資訊安全實習 ②

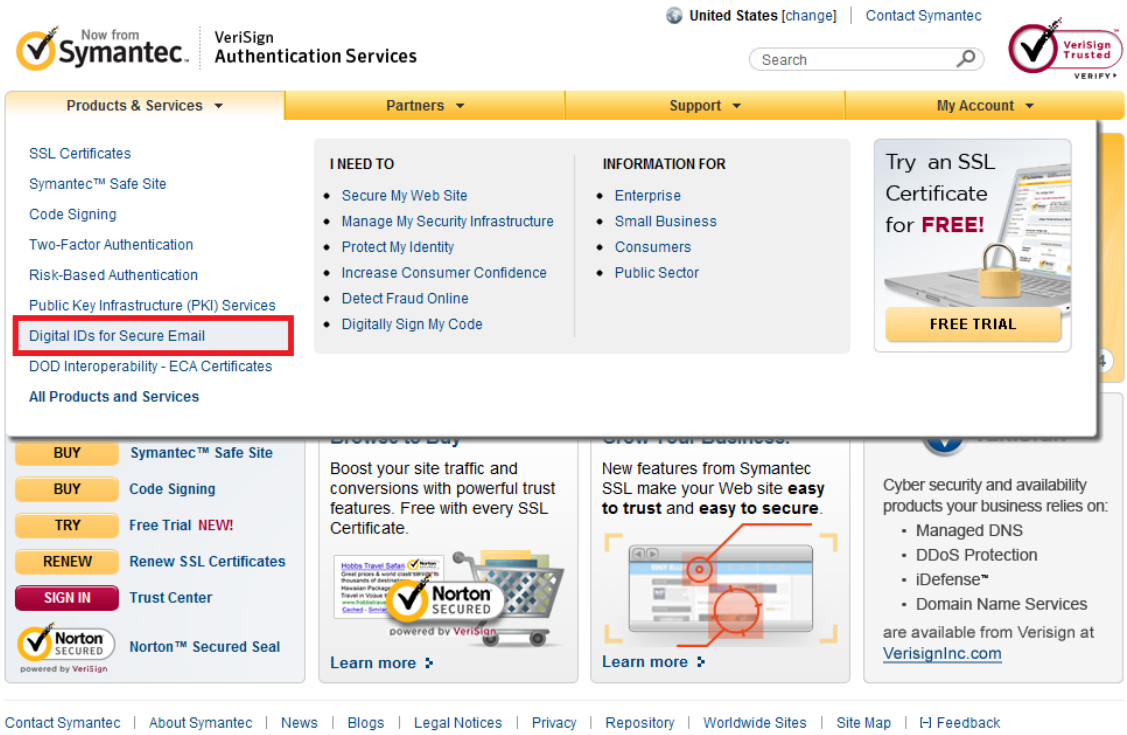
實驗名稱 － 個人憑證申請與 SMIME

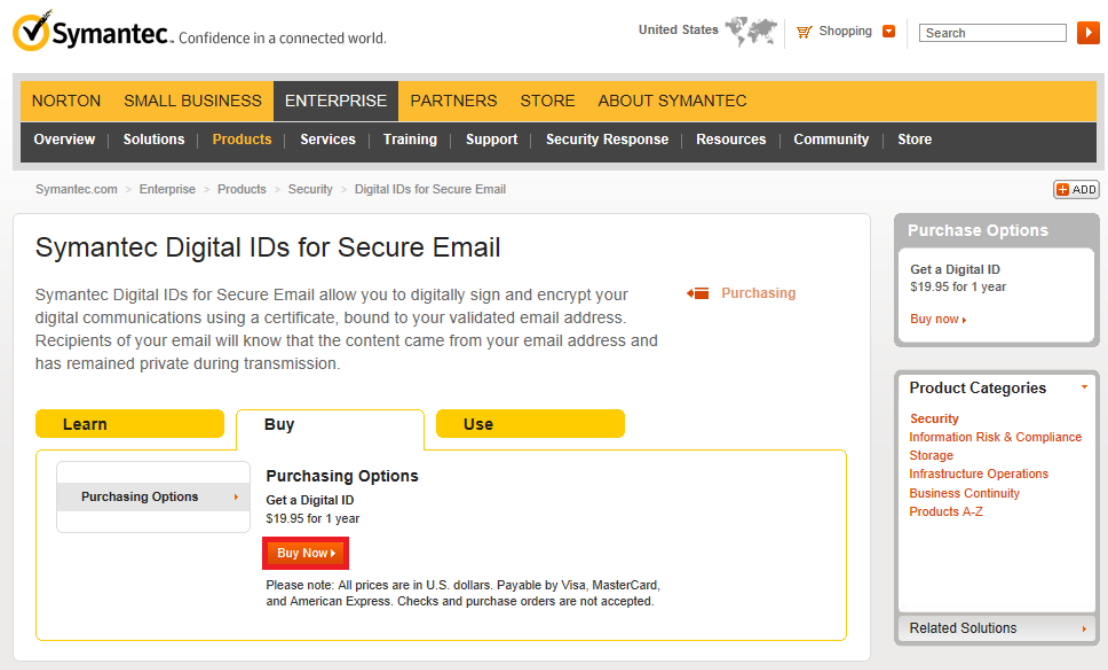
本實驗之目的主要讓學員瞭解憑證申請、安裝以及 Secure MIME 之實際操作。學員可由安裝過程中瞭解憑證於身份認證與電子郵件中實際運用之流程以及對相關軟體有一定程度之認識。

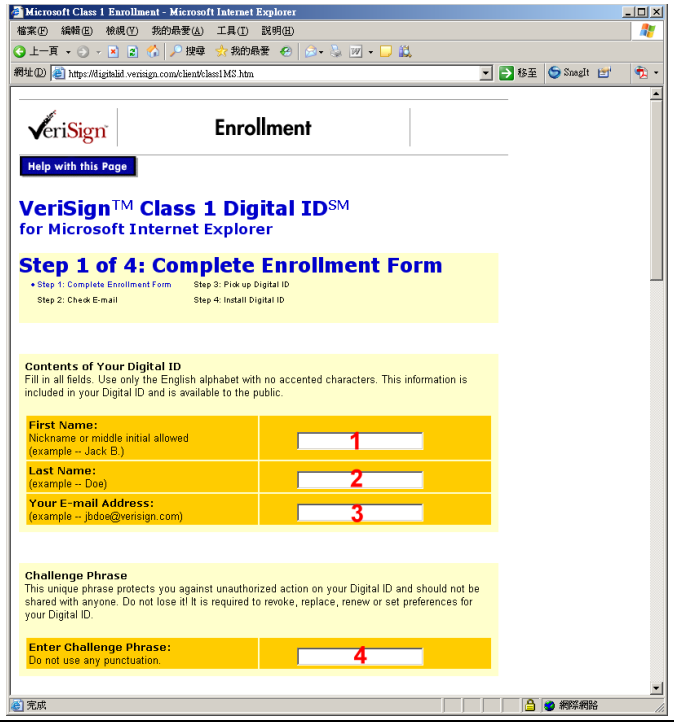
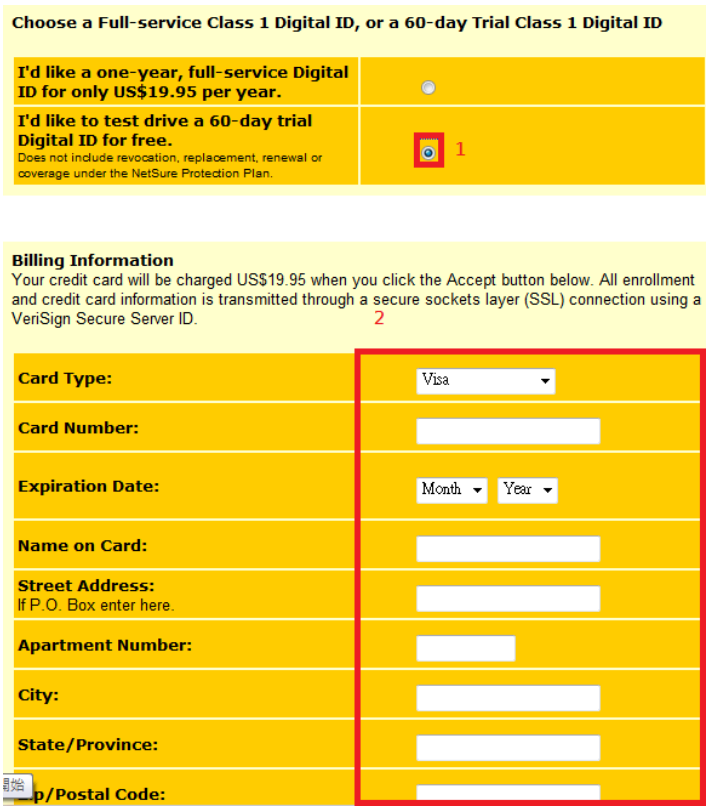
實驗測試步驟

