HiSECURE 6.0 改版說明

(C/C++版 for Windows)

中華電信股份有限公司
電信研究所
資通安全研究室

97/10/22

議程

- 準備工作
- 改版說明
- 注意事項
- 問題反應窗口
- Q & A

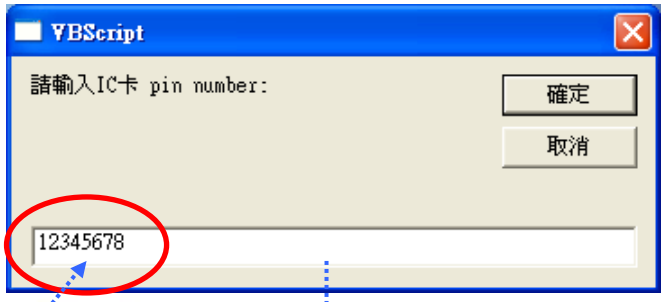
準備工作

- 取得2048 bits測試卡(本次說明會附贈2張)
  - 預設PIN碼為12345678
- 安裝HiCOS卡片管理工具(本次說明會附贈之光碟上含有安裝程式)
- 安裝讀卡機(本次說明會附贈1部)
- 連線到GTestCA 2048 bits憑證測試網頁，申請2048 bits測試憑證
  - 輸入完整網址 http://gtestca.nat.gov.tw/2048Main.html
  - 特別注意：

    以上GTestCA 2048 bits測試憑證網頁僅供配合API改版而修改GPKI相關應用系統機關或廠商測試使用，GTestCA官方網頁上並不會有以上網址的Hyperlink。

準備工作- GTestCA 2048 bits憑證測試網頁

2048 bits測試卡片的PIN碼為“12345678”



準備工作

- 進入GTestCA 2048 bits憑證測試網頁後，會自動下載新元件(ICCard Class - 版本1,0,2,2)覆蓋舊元件(ICCard Class - 版本1,0,1,1) 。確認方式如下：
  - IE→工具/網際網路選項→一般/設定→檢視物件→尋找ICCard Class→查詢版本
  - 或直接在\WINDOWS\Downloaded Program Files →尋找ICCard Class→查詢版本
- 完成安裝HiCOS卡片管理工具後，在\WINDOWS\system32會有HiCOSPKCS11.dll，版本2.0.5.26998。
- 若無法順利申請測試憑證，請依以上兩點檢查新元件是否存在。
- 可開始使用HiSECURE API 6.0版

準備工作

- 若想恢復回原本GTestCA上的ICCard Class版本(1,0,1,1)，請依下列步驟進行：
  - 關閉IE之測試憑證申請網頁
  - 到\WINDOWS\Downloaded Program Files刪除版本為1,0,2,2的ICCard Class
  - 到GTestCA網站的憑證申請→我要申請憑證(http://gtestca.nat.gov.tw/03-01.html)→點選「我要申請」→網頁自動下載元件(版本1,0,1,1)

準備工作

- 本次提供的2048 bits IC卡僅供測試使用，只相容於本次說明會提供之讀卡機，未來正式提供之2048 bits IC卡將會相容於一般讀卡機。
- 光碟中所提供之新版API係供參加本次說明會之機關或廠商對於未來政府GPKI可能改用2048 bits卡片預先修改其相關應用系統。
- 請勿擅自把新版HiCOS卡片管理工具或新版API相關之dll佈署到用戶端電腦，以免影響其他尚未進行API改版之應用系統在用戶端電腦的使用。
- 政府GPKI對於各機關因應2048 bits卡片之修改完成之新版應用系統上線時間，將會有統一的建議時間，請機關及廠商後續注意政府GPKI的新版API上線的統一政策，大家配合在接近的時間才佈署搭配新版API之新版應用系統。

