非IC卡類憑證及伺服器應用軟體憑證作業及應用說明

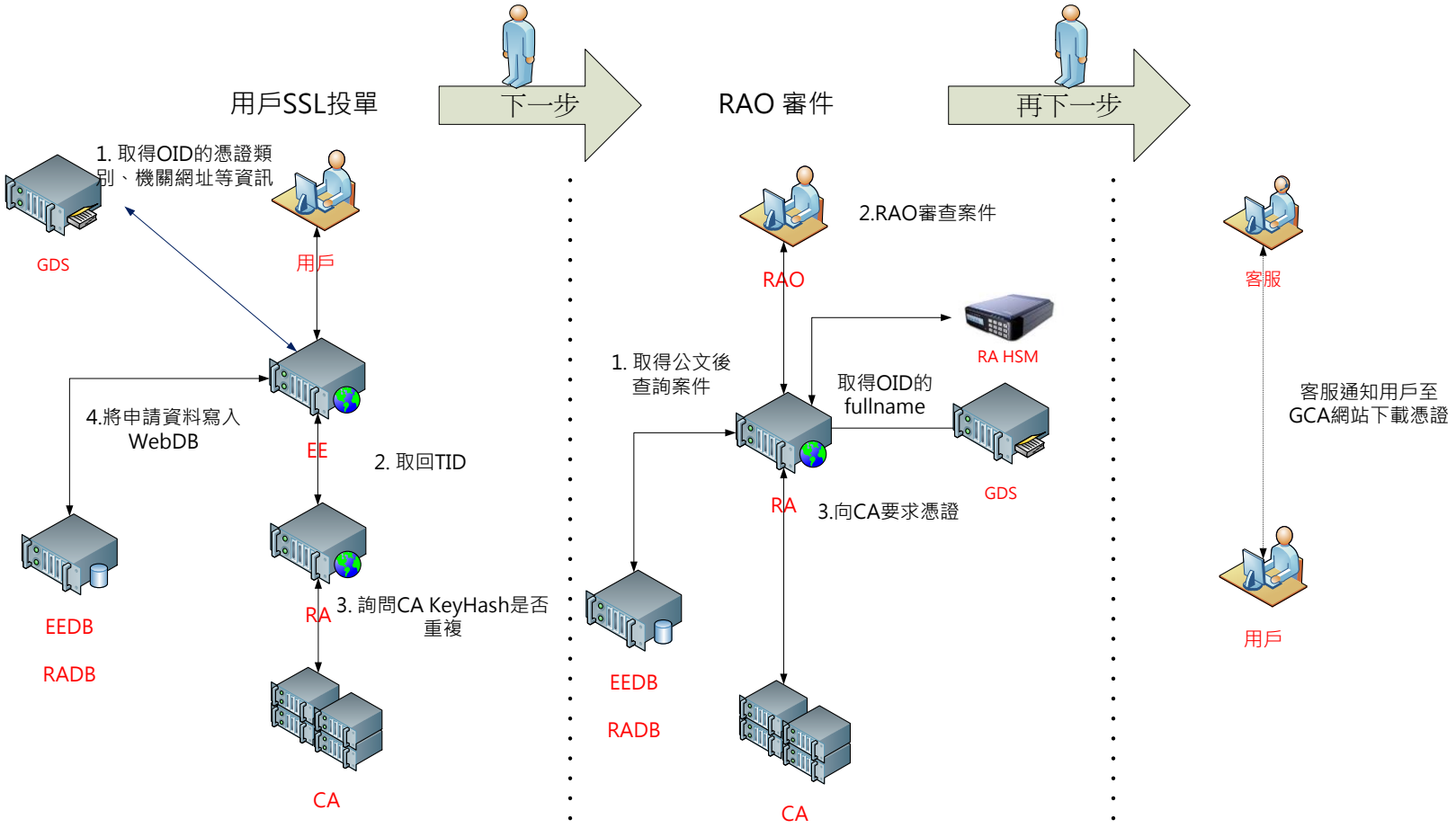
Outline

- GCA非IC卡類及伺服器應用軟體憑證介紹
- GCA 伺服器應用軟體憑證-以SSL為例
  - 處理流程
  - 用戶投單

GCA非IC卡類及伺服器應用軟體憑證介紹

憑證種類	對應用途	憑證註記事項	說明
非IC卡類簽章憑證	寄送簽章電子郵件、機關電子關防	機關名稱、email地址	
非IC卡類加密憑證	寄送加密電子郵件、機關保密資料	機關名稱、email地址	不能用於SSL
伺服器應用軟體加密憑證	網站SSL憑證	應用伺服器名稱，URL	不能用於電子郵件
伺服器應用軟體簽章憑證	應用伺服器認證，如ICS及伺服器資料交換	應用伺服器名稱，URL	不能用於電子郵件

處理流程-以SSL為例


用戶SSL投單
下一步
RAO 審件
再下一步
1. 取得OID的憑證類別、機關網址等資訊
GDS
用戶
4.將申請資料寫入WebDB
EE
2. 取回TID
EEDB
RADB
RA
3. 詢問CA KeyHash是否重複
CA
2.RAO審查案件
RAO
RA HSM
1. 取得公文後查詢案件
取得OID的fullname
RA
3.向CA要求憑證
GDS
EEDB
RADB
CA
客服
客服通知用戶至GCA網站下載憑證
用戶

用戶投單-以SSL為例(步驟1)

用戶投單-以SSL為例(步驟1)

- OID新增及異動申請服務
- 憑證IC卡屆期換發

憑證及IC卡相關作業

表單及資料下載

憑證應用

常用問答集

客戶服務專區

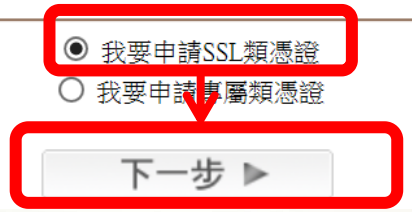
電子憑證應用程式介面配合2048位元改版專區

SSL類伺服應用軟體憑證簽發對象為政府機關（構）、政府單位所建置的SSL（或TLS） Server，例如具有SSL功能的HTTP Server。
專屬類伺服應用軟體憑證之簽發對象為政府機關（構）、政府單位所建置的特殊用途之伺服應用軟體憑證，例如用來提供身分識別服務的Server等。
伺服器應用軟體憑證憑證之效期為3年、專屬類伺服應用軟體憑證為5年。憑證格式請參見政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪，申請時請參考問與答。

