內政部憑證管理中心

自然人憑證之保密郵件

設定暨應用說明操作手冊

V2.0

內政部憑證管理中心

中華民國九十五年十月

壹、 使用自然人憑證進行保密郵件(Secure E-mail)之要件

一、基於安全性考慮，建議使用 Windows 2000 或 XP 以上之作業系統，並需於電腦上安裝讀卡機以讀取憑證 IC 卡。

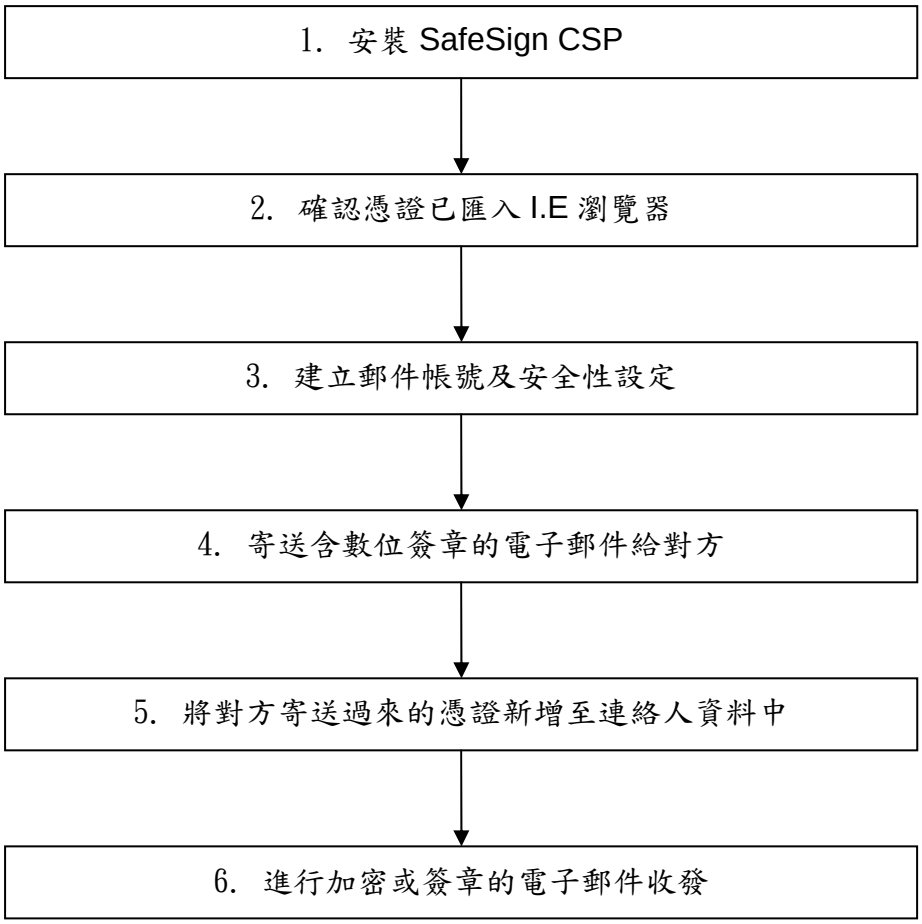
二、需將欲進行保密郵件收發之 E-mail 信箱寫入憑證之中。

三、此 E-mail 信箱必須支援 POP3，並使用 Microsoft Outlook 或 Outlook Express 等有提供 S/MIME 功能的收信軟體進行郵件收發。

四、欲進行保密郵件往來的雙方，都必須持有內政部憑證管理中心所簽發之自然人憑證 IC 卡。

五、有關申辦自然人憑證或修改電子信箱作業，請逕洽鄰近任一戶政事務所進行辦理，或請致電自然人憑證 24 小時客服專線 0800-080-117 洽詢。

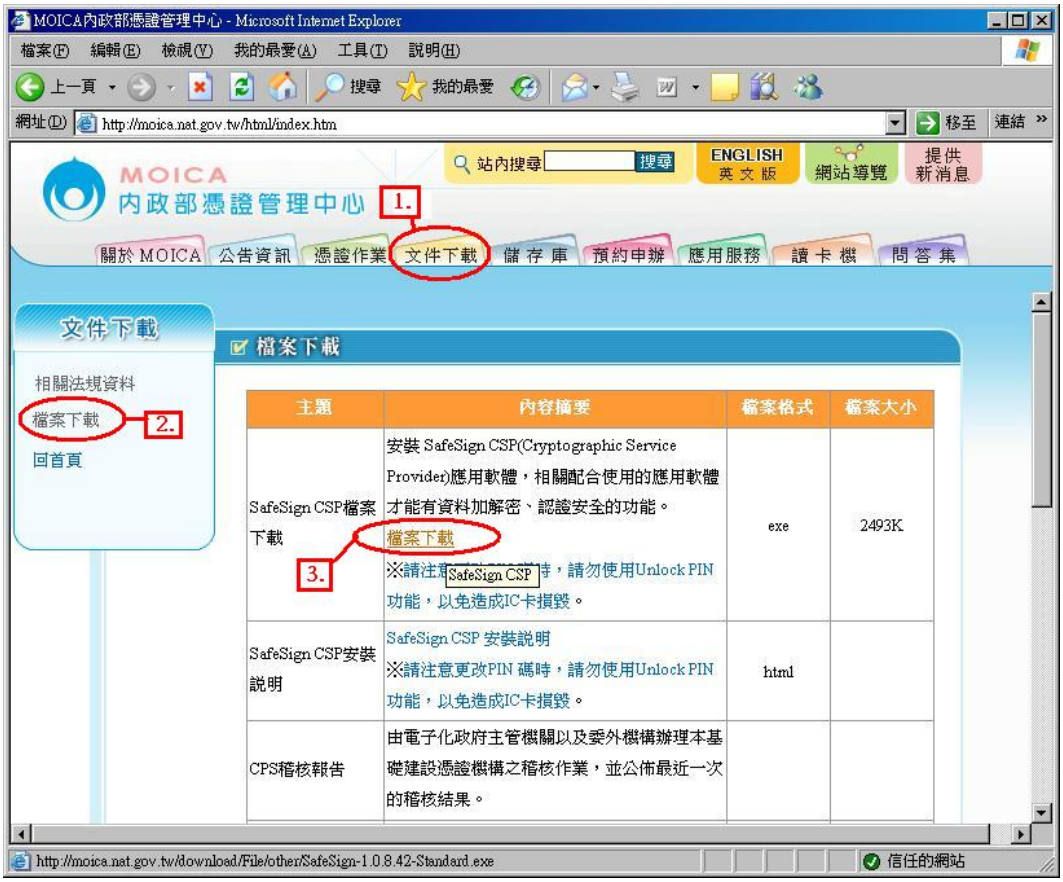
貳、 如何建立保密郵件(Secure E-mail)？



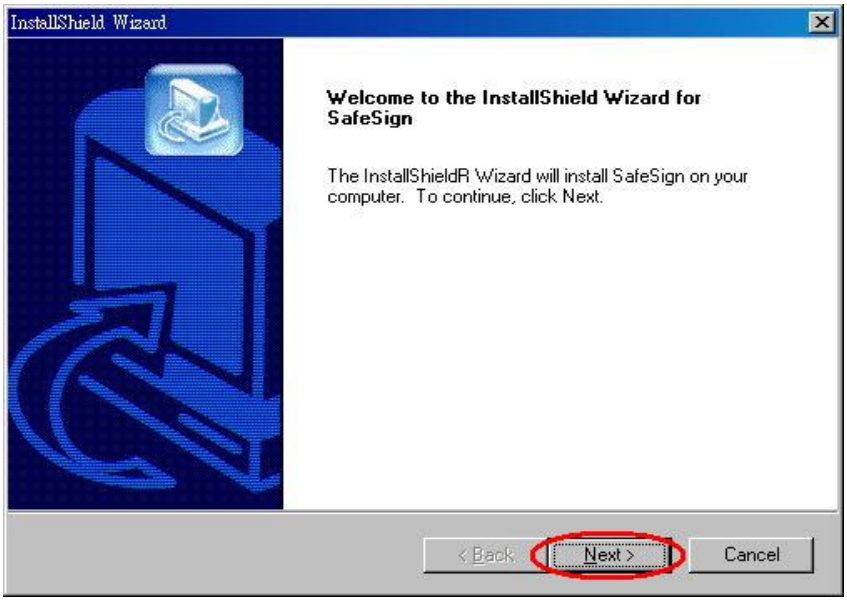
參、　建立保密郵件(Secure E-mail)的前置作業

一、 安裝 Safesign CSP(密碼服務提供者)軟體

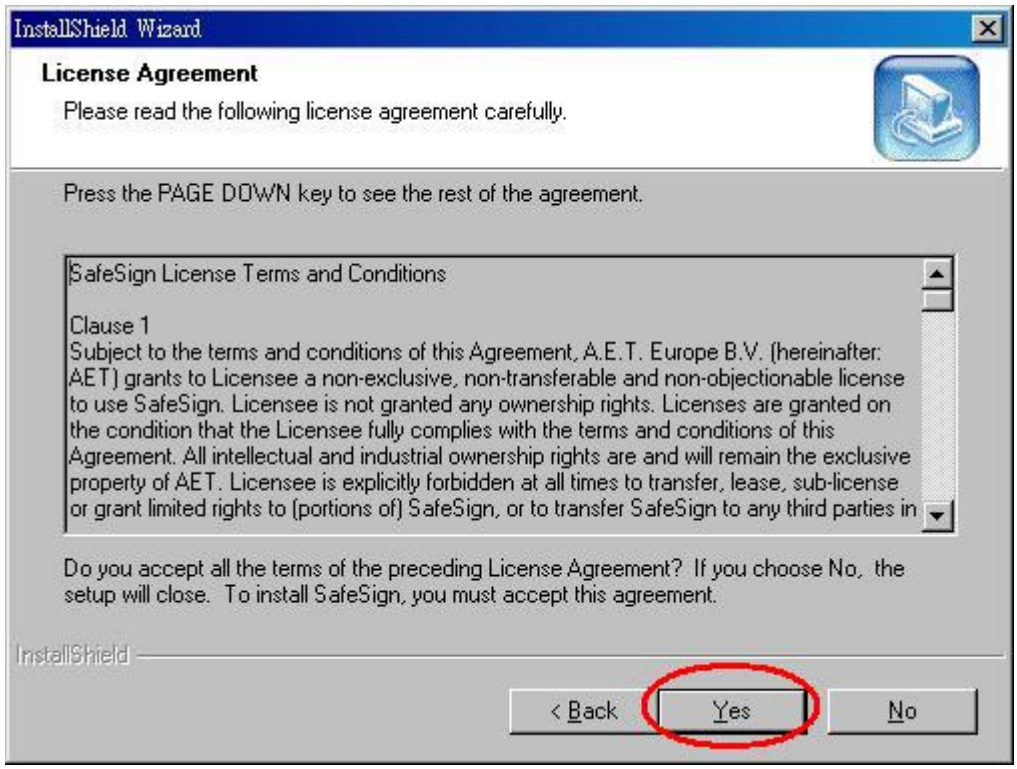
1. 請先至內政部憑證管理中心下載 SafeSign CSP 應用軟體，網址：http://moica.nat.gov.tw/（文件下載／檔案下載／SafeSign CSP 檔案下載）