改版說明

- 6.0 版與 5.3 版的差異
- 5.3 版錯誤修正
- 新增錯誤代碼
- 範例程式的更新(錯誤控制和新增註解)
- 操作手冊等文件更新

改版說明-6.0 版與 5.3 版的差異

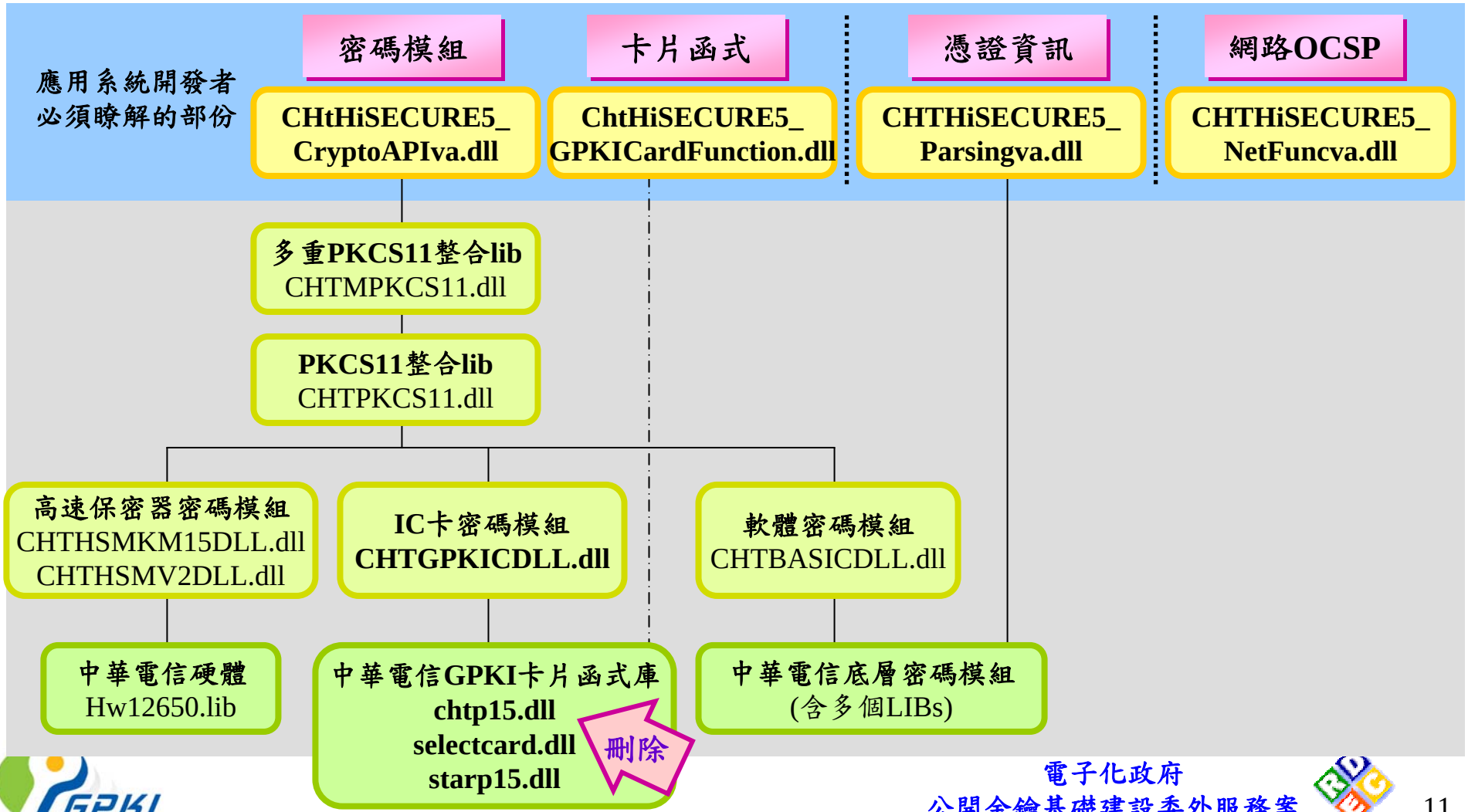
- 更換DLL
  - 為了支援 Hicos 2048 bits 卡片，以及整合舊版智慧卡函式庫之需求，新增一個動態連結檔為 HiCOSPKCS11.dll，此為 HiSECURE API 函式架構界面圖中的 pkcs11 DLL 部分，其運作原理為利用呼叫 HiCOS PKCS#11 來實作整合性智慧卡函式庫的輸出介面功能。

