## 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册

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)?



## 冬、 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

 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』。



 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』。

×
int carefully.
st of the agreement.
s Agreement, A.E.T. Europe B.V. (hereinafter: non-transferable and non-objectionable license any ownership rights. Licenses are granted on lies with the terms and conditions of this whership rights are and will remain the exclusive bidden at all times to transfer, lease, sub-license Sign, or to transfer SafeSign to any third parties in
ng License Agreement? If you choose No, the nust accept this agreement.
< Back Yes No

4. 請選擇程式安裝位置,並點選『NEXT』。

InstallShield Wizard	
Choose Destination Location Select folder where Setup will install files.	
Setup will install SafeSign in the following folde	r.
To install to this folder, click Next. To install to a another folder.	a different folder, click Browse and select
Destination Folder C:\Program Files\AET Europe\SafeSign	Browse
InstellShield	< Back

## 5. 請選擇安裝模組,並點選『NEXT』。

InstallShield Wizard	×
Setup Type Select the Setu	up Type to install.
Click the type (	of Setup you prefer, then click Next.
• Typical	Program will be installed with the most common options. Recommended for most users.
C <u>C</u> ompact	Program will be installed with minimum required options.
⊙ C <u>u</u> stom	You may choose the options you want to install. Recommended for advanced users.
InstallShield	< <u>B</u> ack <u>N</u> ext > Cancel

## 6. 確定檔案夾名稱,並點選『NEXT』。

InstallShield Wizard	×
Select Program Folder Please select a program folder.	
Setup will add program icons to the Program name, or select one from the existing folders <u>P</u> rogram Folders:	Folder listed below. You may type a new folder list. Click Next to continue.
SafeSign	
Existing Folders:	
CyberLink PowerDVD HP HP LaserJet 1000 IMTV Lavasoft Ad-Aware SE Professional Microsoft Office Real Real RealVNC Storm Codec 5	
InstallShield	< Back Next > Cancel

InstallShield Wizard	
	InstallShield Wizard Complete Setup has finished installing SafeSign on your computer.
	K Back Finish Cancel

程式進行安裝時請稍待片刻,安裝完成,請按『Finish』結束安裝。

7

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

- 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。
- 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。



發給 ····································	發行者 內政部憑證管理中心	到期日 2009/5/4	好記的名 <sup>3</sup> <無>	稱
⊴ 李小華	內政部憑證管理中心	2009/5/4	<無>	
				7
[入① ] _ 匯日	也… 「「「「「」」			進階(A)

#### 三、 無法將憑證匯入 I.E 瀏覽器時

- 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。

Certificate Registration Utility		_ 🗆 ×
<u>File I</u> oken <u>H</u> elp		
Reader or Token Name	Token Status	
CHT Card	operational	
任上统计领码制动法	上继由的上世女书	æ

Token Status
Token Status
absent
的機種型號

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。

Registration Utility		X
<u>File T</u> oken <u>H</u> elp		
Reader or Token Name	Token Status	
	present	
 無法正常偵測到讀-	卡機及卡片資訊	

### 肆、 使用 Microsoft Outlook 2003 進行保密郵件

- 一、 郵件帳號及安全性設定
  - 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。
  - 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。

🕒 Outlook Today - Microsoft Outlook		
結案(F) 編輯(E) 檢視(V) 到(G)	<b>工具(I) 執行(A) 説明(H)</b> 輸入	需要解答的問題
🗄 🔂 新增 🕐 🔹 📑 📑 傳送/接收 🕑	傳送/接收區 ▶   • ◎ • ◎ 上一頁	(B) 🚳 📄 🖪 📲 🦉
郵件 個人	尋找① ▶	2
我的最愛資料夾	Ⅲ 通訊錄(B) Ctd+Shift+B → 相則及通知の)	自訂 Outlook Today(U) 🔤
□ 未讀取的郵件 □ 待處理	<ul> <li>汤 清理 "删除的郵件" 資料夾(2)</li> </ul>	事件
□ 寄件備份	電子郵件帳號(A)	收件匣 0
所有郵件資料夾	<b>∃</b> ]](C)	草稿 0
● ●●●● 日本       ●●●●● 日本       ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	選項(Q) ¥	

3. 點選【安全性】裡的【設定】來增加一個 S/MIME 的設定值。

頃	? >
偏好 加密的 <b>分</b> 子	<ul> <li>郵件設定   郵件格式   拼字檢查 安全性 其他  </li> <li>電子郵件</li> <li>① 外寄郵件的內容及附件加密(匹)</li> <li>□ 在外寄郵件加入數位簽章(D)</li> <li>☑ 當傳送簽名郵件時傳送純文字簽名郵件(I)</li> </ul>
空心地	□ 爲所有 S/MIME 簽名郵件索取 S/MIME 回條 ® 預設設定 (2): □ 設定 ③)
	<ul> <li>安全性區域供您自訂是否可在 HTML 郵件中執行指令碼和主動式內容。</li> <li>區域</li> <li>區域</li> <li>區域設定值 (型)</li> </ul>
下載圖	リ片 一 一 一 一 一 一 一 一 一 一 一 一 一
	● (認證)
	確定 取消 套用(金)