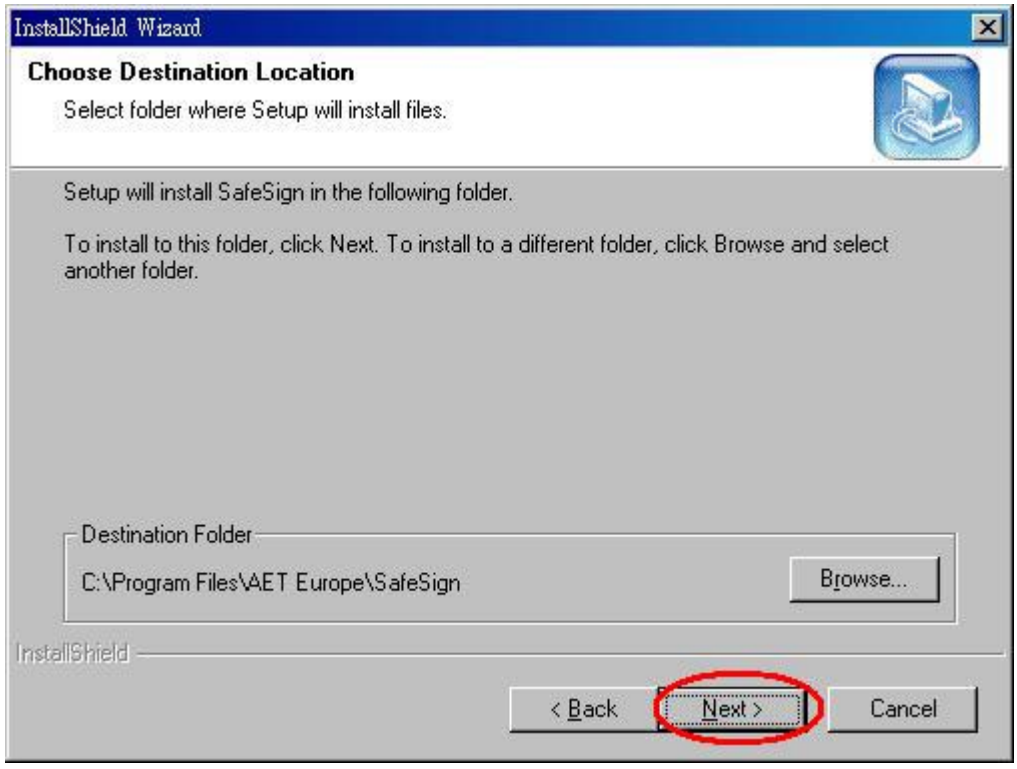
2. 出現安裝畫面，請點選『NEXT』。



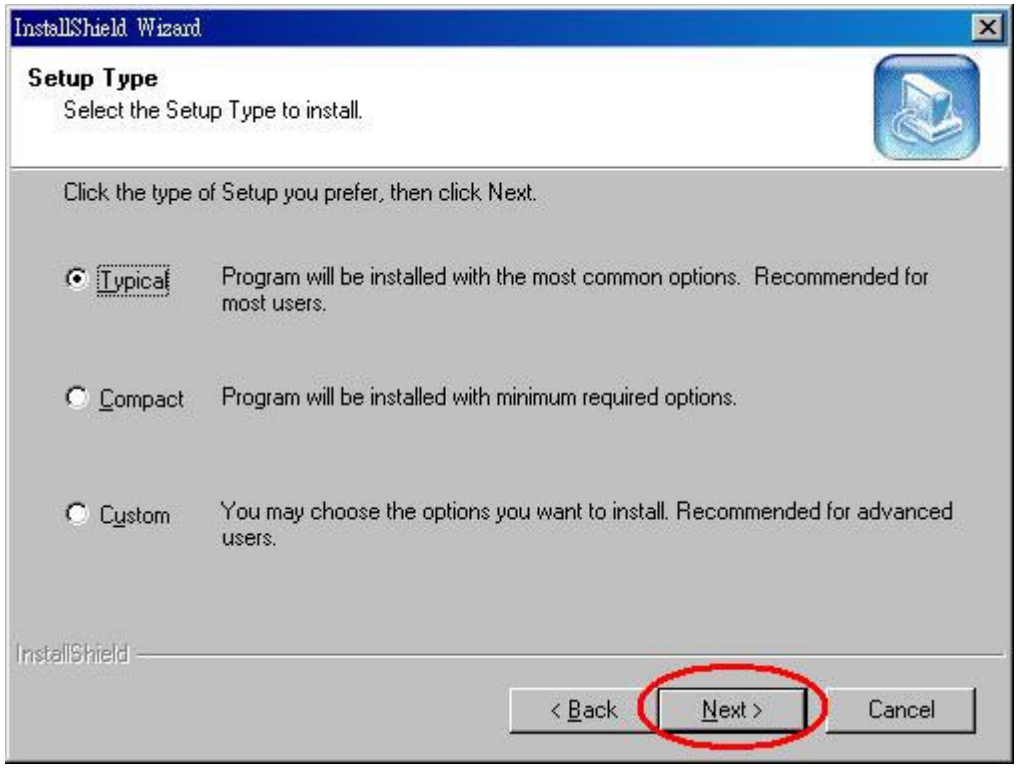
3. 請詳讀合約內容，並下拉視窗內容至最後，如果您接受合約內容，請點選『Yes』。



