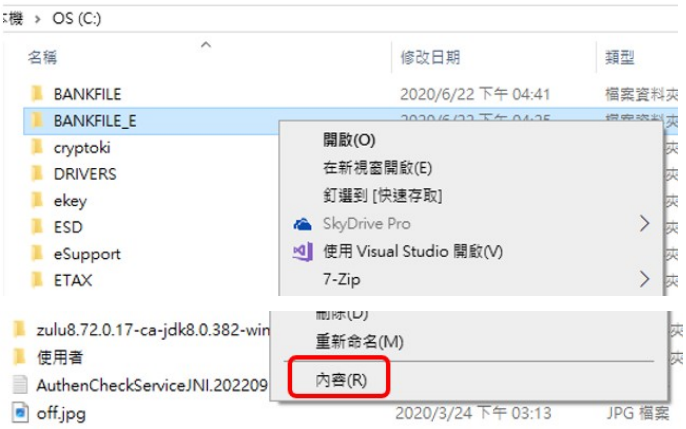


(3) 請確認下列之目錄已存在。

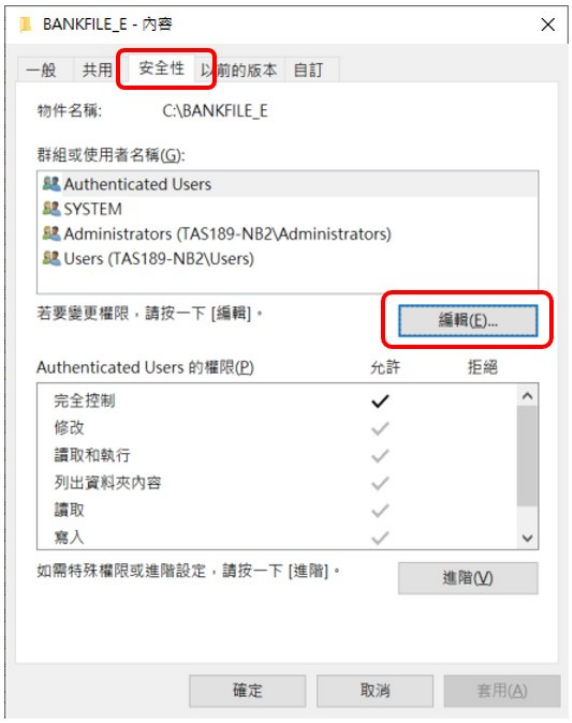
路徑	說明
drive:\BANKFILE_E\TOJCIC	放置欲上傳至聯徵中心的原始檔之目錄
drive:\BANKFILE_E\FROMJCIC	該目錄存放聯徵中心傳送過來，完成解密驗章之明文檔案
drive:\BANKFILE_E\FROMBAK	該目錄存放聯徵中心加密過後傳送過來之加密檔案備份，可做為當雙方其中一方對傳輸過後之內容有疑慮之舉證資料。請各使用單位依需求執行備份及清除檔案等作業。
drive:\BANKFILE_E\TOBAK	該目錄存放使用單位端傳送至聯徵中心之原始未加密的檔案備份。請各使用單位依需求執行備份及清除檔案等作業。
註：「drive:」代表原 BANKFILE 目錄所在之磁碟，如「C:\」或「D:\」	

(4) 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

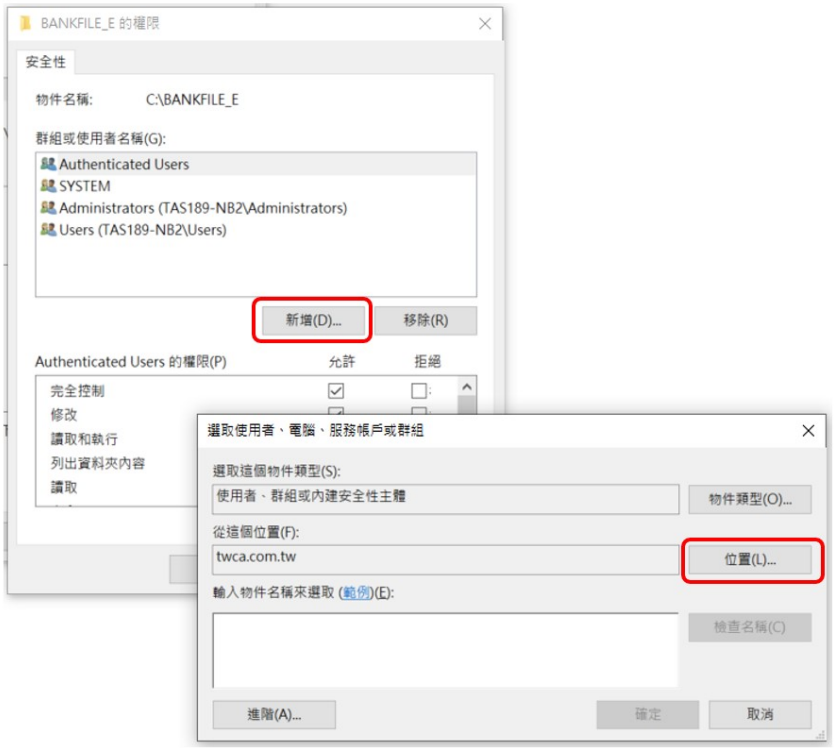
a. 於 BANKFILE_E 目錄點擊右鍵後，選取「內容」



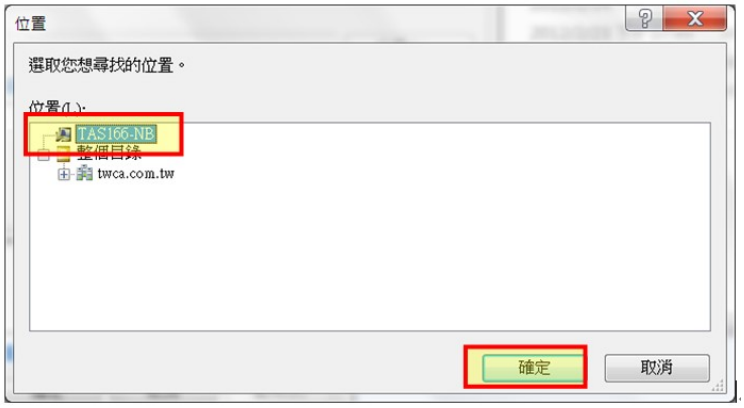
b. 切換主選單為「安全性」後點擊「編輯」鈕。



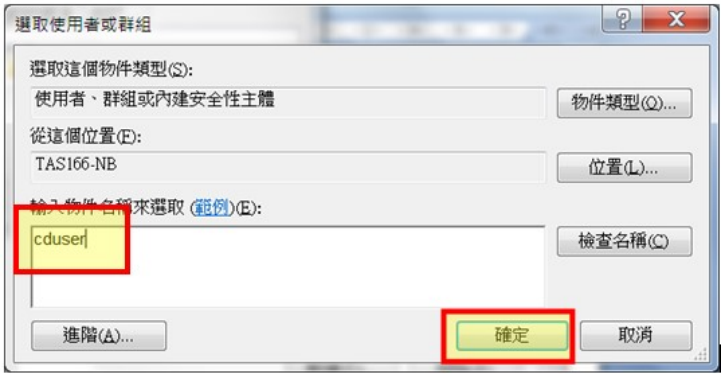
c. 點擊「新增」鈕後，系統出現選取使用者或群組的視窗，請點擊該視窗之「位置」鍵。



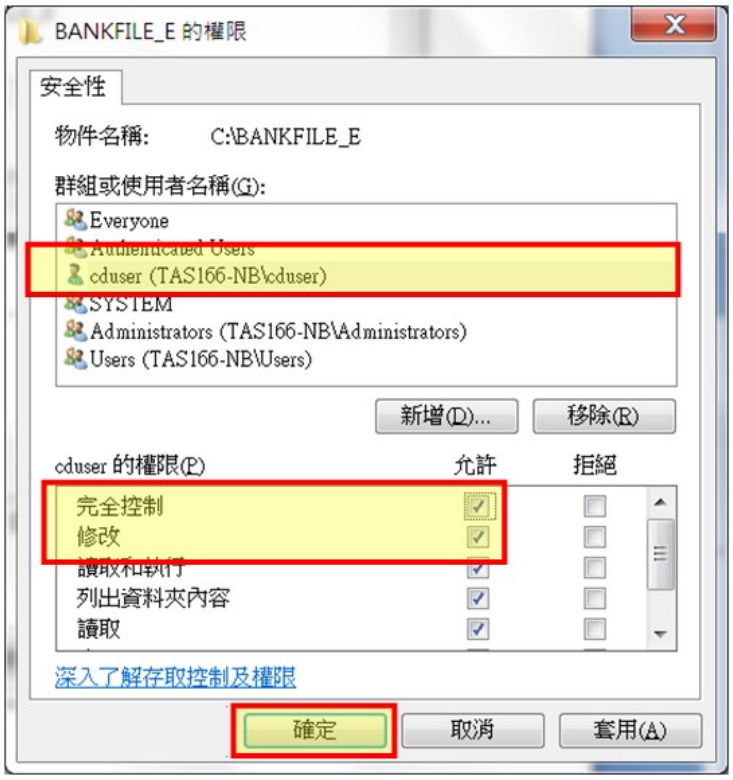
d. 於位置視窗中選取目前使用之本機名稱後，按「確定」鈕。以下圖為例，本機名稱為「TAS166-NB」。