改版說明-6.0 版與 5.3 版的差異

- 取代 5.3 版舊版智慧卡函式庫之三個動態連結檔 chtp15.dll、selectcard.dll、starp15.dll。
- 同時亦需更新
  - ChtHiSECURE5_GPKICardFunction.dll
  - CHTGPKICDLL.dll

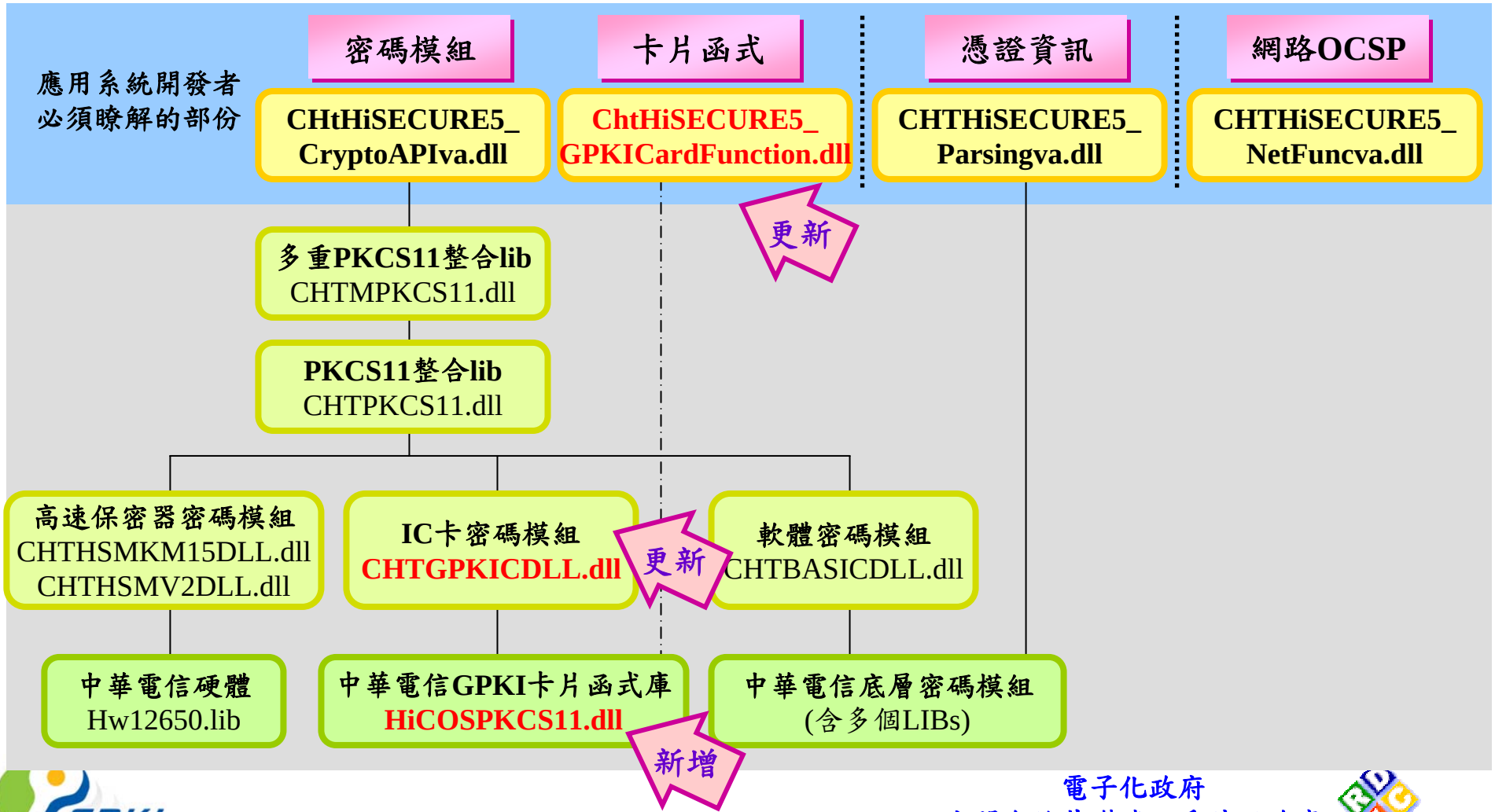
改版說明-6.0 版與 5.3 版的差異

HiSECURE 5.3 函式介面架構圖



改版說明-6.0 版與 5.3 版的差異

HiSECURE 6.0 函式介面架構圖



改版說明-6.0 版與 5.3 版的差異

- 特別注意：

  用戶端的電腦必須先安裝HiCOS卡片管理工具 (內含HiCOS PKCS#11 dll)，如此利用HiSECURE API 6.0版開發的應用系統才能正常在用戶端電腦使用。

改版說明-5.3版錯誤修正

- GetCRLRecord 函式
  - 功能：從 CRL 中取得第 N 筆資料
  - 修正：假設 CRL 中共有 M 筆資料，發現查詢 index ≧ M+1 會回傳第 M 筆資料的問題，但實際上並無從第 M+1 筆起的資料存在。
- CRLParse 範例程式
  - 修改：查詢 CRL 中所有 Records
  - 新增：查詢單筆 CRL Record

改版說明-新增錯誤代碼(1)