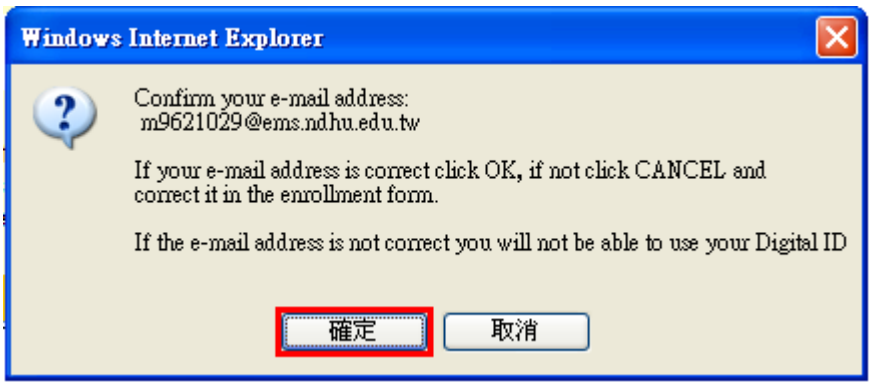
1. 個人 Certificate 申請

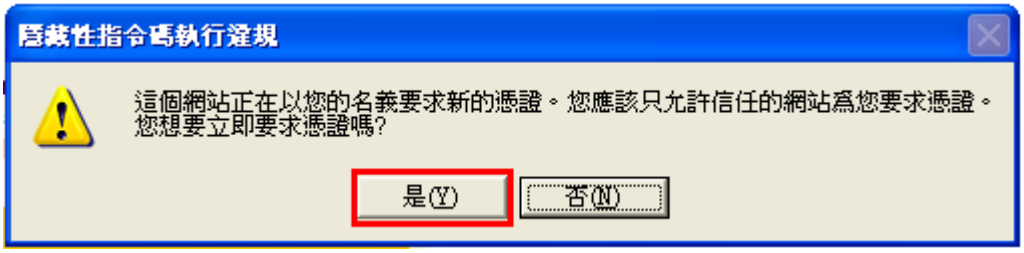
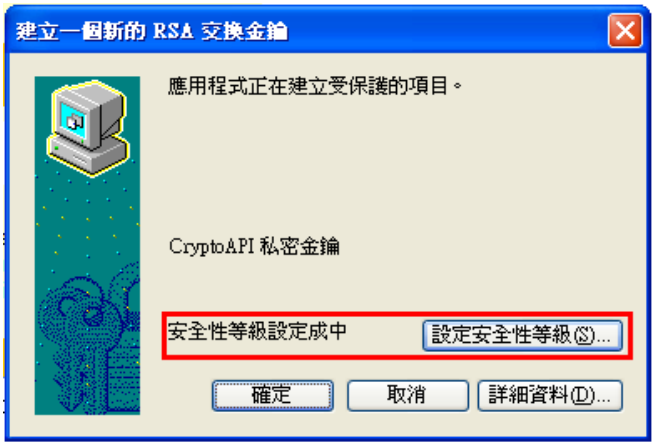
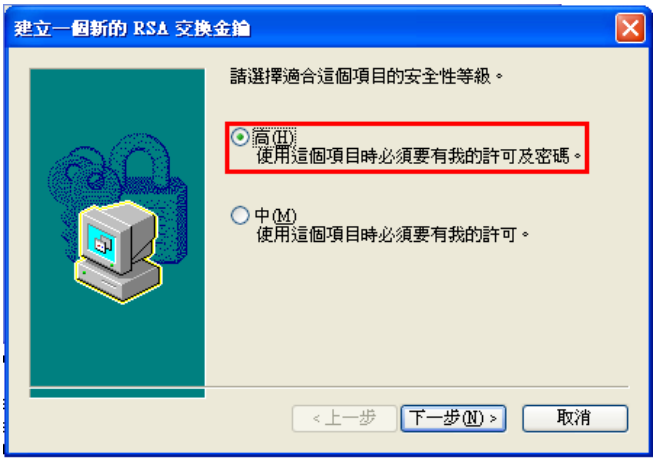
Step 1	開啟瀏覽器，連結至 http://www.verisign.com/官方網站，在”Product&Service”下方找到”Digital IDs for Secure Email”並點選進入。

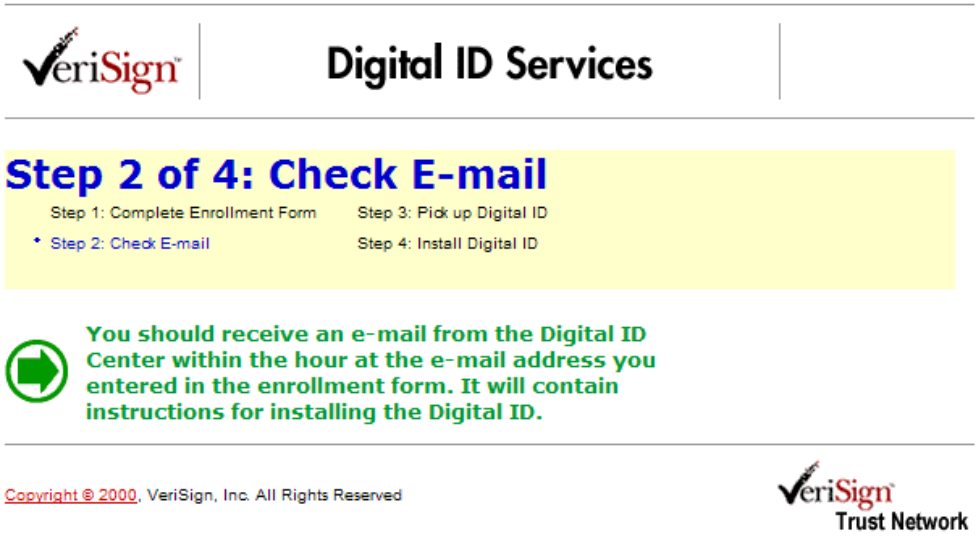


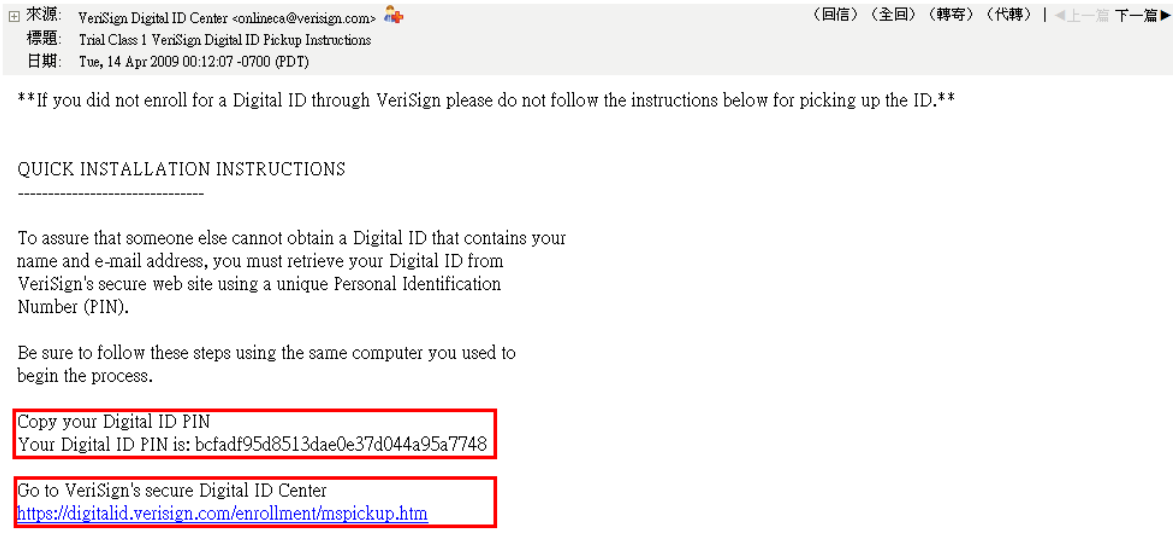
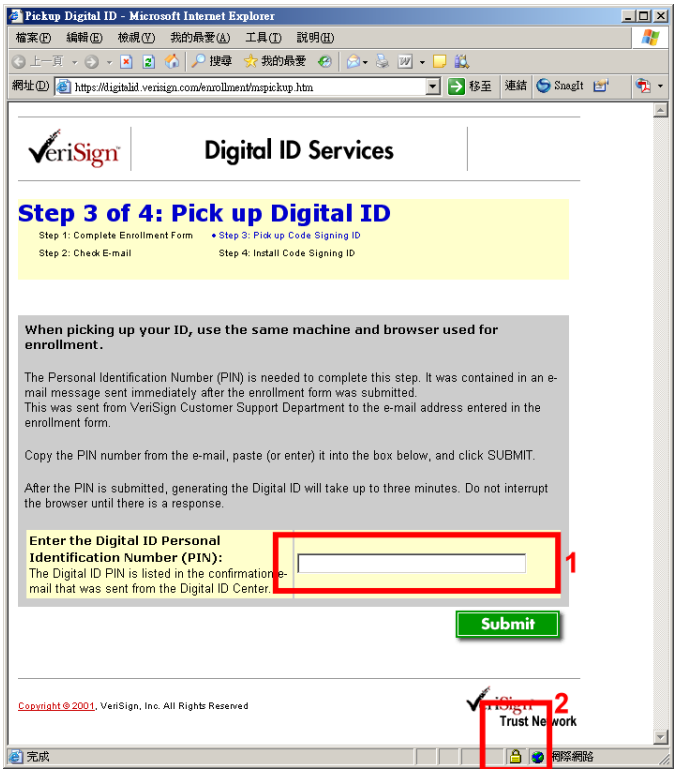
Step 2	點選 Buy Now 圖示，進入憑證申請選單 
Step 3	選擇所使用之瀏覽器種類，以便未來安裝憑證辨別使用。 