 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。

變更安全性設定		×
安全性偏好設定 安全性設定名稱(S):	· · · · ·	
I		-
密碼編譯格式(F):	S/MIME	•
□ 此密碼編譯郵件	格式的預設安全性設定(I)	
▶ 所有密碼編	澤郵件的預設安全性設定(型)	
安全性標籤([]	) (新增10) 刑除(2)	密碼(2)
憑證及演算法		
簽章憑證:		選擇( <u>C</u> )
雜湊演算法(上):	<u> </u>	
加密憑證:		選擇(出)
加密演算法(L);	v V	
☑ 以簽名郵件傳送	這些憑證(正)	
	確定	取消

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。

安全性設定名稱(3): 我的 S/MIME 設定(	直 (jamie@moica.nat.gov.tw)
密碼編譯格式(E):	S/MIME
✓ 此密碼編譯郵件 ✓ 所有密碼編	
	<u>)  新増型   耐味型   名時世</u>
證次俱算伝 簽章憑證:	李小華
雜湊演算法(A):	SHA1
加密憑證:	李小華 選擇Ш
加密演算法(止):	3DES 💌
	清此) 語音(F)

井 みわれど用 入加 何 0000
▶●● 内政部徳… 〈全部〉 無 2009/
·華 內政部憲 <至部> 無 2009/

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

- 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。
- 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。

SafeSign Login		1
	. <u></u>	<u>0</u> K
PIN :	******	<u>C</u> ancel

 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。

📴 CH-SI - Microsoft Outlook				
結案 E 編輯 E 檢視 (V)	到(G) 工具(T) 執行(A) 說明(H)	輸入需要解答的問題 👻		
分新増化 🔸 🎯 🗙 🎭	回覆 (R) 🦂 全部回覆 (L) 🙈 轉寄 (W) 📑 傳送/接收 (C)	▼   🎝 尋找①   鍵入要尋找的連絡人 🔹 🦉		
郵件 我的最愛資料夾	CH-SI 排列: 日期	■ 最新的在上面 マ▲		
○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○	- 今天			
□2 侍庭理 □2 寄件備份 □2 刪除的郵件	▶ Jamie jamie的數位簽章	下午 5:47		
▶ 草稿 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	☐ 自然人憑證管理中心 保密郵件設定説明文件	下午 5:30 ፻ ❷ 🌾		
所有郵件資料夾				
□ 砂 個人資料夾 □ □ 收件匣 □ CH-SI □ MSA □ Umail ▼				
11 17 争磨				
<b>多</b> 連絡人				
🏂 工作	5			
🗧 🖬 🖉 🐐		<b>_</b>		
472 個項目				

 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。

🖂 我的數(	位簽章 - 郵件 (HTML)	- D ×
檔案E	編輯(E) 檢視(V) 插入(L) 格式(Q) 工具(L) 執行(A) 說明(H)	
🛛 🚑 回覆(	R)   🖓 全部回覆 (L)   🖂 轉寄 (W)   🛃 🐚   号   🔻   🍲   🐴 🗙   🔺	• 🔞 🛱
寄件者: 收件者: 副本:	● Jamie [jamie@moica.nat.gov.tw] 寄件日期: 2006/9/27 (星期三)下午   david@moica.nat.gov.tw	05:52
主旨:	Jamie的數位簽章	
簽名者:	jamie@moica.nat.gov.tw	
本信內含	含我的數位簽章!	4
		¥

 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。

數位簽章	计有效	×
主旨: 寄件者: 簽名者:	我的數位簽章 Jamie jamie@moica.nat.gov.tw 此郵件的數位簽章為[有效]且[受信任的]。	
-	如需有關用於郵件數位簽章憑證的詳細資訊,請按一下[詳 細資料]。	
	詳細資料(型)	
□ 開啓	郵件之前,警告我關於數位簽章電子郵件的錯誤。(W) [[關閉(C]]]	-

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。

 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。

ģ視憑證 ? ×
一般 ┃詳細資料   憑證路徑 信任   [信任狀態] 可表示您是否信任擁有這個憑證的個人、團體或公司。
憑證也可用於特定目的如收送電子郵件、信任擁有憑證的網站等等。
信任的憑證 電子郵件加密及驗證
给起库红、赞酒
○ 沿用發行者的信任 ● 明確宣告信任這個憑證 ● 明確宣告信任這個憑證
確定