- **0x8301**, E_NO_TOKEN_SLOT：讀卡機未插卡
- **0x8302**, E_INVALID_CONTEXT：傳入的context不正確
- **0x8303**, E_DATA_LENGTH：資料長度不對
- **0x8304**, E_INIT_CARD：建立卡片通訊連結失敗
- **0x8305**, E_PARAMETER：傳入的參數不正確
- **0x8306**, E_INVALID_P11VERSION：傳入的 P11 版本不正確
- **0x8307**, E_BUFFERTOOSMALL：傳入的 buffer 太小
- **0x8308**, E_NOT_FIND_OBJECT：找不到物件

改版說明-新增錯誤代碼(2)

- **0x8309**, E_P11FUNCTION_FAILED：函式庫內部呼叫PKCS#11 function錯誤
- **0x830A**, E_GET_SLOT_LIST：列舉讀卡機失敗
- **0x830B**, E_GET_SLOT_INFO：讀取讀卡機資訊失敗
- **0x830C**, E_GET_TOKEN_INFO：讀取卡片資訊失敗
- **0x830D**, E_CREATE_OBJECT：物件產生失敗
- **0x830E**, E_SET_ATTRIBUTE：物件屬性更新失敗
- **0x830F**, E_GET_ATTRIBUTE：讀取物件屬性失敗