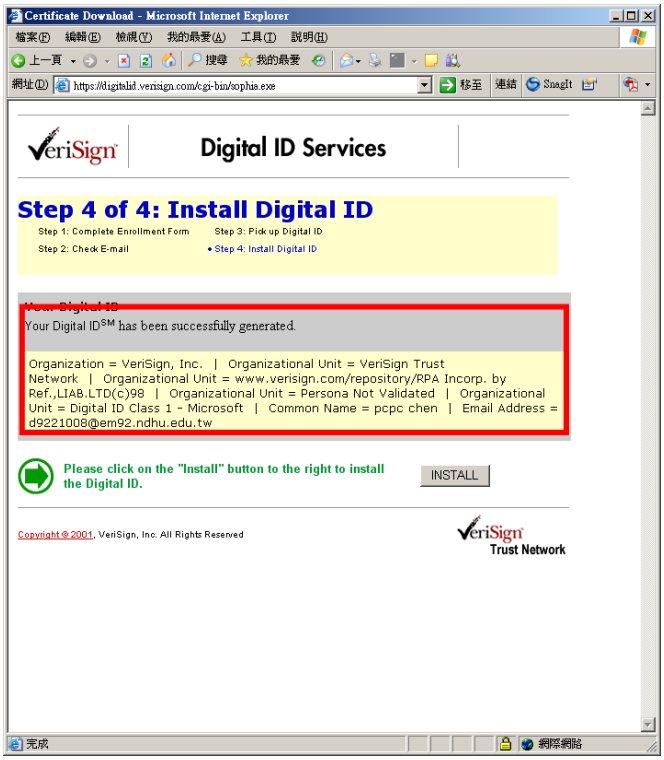
Step 4	1. 2. 填入姓名 3. 填入 **正確** E-amil 用以接收確認信 4. 填入未來查詢、更新、廢除憑證時用之 安全密碼 
Step 5	1. 同一頁面往下拉，選擇試用 60 天 2. 若選擇正式購買，則需填寫此處付款訊息 

Step 6	1. 同一頁面往下拉，選取加密器使用，使用智慧 IC 卡時可選取 Schlumberger 2. 勾選加強私密金鑰保護，設定私密金鑰需通行片語保護 3. 點選完後選取 ACCEPT 完成資料填寫 
Step 7	此時跳出 E-mail 確認訊息，請再次檢查 E-mail 是否正確，若無誤請點選 確定。 

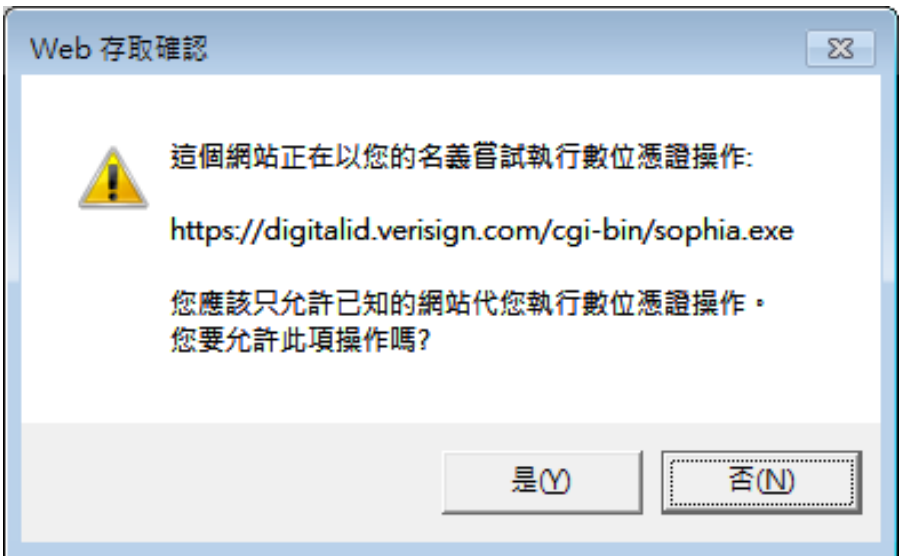
Step 8	憑證要求訊息，若無誤請點選 是。 
Step 9	點選設定私密金鑰使用時之安全等級：可設定 高、中、低 安全等級 高安全等級：使用私密金鑰時 **必須** 配合通行片語。 中安全等級：使用私密金鑰時 **不須** 配合通行片語，僅通知使用者。 低安全等級：若未勾選 Step 6 中之第二項，則使用私密金鑰時 **不須** 配合通行片語， 也 **不須** 通知使用者，並逕行採用私密金鑰。(不建議)  

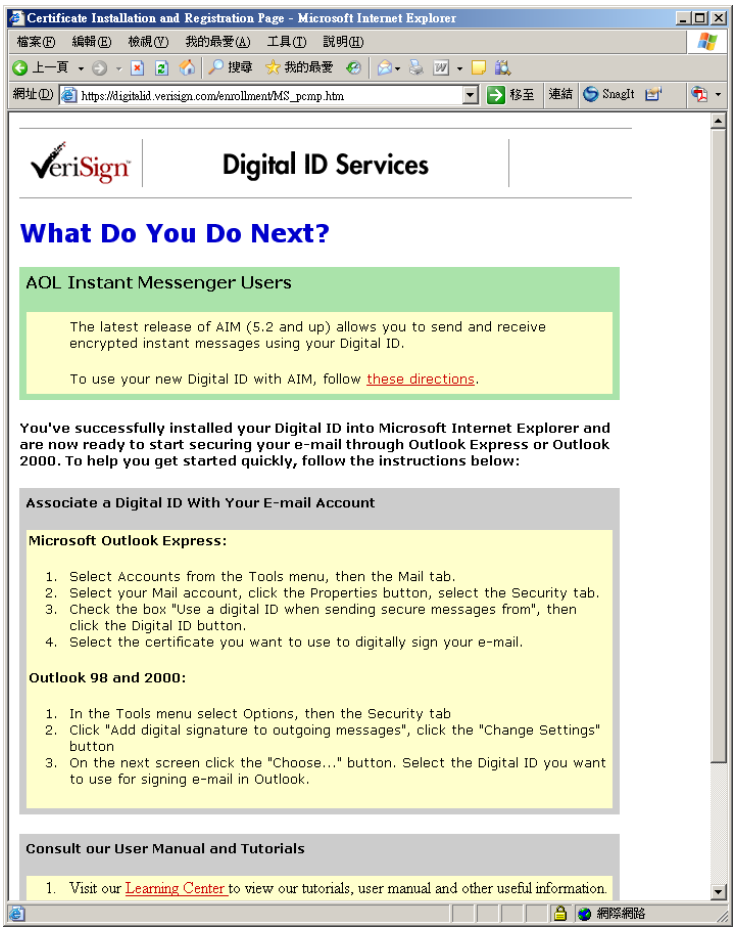
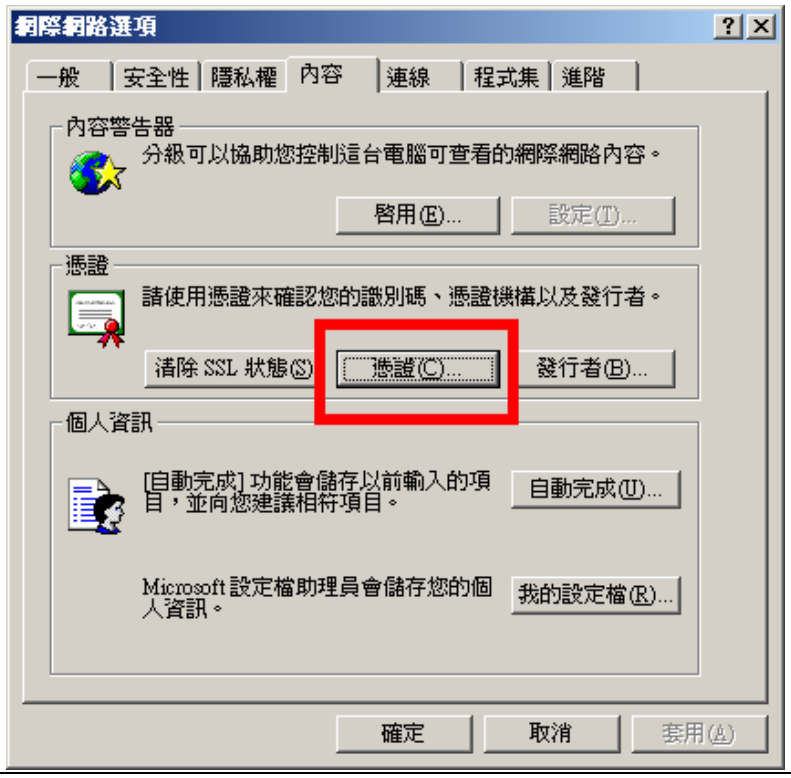
Step 10	建立私密金鑰採用時，所需要之通行片語，設定後請點選 完成。  
Step 11	請接收 E-mail 信箱，檢查是否有 CA 寄出之認證信件。 

