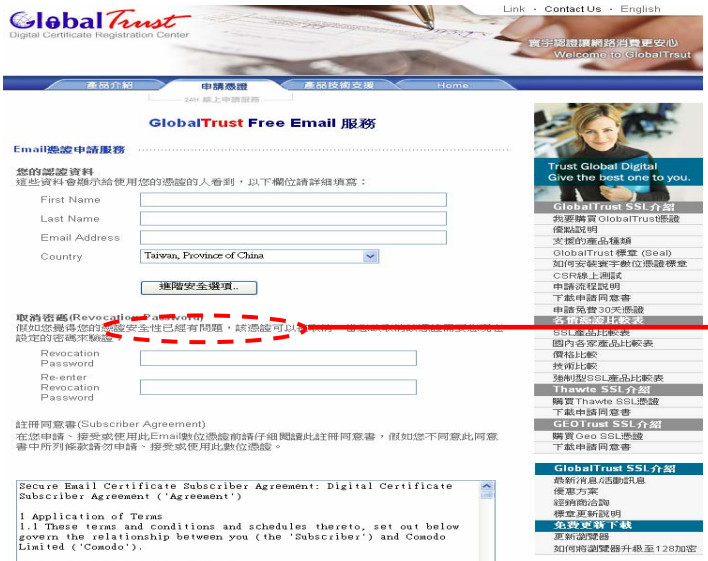
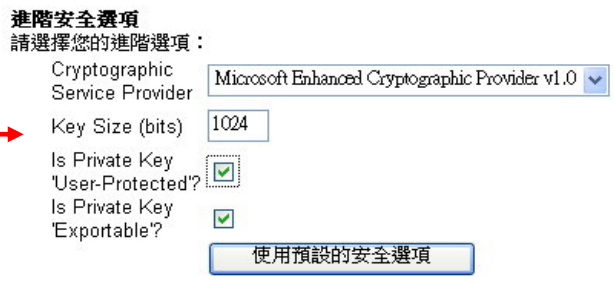
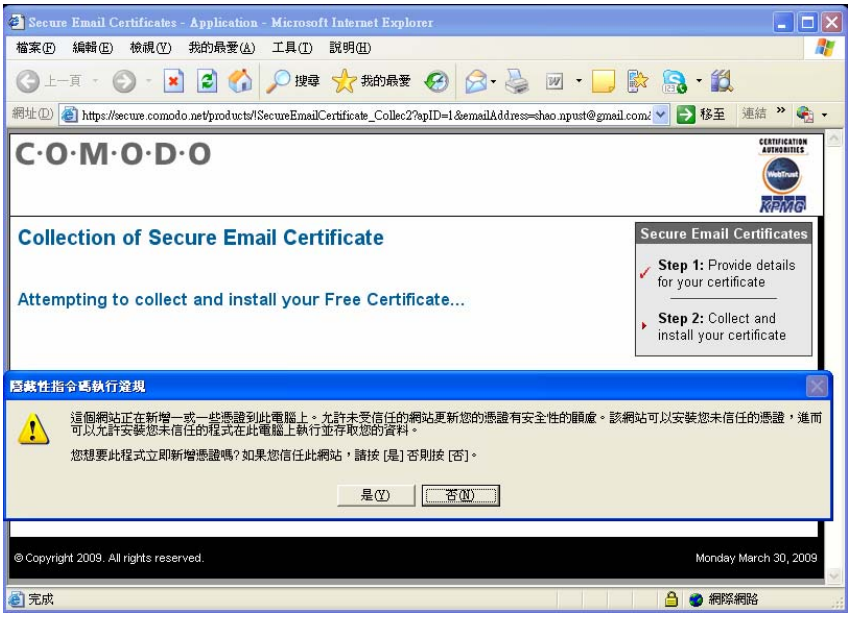
■ 申請個人數位憑證

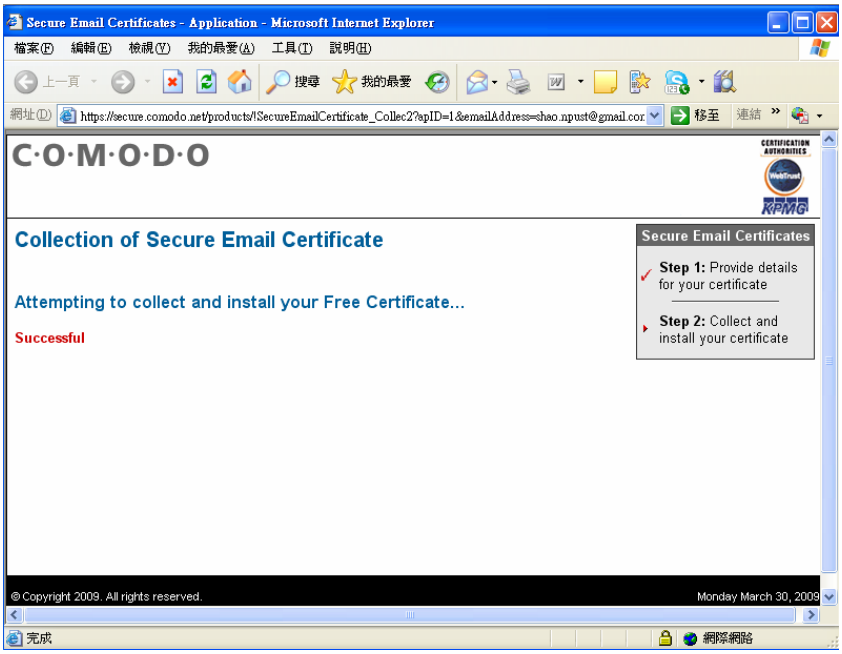
➢ 以「Global Trust」為電子郵件用之數位安全憑證服務為例 (http://www.globaltrust.com.tw/)