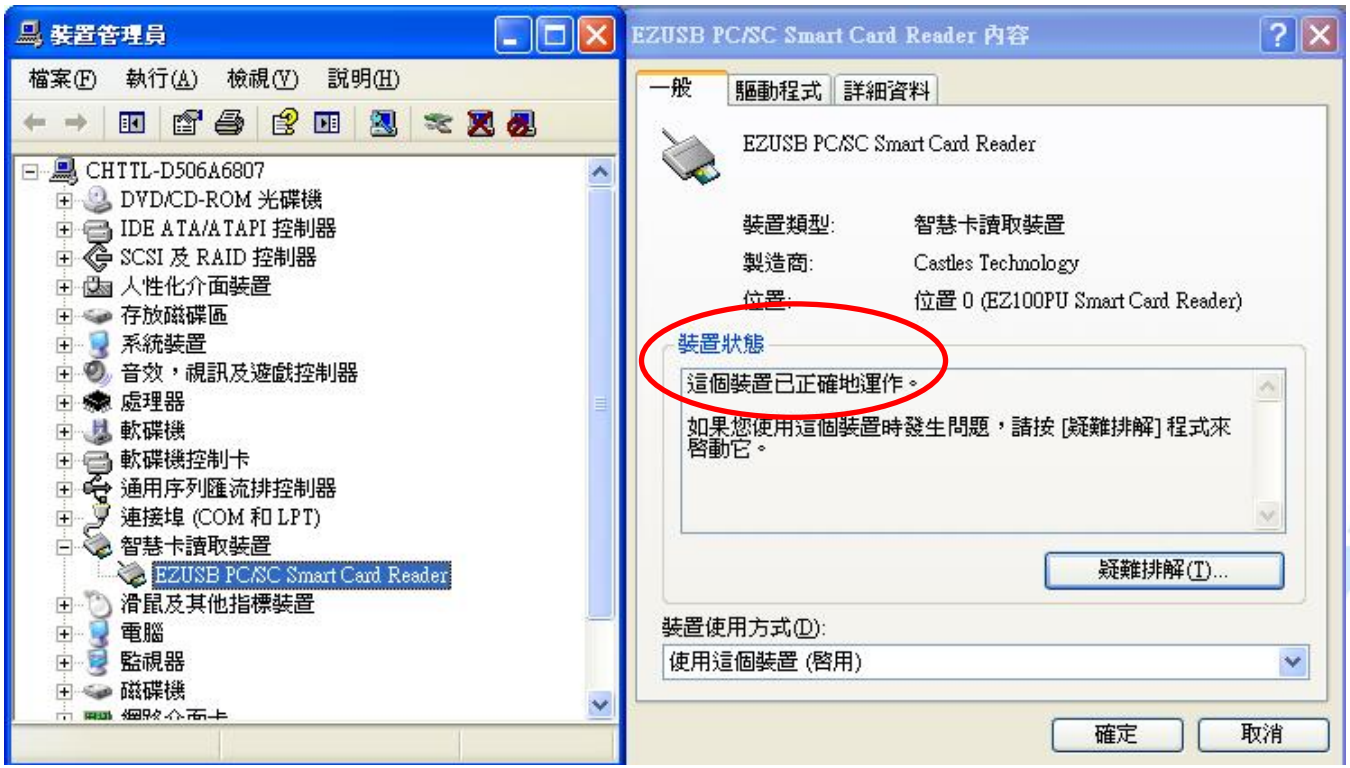
以上錯誤代碼皆為HiSECURE API使用到HiCOSPKCS11.dll發生錯誤時所傳出