填表前，請使用適合於應用系統所使用之密碼模組的工具程式來產製金鑰及憑證請求檔(CSR)，若有疑問請向應用系統開發廠商詢問清楚。

注意事項：

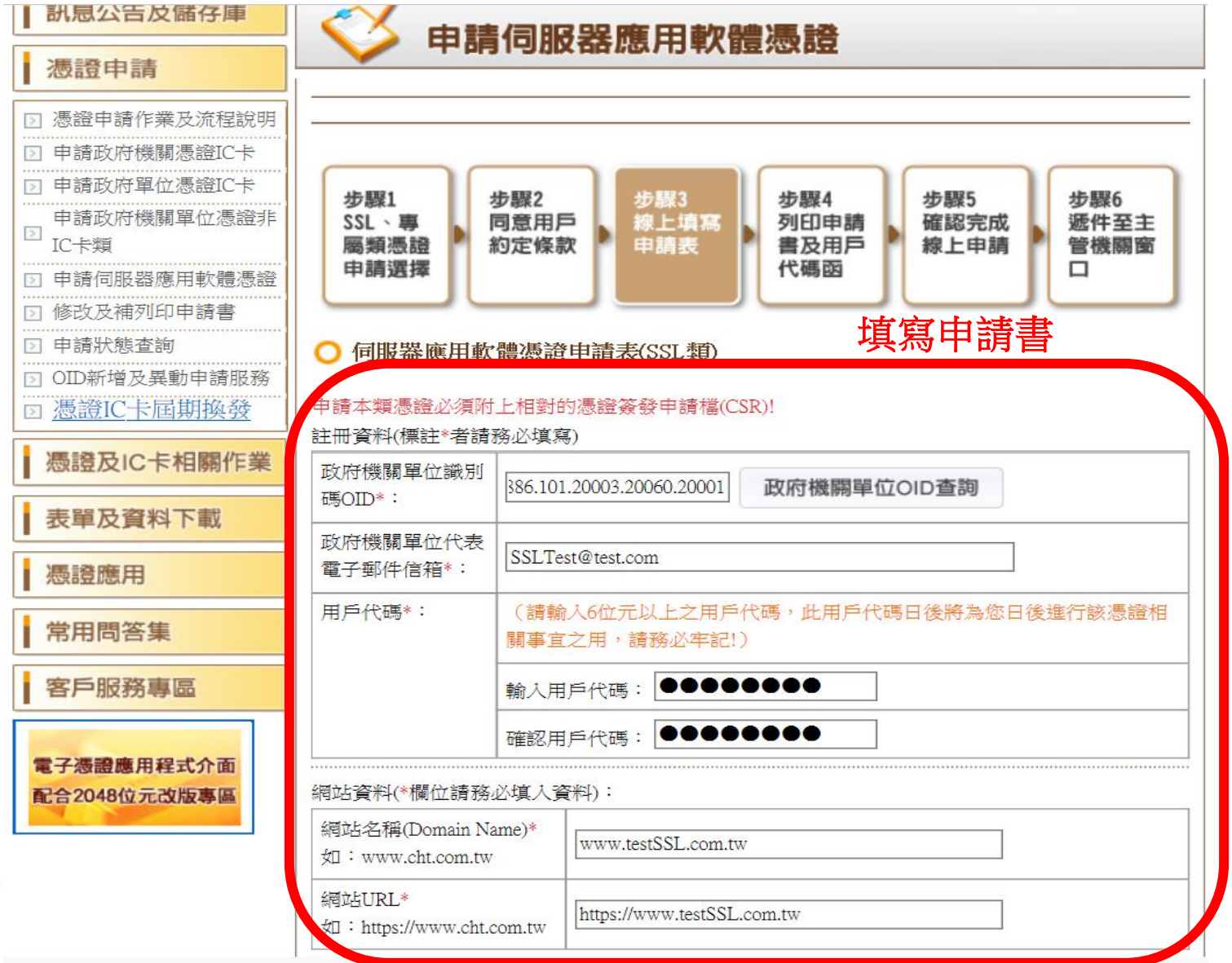
- 一個憑證請求檔(CSR)，只能對應申請一個案號。
- 同一機關多張憑證申請書可以合併於1份公文下遞送，請提供正確之公文附件(憑證申請書)。
- 請多利用公文電子交換將憑證申請書於發文時以PDF檔案格式或影像掃瞄檔附件傳送。
- 憑證申請過程有問題時可先參考“問與答”，若無法解決再請洽客服中心。
- 若申請內容資料不符，將Email通知退件處理；申請書補件請傳真至(02)2344-4724。
- 依據國家發展委員會於98年7月1日函請各機關單位配合2048位元憑證申請時程(發文字號:會訊字第0982460725號)，98年9月1日起只受理2048位元伺服器應用軟體憑證或非IC卡類憑證之申請。
- 國家發展委員會收文時如遇申請案件附件缺漏者，將電話通知申請人於3日內透過傳真補件，如未補件則採退文方式辦理。
- 伺服器應用軟體憑證效期自102年4月1日起，由5年改為縮減為3年。



用戶投單-以SSL為例(步驟2)

用戶投單-以SSL為例(續步驟2)

用戶投單-以SSL為例(步驟3)



用戶投單-以SSL為例(續步驟3)

憑證聯絡人資料(標註*者請務必填寫)

說明：

1.憑證連絡人負責擔任憑證申請的聯絡窗口，需由機關（構）單位相關人員擔任。

2.自101年4月26日起，憑證聯絡人資料表格欄位異動，原「職稱」一欄，已更訂為「憑證用途」，請依業務需要註明憑證用途，以利複審作業進行；若未註明憑證用途或用途不明者，憑證管理中心將以退件方式處理。

姓 名*：	測試SSL
憑證用途*：	測試SSL
公務電子郵件信箱：	testSSL@cht.com
公務通訊地址*：	桃園縣 楊梅市 326 電研路99號
公務電話*：	03-4245161
公務傳真：	

憑證請求檔（CSR）上傳

說明： 請將您所製作完成的憑證請求檔（CSR）上傳，請輸入檔案所存放之位置，可按"瀏覽"按鈕尋找您的檔案

來源檔案路徑：	C:\Users\akdsy\Desktop\test 瀏 覽

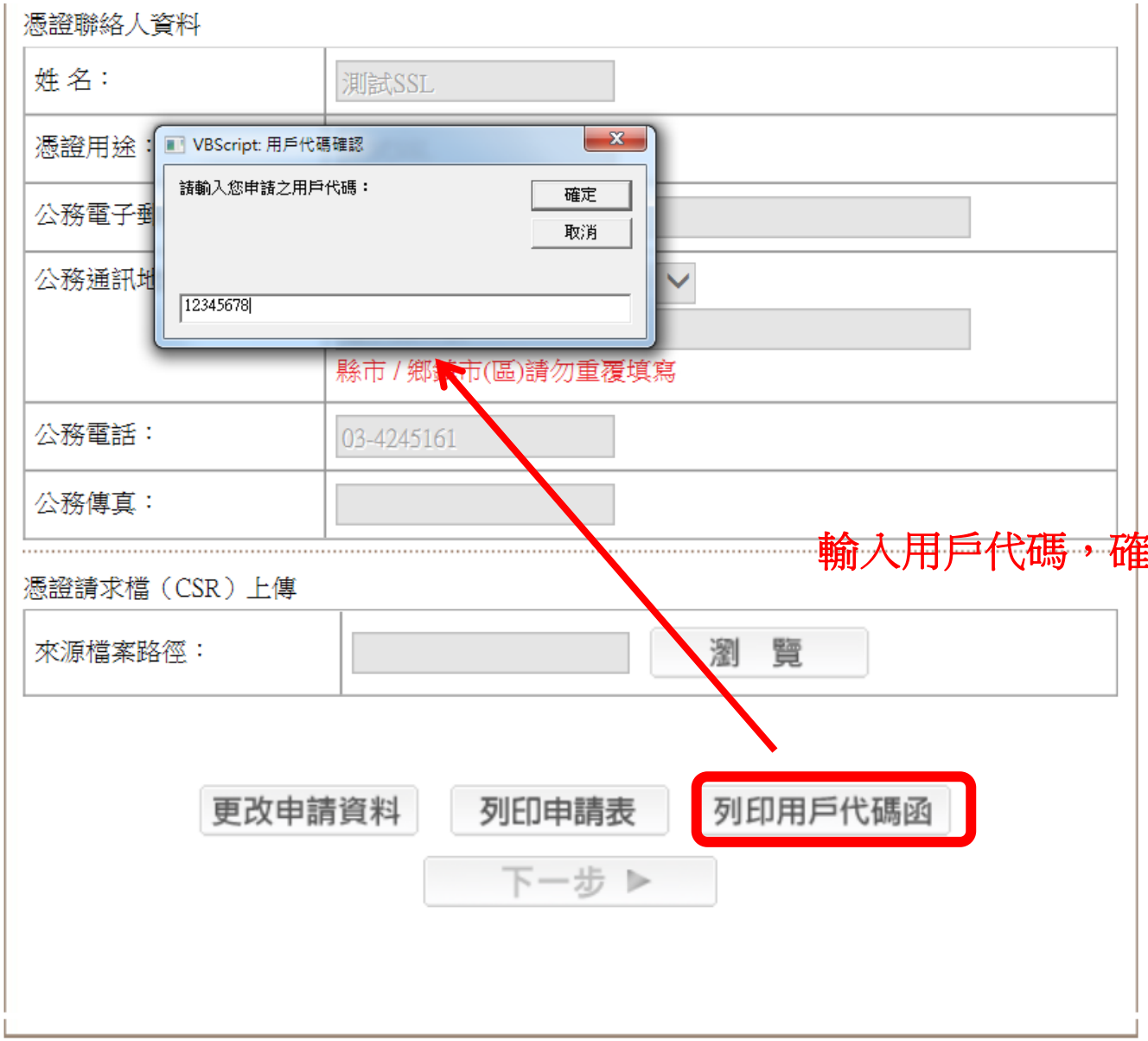
儲存申請資料　讀取儲存資料　務必上傳申請資料

填寫申請書

CSR檔來源

用戶投單-以SSL為例(步驟4)

用戶投單-以SSL為例(續步驟4)



用戶投單-以SSL為例(續步驟4)

- 用戶代碼函

用戶代碼函

※此用戶代碼日後將為您日後進行該憑證相關事宜之用，本憑證管理中心無法提供查詢用戶代碼之功能，請務必妥善保存!