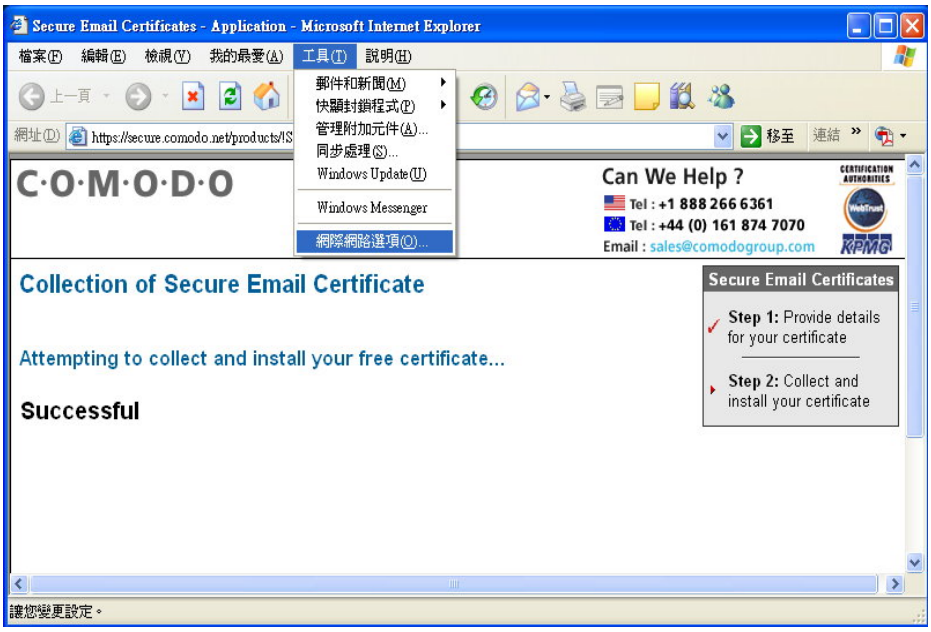

收件匣 - Outlook Express
C·O·M·O·D·O
Your Comodo FREE
Personal Email Certificate
is now ready for collection!
Dear MH SHAO,
Congratulations - your Comodo FREE Personal Secure Email Certificate is now ready for collection! You are almost able to send secure email!
Simply click on the button below to collect your certificate.
Click & Install Comodo Email Certificate
How to encrypt mail
Step 1
Step 2

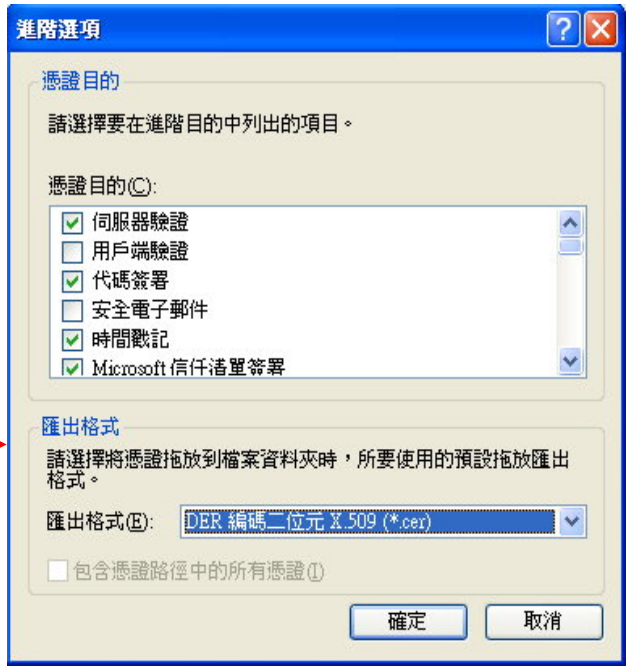

Secure Email Certificates - Application - Microsoft Internet Explorer
C·O·M·O·D·O
Collection of Secure Email Certificate
Attempting to collect and install your Free Certificate...
Secure Email Certificates
Step 1: Provide details for your certificate
Step 2: Collect and install your certificate
隱藏性指令碼執行違規
是(Y)
否(N)
© Copyright 2009. All rights reserved.
Monday March 30, 2009


Secure Email Certificates - Application - Microsoft Internet Explorer
C·O·M·O·D·O
Collection of Secure Email Certificate
Attempting to collect and install your Free Certificate...
Successful
Secure Email Certificates
Step 1: Provide details for your certificate
Step 2: Collect and install your certificate
© Copyright 2009. All rights reserved.
Monday March 30, 2009

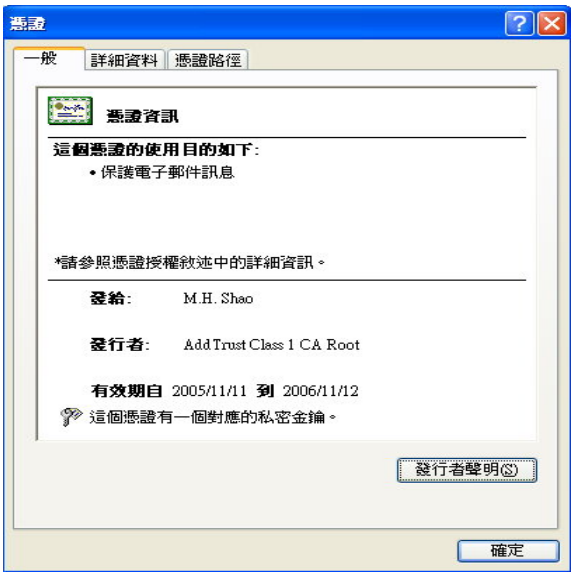
■ 備份數位憑證

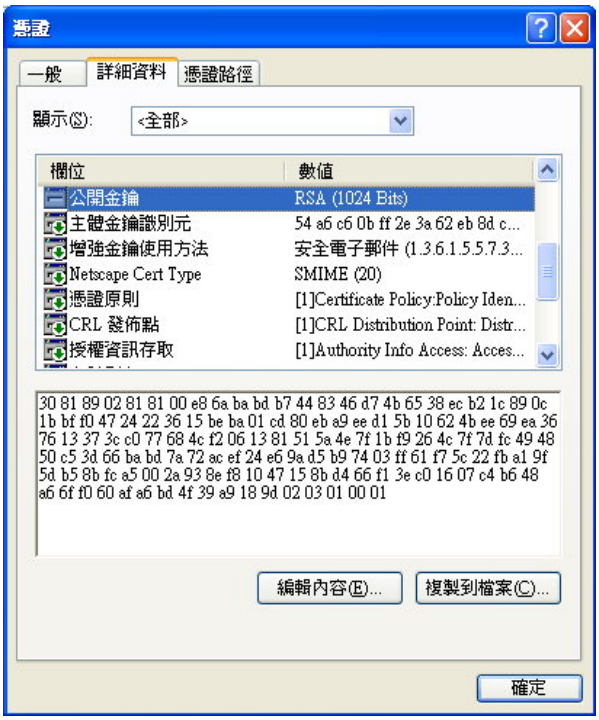
➢ Internet Explore：功能表【工具】→「網際網路選項」→「內容」標籤