注意事項

- 確認讀卡機
- 確認卡片
- 確認卡片內憑證
- 確認 API 版本
- 確認程式執行所需檔案(h/lib/dll)放置位置
- 常見錯誤代碼說明

注意事項-確認讀卡機

- 裝置管理員→智慧卡讀取裝置→裝置狀態

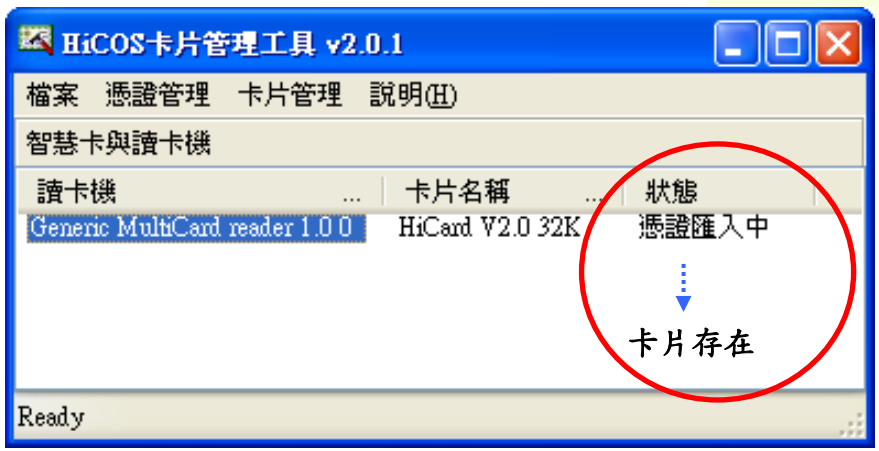


注意事項-確認卡片

- 依卡片種類到相關網站檢視 IC 卡資訊
  - 自然人憑證可在 MOICA 網站的「憑證作業」→「檢視憑證IC卡資訊」→得知卡號、發行者名稱、卡片持有者資訊、憑證期限。
  - GCA憑證可在GCA網站的「憑證及IC卡相關作業」→「檢視憑證IC卡資訊」→得知卡號、…
  - XCA憑證可在XCA網站的「憑證及IC卡相關作業」→「檢視憑證IC卡資訊」→得知卡號、…
  - 工商憑證可在 MOEACA 網站的「憑證IC卡相關作業」→「檢視卡片資訊」→得知卡號、…
- 利用「憑證 IC 卡功能測試程式」網頁的「由 IC 卡讀取用戶憑證」功能
  - 顯示驗證簽章用憑證的資訊
  - 顯示資料加密用憑證的資訊