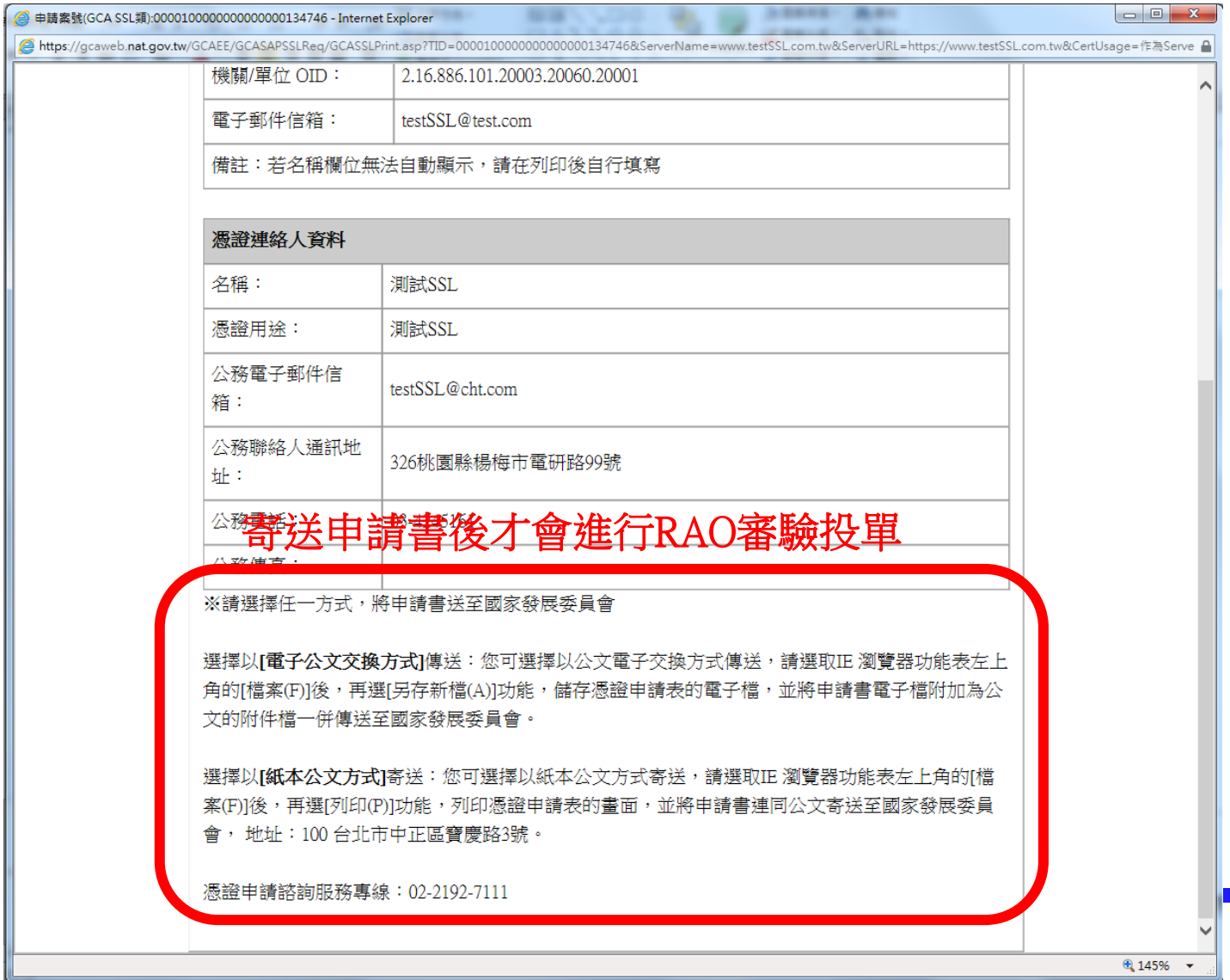
用戶代碼資料	
案件流水號：	00001000000000000000134746
用戶代碼：	12345678

憑證申請諮詢服務專線：02-2192-7111
(開放時間 08:00-18:00，例假日暫停服務)

用戶投單-以SSL為例(續步驟4)

- 申請書

用戶投單-以SSL為例(續步驟4)



用戶投單-以SSL為例(步驟5)

用戶投單-以SSL為例(步驟6)

寄送申請書後才會進行RAO審驗投單

憑證相關檔案格式介紹(1/3)

- 私密金鑰(Private Key)，未加密Base64格式

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA7Oyjvmm06Bc8QQ
hKPNIG5wsli/jpgK/cQAbtaJ2inh084F6PsJQ
STQN394OmzSVwBXkuTfkCmUzgeef+w6
……..
O0+/A9jwHWynn5v9CPGcOz1MkdBqeq6l
+Af4hrqA==
-----END RSA PRIVATE KEY-----

- 憑證請求檔(Certification Request, CSR)，Base64格式

-----BEGIN CERTIFICATE REQUEST-----
MIICijCCAXICAQAwRTELMAkGA1UEB
hMCVFcxEzARBgNVBAgMClNvbWUtU3
RhdGUxITAfBgNVBAoMGEludGVybmV0
……
WT2uxZRLEXM11au25oGhU59Ne70G0Ffr
LEAl+6pbwNar0aVrwRD6CkAHJam14TB1
u
-----END CERTIFICATE REQUEST-----

憑證相關檔案格式介紹(2/3)

- 憑證(Certificate)，Base64格式

```
-----BEGIN CERTIFICATE-----
MIIEojCCA4qgAwIBAgIQQmeHpxUnWJz
uqf6JLa6tAjANBgkqhkiG9w0BAQsFADB
W
……
5W3Bk0j7FaDnbU1dx+hTMDArGXkYXe/
Ejy/LKAnaAlnfMNpr/v8=
-----END CERTIFICATE-----
```

- 根憑證(Root Certificate)，Base64格式

```
-----BEGIN TRUSTED CERTIFICATE-----
MIIFYzCCA0ugAwIBAgIRAO7bq64VfoW
1uTykycGzeIYwDQYJKoZIhvcNAQELBQ
Aw
……
5W3Bk0j7FaDnbU1dx+hTMDArGXkYXe/
Ejy/LKAnaAlnfMNpr/v8=
-----END TRUSTED CERTIFICATE-----
```

憑證相關檔案格式介紹(3/3)

常見附檔名	檔案內容	用途說明
.pfx	PKCS#12 憑證/金鑰封裝檔	金鑰匯入匯出、備份，或是在不同應用伺服器交換使用(如IIS轉至tomcat)
.p7b	PKCS#7 多張憑證封包	將多張憑證封於單一檔案，常用於存放CA憑證
.jks	Java金鑰儲存檔	以Java keytool工具產製的金鑰/憑證儲存檔

伺服器應用軟體憑證(SSL類)安裝及應用說明

內容

- 伺服器應用軟體憑證(SSL類)安裝教學
- SSL類憑證常見問題集
- OCSP Stapling
  - 介紹說明
  - 運轉模式
  - GCA OCSP Stapling配合作業
  - Apache OCSP Stapling運轉測試

伺服器應用軟體憑證(SSL類)安裝教學

- 各式伺服器安裝教學資料，包含Weblogic/ Tomcat/ Apache/ Microsoft IIS
  - http://gca.nat.gov.tw/05-02.html
- Microsoft IIS安裝簡介
- Apache安裝簡介
- Tomcat安裝簡介

SSL類憑證常見問題集

- Windows IIS
  - SHA2支援性(Win2000與XP SP2以下不支援)
  - 匯入GRCA, GCA要匯入正確憑證串鍊：GRCA(根憑證)->New-with-Old(中繼)->GCA2(中繼)
  - IIS就算匯入GRCA，GCA2憑證，Firefox還是會出現憑證串鍊無法串起來的問題(IIS的問題)
  - Win2003更新憑證時，很容易出現新金鑰被覆蓋的問題，要先備份
  - Win2003若要一次申請兩張憑證時，會出現新申請的私密金鑰覆蓋先申請的那把私密金鑰，所以要注意備份，2003私密金鑰會被後產製的覆蓋，而2008以上則無此問題

SSL類憑證常見問題集

- Apache
  - 直接用GCA的p7b檔，再用openssl轉為Base64格式
  - 憑證要轉為Base64格式，可用Windows或Openssl完成
  - httpd-ssl.conf需要設定對應的私密金鑰與憑證放置目錄
  - 請注意 private key檔案的保存
- 手機支援性
  - Android目前無法支援GCA SHA2 SSL憑證
  - iOS已經有植入GRCA2憑證等

