資訊安全實驗報告

實驗 1 –憑證申請

班級:資訊工程四A 學號:10503301A 姓名:鍾俊傑

問題與討論

1. 請實際到 GTestCA 申請非 IC 卡憑證(檔案型憑證)，說明申請過程與相關問題。

根據網頁\*號填入必須資料，然後使用OpenSSL建立MyCA.key和MyCA.req檔案，然後上傳MyCA.req到網頁中，再按下憑證申請，便可以下載已產生之憑證到電腦中。

2. 請實際到寰宇數位認證中心申請 Free Email Certificate，說明申請過程與相關問題。

根據網頁申請步驟，填完姓名及郵箱地址後，無法申請憑證，網頁彈出提示窗口，要求使用ie8或Chrome瀏覽器申請，然而使用ie8內核或Chrome瀏覽器進行申請動作，依然會彈出該提示而無法進行下一步動作，因此無法完整進行申請該憑證的實驗。

3. 以上兩種憑證申請有何差異? 寫下你的心得。

GtestCA的憑證需要使用OpenSSL建立密碼檔案，再上傳到網頁申請憑證，而Free Email Certificate憑證申請只需要填入個人資料及郵箱便可以獲取憑證，使用上較前者方便。

4. 請問你如何檢視所申請憑證檔案之身分? 如何儲存憑證?

憑證將存放於副檔名為.cer的檔案中，雙擊檔案便可以於詳細資料標籤中查看憑證中之身份。

5. 請說明如何在 OpenSSL 環境下，使用 RSA 金鑰簽署資料，並使用憑證驗證數位簽章 之方式，可以這次申請之憑證為例。

openssl rsautl -encrypt -certin -inkey 5BC22EE5ABF440F004C5E4C8AFFA0ED6.cer -in test1.txt -out test1.out

這條指令中的-certin的功能是Input is a cert carrying an RSA，這樣便可以使用憑證驗證數位簽章的方式去簽署加密資料。

openssl rsautl -decrypt -inkey MyCA.key -in test1.out -out test1chk.txt

以上這條指令可以解密以憑證加密的資料。

6. 你所申請的憑證有作用? 簡要說明你的心得。

憑證可作為個人於網絡上之身份證明，例如有了電子郵箱憑證後，就能確保我的email內容不會在傳輸過程中被非法竊聽、竊取和篡改，確保我的email裡的機密資訊不會被洩露。