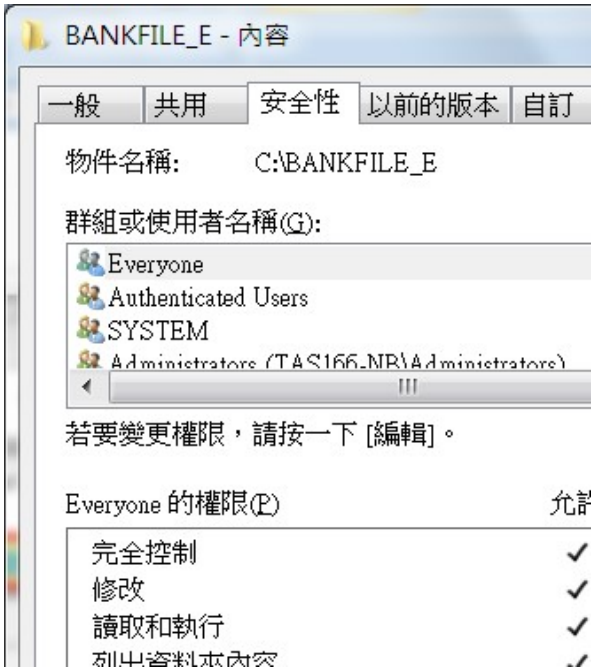
e. 於輸入物件名稱來選取欄位中，輸入「cduser」後點選「確定」。



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」。

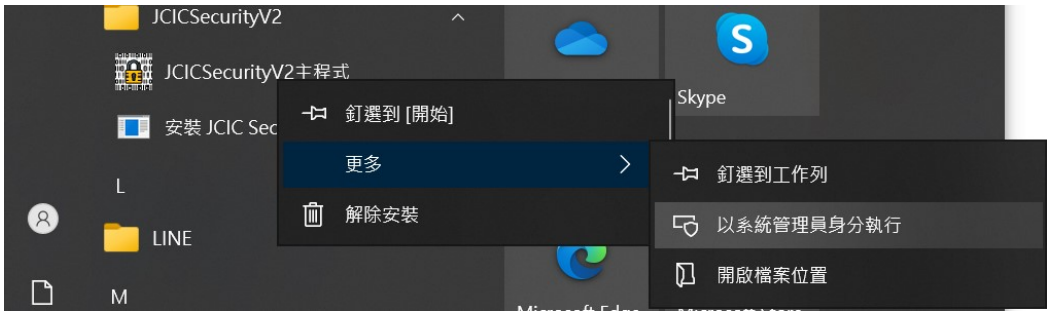


g. 點擊「確定」完成目錄權限調整作業。

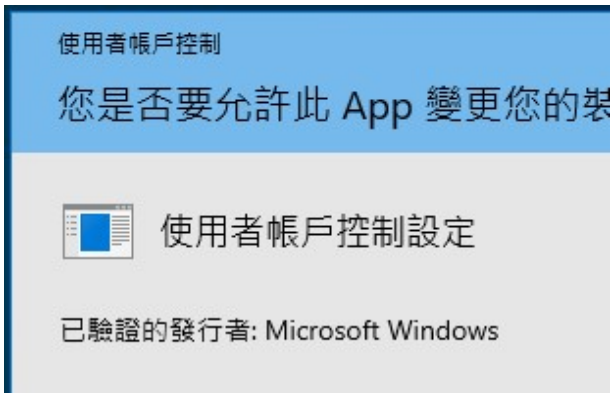


3.3.2 啟動憑證安控模組，並讀取晶片卡憑證資料

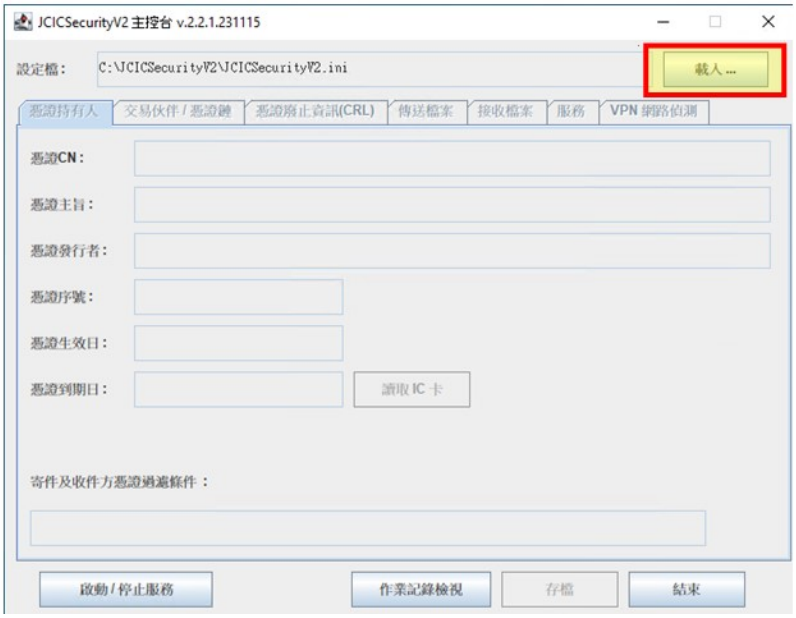
(1) 主控台中找到「JCICSecurityV2 主程式」並以「系統管理員身份執行」。



(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

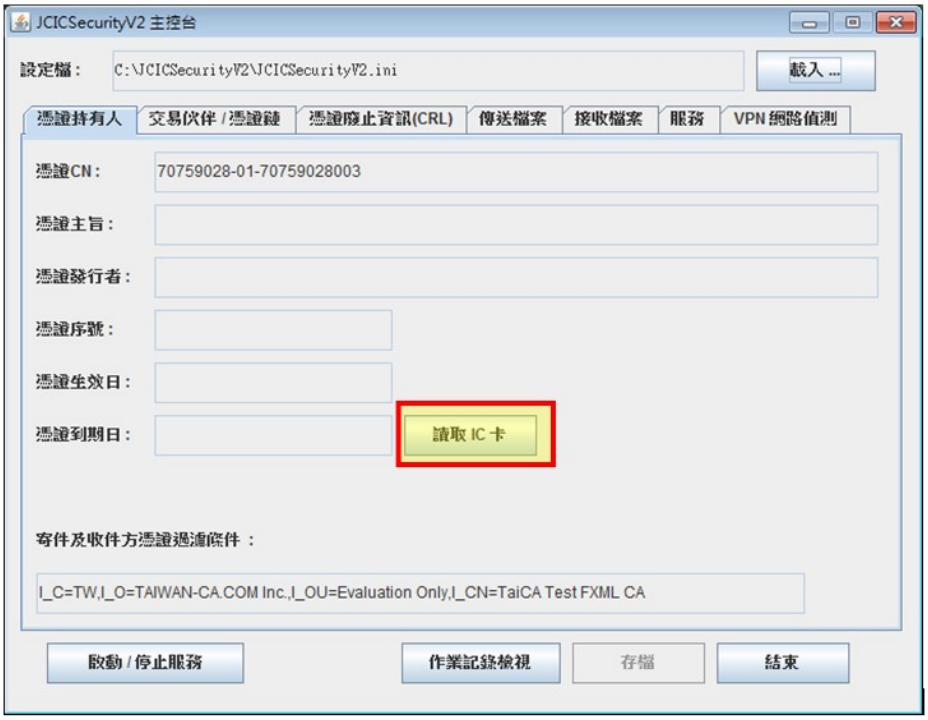


(3) 成功開啟 JCICSecurityV2 主控台。點擊「載入」讀取加解密軟體目前之設定值。

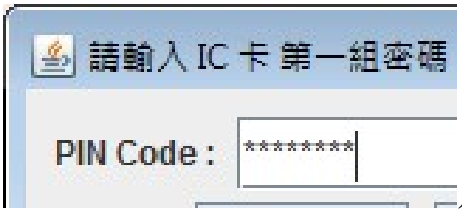


(4) 當點選載入之後，『JCIC Security V2 主程式』會將加解密軟體目前之『憑證持有人』設定載入。畫面如下:

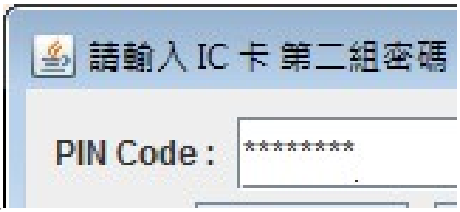
(5) 點選『讀取 IC 卡』以取得晶片卡中之憑證資訊。



(6) 點選『讀取 IC 卡』之後，請輸入兩組晶片卡密碼



及

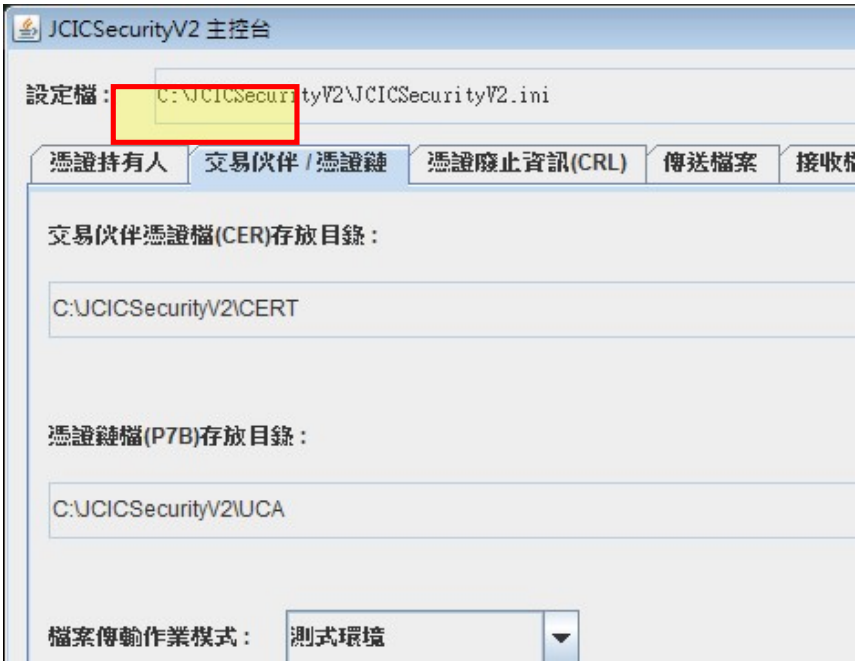


(7) 完成『讀取 IC 卡』之後，出現下圖。完成後，請點選「存檔」。

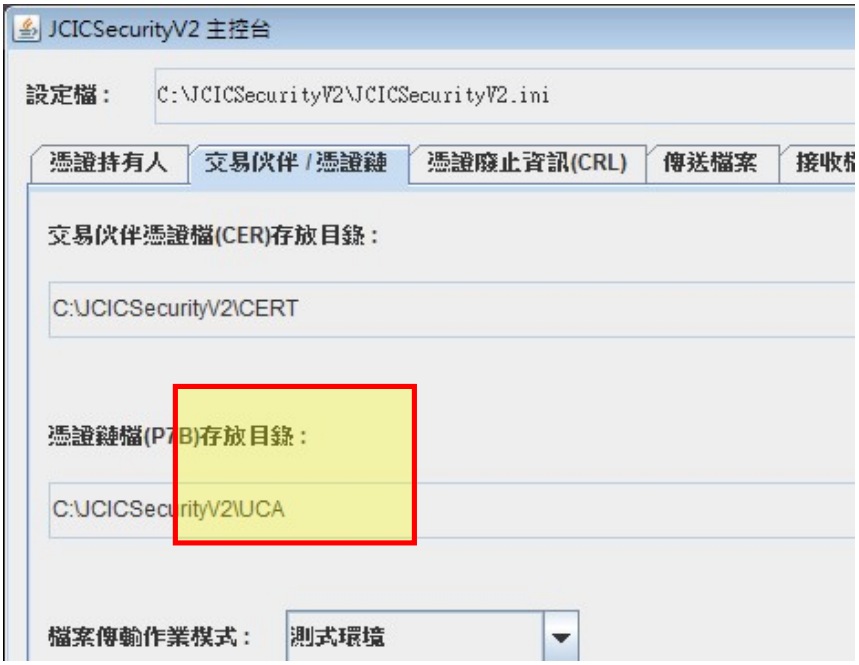
(8) 設定檔存檔成功。

3.3.3 設定交易夥伴/憑證鏈

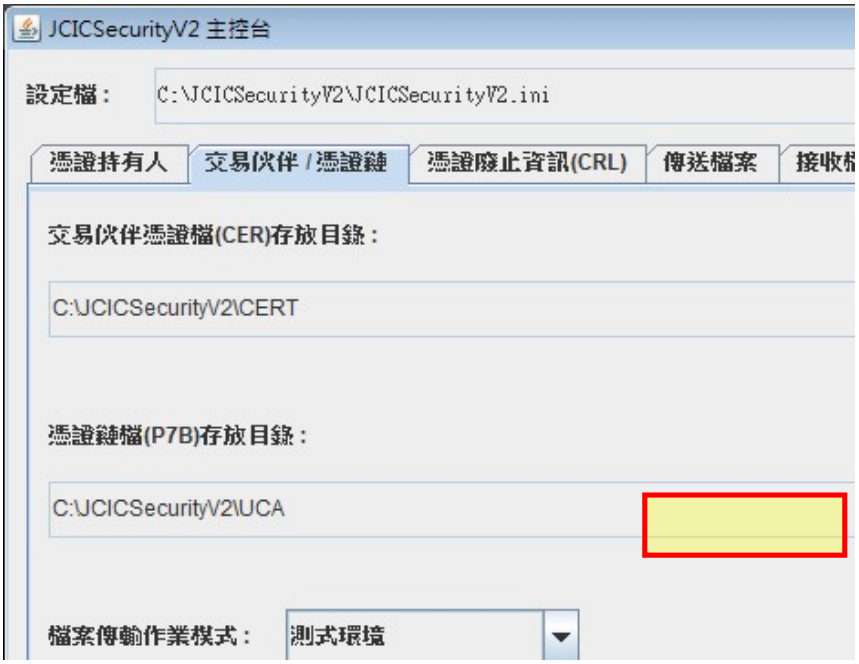
(1) 於 JCICSecurityV2 控制台上方功能選單中點擊『交易伙伴/憑證鏈』。



(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。
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。

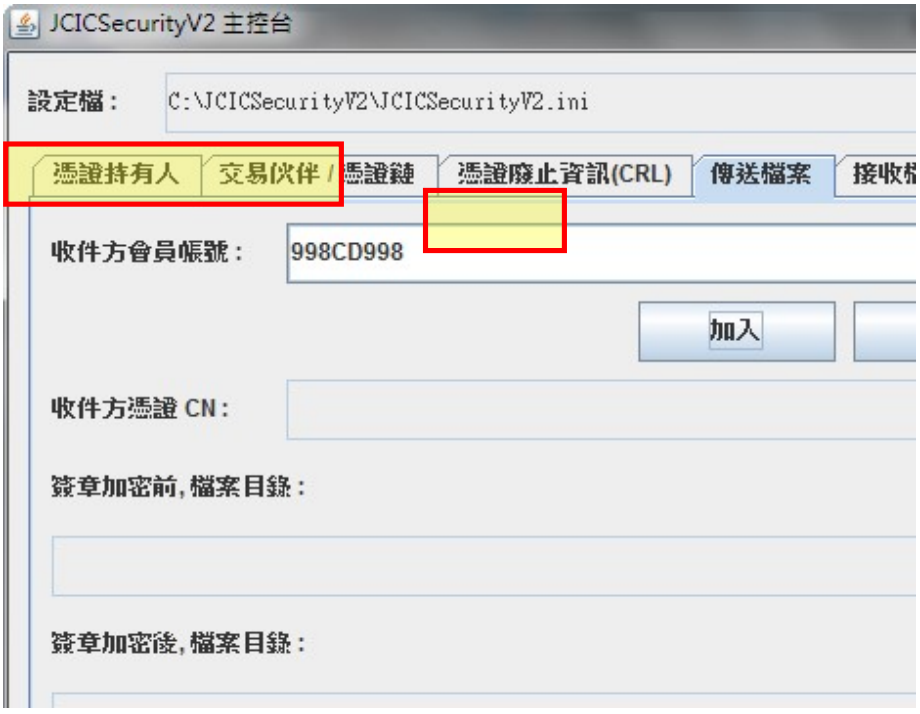
(8) 點擊『存檔』，儲存目前設定值。

(9) 設定檔存檔成功。

3.3.4 傳送檔案設定

(1) 於 JCICSecurityV2 控制台上方功能選單中點擊『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」。

需注意：正式環境收送件方憑證 CN 的選取為

00999340-01-998CD0000003_54D28B1B

測試環境收送件方憑證 CN 的選取為

00999340-01-998CD9980001_4EF35C5B

(5) 選取簽章加密前，點選檔案目錄「瀏覽」鍵選取「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: 請依「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