 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。

郵件安全性內容	1
▲ 主旨: 數位簽章	
郵件中可能含有加密或數位簽章層。每個數位簽章層可能包含多個簽 名 	
<b>支王在局款</b> 在下面選取一層以檢視其描述。(2)	
<ul> <li>✓ 主旨:數位簽章</li> <li>▲ 數位簽章層級</li> <li>▲ ✓ 簽名者: david@moica.nat.gov.tw</li> </ul>	
 描述(D):	
確定: 簽名者為david@moica.nat.gov.tw(使用 RSA/SHA1 於 下午 12:18:28 2006/9/28)。	
按一下下列任何按鈕來檢視選取層的詳細資訊,或對選取層進行變更:	
編輯信任 (四) 檢視詳細資料 (7) 信任憑證授權 (1)	
□ 永遠警告數位簽章電子郵件中的錯誤(W) 關閉(C)	

10. 點選【檢視憑證】可清楚的看到憑證簽發單位及效期。

🧫 签名資訊		馬登雪麗 法教育部
郵件格式: 签名者: 签名状態: 签名时間: 摘要 <b>演</b> 首法·	S/MIME david@moica.nat.gov.tw 確定 下午 12:18:28 2006/9/28 SHA 1	這個意識的使用目的如下: •保護電子郵件訊息
签名演算法:	RSA (1024 位元)	<b>登給:</b> 王大偉 <b>登行者:</b> 內政部憑證管理中心
<b>登</b> 行者: <b>●意意状態</b> :	C=TW, O=行政院, OU=內政部憑證管 💼 確定	有效期自 2006/4/4 到 2011/4/4

 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。

🛁 我的數位簽章 - 郵件 (HTM	L)	
結案(P) 編輯(E) 検視()	7) 插入(1) 格式(0) 工具(1) 執行(2) 説明(日)	- 0 "
至中國復(K) 至前回復( 寄件者: Jamie Jamie Jamie 收件者: david @mouca.na 副本: 主旨: Jamie的數位簽章 簽名者: jamie @moica.nat.	2) □ 轉母(W) □ 每件日期: 2006/9/27 (星期三)下午 Jamie [jamie@moica.nat.gov.tw] 不是線上連絡人 Ⅲ 排定會議時程(E) 呼叫(L) ● 傳送郵件(jamie@moica.nat.gov.tw)(I) 新增至訊息連絡人(M)	05:52
5%H 35% I ⊥ 98 +	<ul> <li>其他動作①)</li> <li>建立規則(R)</li> <li>傳送選項(O)</li> <li>新增至 Outlook 連絡人(N)</li> <li>建尋 Outlook 連絡人(U)</li> </ul>	>
	Outlook 內容(K) 建製(Y)	7

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。

転置 ( )	內容 愛 ┃詳細資料┃憑證路徑┃信任 ┃	? ×
	<ul> <li></li></ul>	
	<b>瓷給:</b> 李小華	
	<b>登行者:</b> 内政部憑證管理中心	
	<b>有效期自</b> 2006/9/11 <b>到</b> 2011/9/11	
		發行者聲明(3)
		「確定」

- 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。

全保密郵件測	試 - 郵件	- D ×
· 檔案 E 編	輯(E) 檢視(Y) 插入(I) 格式(2) 工具(I) 表格(A) 視窗(W) 説明(H)	×
; 🖃 傳送(3)	🔰 -   💷 🍫   🧏 🕴   🔻   🍅   🖹 選項@   HTML 🛛 💽 種類 🗋	
🛄 收件者	jamie@moica.nat.gov.tw	
🛄 副本	司大师忠敏魂自不	fer 1
主旨:	保密郵件測試 「現在の一個人の一個人の一個人の一個人の一個人の一個人の一個人の一個人の一個人の一個人	<i>岩</i> ^□
10 0 X	■ 📇   新細明體 - 11 - <u>A</u> -   B I U - 【郵件加密】。	
保密郵件 ↓ 内政 網址 客服	測試↩ 部自然人憑證管理中心 ↓ : <u>http://moica.nat.gov.tw</u> ↓ 信箱:cse@moica.nat.gov.tw ↩	* * *

## 伍、 使用 Microsoft Outlook Express 進行保密郵件

#### 一、 郵件帳號及安全性設定

- 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。
- 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。

祭網路帳戶			?
全部 郵件	新聞   目錄服務		, 新增(鱼) ▶
帳戶	類型	連線	移除( <u>R</u> )
amoica.nat.gov.tv	/ 郵件 (預設)	任何可使用的	内容(P)
			目的成績目的(南方))
			Se 3 (D)
			設定順序(2)
			關閉