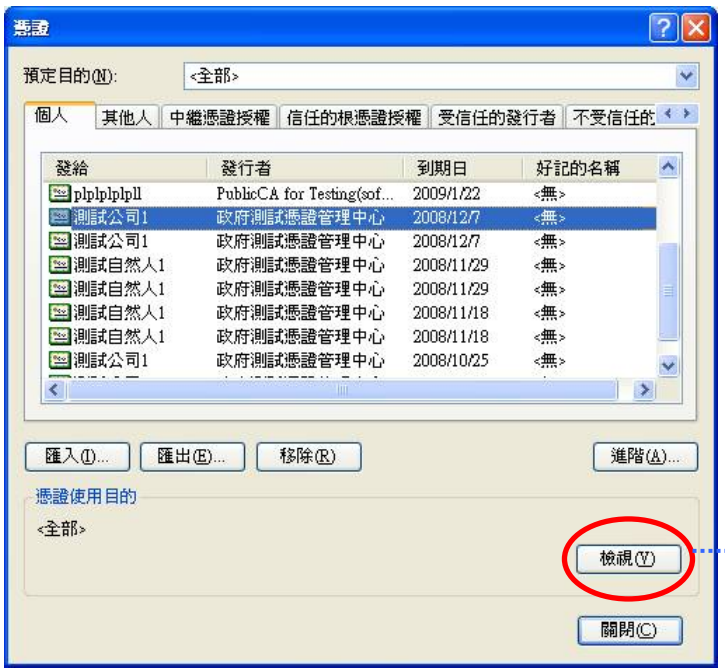
注意事項-確認卡片內憑證

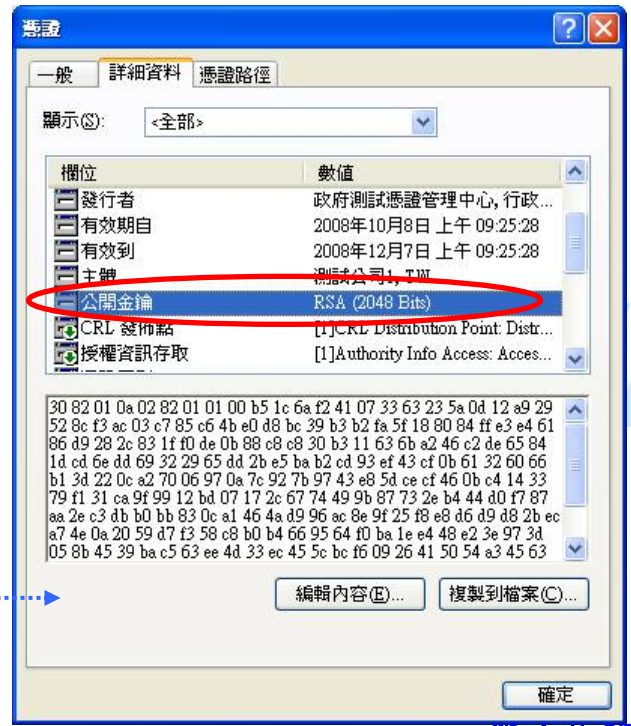
- 使用HiCOS卡片管理工具匯入憑證至系統憑證區
  - 開始→程式集→HiCOS PKI Smart Card→HiCOS卡片管理工具
  - 將卡片放入讀卡機中，狀態變化為卡片不存在→卡片存在→憑證匯入中→卡片存在



注意事項-確認卡片內憑證

- 檢視憑證中的金鑰長度是否為2048 bits
  - IE→工具/網際網路選項→內容/憑證→選取測試憑證「檢視」→查看「公開金鑰」欄位數值為“RSA(2048 bits)”



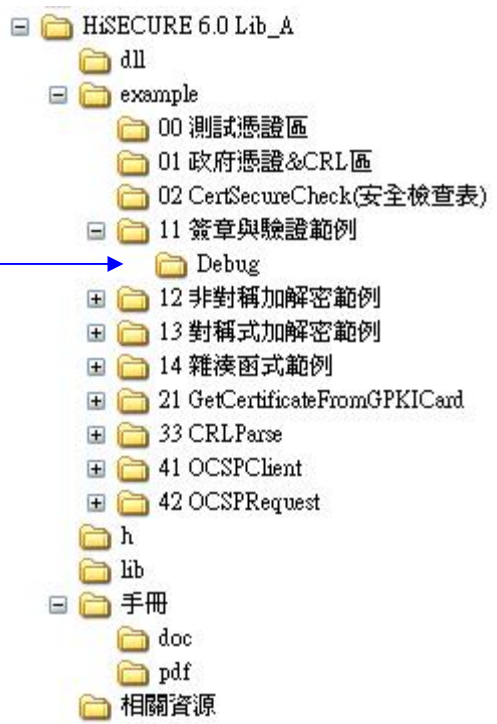


注意事項-確認API版本

- 本次說明會 HiSECURE API 測試版本為 6.0.0.0
  - CHTBASICDLL.dll
  - CHTGPKICDLL.dll
  - ChtHiSECURE5_CryptoAPIva.dll
  - ChtHiSECURE5_GPKICardFunction.dll
  - CHTHiSECURE5_NetFuncva.dll
  - CHTHiSECURE5_Parsingva.dll
- 其餘相關dll版本不變(同5.3版)
- HiCOSPKCS11.dll 版本為 2.0.5.26998

注意事項-確認程式執行所需檔案(h/lib/dll)放置位置

- HiSECURE API release 時的檔案目錄結構
  - **dll**
  - example
  - **h**
  - **lib**
  - 手冊
  - 相關資源



注意事項-常見錯誤代碼說明(1)

- **0x7303**(29443)或 E_SLOT：

  SLOT 錯誤，有可能是卡片未完全放入讀卡機中，或卡片本身有問題以致讀卡機讀取不到。

  (檢查 GetCertificateFromGPKICard 函式的回傳值可能得到)

- **0x7302**(29442)或 E_NOT_SUPPORT_FUNCTION：

  函式未支援，可能原因為 .dll 版本不對。

- **0x7301**(29441)或 E_NOT_LOAD_DLL：

  PKCS#11 函式庫載入失敗，原因為HiCOSPKCS11.dll 未放在 Debug 或 system32 資料夾內。

注意事項-常見錯誤代碼說明(2)