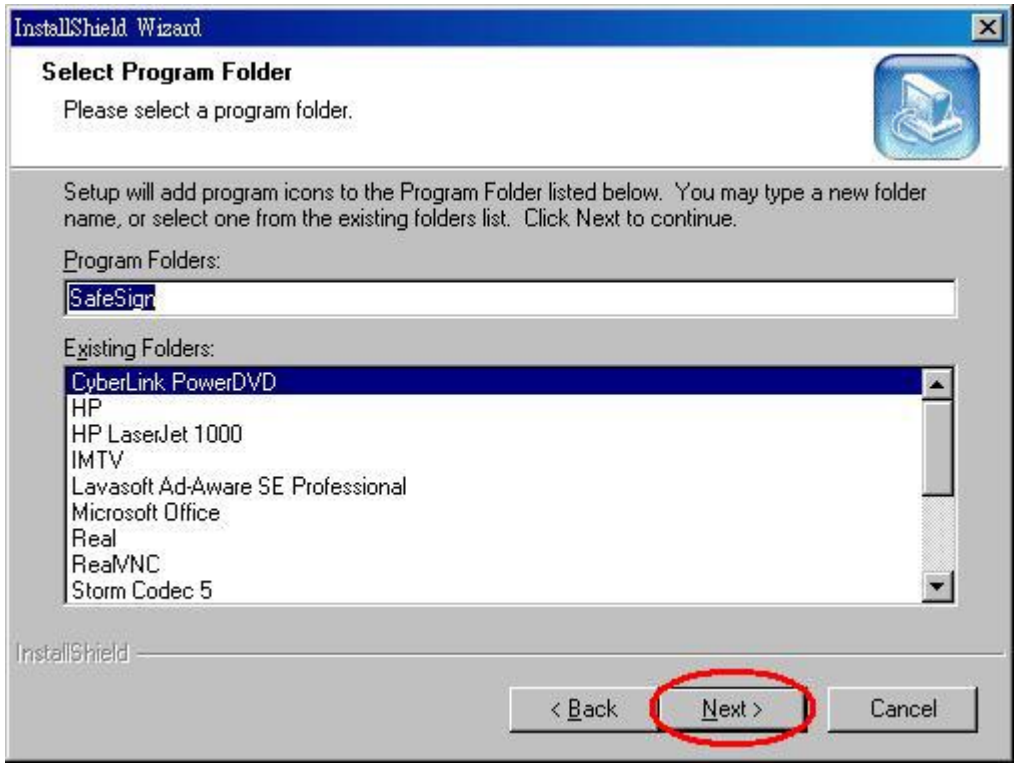
4. 請選擇程式安裝位置，並點選『NEXT』。



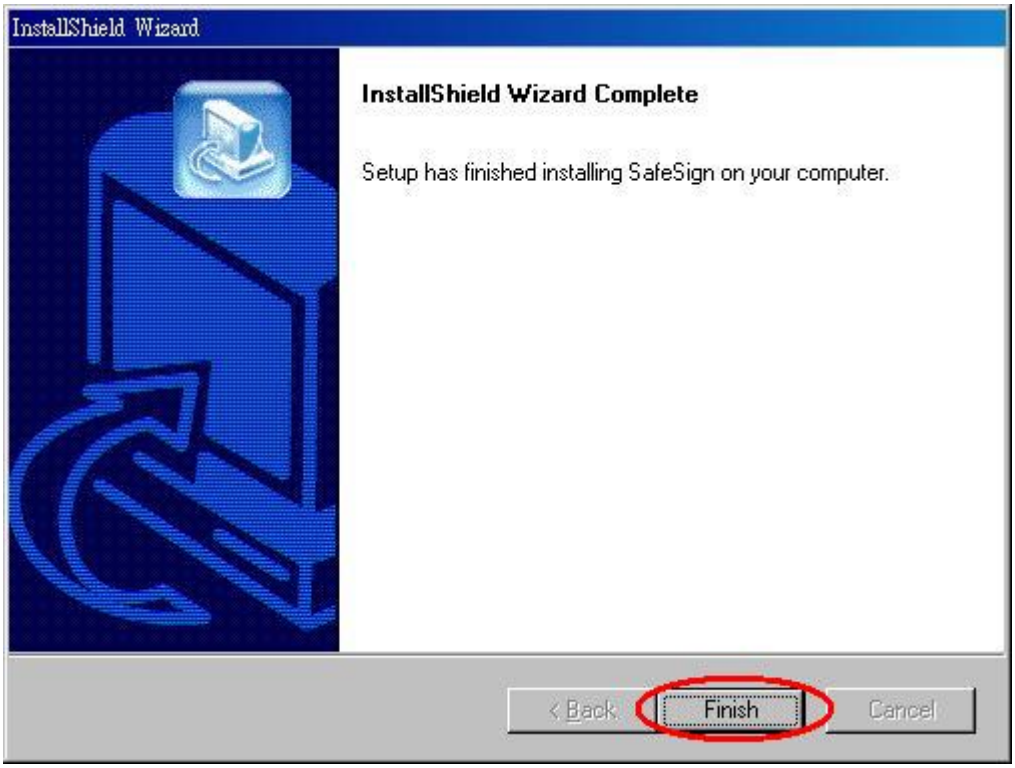
5. 請選擇安裝模組，並點選『NEXT』。



6. 確定檔案夾名稱，並點選『NEXT』。

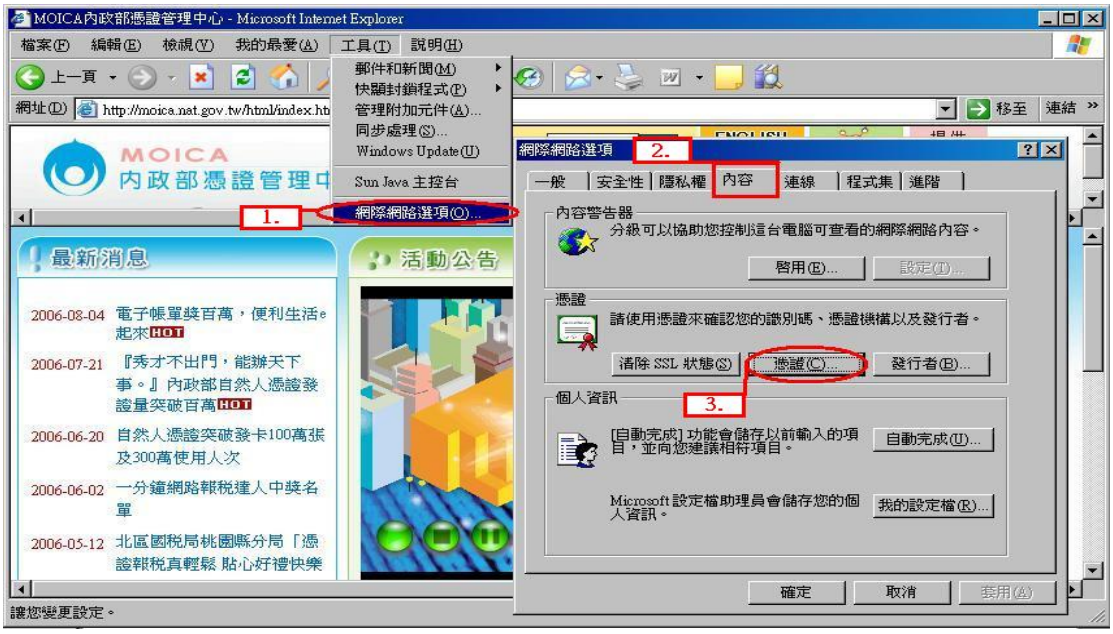


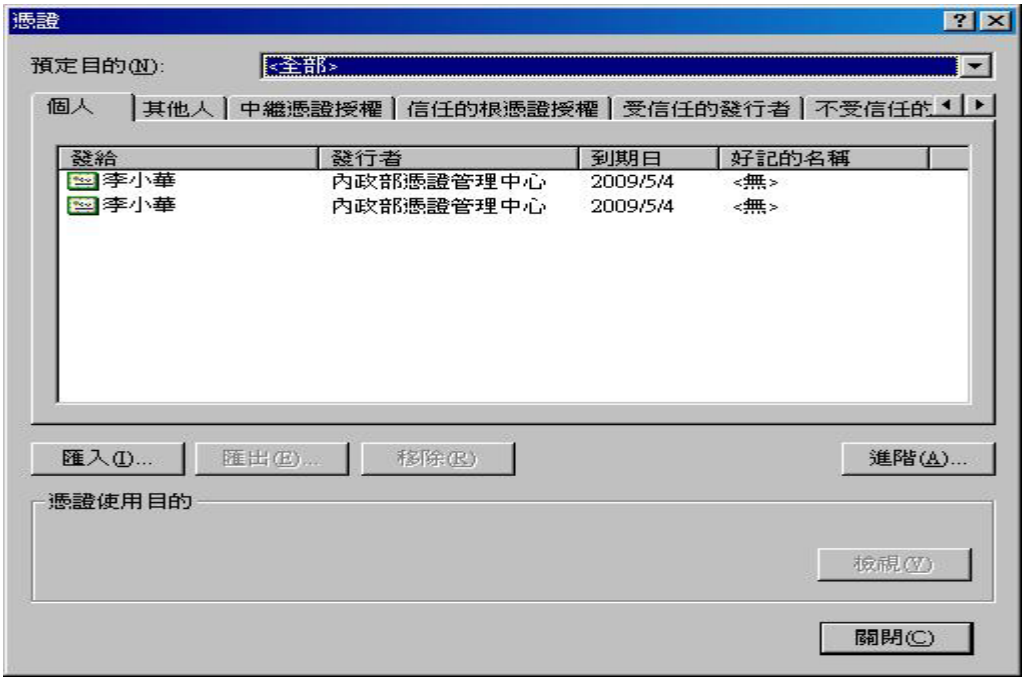
7. 程式進行安裝時請稍待片刻，安裝完成，請按『Finish』結束安裝。



二、 將憑證匯入 Microsoft Internet Explorer 瀏覽器之中

1. 安裝完成 SafeSign CSP 之後，請將憑證 IC 卡置入之前安裝好的讀卡機內。重新開機後，CSP 應用軟體將會自動把 IC 卡內的憑證匯入至 I.E 瀏覽器。此後便可搭配 Microsoft Outlook 或 Outlook Express 等收信軟體，進行安全電子郵件的傳遞。
2. 欲查詢已匯入之憑證，可至 I.E 瀏覽器上方功能表(工具／網際網路選項／內容／憑證)，即可在個人憑證區看到已匯入的憑證。





三、 無法將憑證匯入 I.E 瀏覽器時

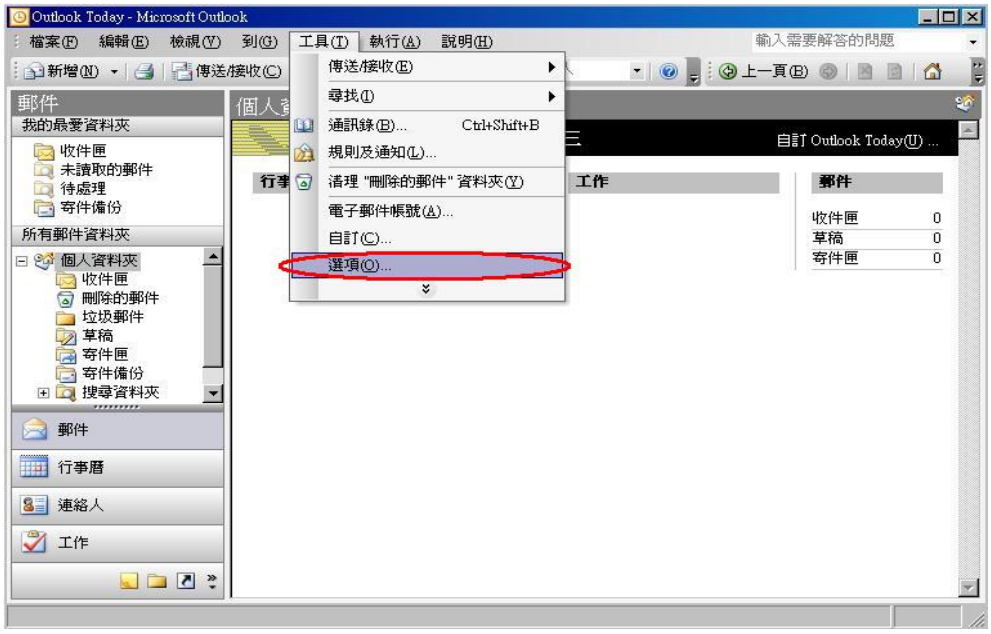
1. 請先完整移除 Safesign CSP 軟體，重新開機後再次安裝 Safesign CSP 軟體，並依第二項-第 1 點之說明重新開機將憑證匯入。
2. 重新開機時 Safesign CSP 程式會自動啟動，並開啟主程式視窗。
   A. SafeSign CSP 程式在可進行憑證讀取時，將於視窗中顯示卡片或讀卡機型號。

B. 如無法顯示卡片或讀卡機型號時，即表示系統無法正常啟動智慧卡讀取及匯入服務，請移除讀卡機驅動程式，並重新安裝讀卡機後再進行憑證匯入。

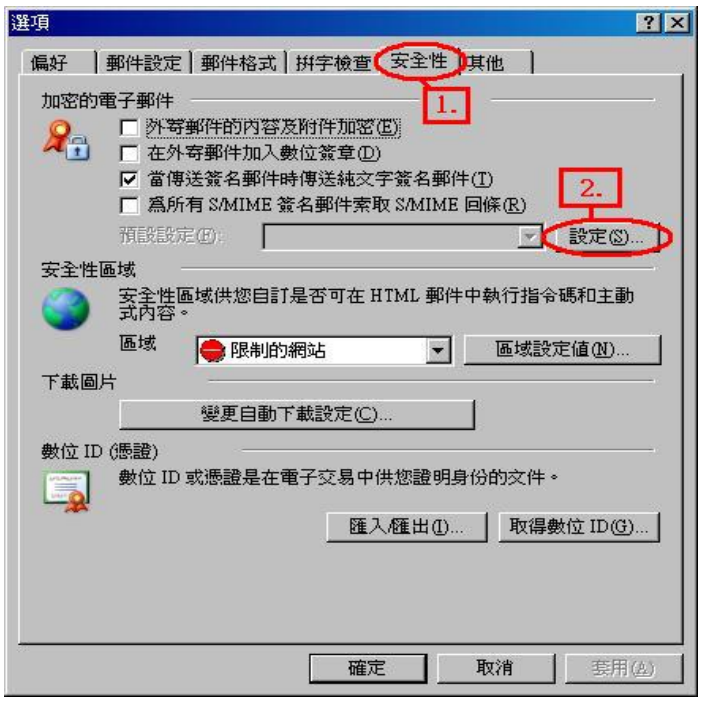
肆、 使用 Microsoft Outlook 2003 進行保密郵件

一、 郵件帳號及安全性設定

1. 啟動 Microsoft Outlook 2003 之後，請先依照 Microsoft Outlook 2003 之使用說明，將寫入至憑證中的電子郵件帳號建立起來，方可進行保密郵件的收發。
2. 電子郵件帳號設定完成後，請點選【工具】裡的【選項】來進行電子郵件的安全性設定。