SSL類憑證常見問題集

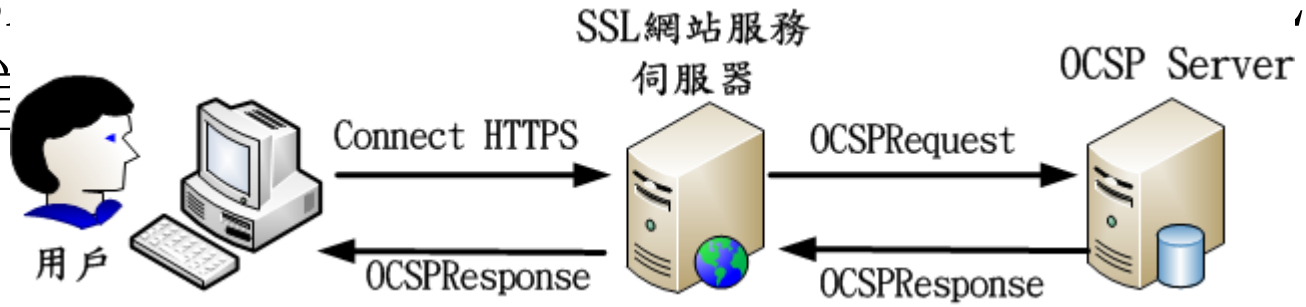
- Tomcat
  - 重複執行產製金鑰會導致原本的金鑰被後面產製的金鑰覆蓋，因而與實際申請憑證的CSR對不起來
  - Keystore很容易匯入錯誤，例如：alias名稱不一致
  - 匯入client憑證時，alias name請匯入到之前建立keystore所使用的alias name或是 privatekey entry
  - GRCA, GCA憑證需依照手冊順序匯入，匯錯順序就無法串起來串鍊
  - 憑證若匯錯後，建議移除所有憑證，但private key entry請不要刪除，之後使用原private key透過openssl產生自簽憑證，再匯入到privatekey entry，以打斷原本匯入錯誤的憑證串鍊，匯入自簽憑證後，再依序重新匯入所有憑證
  - 匯入時，請確認匯入的 Keystore檔是之前產生的那個

OCSP Stapling介紹說明

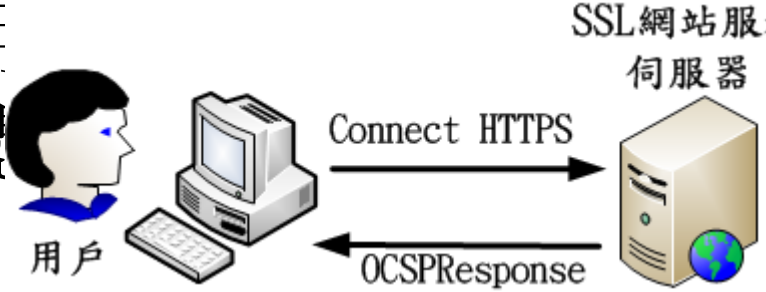
- 起因
  - 用戶每次連線SSL網站服務，就得向OCSP Server確認此SSL憑證是否有效。
  - 另一個衍伸隱私的問題：為OCSP Server會知道”用戶試著連到使用這個 SSL certificate”的相關資訊。
  - 為了加速SSL網站的SSL憑證的驗證，以完成即時線上SSL憑證狀態之驗證作業，故產生此OCSP Stapling運作模式之設計。
- OCSP Stapling
  - 藉由 SSL網站服務伺服器向 OCSP server 要一次有”時間限制”的 OCSPResponse訊息之後，下次該SSL網站服務直接回傳 此OCSPResponse 給予用戶 (通常是Internet Browser)， 以避開了前述狀況。

OCSP Stapling運轉模式

- SSL網站服務第一次被連線與觸發SSL憑證驗證



- SSL網站服務 被連線與觸發SSL憑



GCA OCSP Stapling配合作業

- GCA OCSP Server服務主程式進行新增與改版
  - GCA OCSP Server必須確實地進行系統時間校時作業
  - 所回覆的OCSPResponse訊息封包之ThisUpdate屬性值必須為GMT格林威治時間
  - 所回覆的OCSPResponse訊息封包需要新增NextUpdate屬性值，且此時間欄位必須為GMT格林威治時間
  - GCA OCSP Server主程式必須能夠產製這樣格式的新型OCSPResponse訊息封包給予用戶

Apache OCSP Stapling運轉測試

- 模擬系統環境如下:
  - 使用GCA OCSP Server SHA256
    http://gca.nat.gov.tw/cgi-bin/OCSP2/ocsp_server.exe
  - 使用 Openssl s_client工具進行模擬測試
    - 指令為 /usr/local/ssl/bin/openssl s_client -connect yourIP:443 -tls1 -tlsextdebug – status
  - 接續分成第一次與第二次測試結果來說明

第一次測試先取得OCSPResponse

- 模擬GCA OCSP Server SHA256之Apache HTTP Server LOGS
  - 證明SSL網站確實有來詢問OCSP Server以取得OCSPResponse

```
[root@RH5_GCAXCA logs]# pwd
/export/httpd-2.2.27/logs
[root@RH5_GCAXCA logs]# cat GCA-access_log
192.168.133.250 - - [06/Aug/2014:15:02:24 +0800] "POST /cgi-bin/OCSP2/ocsp_serve
r.exe HTTP/1.0" 200 1542
```

- 模擬SSL網站之Apache HTTP Server LOGS

```
[root@rhtest logs]# pwd
/export/httpd-2.4.10/logs
[root@rhtest logs]# cat ssl_access_log
192.168.133.250 - - [06/Aug/2014:15:02:45 +0800] "-" 408 -
[root@rhtest logs]# cat ssl_request_log
[06/Aug/2014:15:02:45 +0800] 192.168.133.250 TLSv1 ECDHE-RSA-AES256-SHA "-" -
```

OCSP驗證畫面

```
[root@rhtest extra]# date
鈥?  8? ?  6 15:02:08 CST 2014
[root@rhtest extra]# date
鈥?  8? ?  6 15:02:22 CST 2014
[root@rhtest extra]# /usr/local/ssl/bin/openssl s_client -connect 192.168.133.250:443 -tls1 -tlsextdebug -status
CONNECTED(00000003)
TLS server extension "renegotiation info" (id=65281), len=1
0001 - <SPACES/NULS>
TLS server extension "EC point formats" (id=11), len=4
0000 - 03 00 01 02                                      ....
TLS server extension "session ticket" (id=35), len=0
TLS server extension "status request" (id=5), len=0
TLS server extension "heartbeat" (id=15), len=1
0000 - 01                                               .
depth=1 C = TW, O = TL, OU = GCA
verify error:num=20:unable to get local issuer certificate
verify return:0
OCSP response:
======================================
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = TW, O = TL, OU = GCA, OU = OCSP Server, serialNumber = 00000000013018257
    Produced At: Aug  6 07:02:24 2014 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: A9A56FD34796CB6113264BCA4CEADC06D500081C
      Issuer Key Hash: 783CCB3C5EF26BE931B529404B4481F941B6559A
      Serial Number: B030E6BB703C41B5855370DADB329F9B
    Cert Status: good
    This Update: Aug  6 07:02:24 2014 GMT
    Next Update: Aug  6 09:02:24 2014 GMT
```

第二次測試由SSL網站直接回傳OCSPResponse

- 模擬GCA OCSP Server SHA256之Apache HTTP Server LOGS
  - 經過10分鐘左右的再測試，證明SSL網站沒有再來詢問OCSP Server

```
[root@RH5_GCAXCA logs]# date
鈅?  8? ?  6 15:13:04 CST 2014
[root@RH5_GCAXCA logs]# cat GCA-access_log
192.168.133.250 - - [06/Aug/2014:15:02:24 +0800] "POST /cgi-bin/OCSP2/ocsp_serve
r.exe HTTP/1.0" 200 1542
```

- 模擬SSL網站之Apache HTTP Server LOGS
  - OCSP Stapling模式直接回傳OCSPResponse給予用戶端

```
[root@rhtest logs]# pwd
/export/httpd-2.4.10/logs
[root@rhtest logs]# date
鈅?  8? ?  6 15:17:24 CST 2014
[root@rhtest logs]# cat ssl_access_log
192.168.133.250 - - [06/Aug/2014:15:02:45 +0800] "-" 408 -
192.168.133.250 - - [06/Aug/2014:15:08:43 +0800] "-" 408 -
192.168.133.250 - - [06/Aug/2014:15:11:57 +0800] "-" 408 -
[root@rhtest logs]# cat ssl_request_log
[06/Aug/2014:15:02:45 +0800] 192.168.133.250 TLSv1 ECDHE-RSA-AES256-SHA "-" -
[06/Aug/2014:15:08:43 +0800] 192.168.133.250 TLSv1 ECDHE-RSA-AES256-SHA "-" -
[06/Aug/2014:15:11:57 +0800] 192.168.133.250 TLSv1 ECDHE-RSA-AES256-SHA "-" -
```