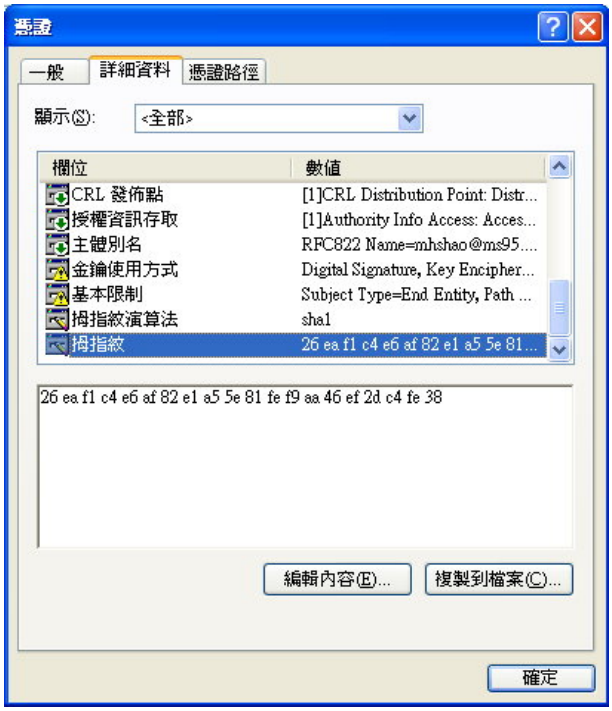


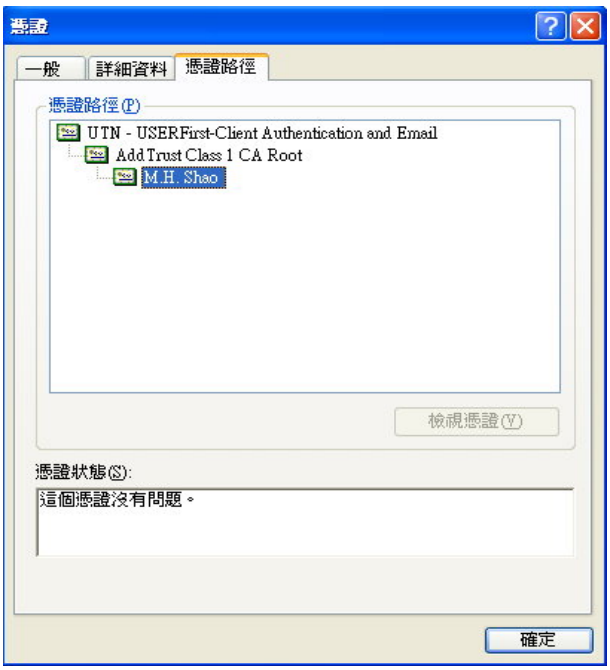


- 檢視

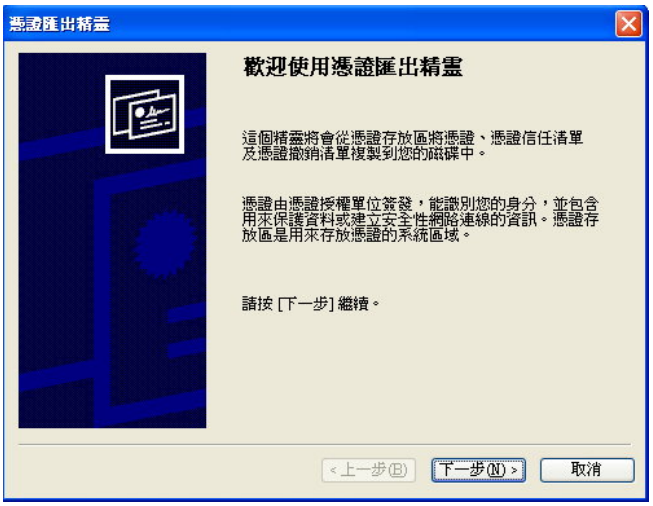

憑證
一般
詳細資料
憑證路徑
憑證資訊
這個憑證的使用目的如下:
• 保護電子郵件訊息
*請參照憑證授權敘述中的詳細資訊。
發給: M.H. Shao
發行者: AddTrust Class 1 CA Root
有效期自 2005/11/11 到 2006/11/12
這個憑證有一個對應的私密金鑰。
發行者聲明(S)
確定

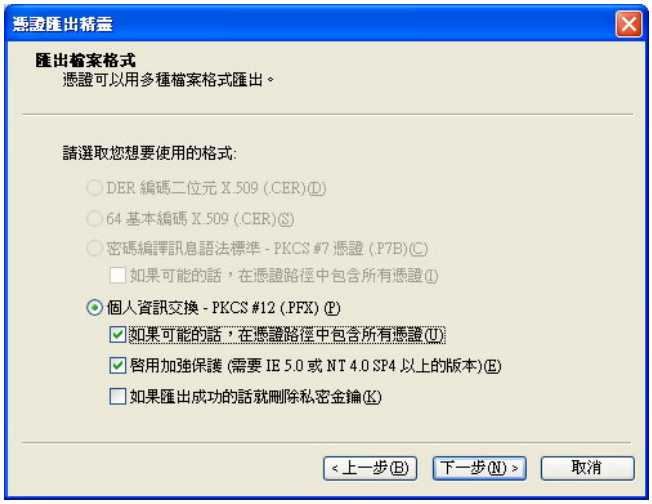

憑證
一般
詳細資料
憑證路徑
顯示(S): <全部>
欄位
數值
公開金鑰 RSA (1024 Bits)
主體金鑰識別元 54 a6 c6 0b ff 2e 3a 62 eb 8d c...
增強金鑰使用方法 安全電子郵件 (1.3.6.1.5.5.7.3...
Netscape Cert Type SMIME (20)
憑證原則 [1]Certificate Policy:Policy Iden...
CRL 發佈點 [1]CRL Distribution Point: Distr...
授權資訊存取 [1]Authority Info Access: Acces...
30 81 89 02 81 81 00 e8 6a ba bd b7 44 83 46 d7 4b 65 38 ec b2 1c 89 0c
1b bf f0 47 24 22 36 15 be ba 01 cd 80 eb a9 ee d1 5b 10 62 4b ee 69 ea 36
76 13 37 3c c0 77 68 4c f2 06 13 81 51 5a 4e 7f 1b f9 26 4c 7f 7d fc 49 48
50 c5 3d 66 ba bd 7a 72 ac ef 24 e6 9a d5 b9 74 03 ff 61 f7 5c 22 fb a1 9f
5d b5 8b fc a5 00 2a 93 8e f8 10 47 15 8b d4 66 f1 3e c0 16 07 c4 b6 48
a6 6f f0 60 af a6 bd 4f 39 a9 18 9d 02 03 01 00 01
編輯內容(E)...
複製到檔案(C)...
確定

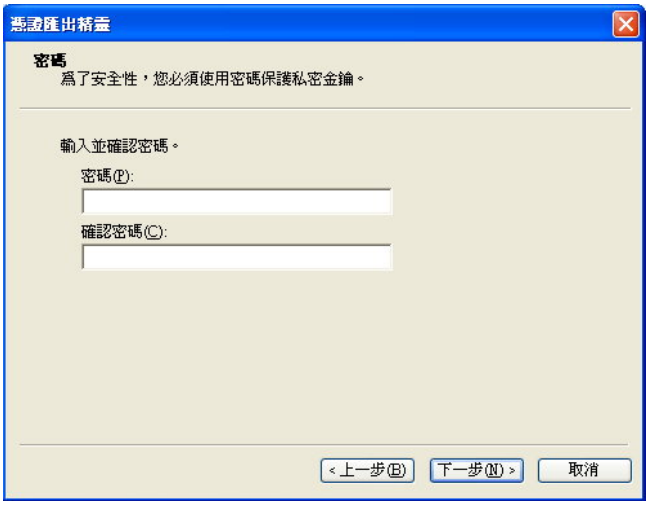

憑證
一般
詳細資料
憑證路徑
顯示(S): <全部>
欄位
數值
CRL 發佈點 [1]CRL Distribution Point: Distr...
授權資訊存取 [1]Authority Info Access: Acces...
主體別名 RFC822 Name=mhshao@ms95....
金鑰使用方式 Digital Signature, Key Encipher...
基本限制 Subject Type=End Entity, Path ...
拇指紋演算法 sha1
拇指紋 26 ea f1 c4 e6 af 82 e1 a5 5e 81...
26 ea f1 c4 e6 af 82 e1 a5 5e 81 fe f9 aa 46 ef 2d c4 fe 38
編輯內容(E)...
複製到檔案(C)...
確定