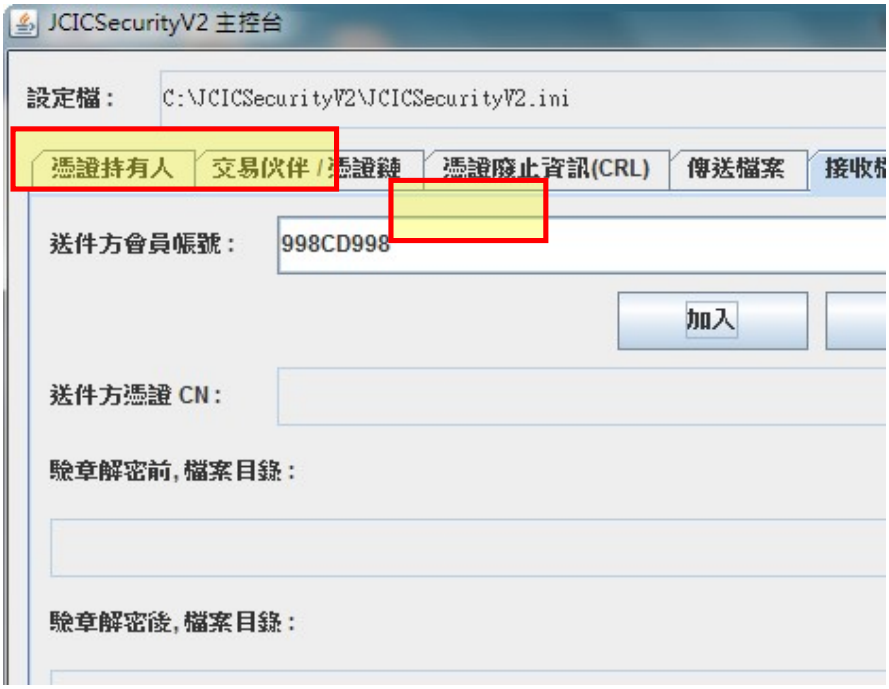
(7) 點擊『存檔』，儲存目前設定值。

(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。

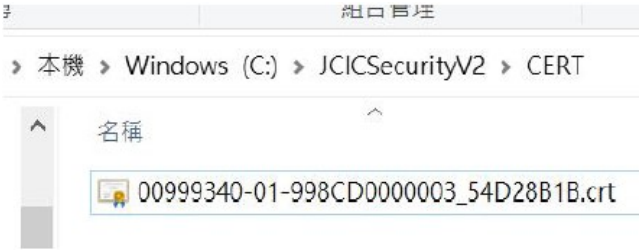


(3) 點擊「選取憑證」鈕。

(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

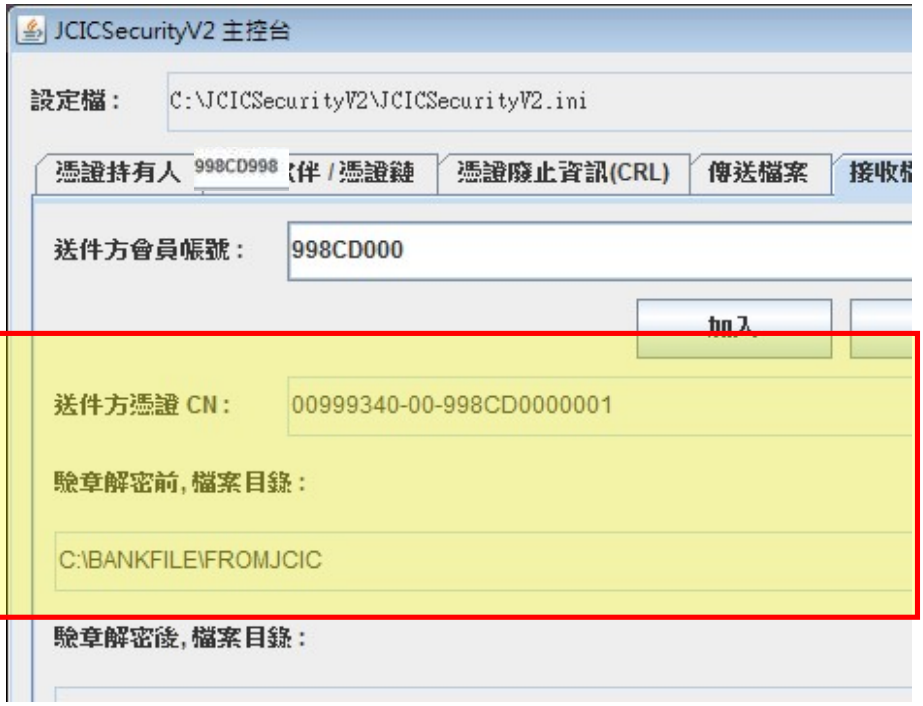
00999340-01-998CD0000003_54D28B1B



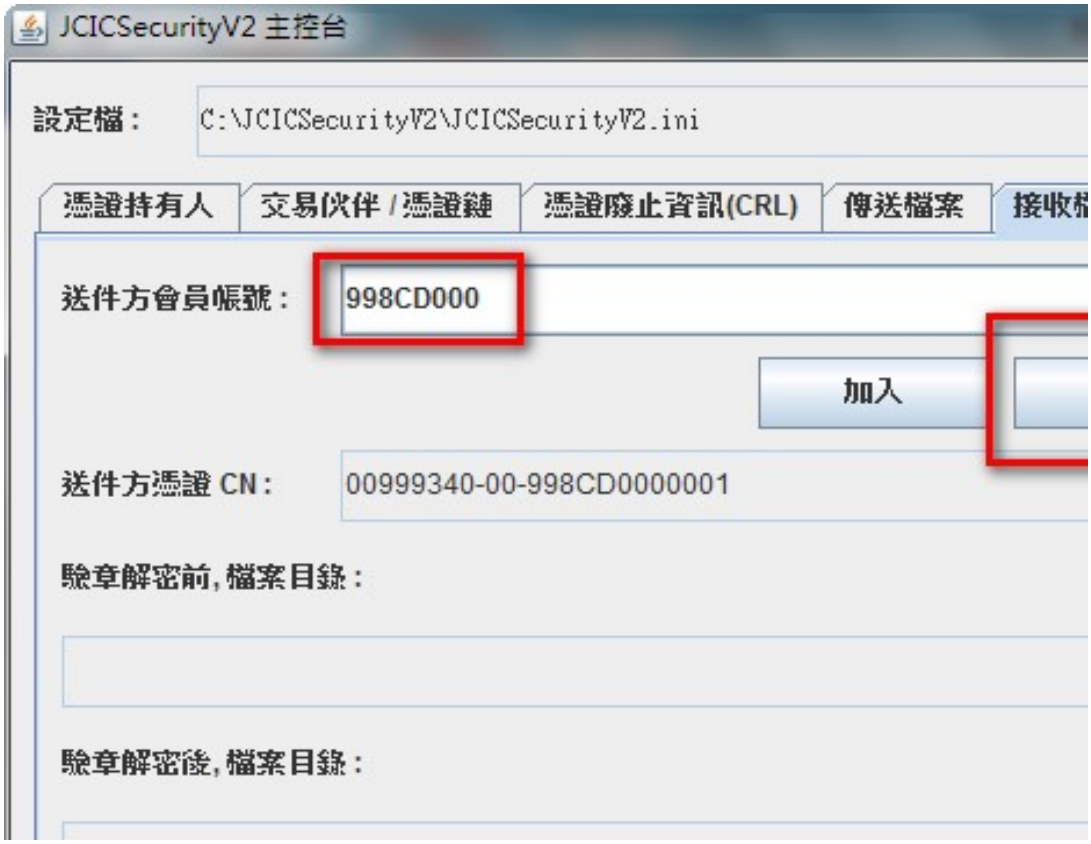
測試環境收送件方憑證 CN 的選取為

00999340-01-998CD9980001_4EF35C5B

(5) 選取驗章解密前，檔案目錄之「瀏覽」鍵並選取「C:\BANKFILE\FROMJCIC」
選取驗章解密後，檔案目錄之「瀏覽」鍵並選取「C:\BANKFILE_E\FROMJCIC」
選取驗章解密後，檔案備份目錄之「瀏覽」鍵並
「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

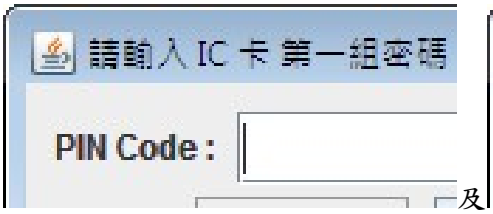
***注意:如使用單位之測試機與正式機為同一部電腦時，請注意進行憑證安控模組啟動測試時，切勿執行正式環境之檔案傳輸作業(包含傳送及接收檔案)。**

3.4.1 憑證安控模組啟動服務

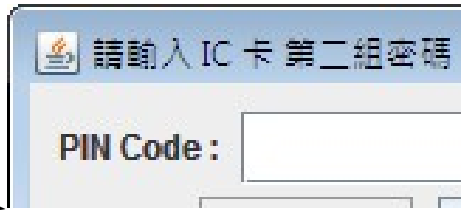
(1) 下圖為『JCIC Security V2 主程式』執行畫面，請點擊『啟動/停止服務』按鈕。