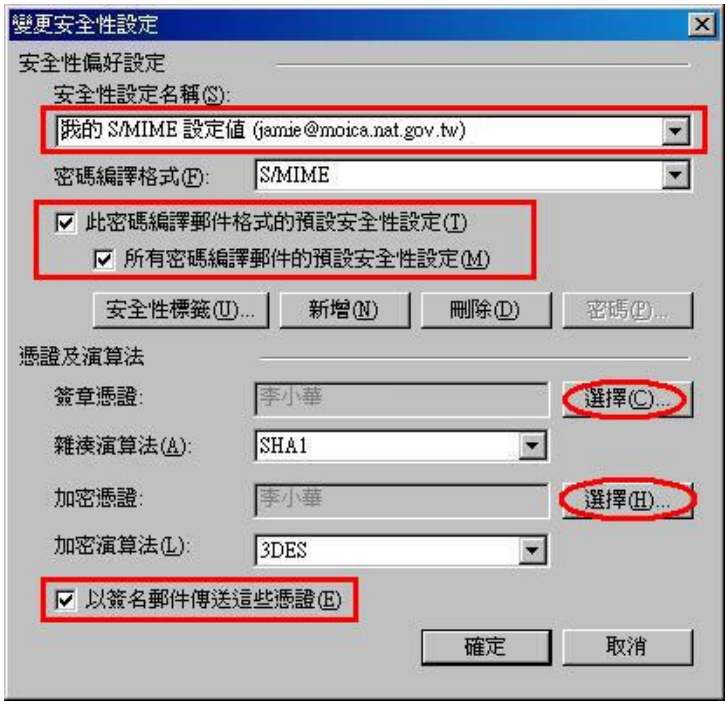


3. 點選【安全性】裡的【設定】來增加一個 S/MIME 的設定值。



4. 點選【新增】來增加一個新的安全性設定，如無特別命名時，系統會自動抓取已設定的電子信箱來命名。

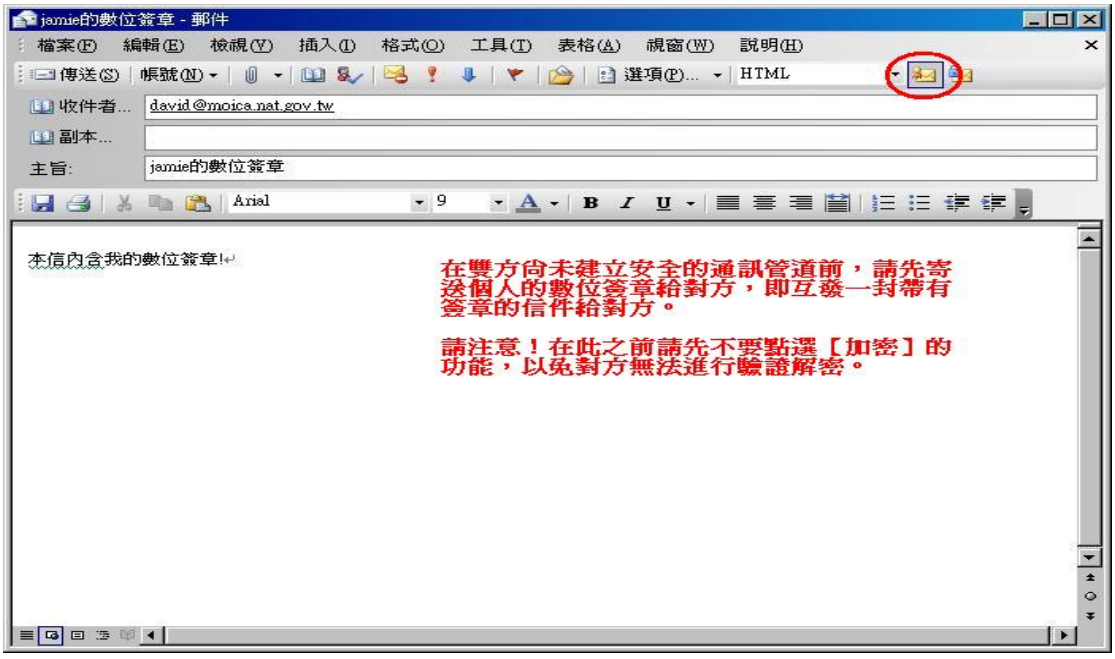
5. 在【憑證及演算法】的部分，點選【選擇】來選取憑證。依據國際標準，不同功能之憑證必須分開存放，因此，如已成功將憑證匯入 I.E 者，系統將自動出現可供選擇的簽章憑證及加密憑證。加密演算法的選擇跟作業系統有關，如不知作業系統是否可支援高加密等級的演算法，建議可使用預設值即可。



6. 完成憑證選取後，點選【套用】及【確定】即完成安全性設定，此時即可開始進行保密郵件的收發了！

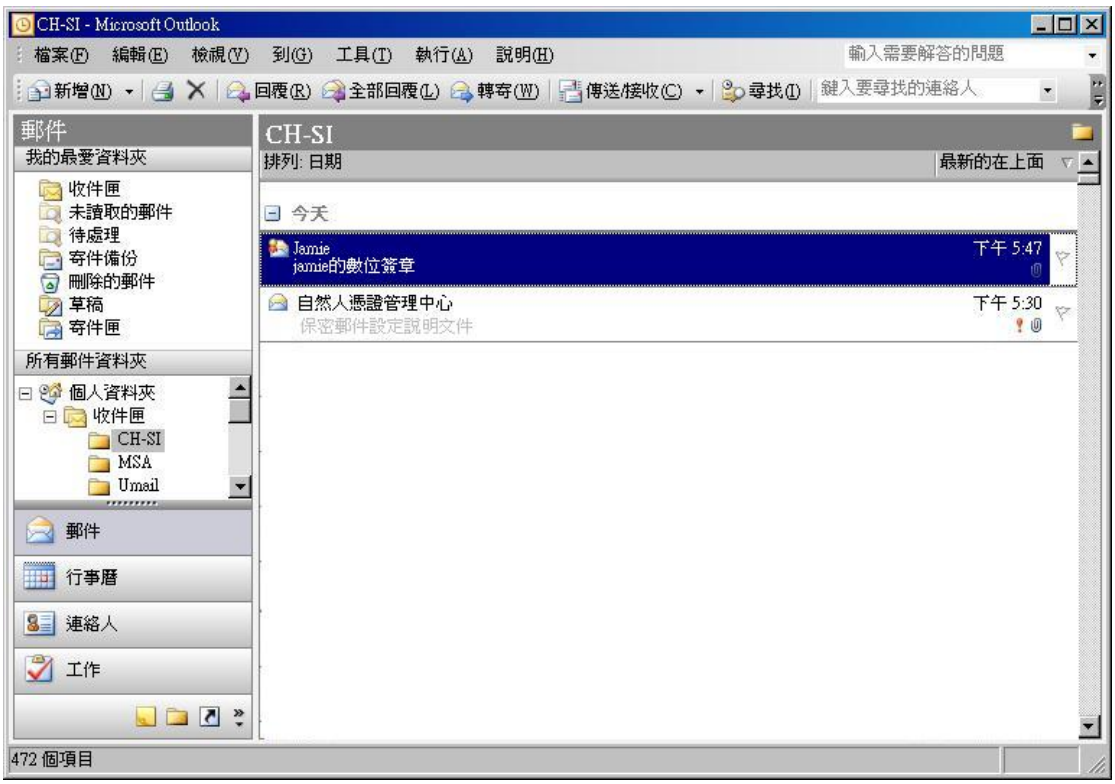
二、 建立保密郵件(Secure E-mail)通訊管道

1. 想與對方進行保密郵件的收發之前，必須先取得對方的公鑰方可使用保密郵件。保密郵件係利用憑證內所含之金鑰對，在 Outlook 或 Outlook Express 等有提供 S/MIME 功能的收信軟體裡，進行數位簽章及資料加解密的作業，因此必須先取得通信對象之公鑰以利日後保密郵件的收發。
2. 點選【新增】來寄送一封加上數位簽章的電子郵件給欲通信之對象。

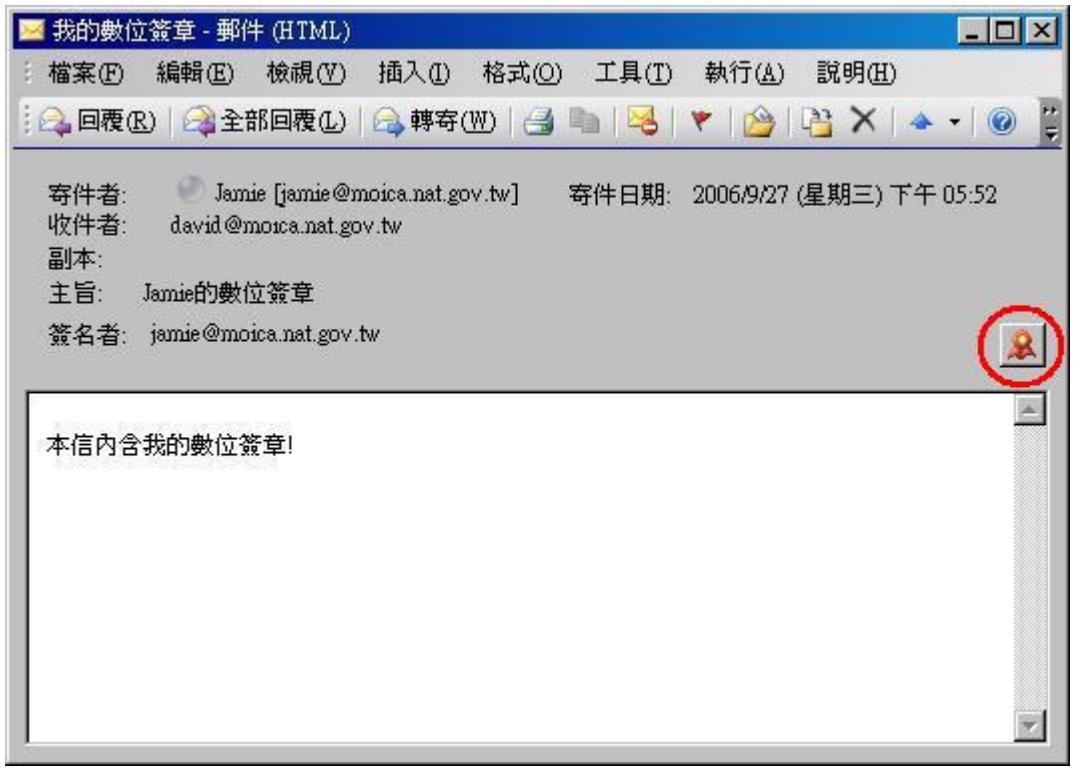


3. 電子郵件寄送時，系統會要求輸入憑證 PIN 碼來進行數位簽章作業。PIN 碼一旦驗證成功後，只要憑證並未取出或收信軟體並未重新啟動前，系統都將延用驗證成功的結果，直接進行保密郵件的收發。意即登入成功後只要不取出憑證 IC 卡，當收到保密郵件時，是可以直接開啟電子郵件的，因此請於離開座位時務必將憑證 IC 卡取出，以確保個人隱私及資料安全。