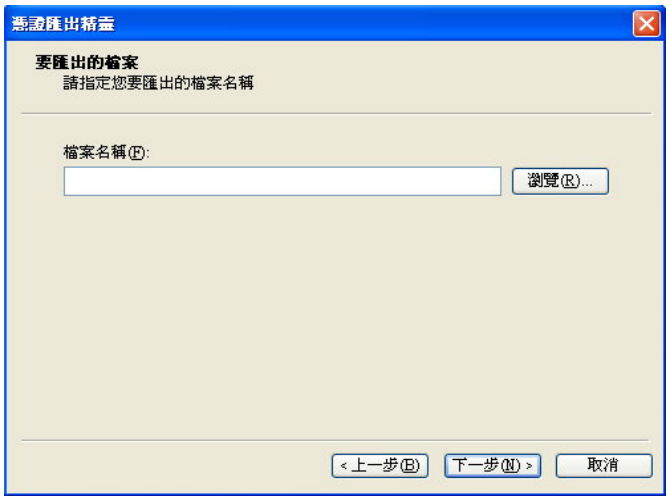

憑證
一般
詳細資料
憑證路徑
憑證路徑(P)
UTN - USERFirst-Client Authentication and Email
AddTrust Class 1 CA Root
M.H. Shao
檢視憑證(V)
憑證狀態(S):
這個憑證沒有問題。
確定

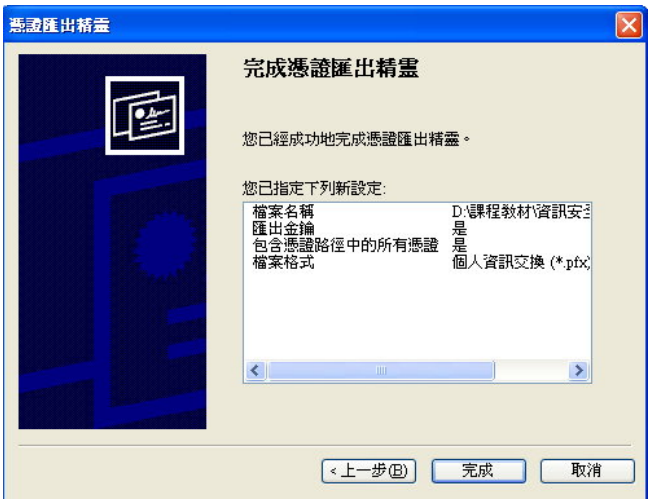
➢ 匯出


憑證匯出精靈
歡迎使用憑證匯出精靈
這個精靈將會從憑證存放區將憑證、憑證信任清單及憑證撤銷清單複製到您的磁碟中。
憑證由憑證授權單位簽發，能識別您的身分，並包含用來保護資料或建立安全性網路連線的資訊。憑證存放區是用來存放憑證的系統區域。
請按 [下一步] 繼續。
< 上一步(B)
下一步(N) >
取消


憑證匯出精靈
匯出檔案格式
憑證可以用多種檔案格式匯出。
請選取您想要使用的格式:
DER 編碼二位元 X.509 (.CER)(D)
64 基本編碼 X.509 (.CER)(S)
密碼編譯訊息語法標準 - PKCS #7 憑證 (.P7B)(C)
如果可能的話，在憑證路徑中包含所有憑證(I)
個人資訊交換 - PKCS #12 (.PFX) (P)
如果可能的話，在憑證路徑中包含所有憑證(U)
啓用加強保護 (需要 IE 5.0 或 NT 4.0 SP4 以上的版本)(E)
如果匯出成功的話就刪除私密金鑰(K)
< 上一步(B)
下一步(N) >
取消