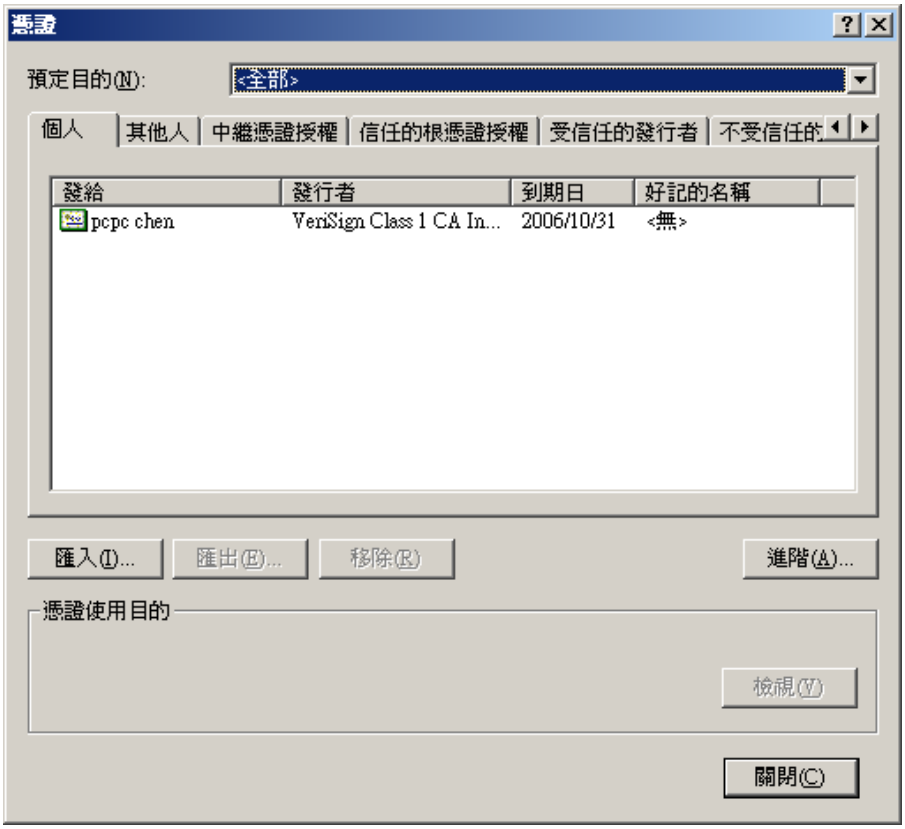
Step 12	接收 CA 寄到之認證信件，打開後應有內容： 1. 取得數位憑證之對應 PIN 碼。 2. 取得數位憑證之連結網址。 此時需點選連結網址，連結至數位憑證取得網頁。  來源: VeriSign Digital ID Center <onlineca@verisign.com> 標題: Trial Class 1 VeriSign Digital ID Pickup Instructions 日期: Tue, 14 Apr 2009 00:12:07 -0700 (PDT) 〈回信〉〈全回〉〈轉寄〉〈代轉〉 | 上一篇 下一篇 **If you did not enroll for a Digital ID through VeriSign please do not follow the instructions below for picking up the ID.** QUICK INSTALLATION INSTRUCTIONS To assure that someone else cannot obtain a Digital ID that contains your name and e-mail address, you must retrieve your Digital ID from VeriSign's secure web site using a unique Personal Identification Number (PIN). Be sure to follow these steps using the same computer you used to begin the process. Copy your Digital ID PIN Your Digital ID PIN is: bcfadf95d8513dae0e37d044a95a7748 Go to VeriSign's secure Digital ID Center https://digitalid.verisign.com/enrollment/mspickup.htm
Step 13	1. 在數位憑證取得網頁中，填入 PIN 碼。 2. 可雙擊確認連結網頁確實為 CA 所簽署過之安全網頁。  Pickup Digital ID - Microsoft Internet Explorer VeriSign Digital ID Services Step 3 of 4: Pick up Digital ID Step 1: Complete Enrollment Form • Step 3: Pick up Code Signing ID Step 2: Check E-mail Step 4: Install Code Signing ID When picking up your ID, use the same machine and browser used for enrollment. The Personal Identification Number (PIN) is needed to complete this step. It was contained in an e-mail message sent immediately after the enrollment form was submitted. This was sent from VeriSign Customer Support Department to the e-mail address entered in the enrollment form. Copy the PIN number from the e-mail, paste (or enter) it into the box below, and click SUBMIT. After the PIN is submitted, generating the Digital ID will take up to three minutes. Do not interrupt the browser until there is a response. Enter the Digital ID Personal Identification Number (PIN): The Digital ID PIN is listed in the confirmation e-mail that was sent from the Digital ID Center. 1 Submit Copyright © 2001, VeriSign, Inc. All Rights Reserved 2  憑證 一般 | 詳細資料 | 憑證路徑 憑證資訊 這個憑證的使用目的如下: • 確保遠端電腦的識別 *請參照憑證授權敘述中的詳細資訊。 發給: www.verisign.com 發行者: www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign 有效期自 2005/6/1 到 2007/6/2 安裝憑證(I)... 發行者聲明(S) 確定

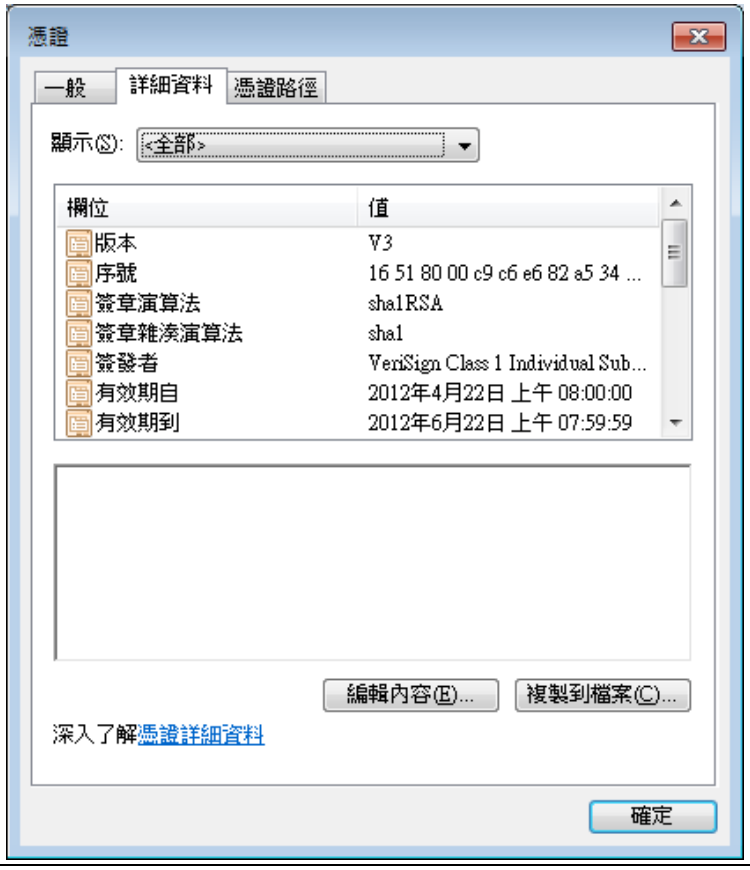
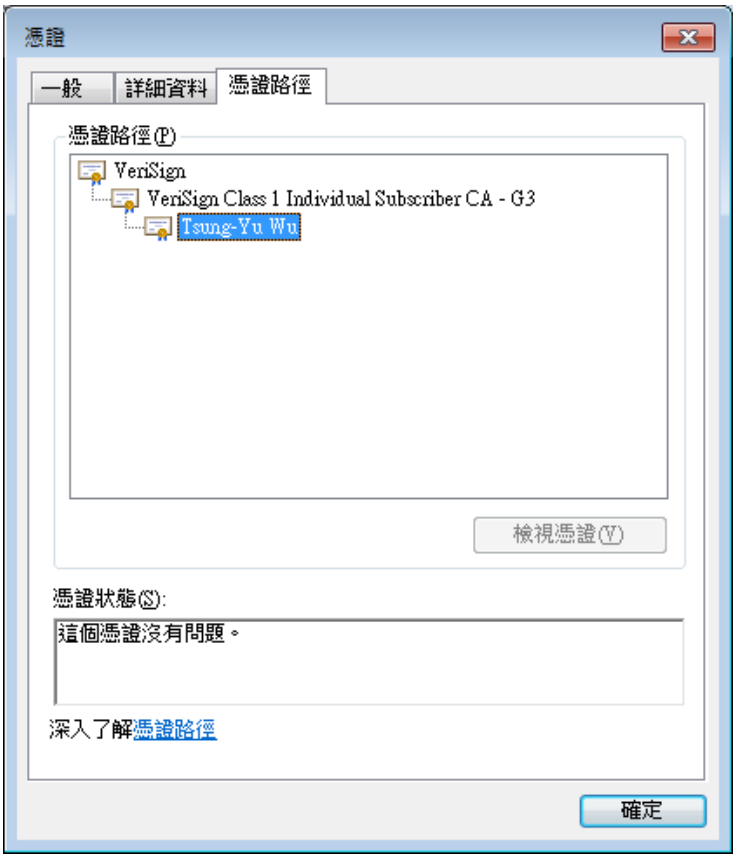
Step 14	確認憑證內容是否無誤，即可點取 INSTALL 按鈕安裝憑證。 