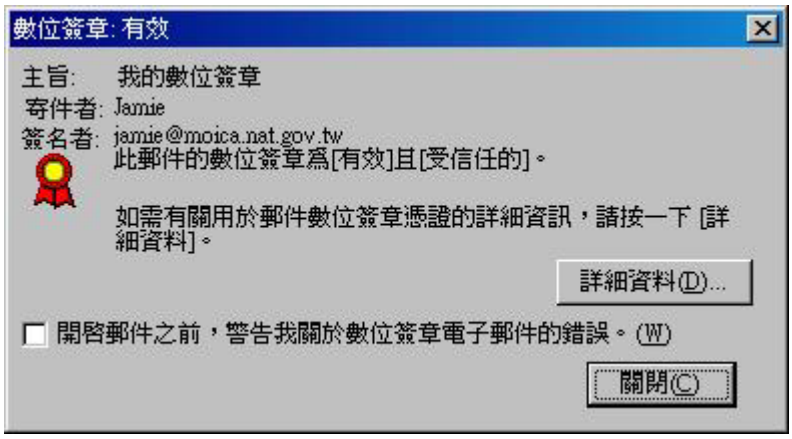
4. 當收到含有數位簽章的電子郵件時，在預覽信件主旨時會看到有徽章圖樣的信件標示。



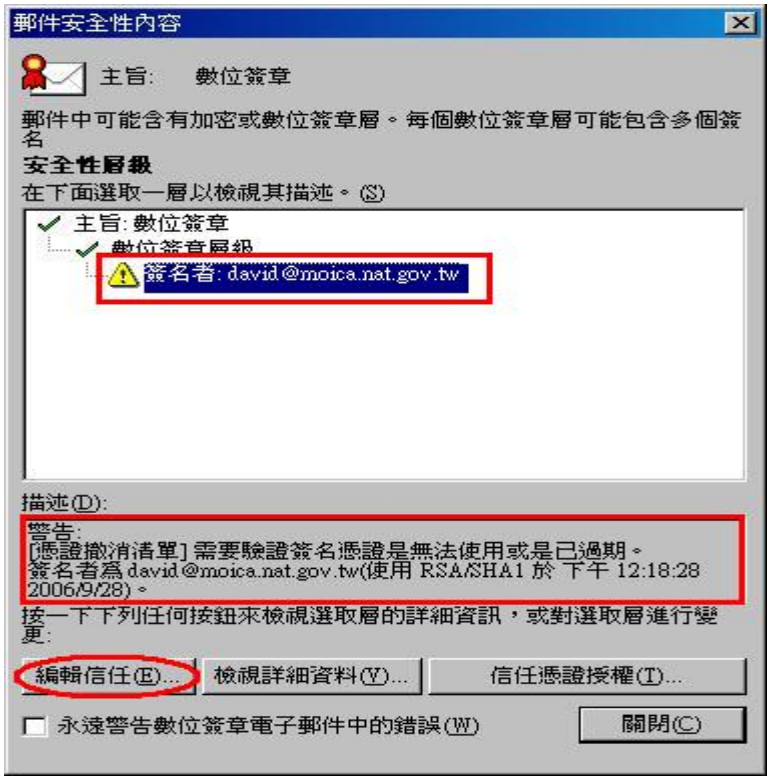
5. 開啟含有數位簽章的電子郵件後，可點選右側的徽章圖示來檢視數位簽章的內容。



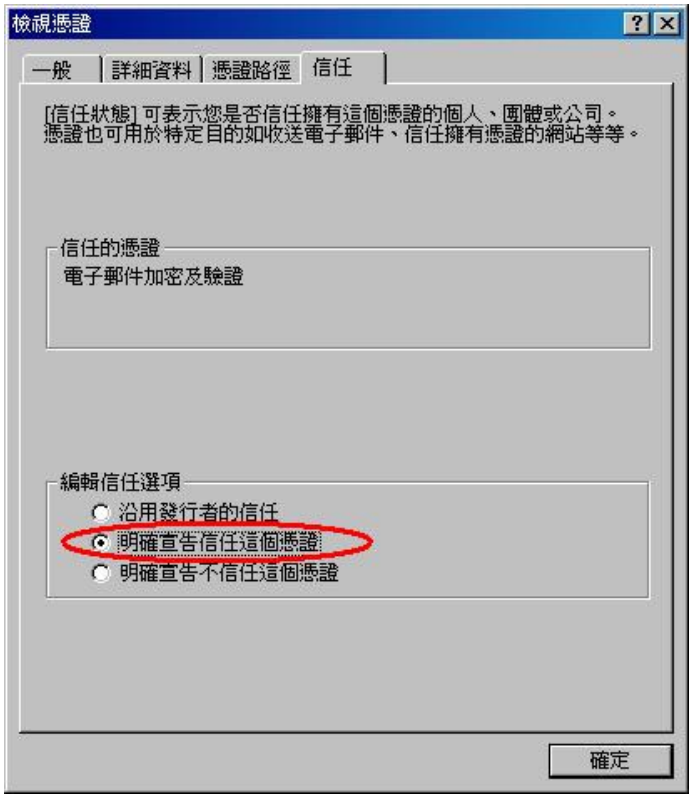
6. 此時可看到數位簽章的狀態是否有效，如欲進一步檢視憑證資訊，可點選【詳細資料】來進行檢視。



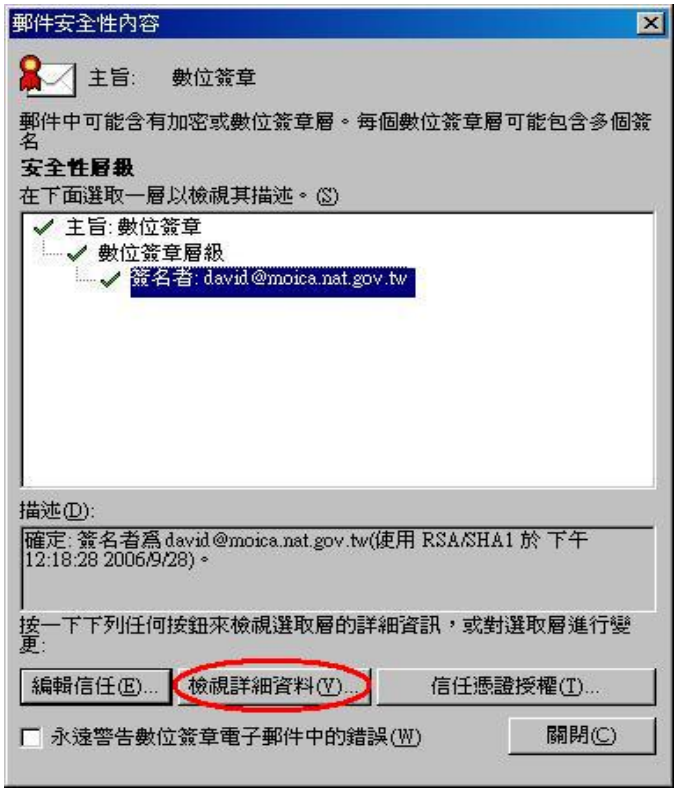
7. 系統如無法取得憑證撤消清單來進行效期驗證時，可點選【編輯信任】來更改憑證信任狀態。



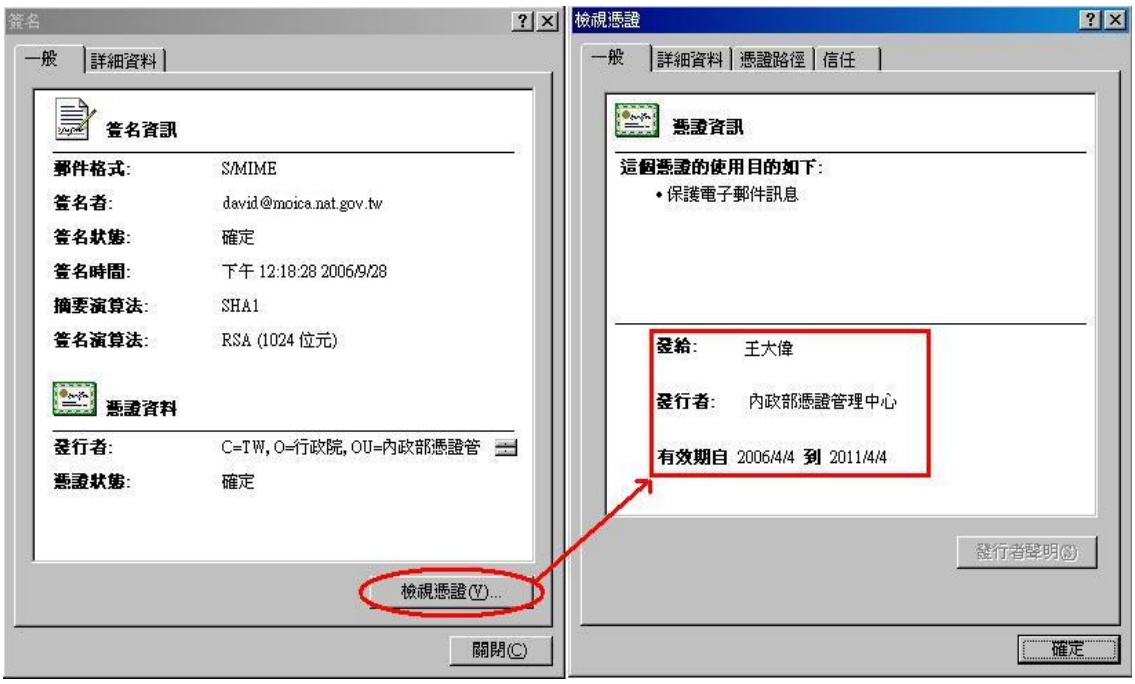
8. 在【信任】的編輯信任選項裡，點選【明確宣告信任這個憑證】即可自行修正憑證的信任狀態。