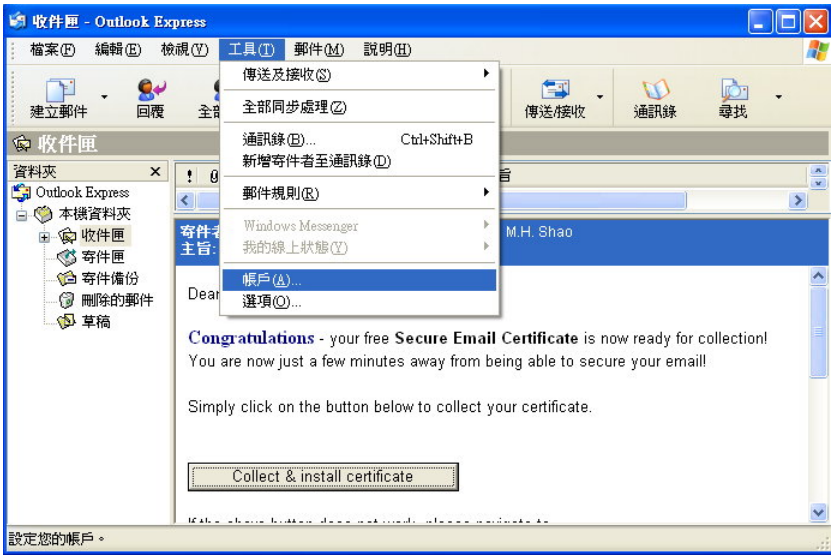

憑證匯出精靈
密碼
爲了安全性，您必須使用密碼保護私密金鑰。
輸入並確認密碼。
密碼(P):
確認密碼(C):
< 上一步(B)
下一步(N) >
取消

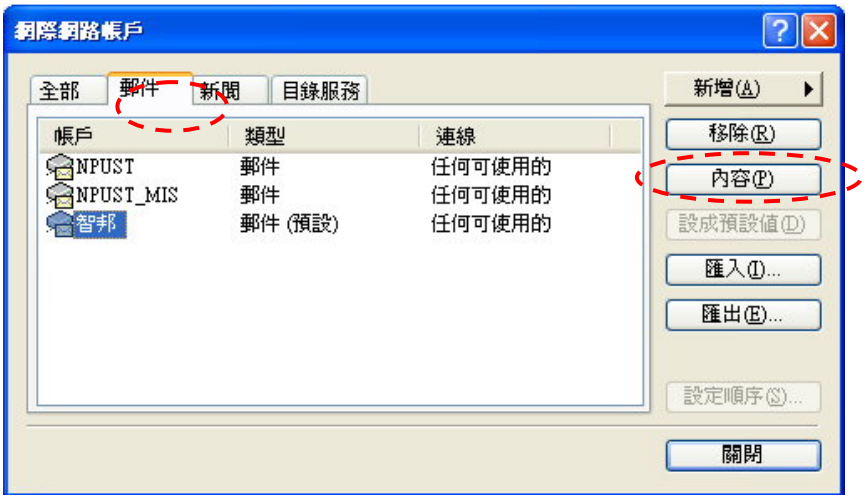

憑證匯出精靈
要匯出的檔案
請指定您要匯出的檔案名稱
檔案名稱(F):
瀏覽(R)...
< 上一步(B)
下一步(N) >
取消

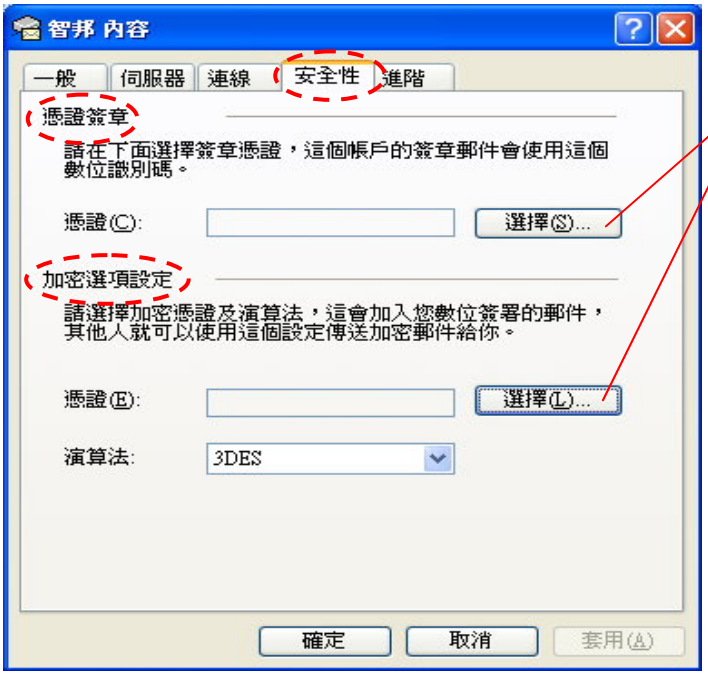

憑證匯出精靈
完成憑證匯出精靈
您已經成功地完成憑證匯出精靈。
您已指定下列新設定:
檔案名稱 D:\課程教材\資訊安全
匯出金鑰 是
包含憑證路徑中的所有憑證 是
檔案格式 個人資訊交換 (*.pfx)
< 上一步(B)
完成
取消