- **0xDB011201**(-620686847)或
  Input_Error_Card_Pin_First：PIN碼錯誤一次
- **0xDB011202**(-620686846)或
  Input_Error_Card_Pin_Second：PIN碼錯誤兩次
- **0xDB011203**(-620686845)或
  Input_Error_Card_Pin_Third：PIN碼錯誤三次
- **0xDB011204**(-620686844)或
  Smard_Card_Pin_Is_Locked：鎖卡

注意事項-常見錯誤代碼說明(2)

- 檢查 InitSession 函式的回傳值可能得到以上代碼
- 右圖為執行「簽章與驗證範例」測試 PIN 碼輸入錯誤的情形
- GTestCA政府測試憑證管理中心-鎖卡解碼/重設 PIN 碼
  網址：http://gtestca.nat.gov.tw/05-03.html

```
1.簽章&驗證簽章
成功取得IC卡憑證!
請輸入 Pin Code (三次機會):abcdef
InitSession RetValue = -620686847

Pin Code 錯誤, 請重新輸入:123456
InitSession RetValue = -620686846

Pin Code 錯誤, 請重新輸入:1234qwer
InitSession RetValue = -620686845

卡片已被鎖住!
回傳值: -620686844 (0xdb011204)
```

注意事項-常見錯誤代碼說明(3)

- **0xDA010001**(-637468671)或 Buffer_Too_Small：第一次呼叫以下函式時，正常情況應回傳此值。
  - GetCertificateFromGPKICard
  - MakeSignature
  - PublicKeyEncryption
  - PrivateKeyDecryption
  - SymEncryptionAlg
  - SymDecryptionAlg
  - HashFunction

注意事項-常見錯誤代碼說明(3)

- 關於Buffer_Too_Small的程式撰寫方式

```
/*-----------------------------
  步驟 1. 從 IC 卡中讀取憑證
-----------------------------*/
    int             iCertID = 1;              // 取出卡片內部第一張憑證(簽章用)
    unsigned char   *pCertfromICCard = NULL;  // 取出之憑證資料
    int             iCertLength = 0;          // 取出之憑證資料長度

    // 呼叫兩次 GetCertificateFromGPKICard 函式，第一次目的爲取得憑證資料的實際長度(iCertLength)
    iRetValue = GetCertificateFromGPKICard(iCertID, pCertfromICCard, &iCertLength, NULL);

    // 呼叫第一次後必須檢查 iRetValue 是否爲 Buffer_Too_Small (正常情況下)
    if (iRetValue != 0)
    {
        if (iRetValue != Buffer_Too_Small)
        {
            printf("無法取得IC卡憑證!\n");
            return iRetValue;
        }
        else {
            // 宣告足夠大的記憶體空間，來存放憑證資料
            pCertfromICCard = new unsigned char[iCertLength];
            iRetValue = GetCertificateFromGPKICard(iCertID, pCertfromICCard, &iCertLength, NULL);

            if (iRetValue != 0)
            {
                printf("無法取得IC卡憑證!\n");
                return iRetValue;
            }
        }
    }
    printf("成功取得IC卡憑證!\n");
```

問題反應窗口

- GCA/XCA/GTestCA客服中心：
  - Mail至GCA服務信箱：egov@service.gov.tw
  - 電話02-7738-8066
- MOEACA客服專線：
  - 電話412-1166
    - 當地電話號碼七碼或八碼地區(含金門地區)，請撥：412-1166
    - 當地電話號碼六碼地區，請撥：41-1166
    - 外島(如馬祖,烏坵,東沙,綠島,蘭嶼等地區)及國內行動電話，請撥：(02或04或07)-412-1166
    - 國外地區，請撥：886-(2或4或7)-412-1166
- MOICA「API問題/障礙申告」網頁：
  - 進入MOICA網站(http://moica.nat.gov.tw)，點選網頁上方的「應用服務」，然後點選網頁左方功能表的「API問題/障礙申告」

Q & A

報告完畢

請多指教