OCSP驗證畫面

- 經過10分鐘再測試的結果
  - 經過10分鐘之後測試，一樣只取得十分鐘前的OCSPResponse

```
[root@rhtest extra]# date
鍗?  8? ?  6 15:11:30 CST 2014
[root@rhtest extra]# /usr/local/ssl/bin/openssl s_client -connect 192.168.133.250:443 -tls1 -tlsextdebug -status
CONNECTED(00000003)
TLS server extension "renegotiation info" (id=65281), len=1
0001 - <SPACES/NULS>
TLS server extension "EC point formats" (id=11), len=4
0000 - 03 00 01 02                                      ....
TLS server extension "session ticket" (id=35), len=0
TLS server extension "status request" (id=5), len=0
TLS server extension "heartbeat" (id=15), len=1
0000 - 01                                               .
depth=1 C = TW, O = TL, OU = GCA
verify error:num=20:unable to get local issuer certificate
verify return:0
OCSP response:
======================================
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = TW, O = TL, OU = GCA, OU = OCSP Server, serialNumber = 0000000013018257
    Produced At: Aug  6 07:02:24 2014 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: A9A56FD34796CB6113264BCA4CEADC06D500081C
      Issuer Key Hash: 783CCB3C5EF26BE931B529404B4481F941B6559A
      Serial Number: B030E6BB703C41B5855370DADB329F9B
    Cert Status: good
    This Update: Aug  6 07:02:24 2014 GMT
    Next Update: Aug  6 09:02:24 2014 GMT
```

安全電子郵件介紹

報告大綱

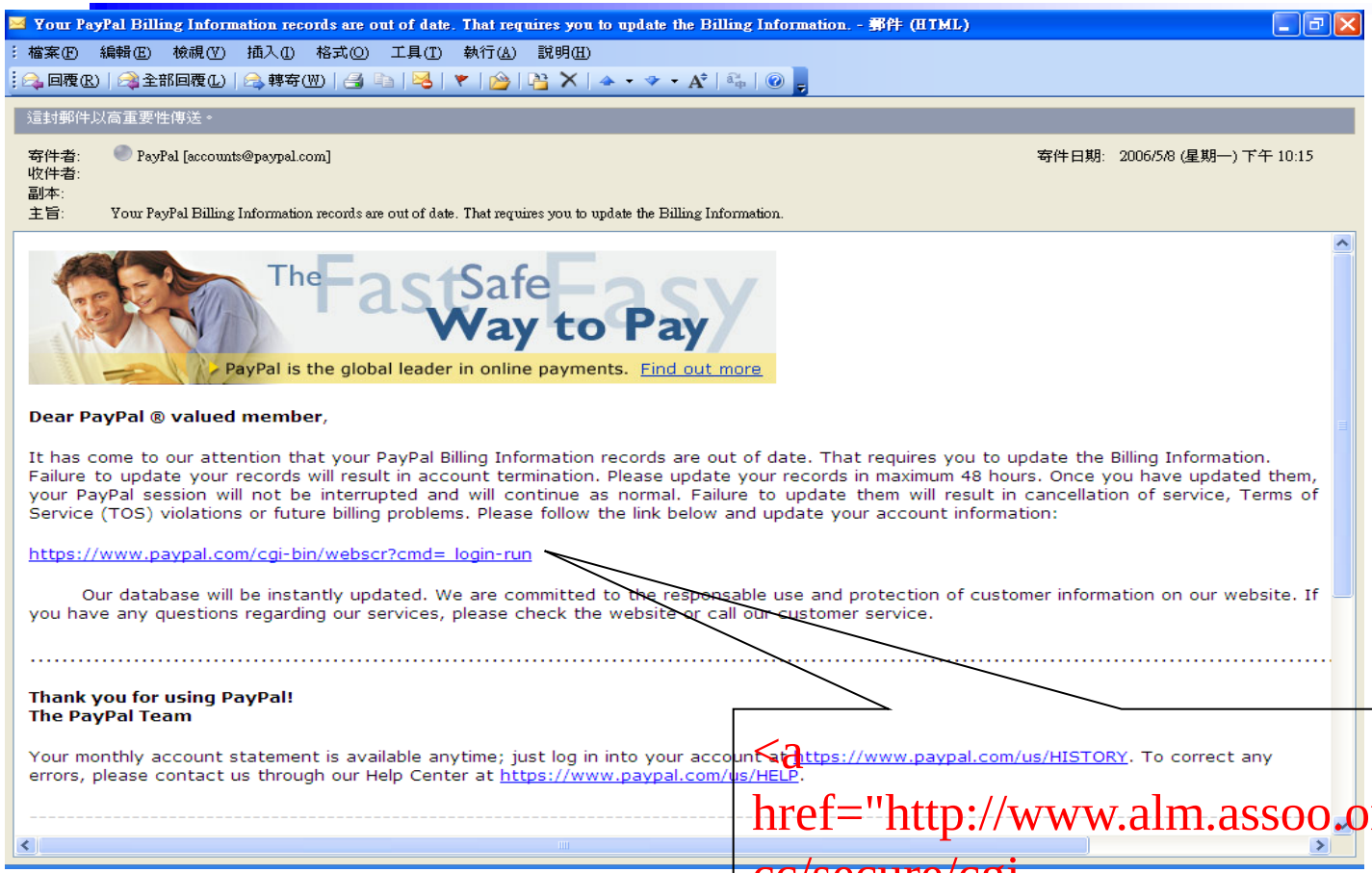
一、為何要使用安全電子郵件
二、安全電子郵件準備工作
三、安全電子郵件設定說明
　　－以Outlook 2010為例
四、Q & A

一、為何要使用安全電子郵件

使用電子郵件所遭遇問題

冒名郵件
垃圾郵件
黑函（詐騙）郵件
病毒(木馬)郵件
釣魚郵件

釣魚郵件




```
<a href="http://www.alm.assoo.org/activites/.acc/secure/cgi-bin/webscrcmd_login.php">https://www.paypal.com/cgi-bin/webscr?cmd=_login-run</a></font></p>
```

冒名郵件

2006/6/6 聯合晚報: 國防部電郵 木馬程式入侵？內部有人搞鬼？記者高凌雲/台北報導

國防部中午針對有人偽冒國防部電子郵件帳號發布新聞稿表示，國防部實施新聞發布均採「紙本傳真、寄送電子郵件及即時簡訊通知」等多重作業程序，媒體若接獲非經本室正常作業程序之電子郵件，請即向本室聯絡查證，俾維新聞正確性。

國防部軍事發言人室表示，昨天傍晚媒體記者查證是否發布新聞稿時，即於第一時間以簡訊向媒體澄清，同時發現軍事發言人室作業用民網電腦硬體內有兩個不明執行檔，已協請資訊部門進行分析瞭解中。

國防部初步調查發現，外界有不明人士將特定郵件寄到國防部信箱中，又有國防部人員在不知情下點選開啟後，使得這個執行檔在國防部的民網電腦中啟動。

軍事發言人室說；國防部設於中華電信多稿傳送信箱，已請中華電信協助查詢該郵件寄送網路位址（IP），以釐清問題癥結。

軍事發言人室說，為避免肇生類似情形，國防部已對作業電腦軟、硬體設施實施檢整，強化提昇作業系統防火牆設定，確保資訊作業安全。

安全電子郵件簡介

傳送電子郵件時可以使用兩項安全功能：

1. **數位簽章**：傳送郵件時加入數位簽章可以確保郵件的**完整性**、**身份鑑別**以及**不可否認性**
2. **加密**：傳送郵件時可以將郵件和附件加密，以確保郵件的**機密性**

數位簽章與加密是兩項獨立的功能，一個郵件可以只加數位簽章但不加密，但是此種郵件只能做為確認寄件者的身分，郵件內容仍以明文形式傳送，無法保持機密；另一方面，一個郵件也可以不加數位簽章而只加密，此種郵件雖然將內容編碼成密文而能夠保持機密，但卻無法確認寄件者身分。

安全電子郵件可使用憑證

MOICA自然人憑證

GCA政府機關(單位)憑證

其他CA憑證(金融憑證、電子商務憑證等)

二、安全電子郵件準備工作

申請GCA非IC卡類憑證(簽章/加解密用)