(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。

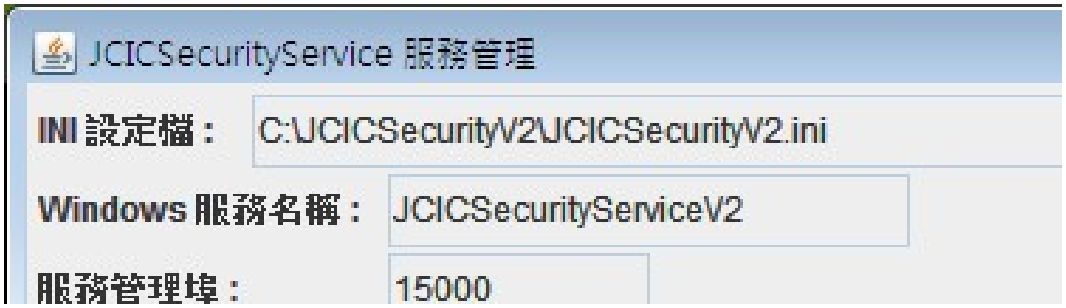


及



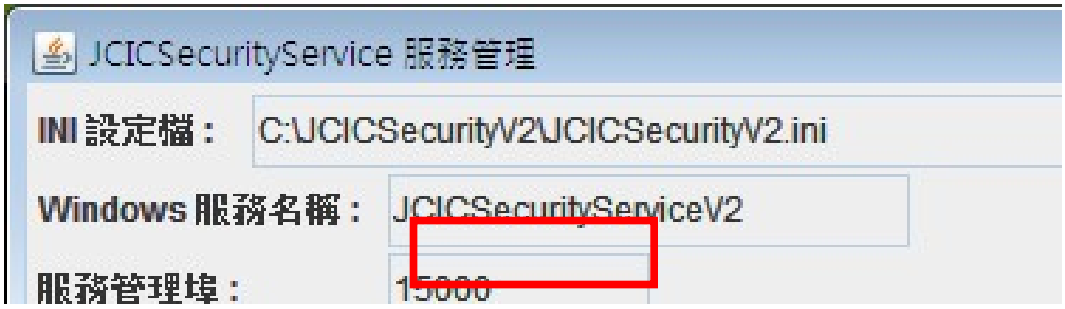
如點選『取消』將取消讀取 IC 卡作業，返回畫面繼續操作。

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

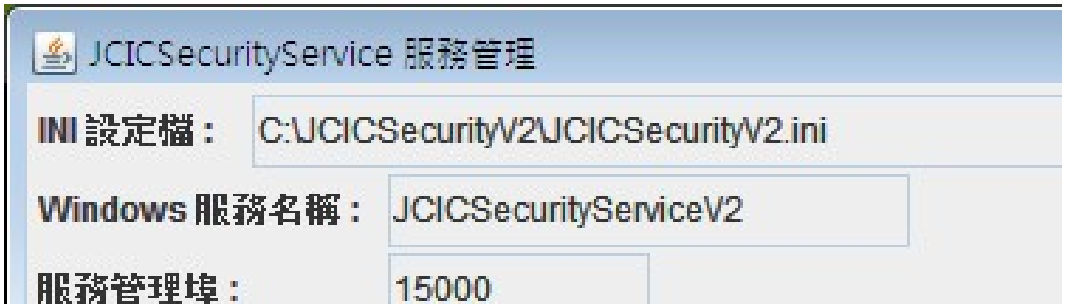
(1) 當服務已經啟動執行中，如下畫面



(2) 點選『暫停服務』，即可將服務暫停，如下畫面

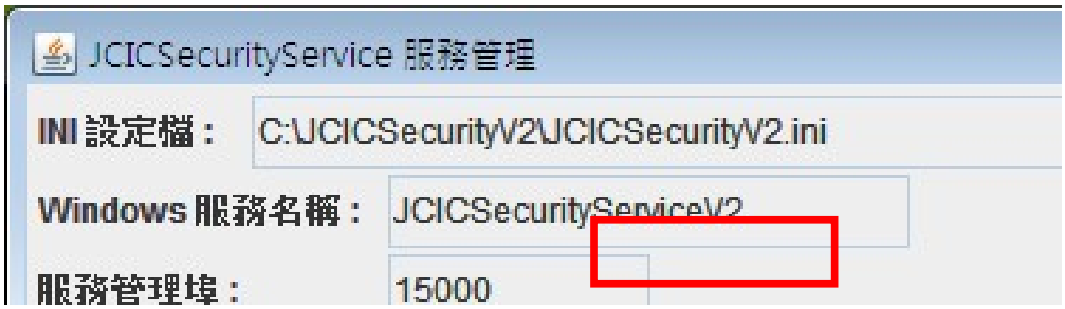
等待十數秒之後，顯示服務暫停成功。

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。



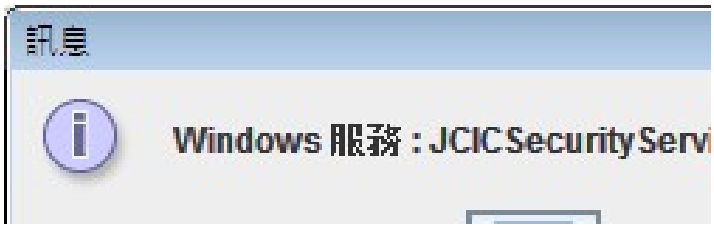
3.4.3 憑證安控模組繼續服務

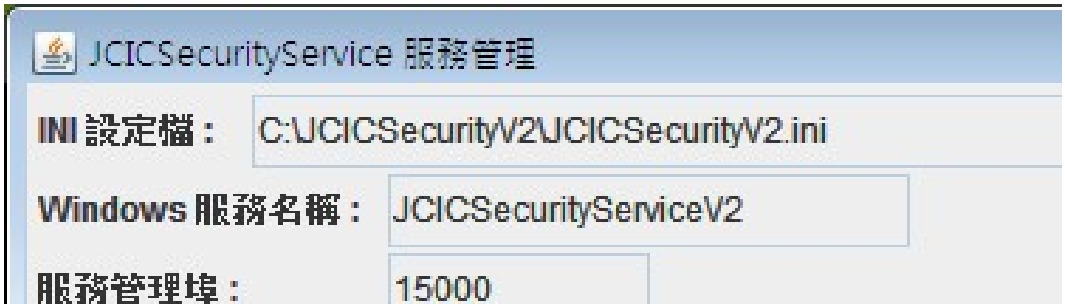
(1) 當服務已經暫停執行中，如下畫面



(2) 點選『繼續服務』，即可將服務繼續，如下畫面

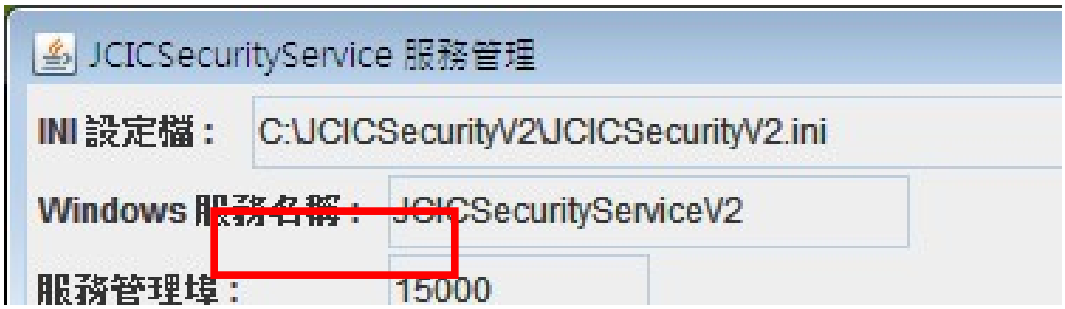
等待十數秒之後，顯示服務繼續成功。





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

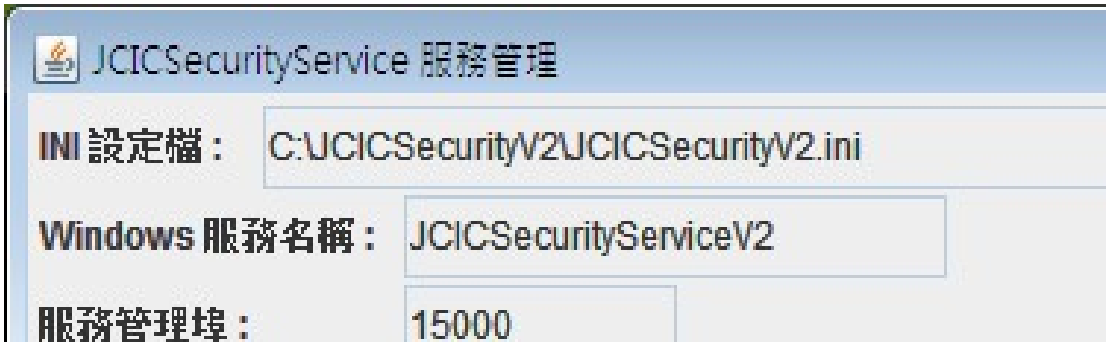


(2) 點選『停止服務』，即可將服務停止，如下畫面

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:

顯示紀綠等級分為: 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

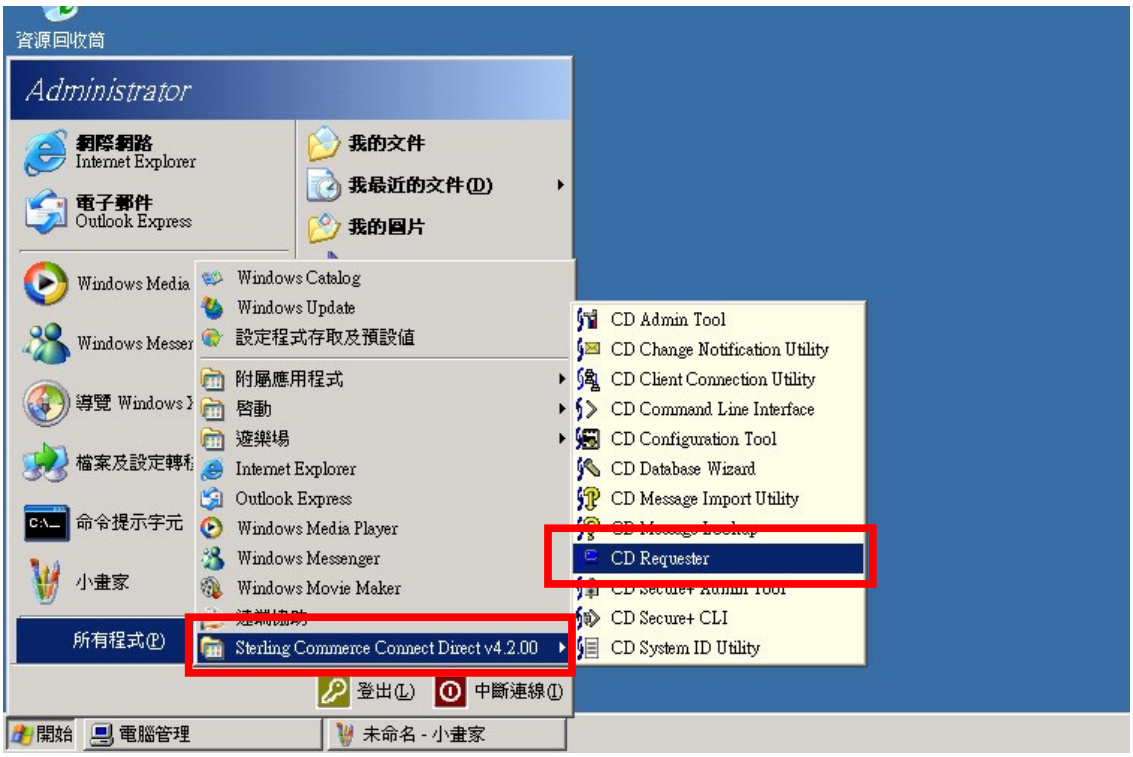
正式: 172.31.200.125

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。

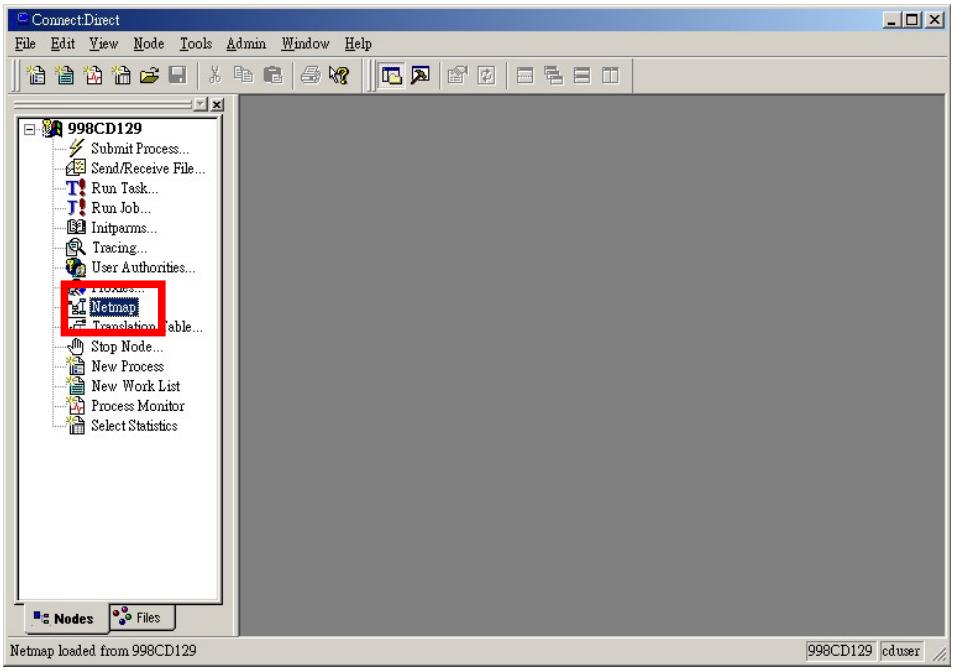
<u>設定 CD Server IP 請參考以下步驟:</u>

Step 01.更改 CD netmap 設定:

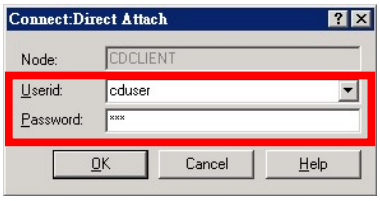
(1) 開始』—『程式集』—『Sterling Commerce Connect Direct v4.2.00』—『CD Requester』。