 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。

😪 moica.nat.gov.tw (1) 內容	? ×
一般   伺服器   連線   安全性   進階	
憑證簽章	
請在下面選擇簽章憑證,這個帳戶的簽章郵件會使用這個 數位識別碼。	
憑證(C): [選擇(C)	
加密選項設定	
諸選擇加密憑證及演算法,這會加入您數位簽署的郵件, 其他人就可以使用這個設定傳送加密郵件給你。	
憑證(E): 選擇(L)	2
演算法: 3DES ▼	
	用(企)

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。

田 毎 2009/3/2	内政部碼 《全部》	52.13-8	24H
10001011	I DEVINE PARTY AND A DEPENDENCE	∖華 内政部憑	李小華

 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。

😤 moica.nat.gov.t	w (1) 內容	? ×
一般   伺服器	ま│連線 安全性   進階	
憑證簽章		
請在下面選 數位識別碼	署簽章憑證,這個帳戶的簽章郵件( 。	會使用這個
憑證(C):	李小華	選擇(2)
加密選項設定		
諸選擇加密 其他人就可	愚證及演算法,這會加入您數位簽 以使用這個設定傳送加密郵件給你	署的郵件, 。
憑證(E):	李小華	選擇(止)
演算法:	3DES 💌	
	3DES RC2 (128-bit) RC2 (64-bit) DES RC2 (40-bit)	

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

- 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。
- 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。

1 我的數位	簽章											
檔案E	編輯(E)	檢視(♡)	插入①	格式(0)	工具( <u>T</u> )	郵件(M)	說明( <u>H</u> )			~		
● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	が	して、	日期上	<b>り</b> 復原	<b>会</b> 検査	AB E 拼字机	)	↓ 「 「案 優先順」	, •	資金	加密	×
國收件者	: davi	d@moica.	nat.gov.tw							郵件加入	數位簽章	(2)
[1] 副本:												V
主旨:	我的	數位簽章										
新細明體		•	10 💌	⊡_ B	IUA	<b>}</b>    Ξ	∃\$≢\$₽	E ± i		- 🐁 🛛	2	
体信内	含我的數价	立簽章!										
h.												

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。

and the second se
<u>0</u> K
<u>C</u> ancel

 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。

🗐 收件匣 - Outlook Express			_ 🗆 🗙
」 檔案(E) 編輯(E) 檢i	視(V) 工具(I) 郵件(M) 說明(H)		
▶ <b>●</b> ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	会新回覆         会         人         L <thl< th=""> <thl< th=""> <thl< th=""> <thl< th=""></thl<></thl<></thl<></thl<>	● 傳送/接收 通訊錄 尋找	
✿ 收件匣		Ĩ	<b>尋找</b>
資料夾 ×	! 0 や 寄件者 主		收件日期  △
<ul> <li>↓ Outlook Express</li> <li>→ 体積資料夾</li> <li>→ ゆ 收件匣</li> <li>→ 切 容件匣</li> <li>→ 切 容件備份</li> <li>● 切 剛除的郵件</li> <li>→ 切 草稿</li> </ul>	<b>♀</b> 小華 	的數位簽章	2006/9/21 F
	<b>寄件者:</b> 李小華 收件者: jamie@mo 主旨: 我的數位簽章	ica.nat.gov.tw	
連絡人(C) ▼ × Pweb 全用戶 李誠 全別失小蔵		安 經數位簽	至性說明 🥐 ]
፼⊇施小棋	🔒 這個郵件已由寄件者數位簽	署。	
	其他人簽署的電子郵件可以 的零件夹,而日本值沿時+	讓您檢查郵件的正確性 也就 她甘他人 新潟毛腳。 签罢的重	就是說郵件是來自正確 那任旦右軍層的答案那 」
2 封郵件,0 封尚未閱讀			1.

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。

MOICA jamie 內容
摘要 名稱 住家 公司 個人 其他 NetMeeting 數位識別碼
選擇電子郵件地址(E):
jamie @moica.nat.gov.tw
與選擇的電子郵件地址關聯的數位識別碼(D):
✓ jamie@moica.nat.gov.tw(損設) 移除(型) 設成預設値(③)
<u>匯入(M)</u> 匯出(X)

- 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。
- 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。

1 加密郵件	測試											
」檔案E	編輯(王)	檢視(♡)	插入①	格式(0)	工具(I)	郵件(M)	說明(H)					
● 「「」 傳送	斯下	自主	日期上	<b>り</b> 復原	<b>会</b> 檢查	AB 拼字檢	· ( 查 附加	<b>〕</b> 檔案 偐	↓! ●先順序	资章	加密	) <sup>»</sup>
國收件者	: 李小	華										8
[]]] 副本:												8
主旨:	加密	郵件測試										
新細明體		<b>_</b>	10 -	<u>I</u> ∃_ B	I U A	. I I≣ B			± 1	- 🔍 🛛	<u></u>	
				•							_	-
這是一封) 	加密郵件)	則試信!										
1												

#### 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。

的演算法,建議可使用預設值即可。

- 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

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。