匯入使用者憑證

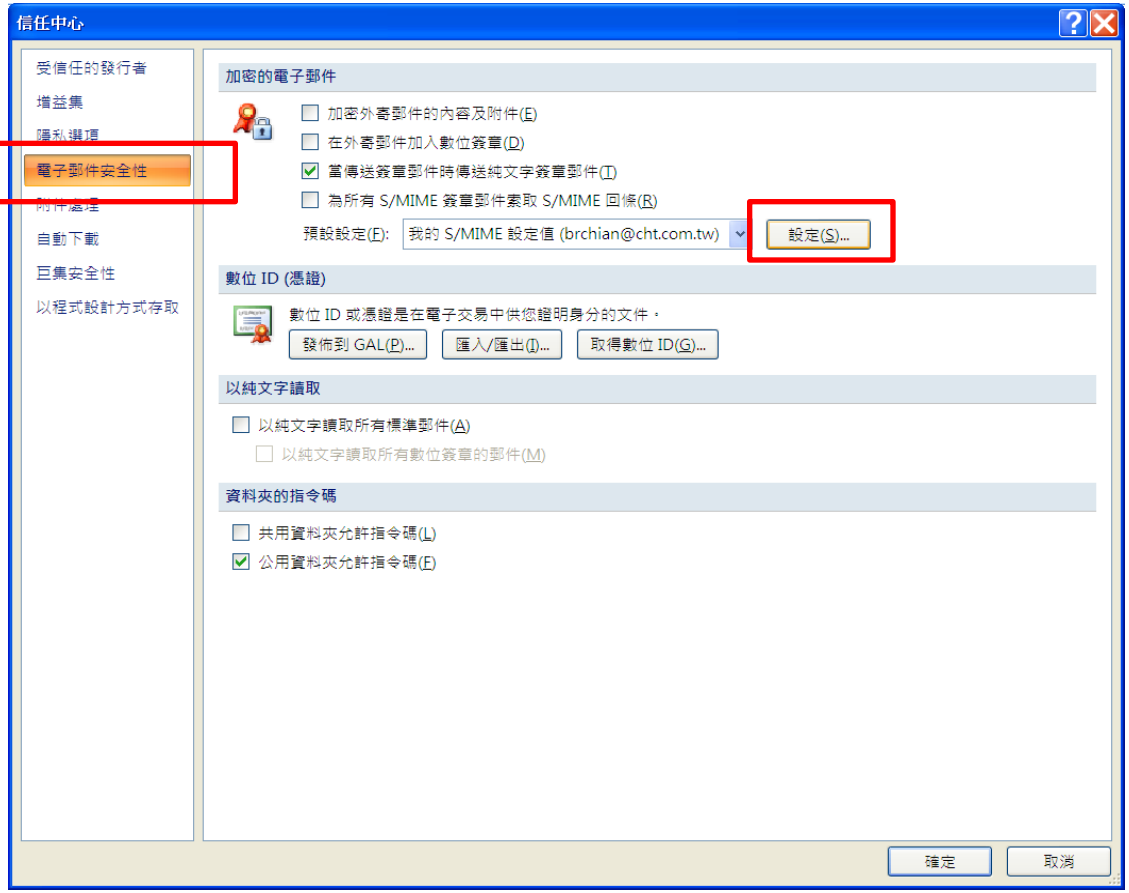
匯入CA憑證

安全電子郵件設定說明

以Outlook 2010為例

安全電子郵件設定

從選單之[工具]->[信任中心]->[電子郵件安全性]->[設定]

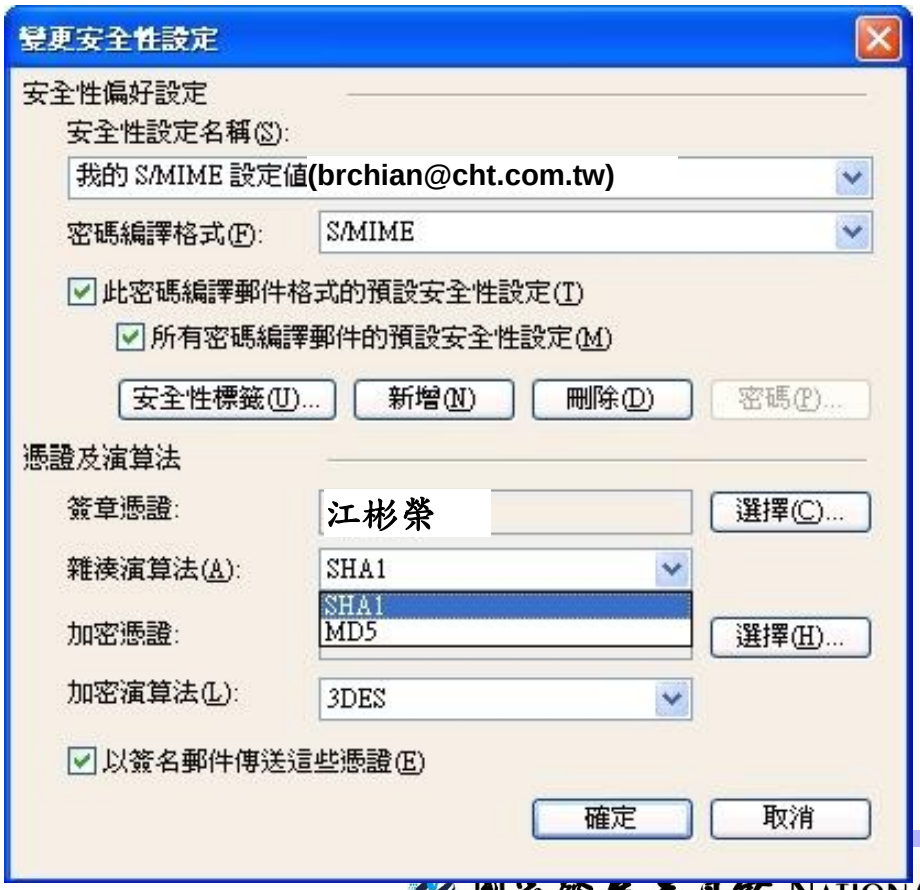


安全電子郵件設定

按[選擇]將此電子郵件帳號之簽章及加密憑證匯入，於[雜湊演算法]選擇SHA1，於[加密演算法]選擇3DES，按[確定]