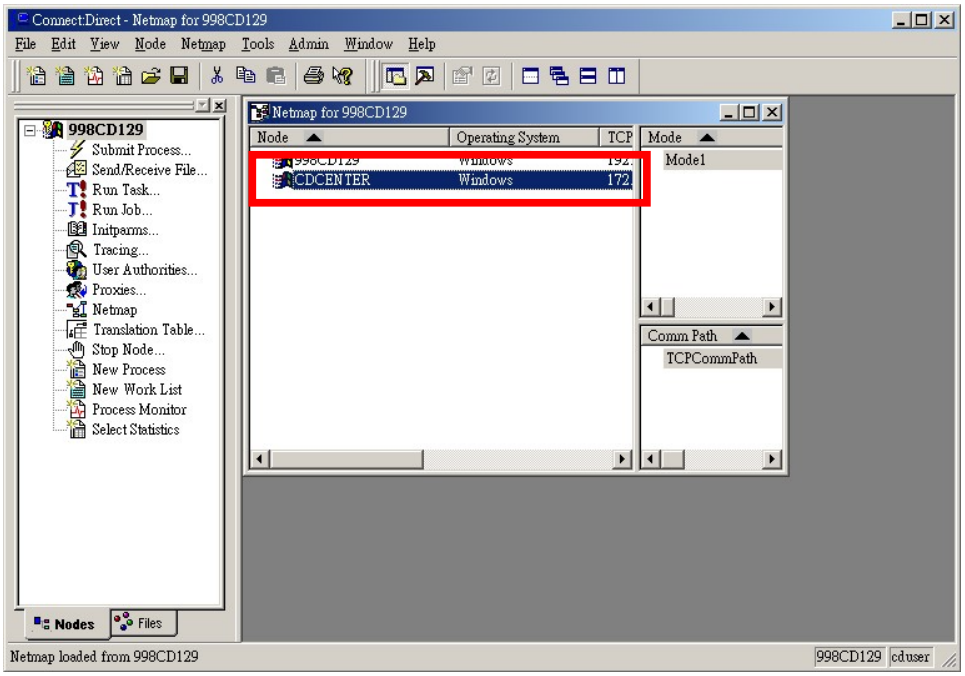
(2) 點選 『Netmap』兩下。



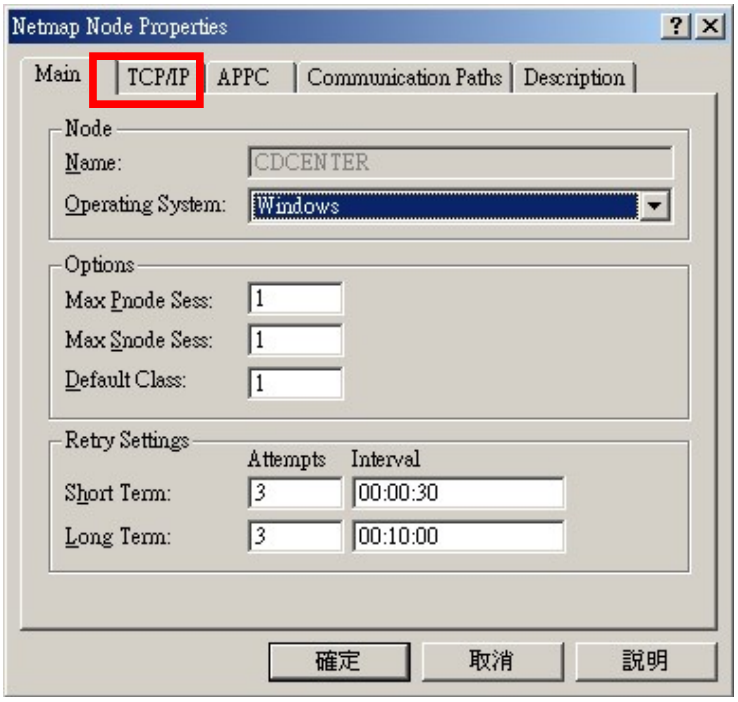
(3) 請輸入 cduser 及密碼，並注意大小寫。



(4) 點選『CDCENTER』。



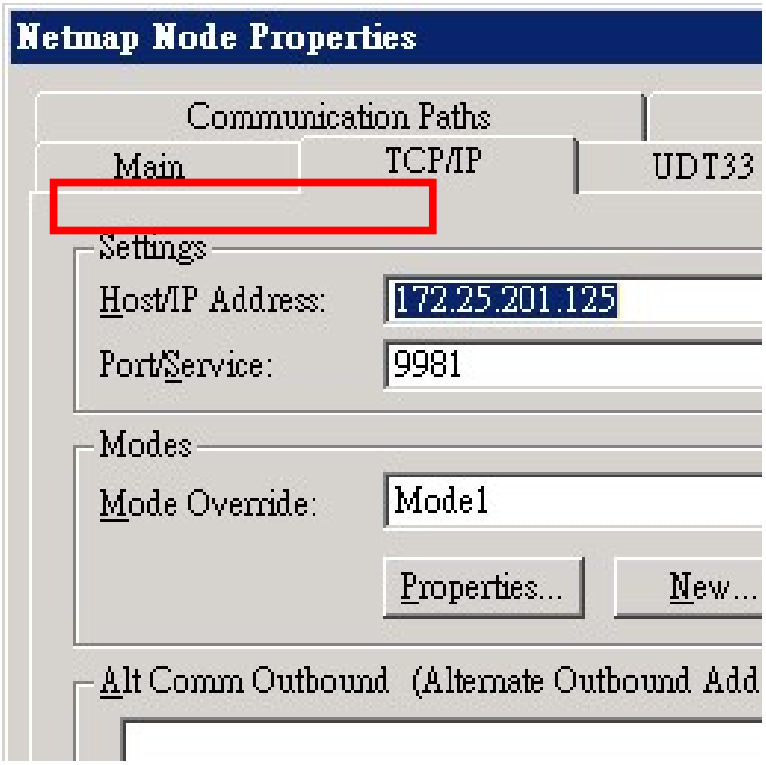
(5) 點選『TCPIP』。



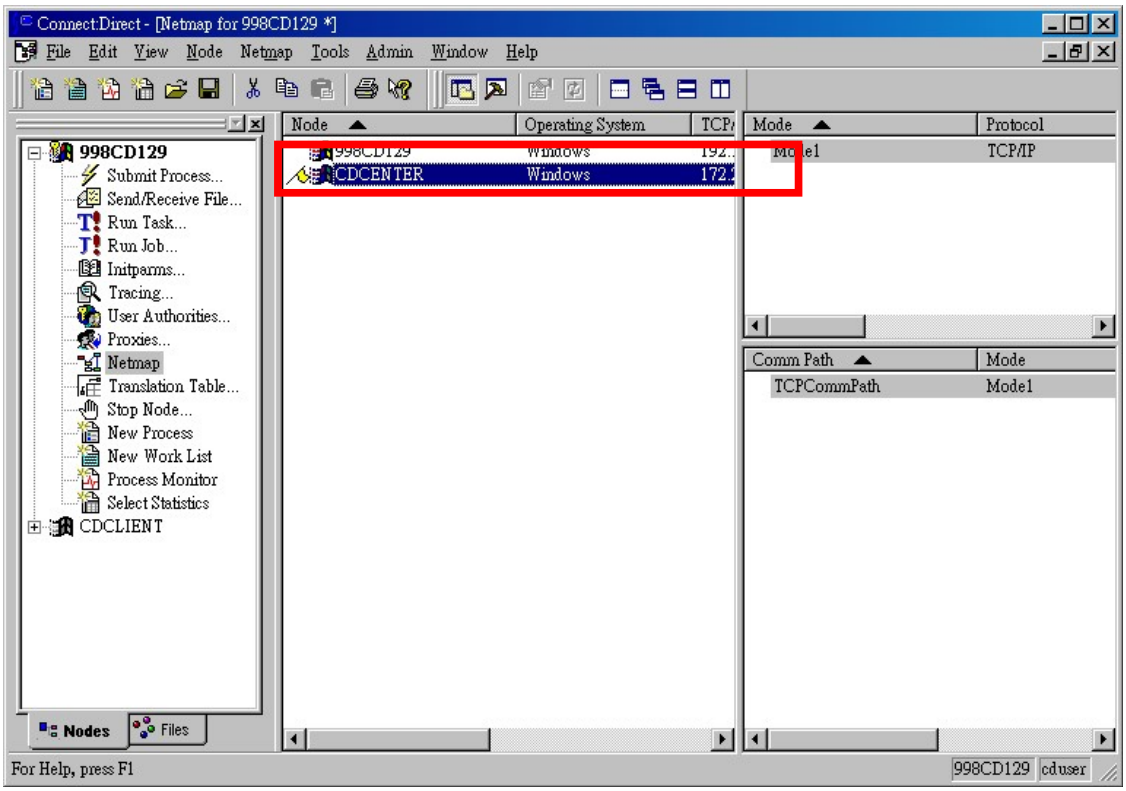
(6) 依需求更改 Host/IP，並按『確定』。

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

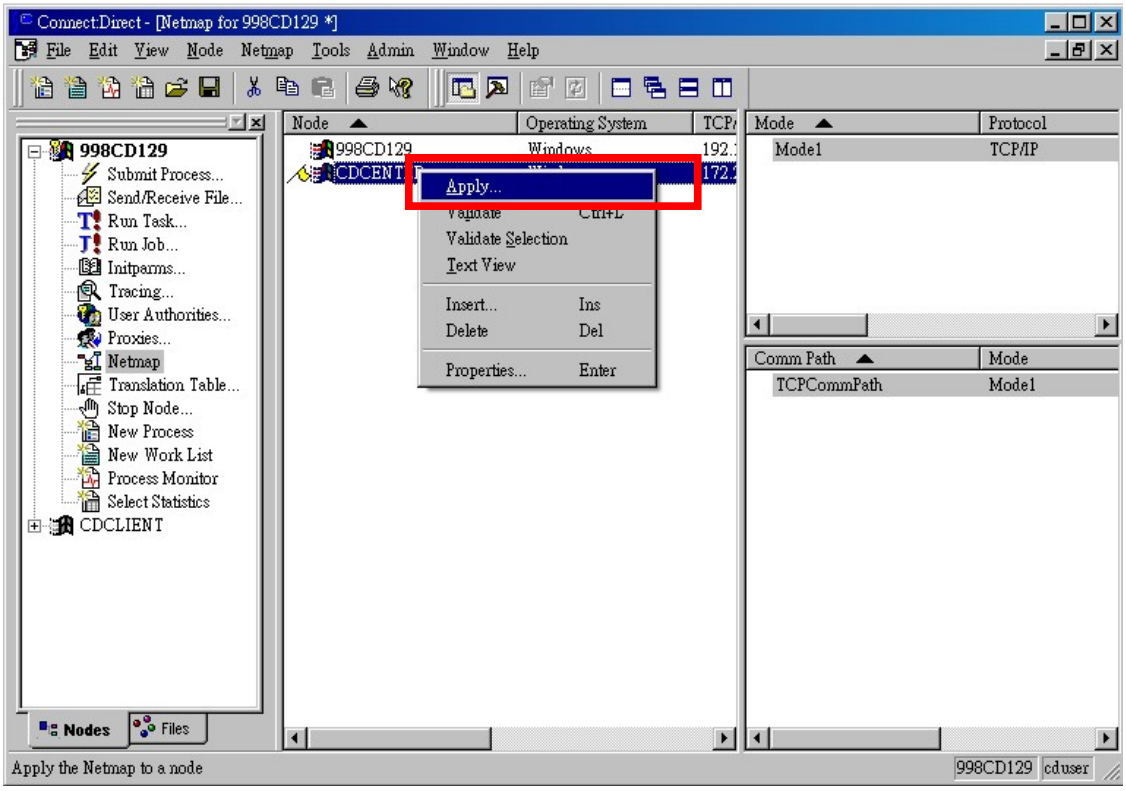
正式環境請將 Host/IP 指定為「**172.31.200.125**」



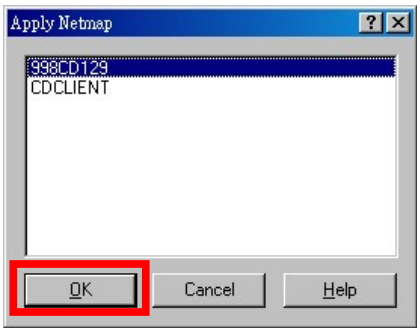
(7) 『CDCENTER』前方出現黃色旗幟，將游標移至『CDCENTER』前按右鍵。