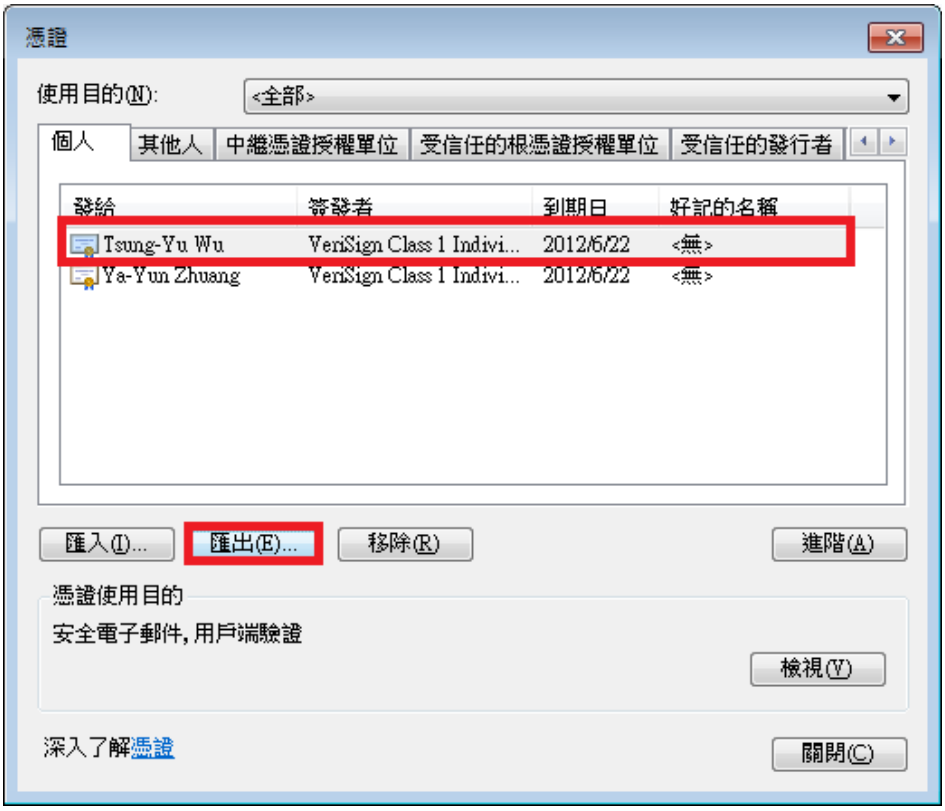
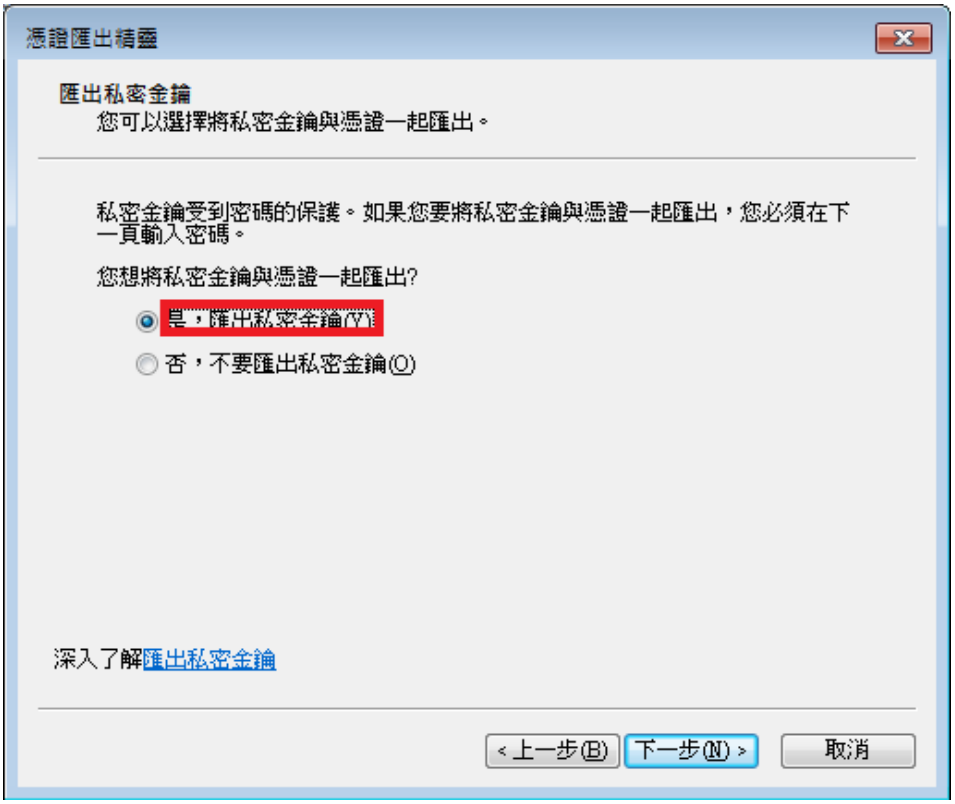
2. Certificate 安裝

Step 1	點選 INSTALL 後，WINDOWS 將會跳出憑證安裝訊息，請點 是 安裝。 

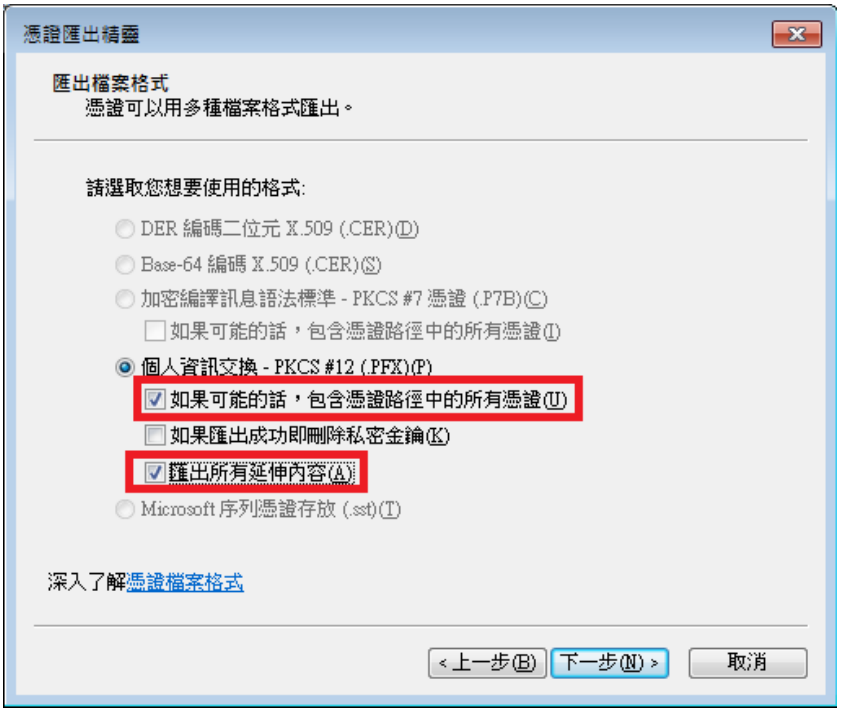
Step 2	安裝完成後將會出現此憑證與各種相對應軟體之安裝方式。 
Step 3	請於 IE 瀏覽器中點選，工具->網際網路選項->內容，並點取 憑證 按鈕。 