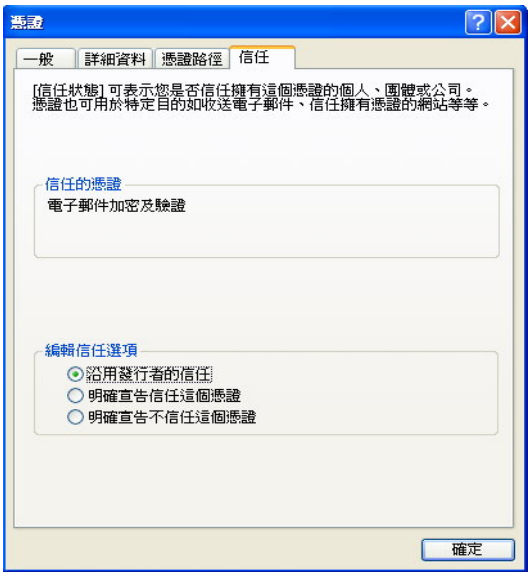
■ 設定「加密用憑證」、「簽章用憑證」

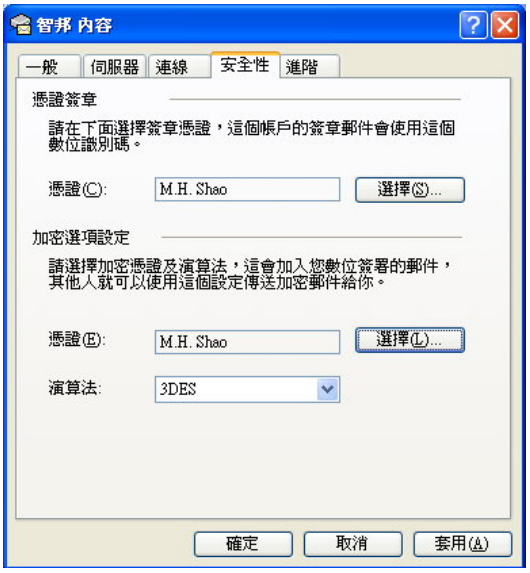
➢ 開啟 Outlook Express →「工具」→「帳戶」









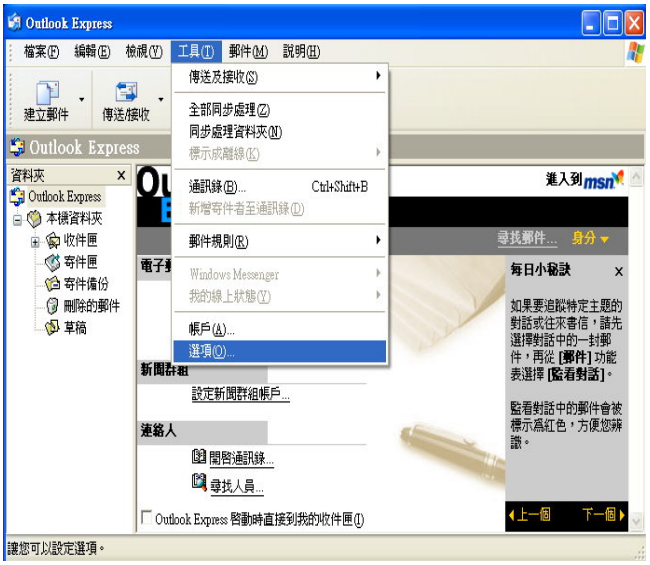


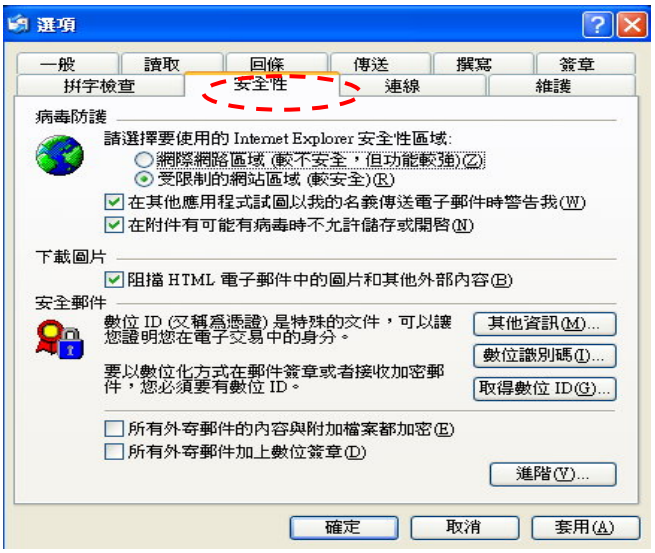
■ 取得他人的數位憑證

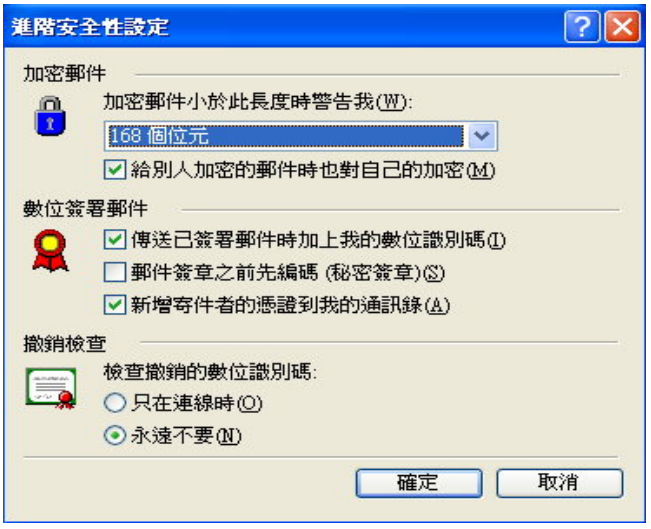
1. 自他人傳送具有數位簽名的電子郵件
2. 搜尋簽證中心網站上的數位憑證資料庫
3. 找尋提供數位憑證等內容的 Internet 目錄服務

1. 自他人傳送具有數位簽名的電子郵件

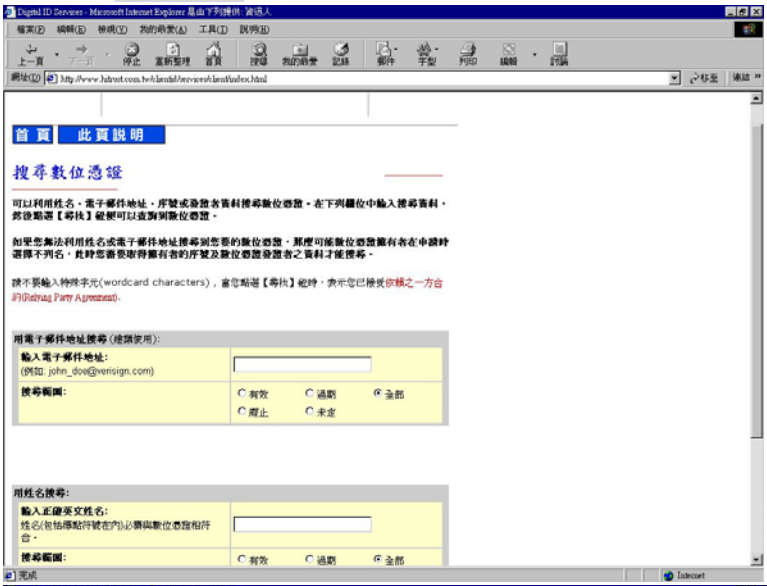
➢ 開啟 Outlook Express →「工具」→「選項」

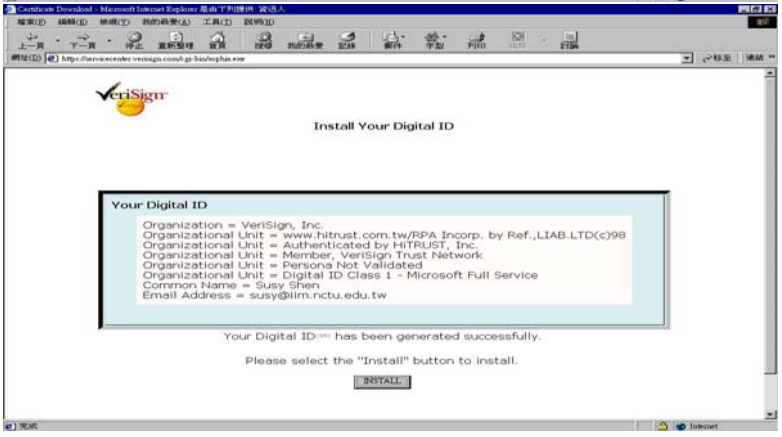




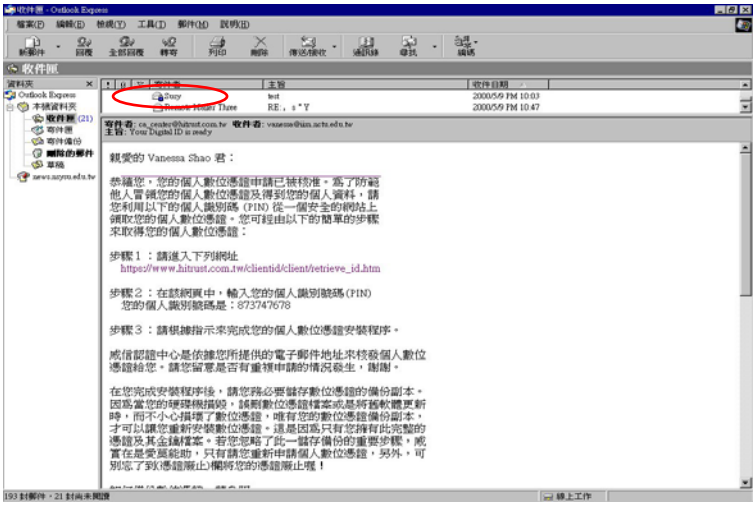


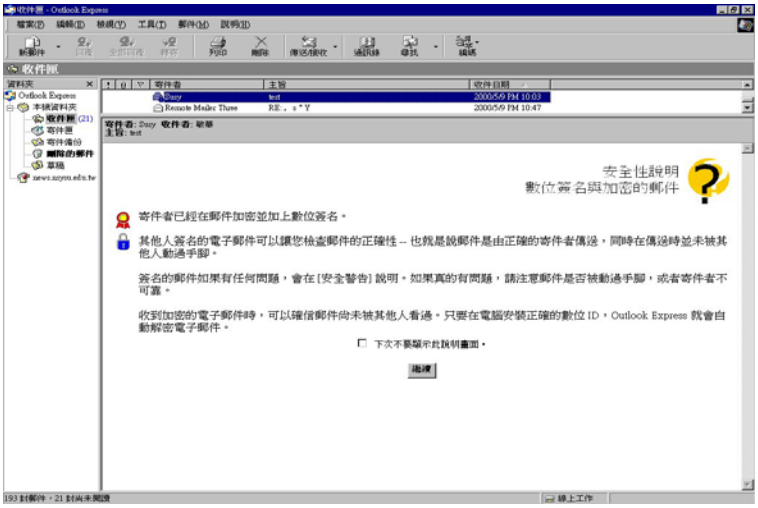
2. 搜尋簽證中心網站上的數位憑證資料庫 (以 VeriSign 為例)