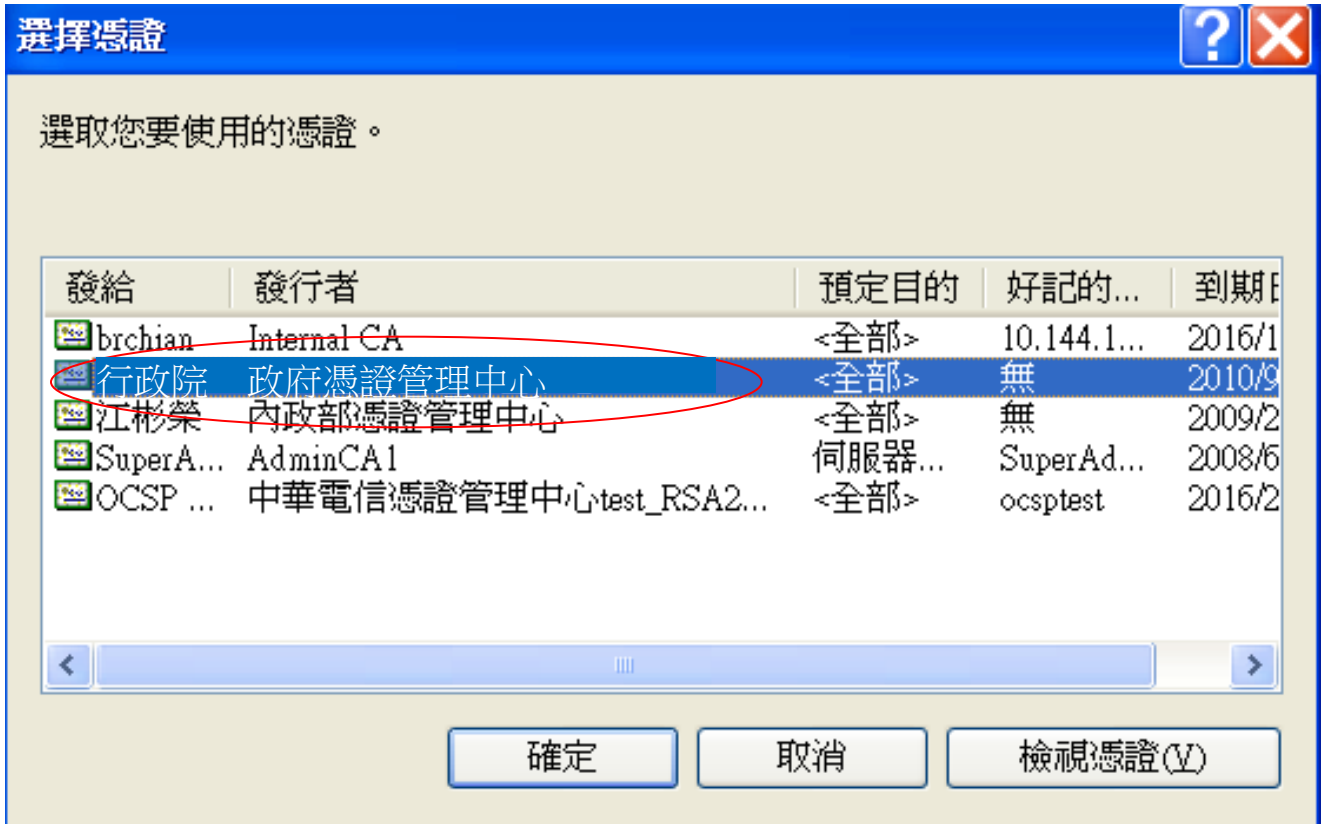
安全電子郵件設定

數位簽章用的雜湊函數演算法有SHA1與MD5兩種，請記得要選擇SHA1，加密所用之演算法選擇強度最強之3DES。



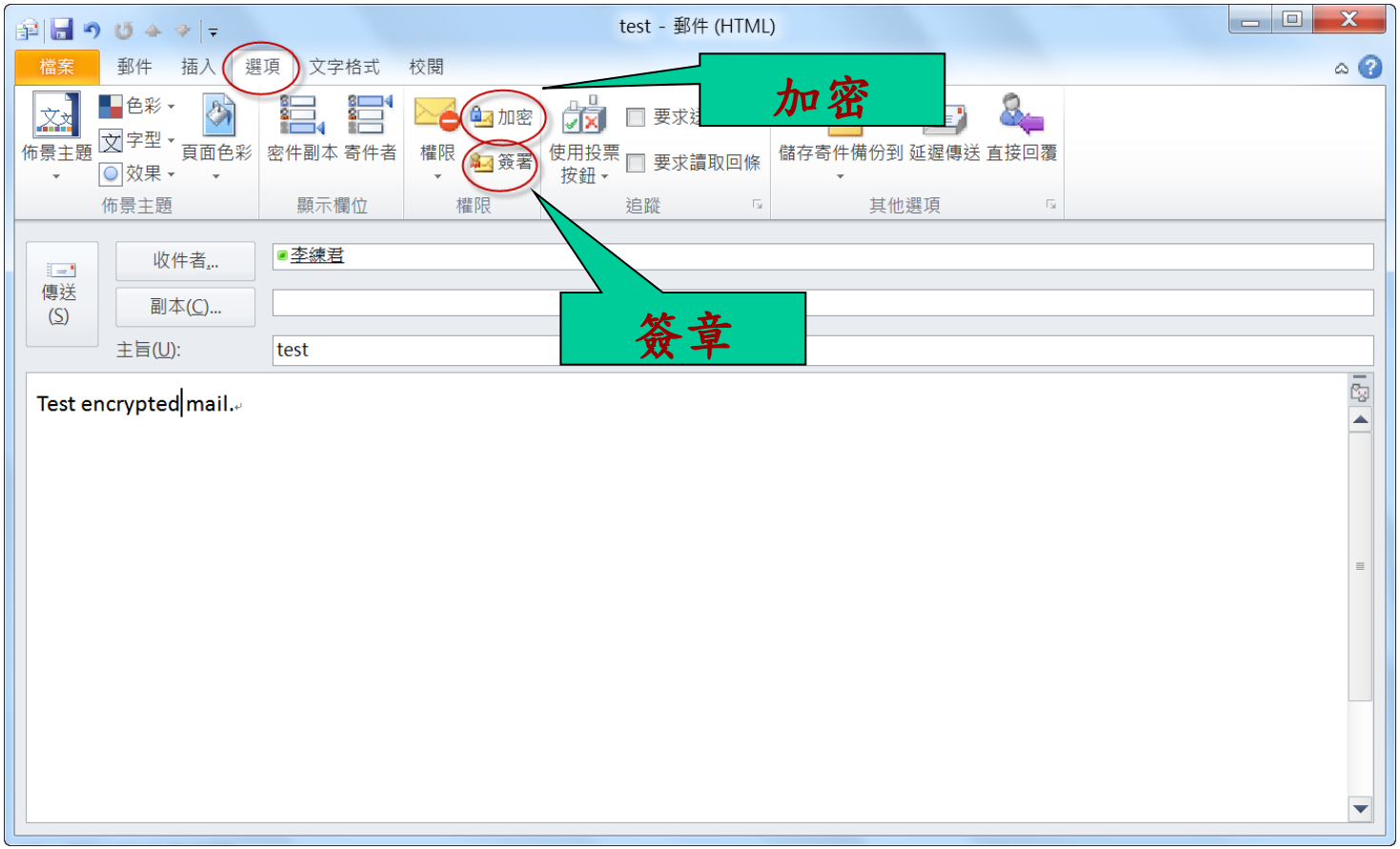
安全電子郵件設定

選擇用來做數位簽章之憑證時，如果在此畫面無法看到可選取的憑證，請確定您已匯入政府



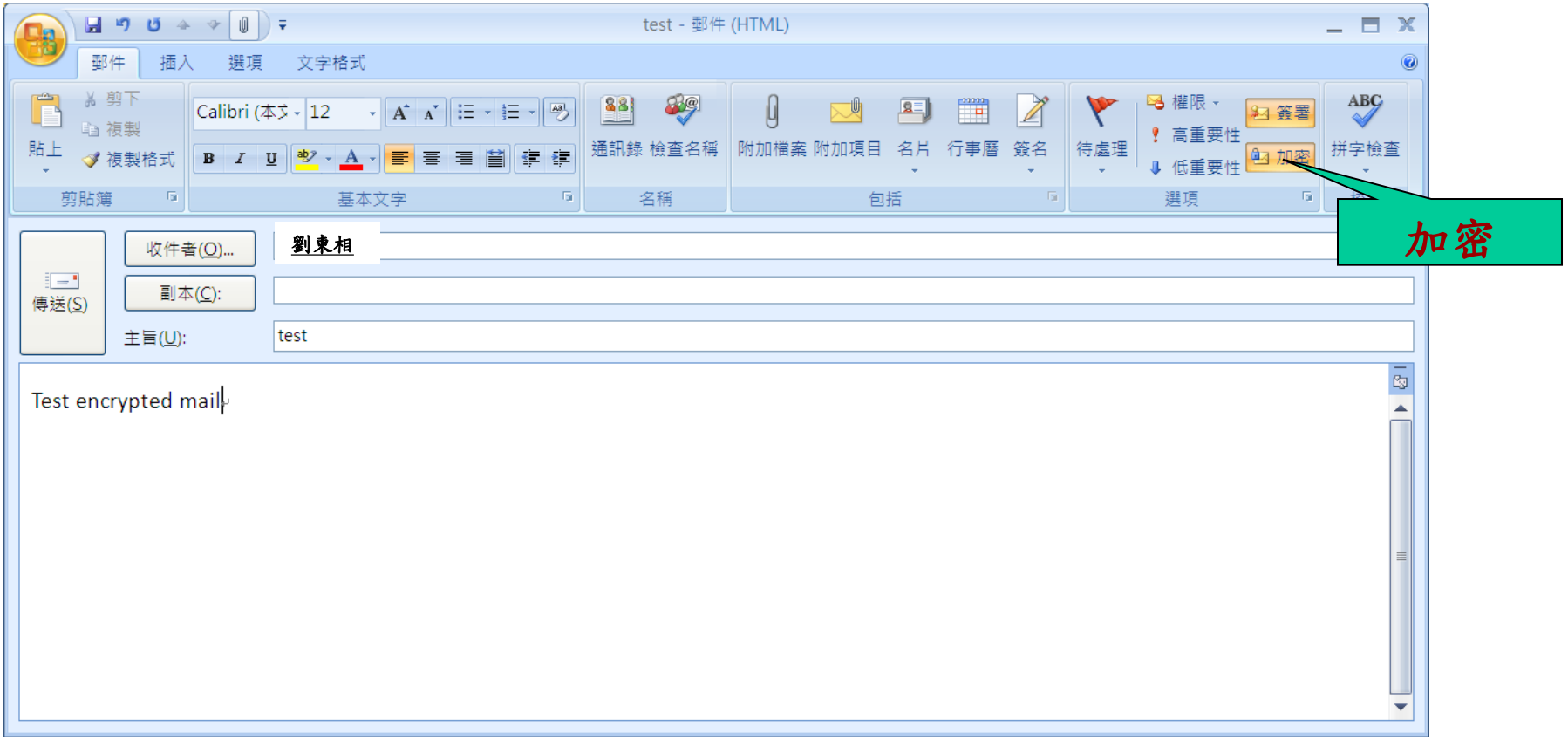
建立安全電子郵件管道

(1)要建立簽章的安全電子郵件給別人時，在指定收件者後請按下簽章的按鈕即可。
(2)要建立加密的安全電子郵件給別人時，先按下加密的按鈕再按收件者進行新增收件者
(3)若需同時簽章加密，則分別按下兩個按鈕即可