Step 4	安裝成功後，可檢視到憑證狀況。 
Step 5	憑證內容可雙擊點開後檢視，下方為憑證之一般內容。 

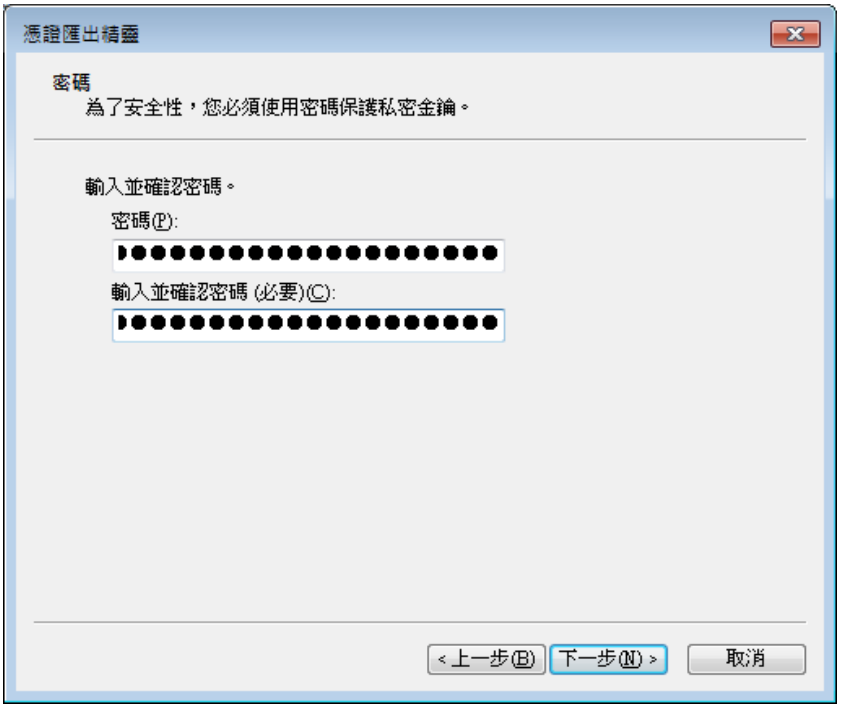
Step 6	檢視憑證詳細資料，憑證細項內容如：版本、簽章演算法、有效日期等。 
Step 7	檢視憑證信任路徑 

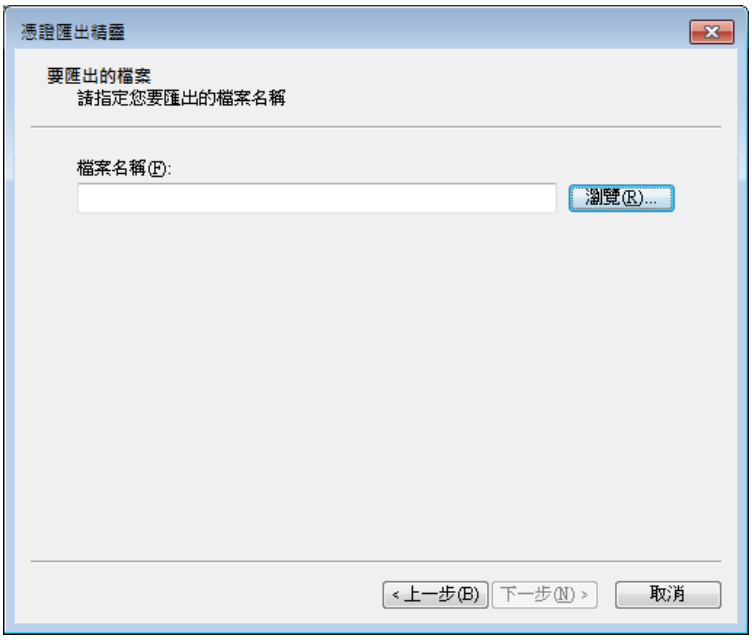
Step 8	Step 1 的憑證安裝只可一次性的安裝在一台電腦上，如果想要在其他電腦上使用申請的憑證，必須要在安裝憑證的電腦上匯出 *.PFX 檔案，然後在欲安裝的電腦上匯入 *.PFX 檔案。  匯出步驟如下。按下匯出後，請選擇”是，匯出私密金鑰”，然後按下”下一步”。 