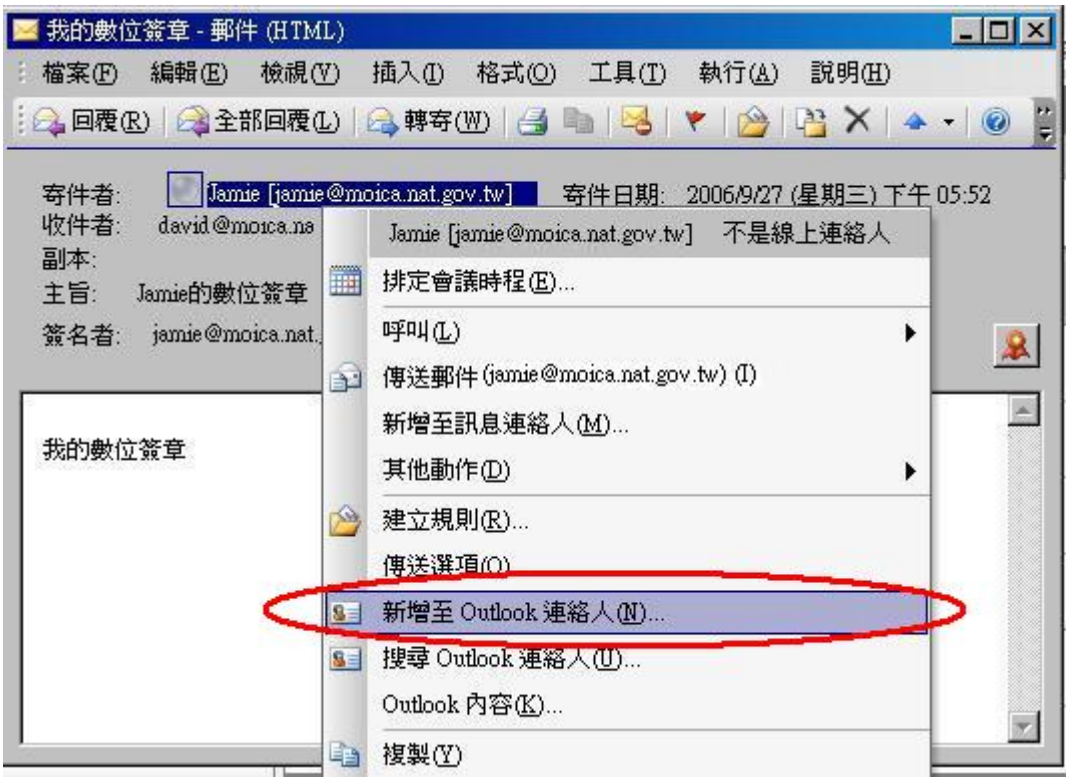
9. 在明確宣告信任這個憑證後，可點選【檢視詳細資料】來檢視憑證資訊裡的效期。



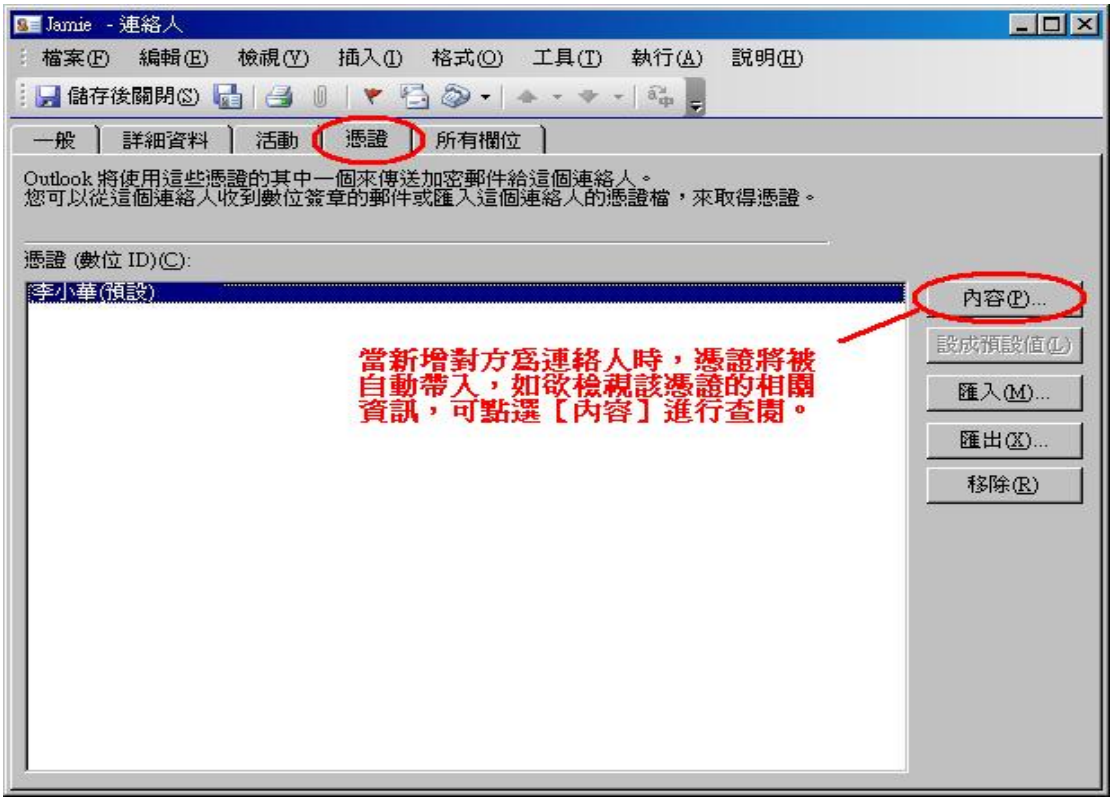
10. 點選【檢視憑證】可清楚的看到憑證簽發單位及效期。



11. 確認數位簽章後將對方加入 Outlook 連絡人之中，即可自動將對方的公鑰憑證一併存入連絡人資料裡。



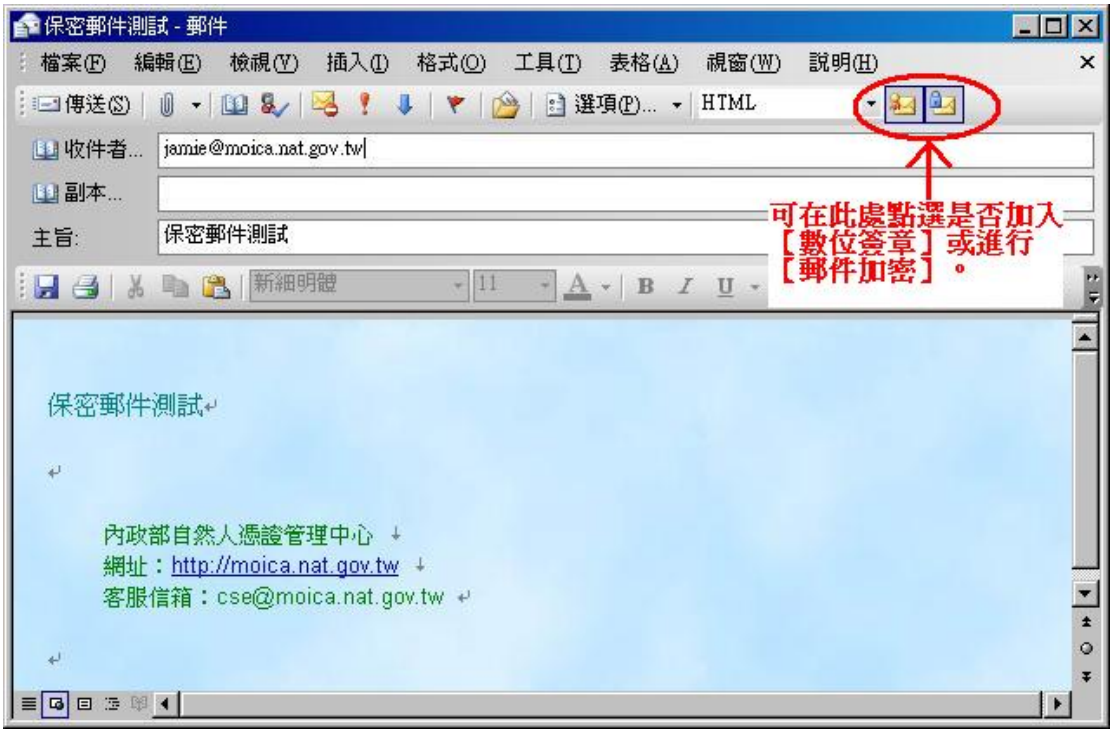
12. 在連絡人資料裡可點選【憑證】裡的【內容】來檢視憑證資訊。



13. 在此處可看到該連絡人憑證簽發的單位及效期。

14. 儲存連絡人之後，請回覆一封含有數位簽章的信件給對方，如此在雙方都取得彼此的公鑰憑證後，就可進行保密郵件的傳送。

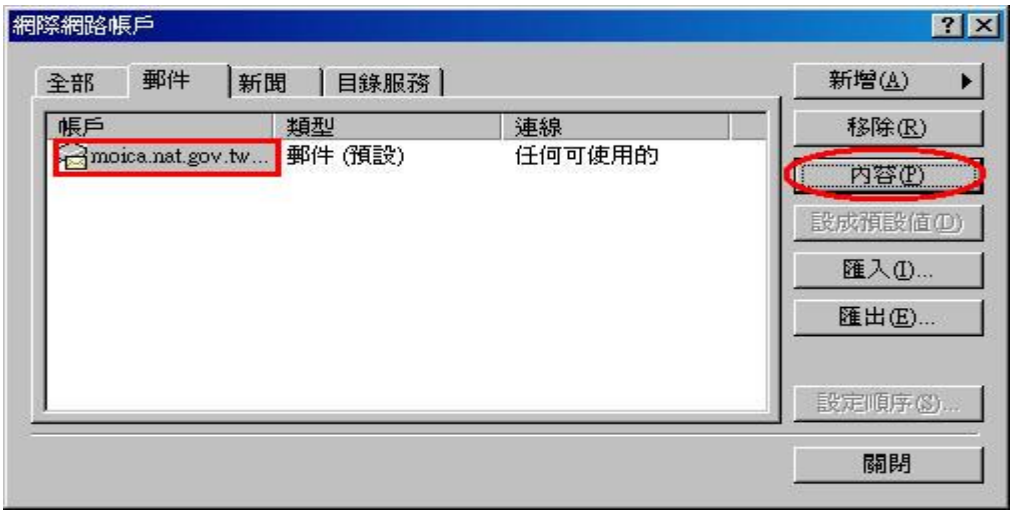
15. 日後如欲進行簽章或加密，只需於右上角點選【數位簽章】或【資料加密】的小圖示，即可輕鬆完成簽章及加密的動作。



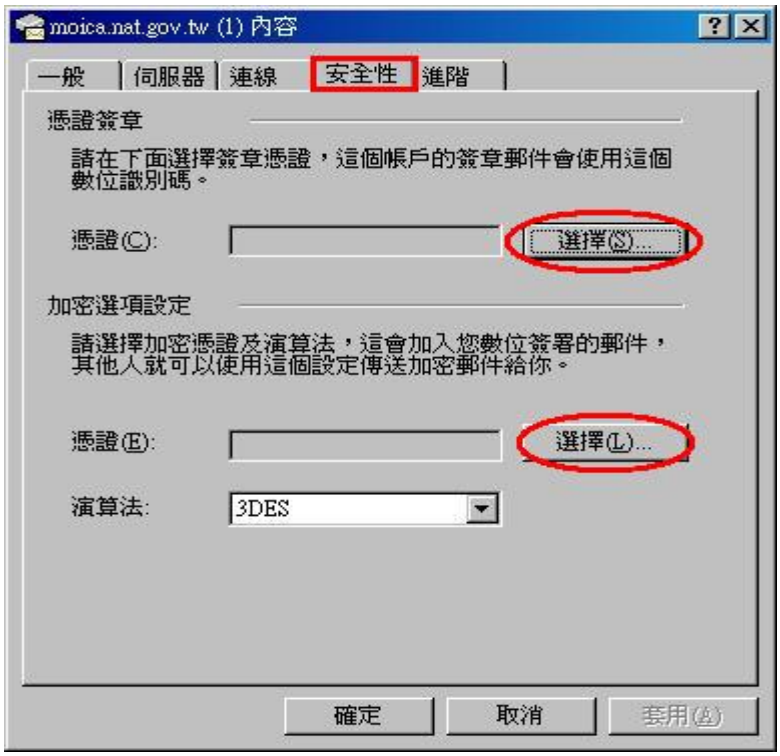
伍、 使用 Microsoft Outlook Express 進行保密郵件

一、 郵件帳號及安全性設定

1. 啟動 Microsoft Outlook Express 之後，請先依照 Microsoft Outlook Express 之使用說明，將寫入至憑證中的電子郵件帳號建立起來，方可進行保密郵件的收發。
2. 完成電子郵件帳號設定後，選擇欲修改安全性設定的帳戶，再點選【內容】來進行安全性設定。