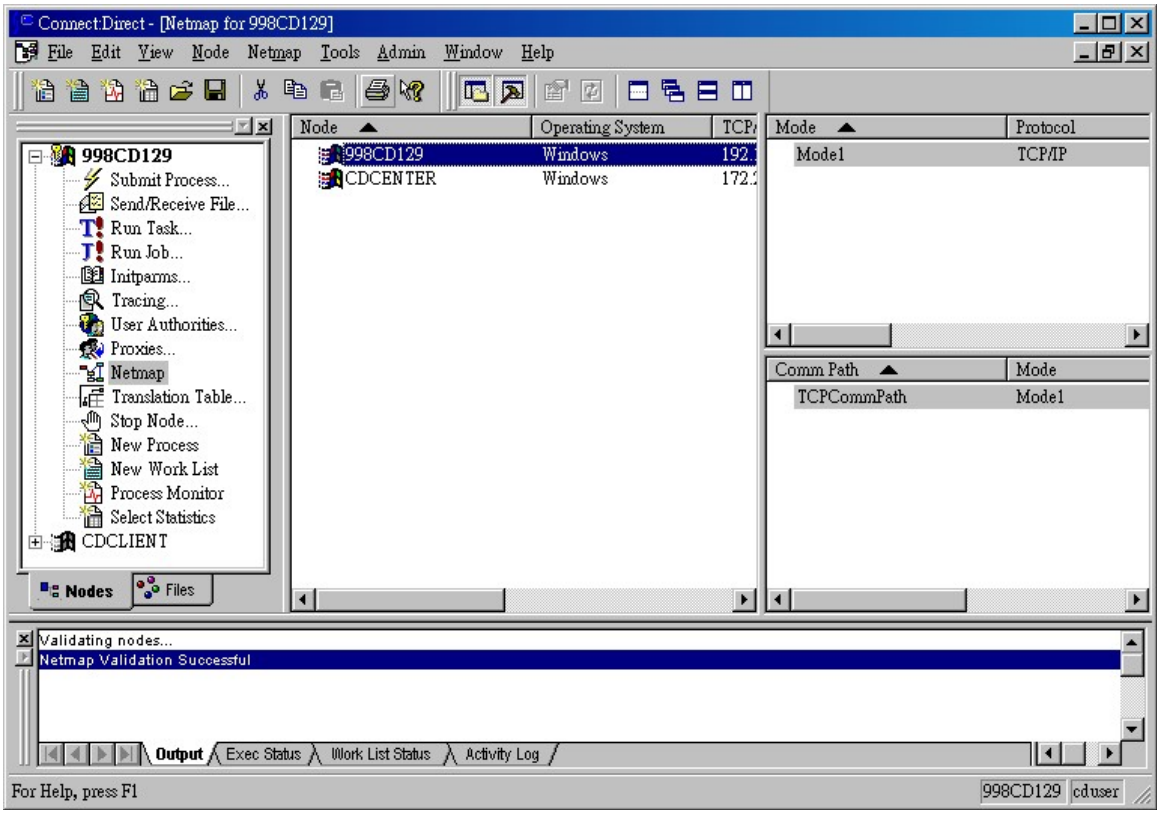
(8) 點選『Apply』。



(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。

及

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

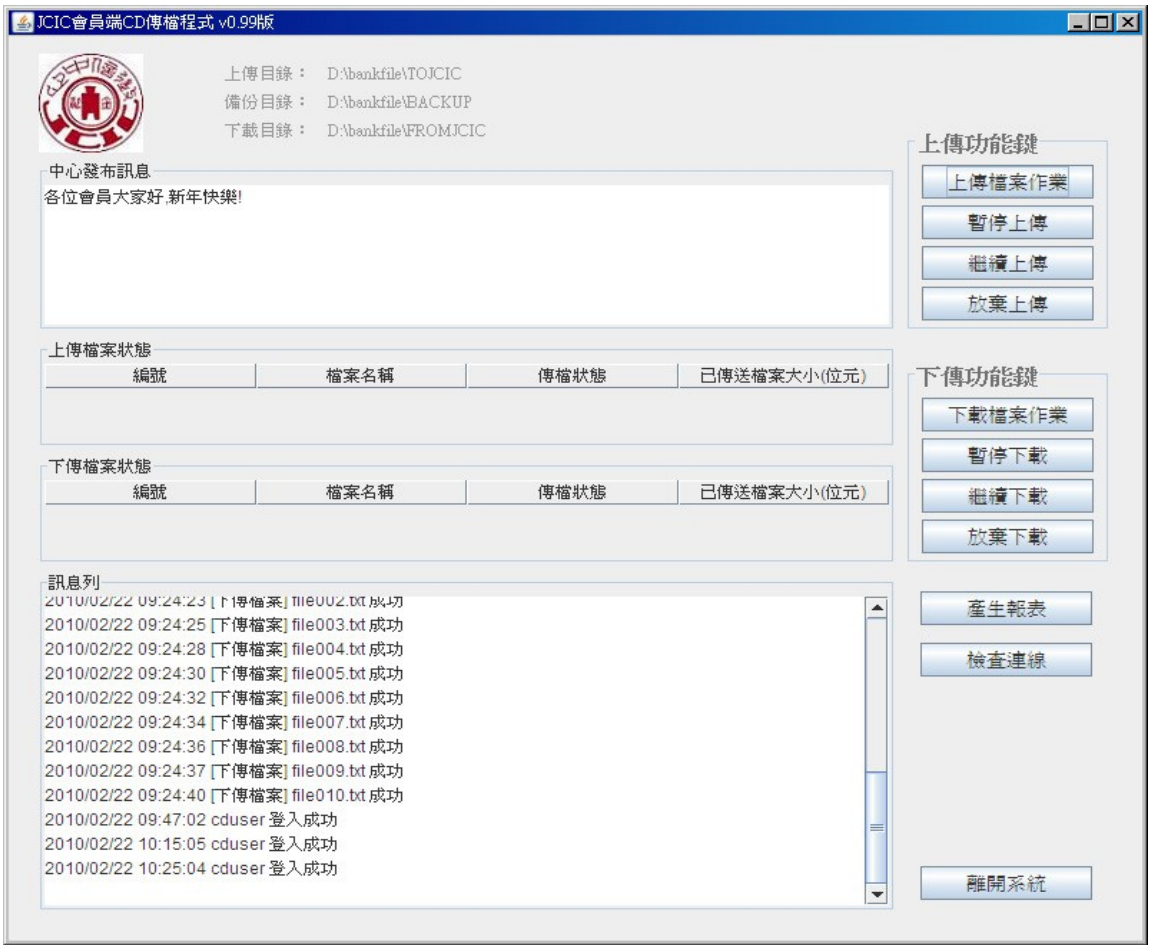
請與聯徵中心測試小組進行聯繫，並進行後續加解密軟體測試作業流程。相關聯絡資訊請參閱「5.聯絡資訊」章節。

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，此時該目錄應新增一「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。

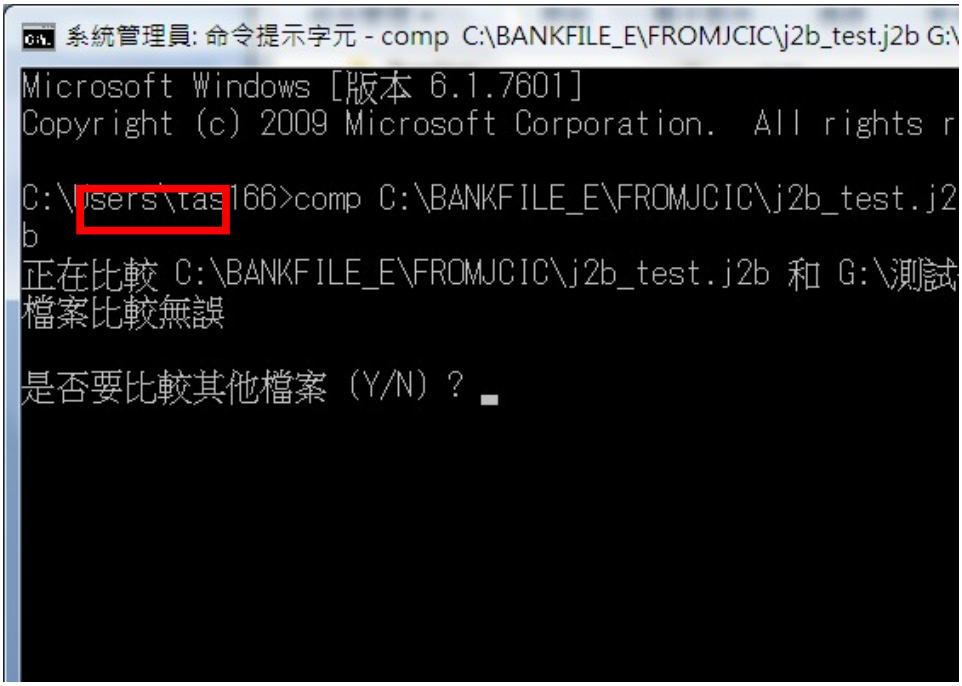


3.7.5 接收聯徵中心之測試用檔案，並測試解密驗章功能

(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) 使用憑證小幫手。

(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」。

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) 使用憑證小幫手，點選上方「卡片解鎖」功能。

(2) 請先將晶片卡插入讀卡機中，畫面將顯示其讀取之讀卡機型號，點選「確定」按鈕後繼續執行。

(3) 小幫手將以用戶註冊之 email 來進行驗證，並發出驗證信至信箱中。

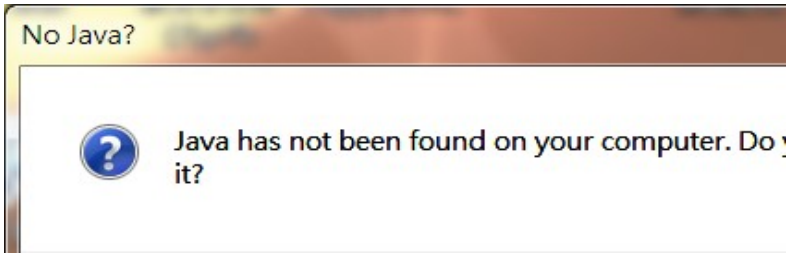
(4) 輸入 email 信箱收到的驗證碼，並按下確定

(5) 輸入新的晶片卡密碼即可進行解鎖卡

。

4.4. 問題處理

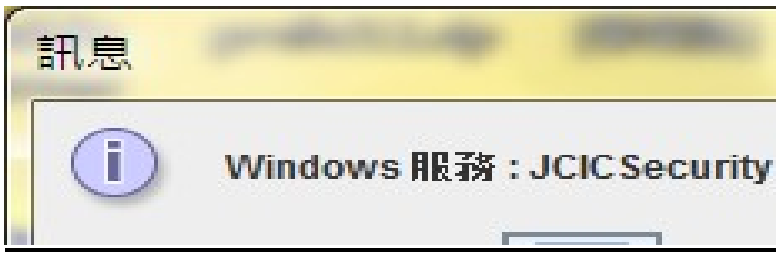
4.4.1 問題描述: 憑證安控模組無法正確啟動並出現下方圖示:



<u>問題處理方式</u>:

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。

4.4.2 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。

4.4.3 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』。

4.4.4 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。

4.4.5 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