接著將”如果可能的話，包含憑證路徑中的所有憑證”和”匯出所有延伸內容”的選項勾選，並按下”下一步”。



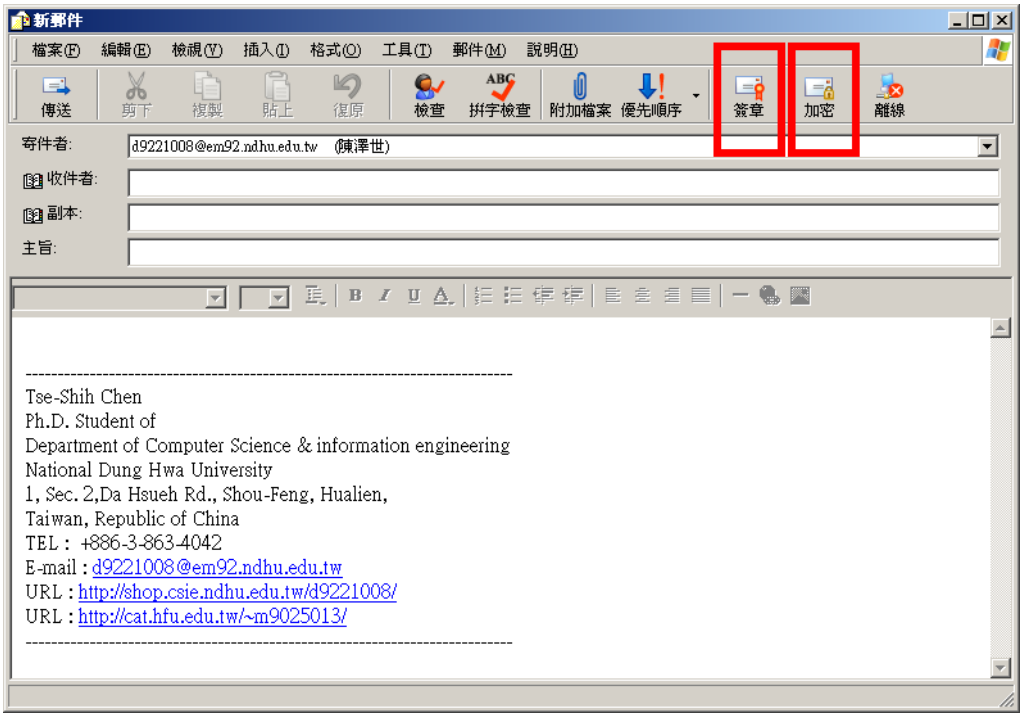
建立私密金鑰採用時，所需要之通行片語

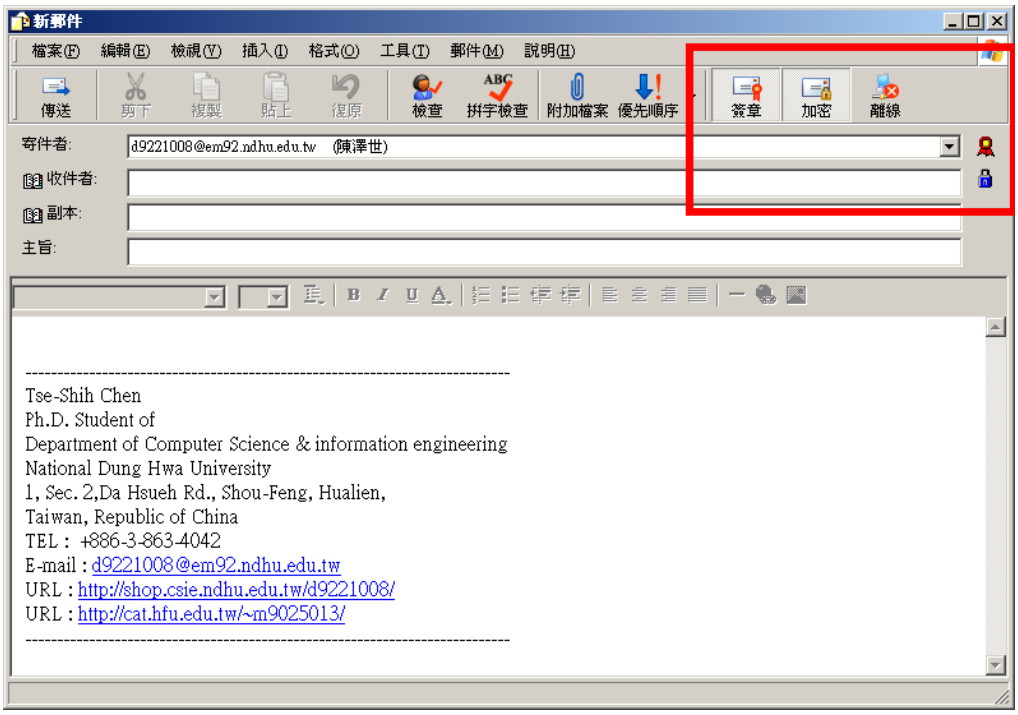
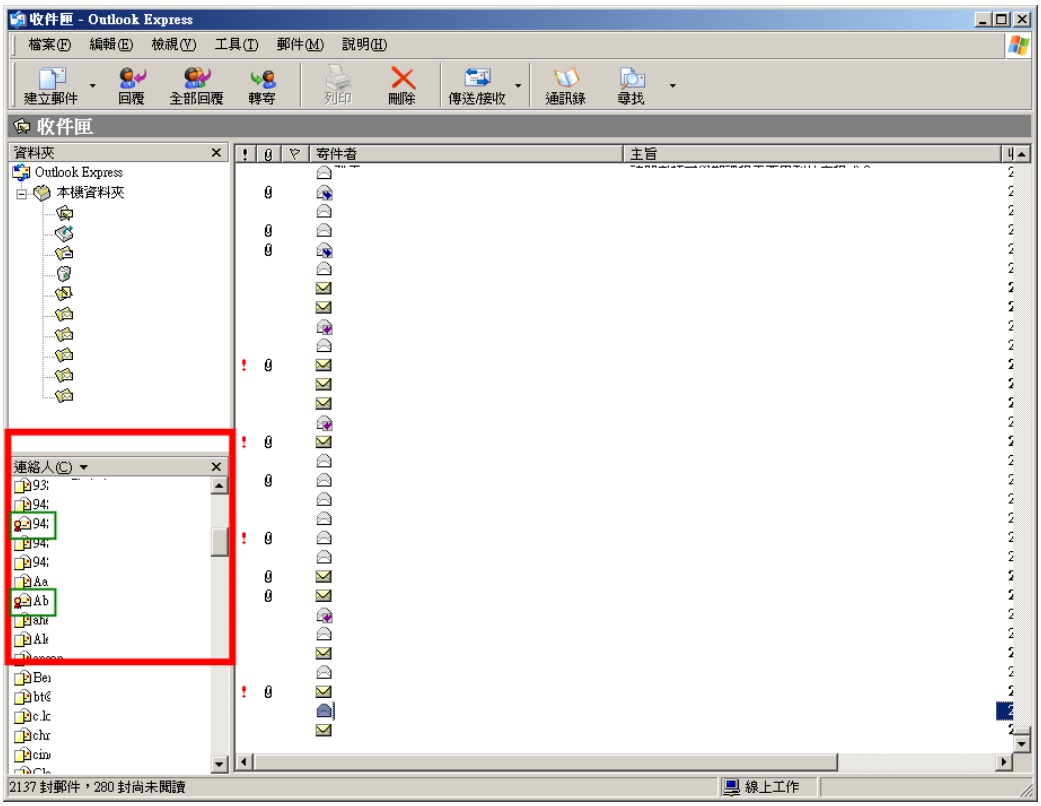


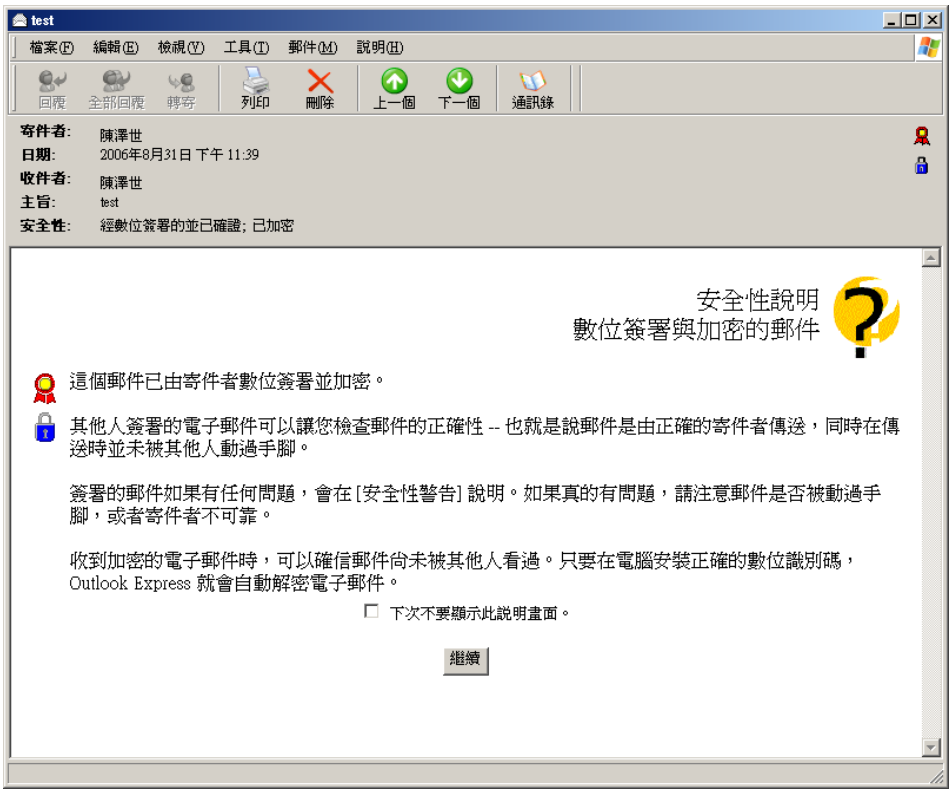
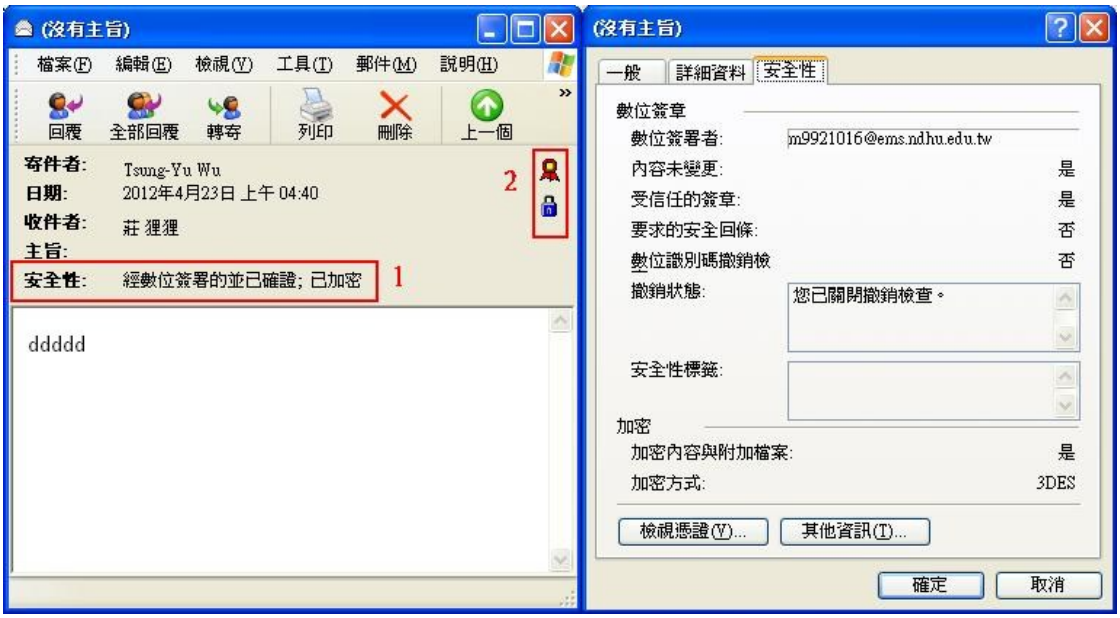
	輸入檔案名稱與選定路徑後匯出。 

3. Secure MIME

此部分需使用 Outlook Express 收信軟體配合操作，請先設定相關設置(請參照附錄一)。

Step 1	安裝完成數位憑證後，可於編輯 E-mail 時點選 簽章、加密 選項 

Step 2	點選簽章、加密選項後，右方會出現相對應圖示。 
Step 3	聯絡人中若有採用數位憑證，則所顯示之圖示會與一般不同。若要寄出 **加密** 信件則 **必須** 要有對方之數位憑證。 

Step 4	收到友人寄來之數位簽章與加密信件時，Outlook Express 會告知收信方。 
Step 5	開啟信件後，可檢視： 1. 安全性描述 2. 安全性圖示 即可得知此信件之加密與簽章之設置。 