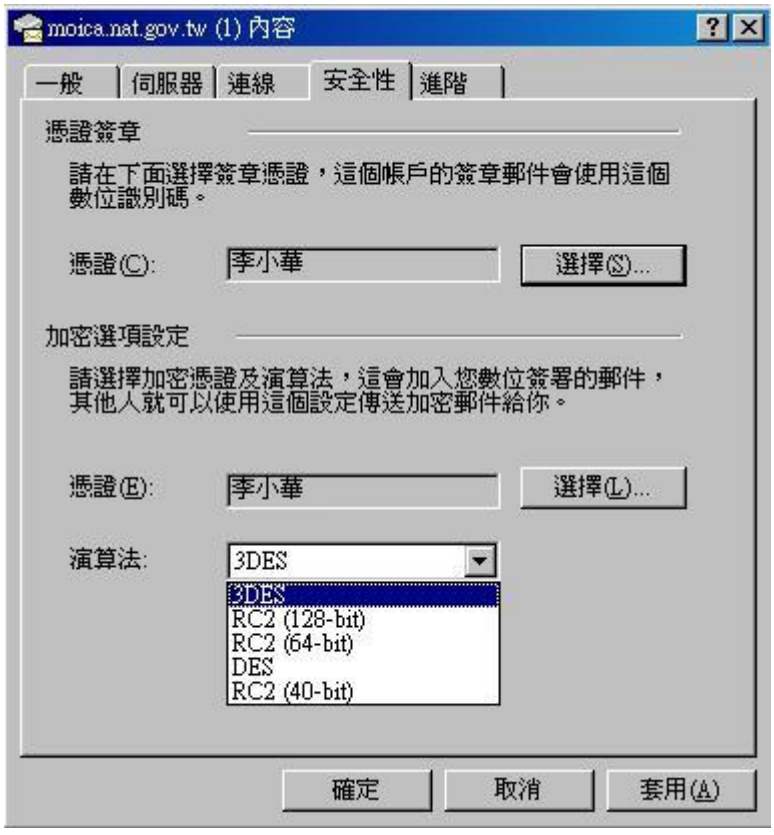


3. 點選【安全性】裡的【選擇】，系統會自動列出可供此電子郵件帳號進行保密郵件的憑證。



4. 依據國際標準，不同功能之憑證必須分開存放，因此，如已成功將憑證匯入I.E者,系統將自動出現可供選擇的簽章憑證及加密憑證。

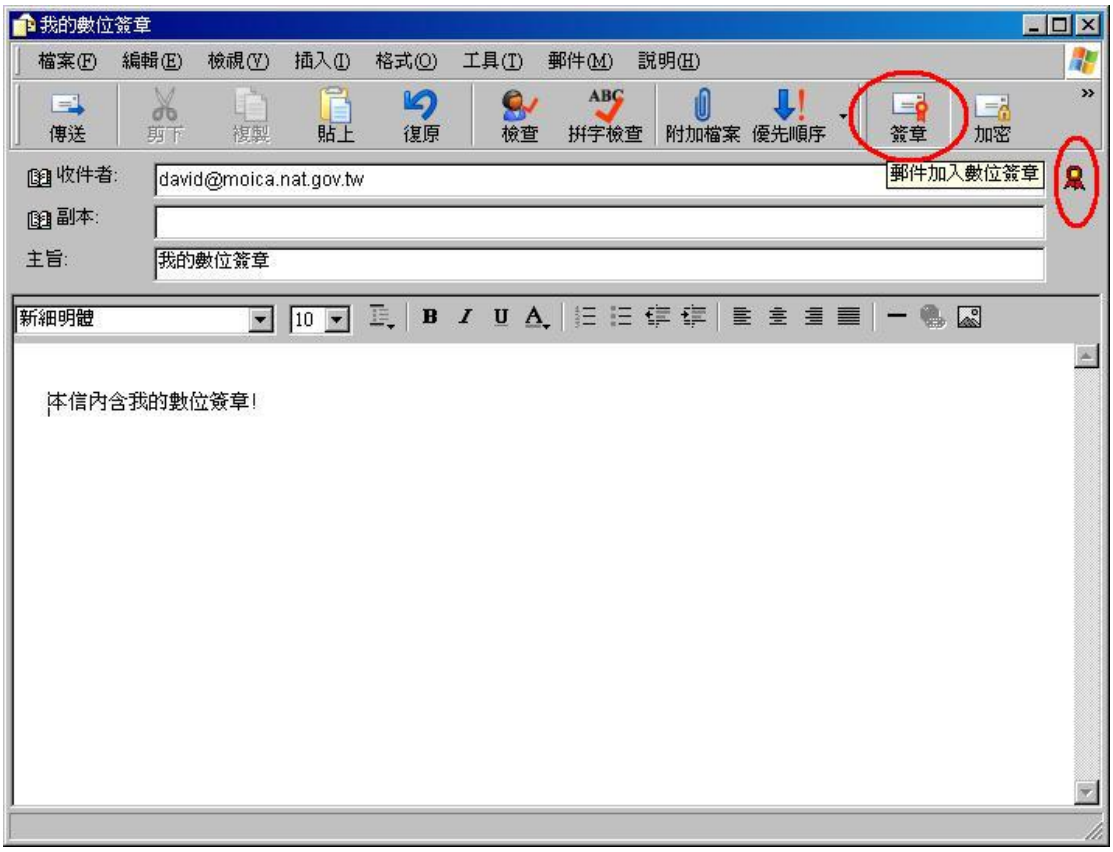
5. 加密演算法的選擇跟作業系統有關,如不知作業系統是否可支援高加密等級的演算法，建議可使用預設值即可。



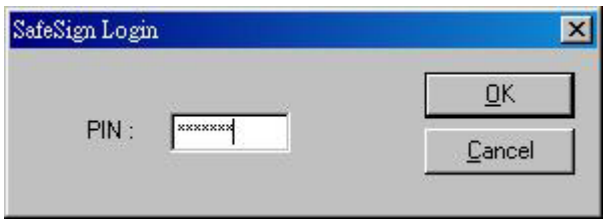
6. 完成憑證選取後，點選【套用】及【確定】即完成安全性設定，此時即可開始進行保密郵件的收發了！

二、 建立保密郵件(Secure E-mail)通訊管道

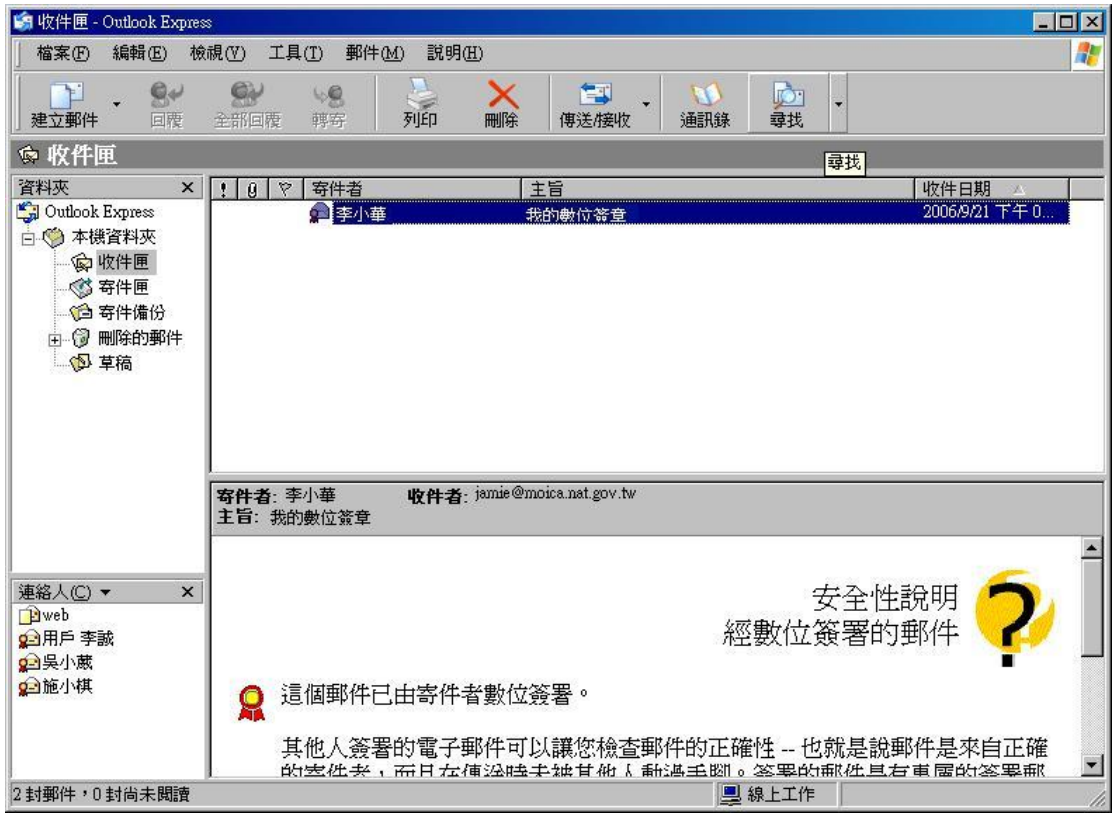
1. 想與對方進行保密郵件的收發之前，必須先取得對方的公鑰方可使用保密郵件。保密郵件係利用憑證內所含之金鑰對，在 Outlook 或 Outlook Express 等有提供 S/MIME 功能的收信軟體裡，進行數位簽章及資料加解密的作業，因此必須先取得通信對象之公鑰以利日後保密郵件的收發。
2. 點選【新增郵件】來寄送一封加上數位簽章的電子郵件給欲通信之對象。點選右上方的【簽章】鈕即可在信件中加入數位簽章。