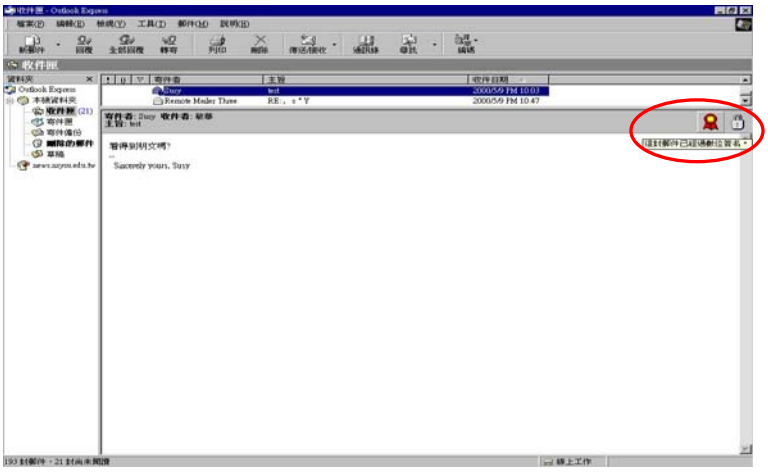


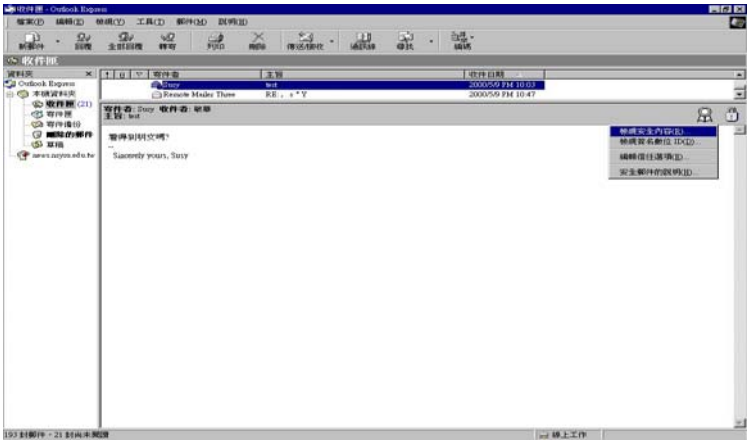


3. 自他人傳送具有數位簽名的電子郵件

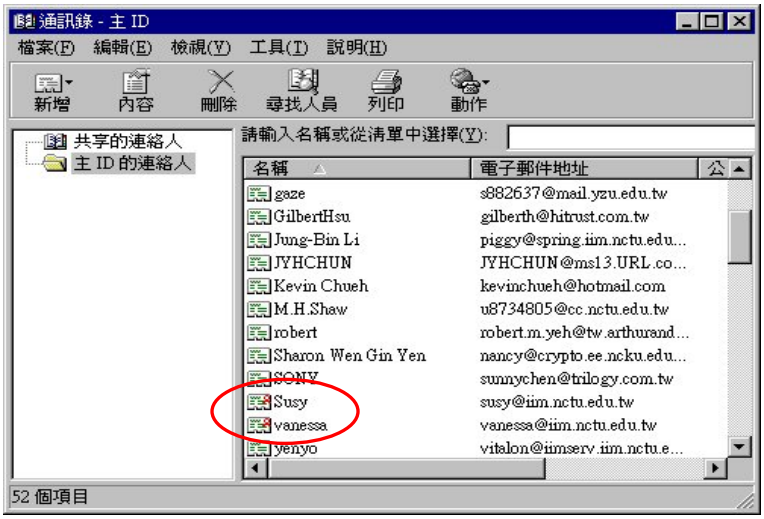




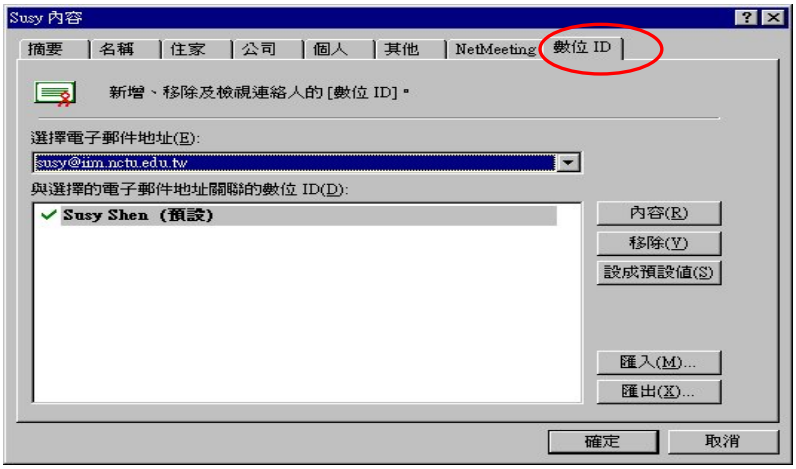




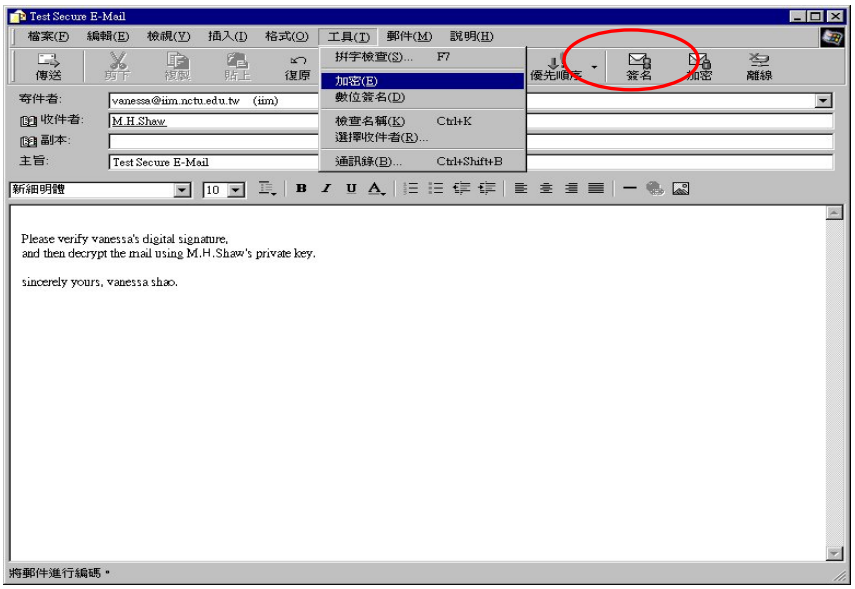
➢ 快捷列「通訊錄」

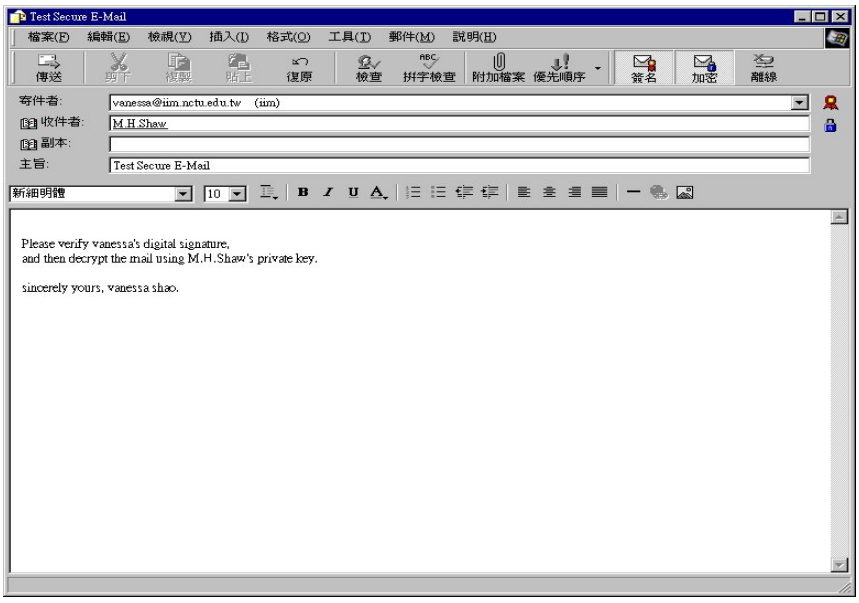


➢ 快捷列「內容」

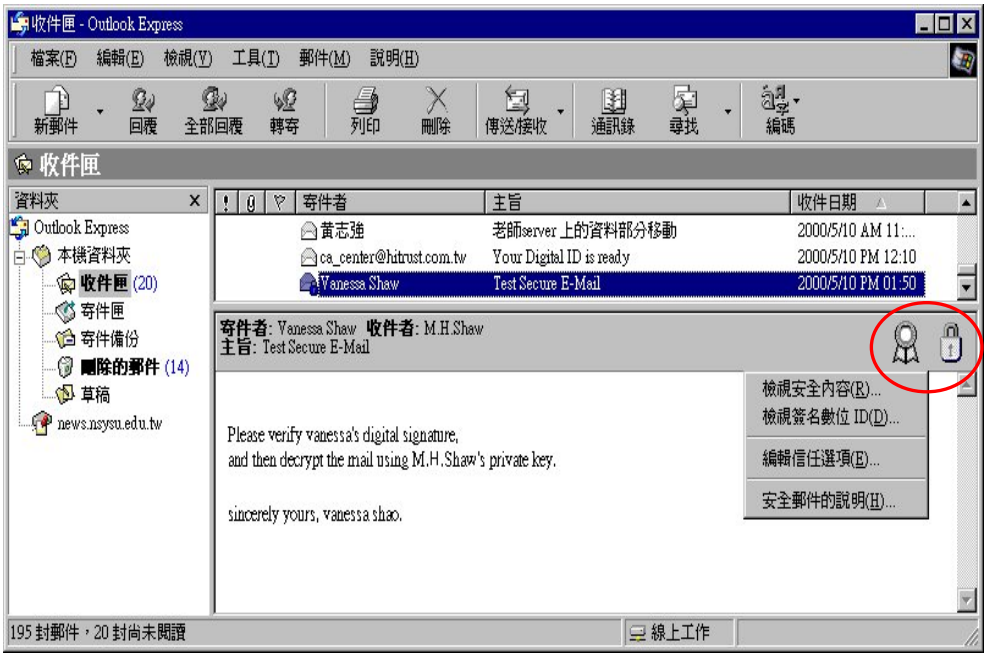


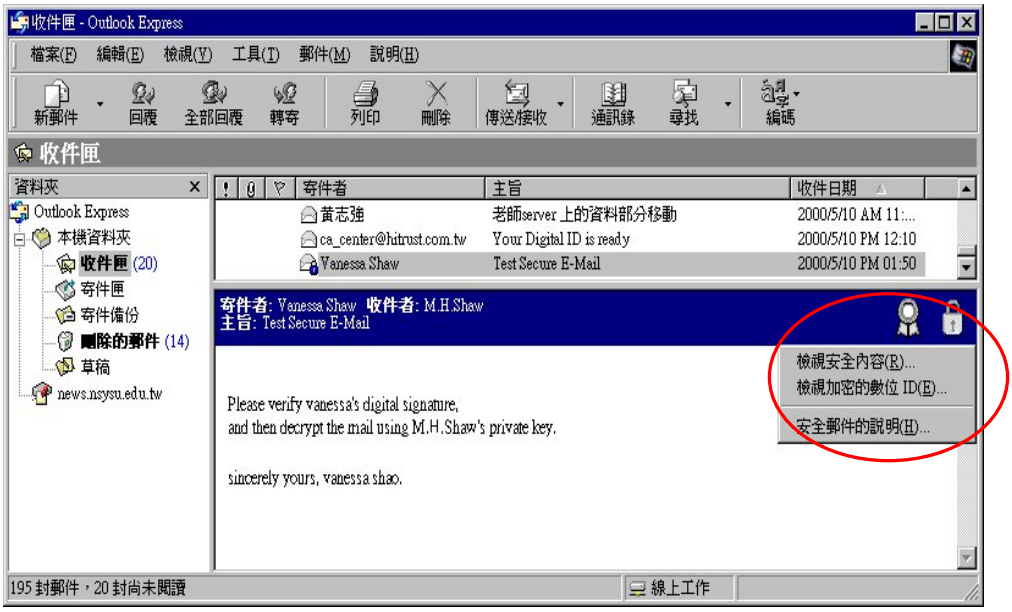
■ 傳送具有數位簽名/加密的郵件





■ 檢驗具有數位簽名的電子郵件/解密






收件匣 - Outlook Express
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
新增(N)
開啓(O) Ctrl+O
另存新檔(A)...
儲存附加檔案(V)...
另存信箱(T)...
資料夾(F)
匯入(I)
匯出(E)
列印(P)... Ctrl+P
切換身份(S)...
身份(D)
內容(R) Alt+Enter
離線工作(W)
結束(X)
轉寄
列印
刪除
傳送/接收
通訊錄
尋找
編碼
寄件者
主旨
收件日期
黃志強
老師server 上的資料部分移動
2000/5/10 AM 11:...
ca_center@hitrust.com.tw
Your Digital ID is ready
2000/5/10 PM 12:10
Vanessa Shaw
Test Secure E-Mail
2000/5/10 PM 01:50
者: Vanessa Shaw 收件者: M.H.Shaw
: Test Secure E-Mail
se verify vanessa's digital signature,
then decrypt the mail using M.H.Shaw's private key.
erely yours, vanessa shao.
顯示所選項目的內容。


私密金鑰容器
Using your private exchange key to decrypt!
密碼給Vanessa:
安全等級設定成 高
確定
取消
詳細資料(D)...


Test Secure E-Mail
一般
詳細資料
安全性
這個郵件的 Internet 標題:
From: "Vanessa Shaw" <vanessa@iim.nctu.edu.tw>
To: "M.H.Shaw" <u8734805@cc.nctu.edu.tw>
Subject: Test Secure E-Mail
Date: Wed, 10 May 2000 13:21:42 +0800
Content-Type: multipart/alternative;
boundary="----=_NextPart_000_0022_01BFBA82.A
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2014.211
安全郵件原始檔(S)...
郵件原始檔(M)...
確定
取消

➢ 安全郵件原始檔

➢ 郵件原始檔