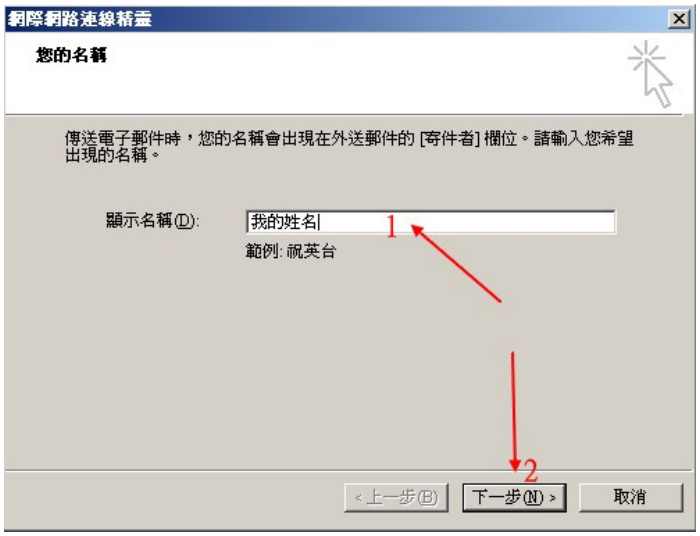
問題與練習：

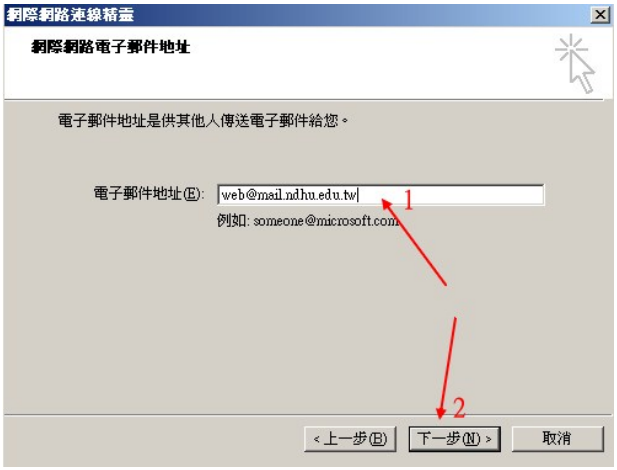
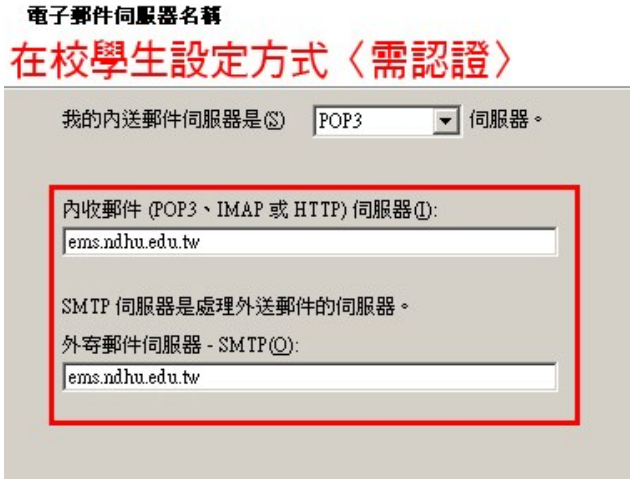
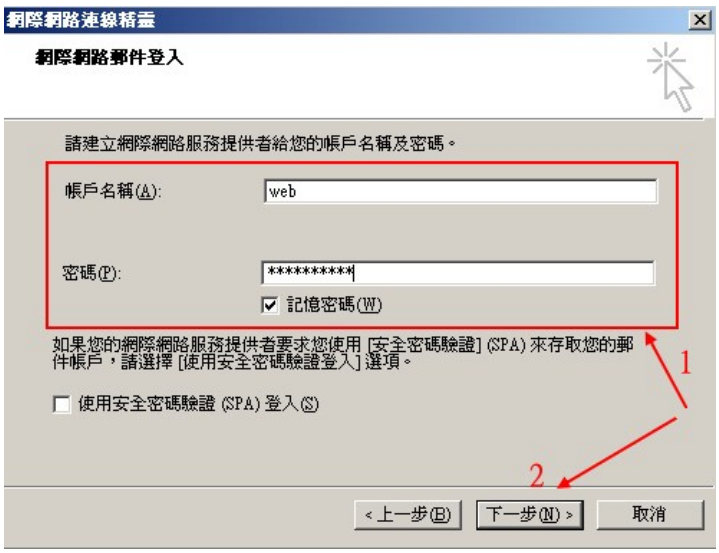
1. 寄送加密信件時，為何需要擁有對方之數位憑證？
2. 寄送簽章信件時，所使用的金鑰為己方之私密金鑰或是公開金鑰？
3. 數位憑證是否為一加密文件？
4. 請實習，與友人互相寄送 **加密** 信件。
5. 請實習，與友人互相寄送 **簽章** 信件。
6. 請實習，與友人互相寄送 **簽章並加密** 信件。

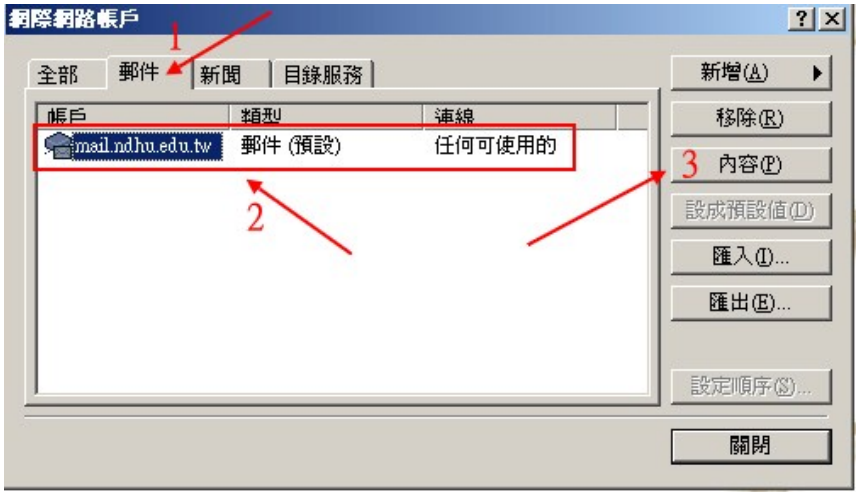
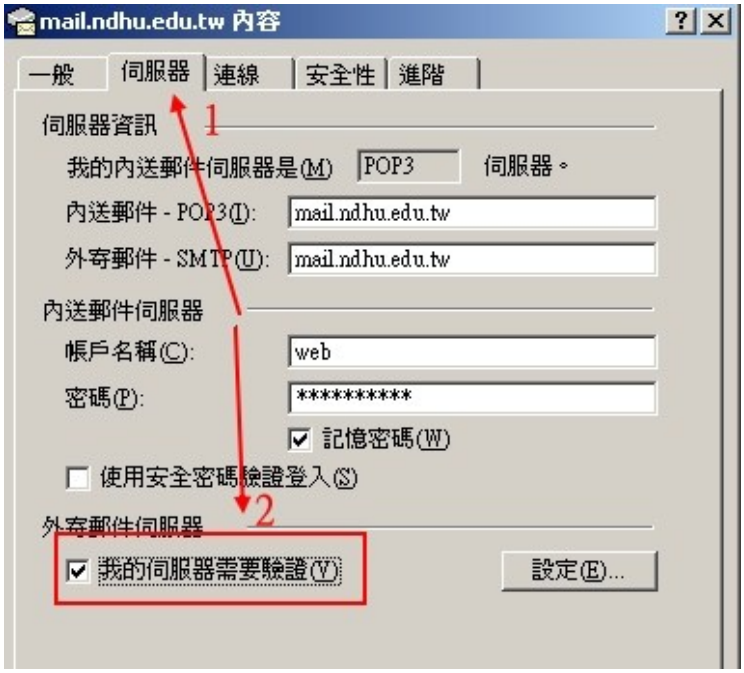
總結測驗：

1. 請分組寄送簽章信件給助教
   組別 1： m9921016@ems.ndhu.edu.tw
   組別 2： m9921042@ems.ndhu.edu.tw
2. 助教會在回信內容中提出一則問題，請接收郵件取得助教憑證，解密後回答助教問題，並寄送加密與簽章文件回答問題給助教。

附錄一 – Outlook Express 設定

Step 1	開啟 Outlook Express 軟體，選取工具列中[工具/帳戶]。 
Step 2	在[網際網路帳戶]視窗中，點選[新增/郵件]。 
Step 3	在[網際網路連線精靈]視窗中，在[顯示名稱]中輸入自己的姓名，並點選[下一步]。 

Step 4	在[網際網路連線精靈]視窗中，在[電子郵件地址]中輸入自己的 e-mail 位置，並點選[下一步]。 
Step 5	在[內收郵件伺服器]中輸入：ems.ndhu.edu.tw； [外寄郵件伺服器]中輸入：ems.ndhu.edu.tw； 
Step 6	在[網際網路連線精靈]視窗中，輸入[帳號名稱]與[密碼]，並點選[下一步]，即完成新增郵件設定，並關閉[網際網路帳戶]視窗。※若您使用的是公用電腦，建議不要勾選[記憶密碼]。 

Step 7	點選工具列上之[工具/帳戶]，在[網際網路帳戶]視窗中點選[郵件]並選取新增之郵件項目，最後點選[內容]。  
Step 8	在[mail.ndhu.edu.tw 內容]視窗中，點選[伺服器]並將[我的伺服器需要驗證]勾選起來。 

Step 9	設定完成之後，點選[傳送/接收]即可直接下載網路上之信件，日後即可正常收發電子郵件。