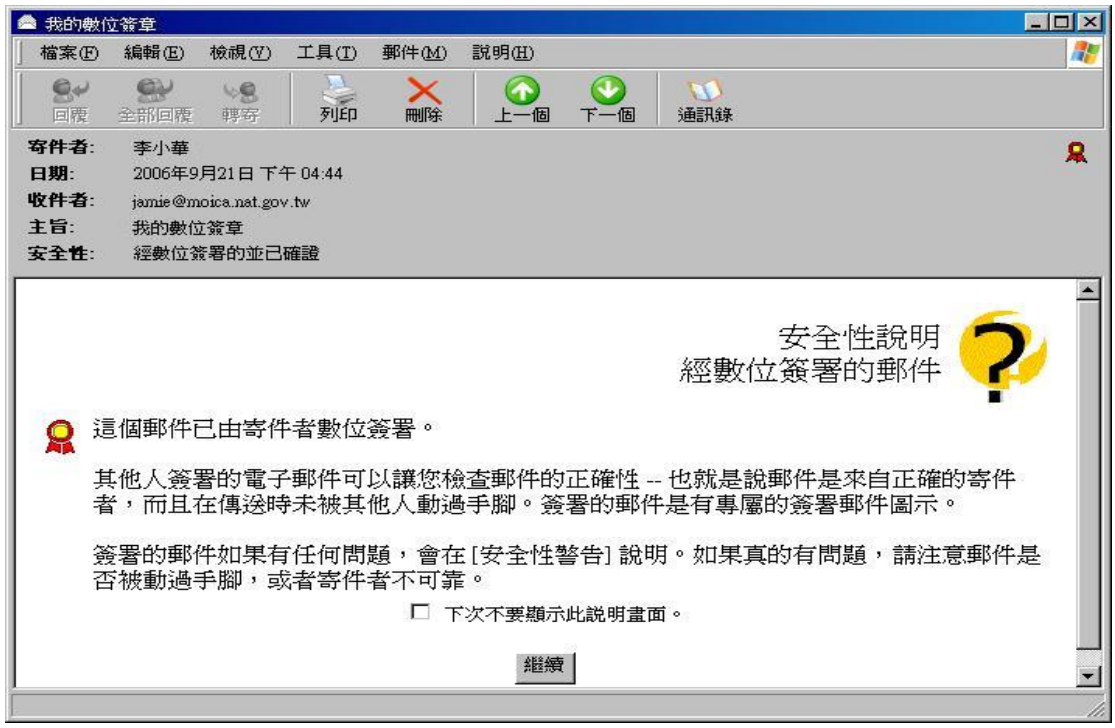
3. 電子郵件寄送時，系統會要求輸入憑證 PIN 碼來進行數位簽章作業。PIN 碼一旦驗證成功後，只要憑證並未取出或收信軟體並未重新啟動前，系統都將延用驗證成功的結果，直接進行保密郵件的收發。意即登入成功後只要不取出憑證 IC 卡，當收到保密郵件時，是可以直接開啟電子郵件的，因此請於離開座位時務必將憑證 IC 卡取出，以確保個人隱私及資料安全。



4. 當收到含有數位簽章的電子郵件時，在預覽信件主旨時會看到有徽章圖樣的信件標示。



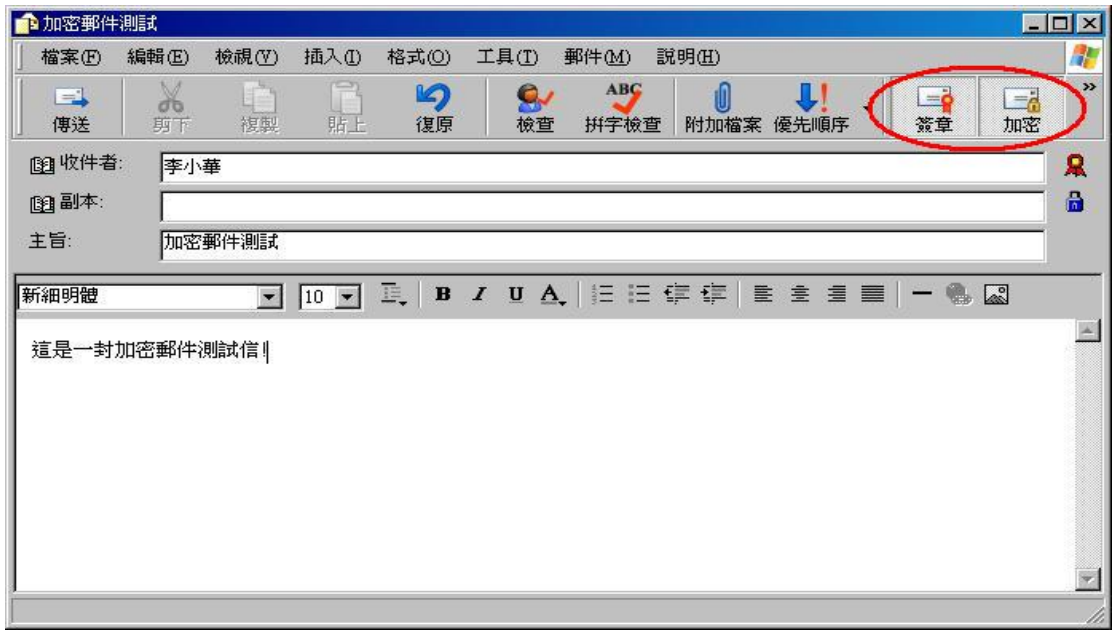
5. 開啟含有數位簽章的電子郵件時，Outlook Express 會自動將寄件者及數位識別碼(即憑證公鑰)新增為通訊錄裡的連絡人。開啟郵件後可點選右側的徽章圖示來檢視數位簽章的內容。在瀏覽完安全性說明後，點選【繼續】即會顯示郵件內容。



6. 如欲檢視連絡人的公鑰憑證是否已正常匯入，可於通訊錄中開啟該連絡人內容來進行檢視。在【數位識別碼】中會顯示已自動匯入的憑證，如欲檢視憑證詳細資料可點選【內容】來進行檢視。

7. 確認連絡人資料無誤後，請回覆一封含有數位簽章的信件給對方，如此在雙方都取得彼此的公鑰憑證後，就可進行保密郵件的傳送。

8. 日後如欲進行簽章或加密，只需於右上角點選【簽章】或【加密】的按鈕，即可輕鬆完成簽章及加密的動作。



陸、 保密郵件常見問題集錦

一、 在同一台電腦上，可以同時設定多個電子郵件帳號來進行保密郵件的收發嗎？

如於設定帳號時有正確的選取到所對應的憑證，是可以在同一台電腦上使用多個電子郵件帳號來收發信件；惟基於維護保密郵件所含資料的安全性，建議最好不要使用多個郵件帳號在同一台電腦上進行保密郵件的收發。

二、 在 Outlook 或 Outlook Express 裡所設定之郵件信箱是否須與寫入憑證中之郵件信箱為同一個？

欲使用自然人憑證在 Outlook 或 Outlook Express 等收信軟體裡進行保密郵件的收發，必須要將用來進行保密郵件收發的電子郵件帳號寫入至憑證裡，否則將無法完成傳送保密郵件時的電子郵件帳號設定。

三、 進行保密郵件設定與收發時，需搭配讀卡機來進行讀取嗎?

由於在設定郵件帳號及讀取保密郵件時，必須先行匯入公鑰憑證及進行憑證 PIN 碼的驗證，故需於電腦上安裝讀卡機以進行讀取憑證 IC 卡的動作，如此方可完成保密郵件的作業。

四、 已依照操作流程完成安全性設定，為什麼寄出含數位簽章的郵件時，會出現【數位簽章：無效】的錯誤訊息而無法寄出？

在寄送保密郵件時，系統會要求輸入自然人憑證的 PIN 碼來進行簽章及加密作業，請先確認已正確插入該郵件帳號使用者的憑證 IC 卡，以免在驗證及簽章時發生錯誤，而無法寄出保密郵件。或請確認是否已將該連絡人之憑證正確的匯入於通訊錄中，如於通訊錄中遺失了該連絡人之公鑰憑證，在寄送保密郵件時亦會因缺乏可供加密的憑證而無法完成加密作業。如已確認上述事項後仍無法正常寄發保密郵件時，建議將該郵件帳號刪除後再重新建立，並請確認在設定郵件安全性時，已正確匯入並選擇了可供使用的憑證，重新設定完成後再行收發保密郵件。

五、 收到對方寄來的保密郵件，憑證仍在有效期限內但卻顯示簽章有問題?

欲檢驗憑證目前的狀態及效期，必須經由取得內政部憑證管理中心的憑證廢止清冊(CRL)來進行憑證撤銷檢查，但由於 Outlook 及 Outlook Express 等收信軟體中關閉了數位識別碼的檢驗功能，以致無法在保密郵件寄達時經由收信軟體直接進行檢驗。使用者可經由檢視憑證詳細內容的方式來確認寄件者的憑證狀態及效期，再以編輯信任的方式將該連絡人加入信任的清單之中，未來收到該連絡人寄來的保密郵件

時就不會出現簽章有問題的情況了。

六、 **寄送含有數位簽章或加密的電子郵件時，是否可同時傳送給多人？**

寄件者如已於收信軟體中匯入了連絡人的公鑰憑證，是可以同時寄送含有數位簽章或加密的電子郵件給多位收件者的。唯連絡人於收到保密郵件時，必須插卡輸入憑證 PIN 碼，方可將保密郵件內文進行解密。

七、 **該如何確認保密郵件是否成功寄出，以及所接收之憑證為有效？**

保密郵件於寄出時，如無法完成簽章或加密作業，則會顯示無法完成簽章或加密的錯誤訊息；如已成功寄出保密郵件，則會於寄件備份的資料夾中看到該封保密郵件。如欲確認所接收之憑證是否有效，可點選保密郵件中的數位簽章，檢視憑證詳細資料即可清楚的看到憑證簽發者資訊及有效期限。

八、 **寄出保密郵件時的安全性設定，如選擇與對方使用不同的演算法是否會影響保密郵件的收發？**

雙方是否選擇相同的演算法，並不會影響到保密郵件的收發。加密演算法的選擇跟作業系統有關，如不知作業系統是否可支援高加密等級的演算法，建議可使用預設值即可。

九、 **第一次設定保密郵件時一定要寄簽章給對方嗎?是否能直接寄送簽章並加密的郵件，這樣對方是否能正常開啟加密郵件？**

保密郵件係利用憑證內所含之金鑰對，在 Outlook 或 Outlook Express 等有提供 S/MIME 功能的收信軟體裡，進行數位簽章及資料加解密的作業，因此在與對方進行保密郵件的收發之前，必須先取得對方的公鑰方可使用保密郵件。在尚未取得對方公鑰憑證之前，是無法將郵件內文進行加密處理的，系統會告知『憑證遺失或找不到連絡人的數位識別碼』，並會詢問該封電子郵件是否要以『只簽章而不加密』的方式寄出，寄件者如仍同意寄出，則收件人將收到的只是含有數位簽章但並無加密的明文電子郵件。