建立安全電子郵件管道

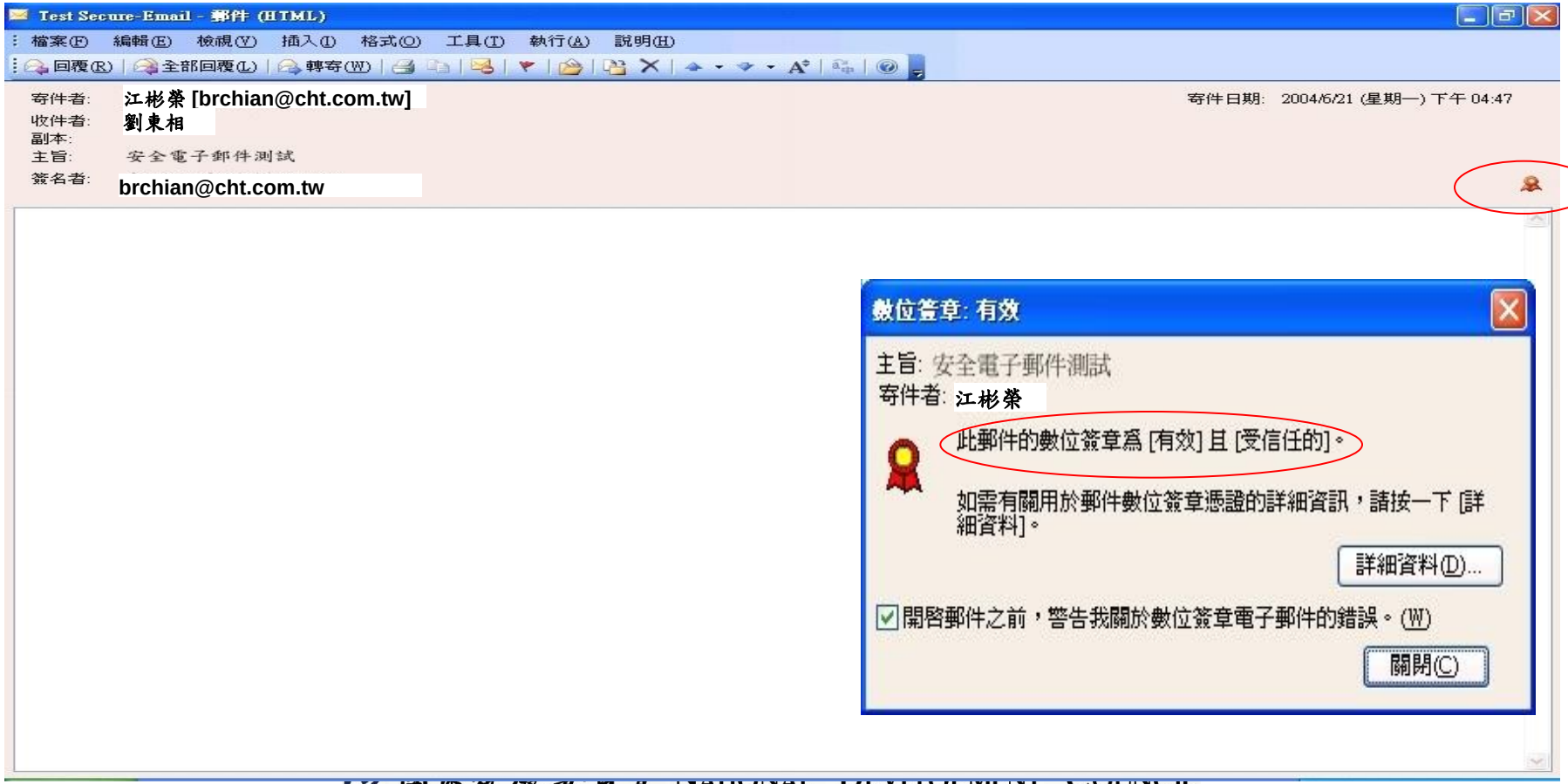
(1)完成設定收件者後，就可以進行加密傳送



收取安全電子郵件

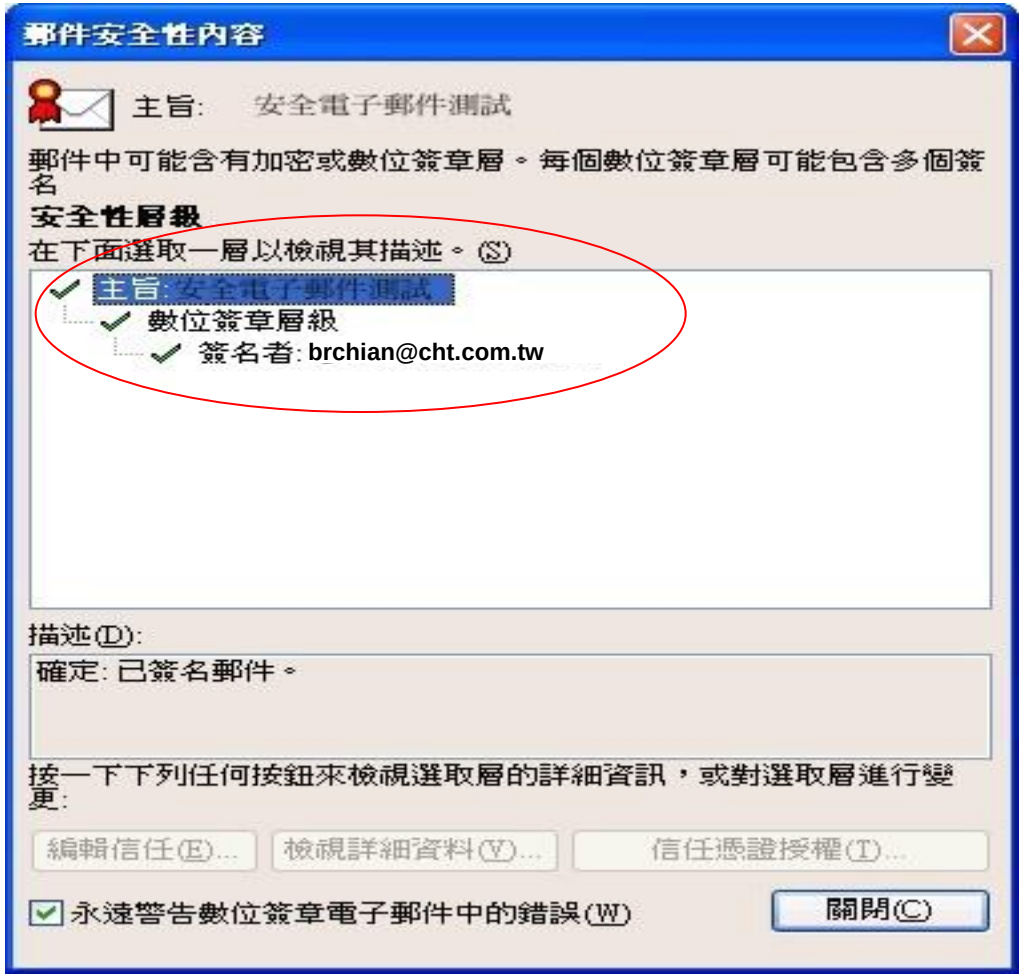
(1)收到對方傳送來，含有數位簽章之電子郵件之後，將之開啟。

(2)點選「數位簽章」圖示(像徽章)，即可檢視此包含數位簽章電子郵件之憑證內容。再按[詳細資料]，可看到下頁圖示。



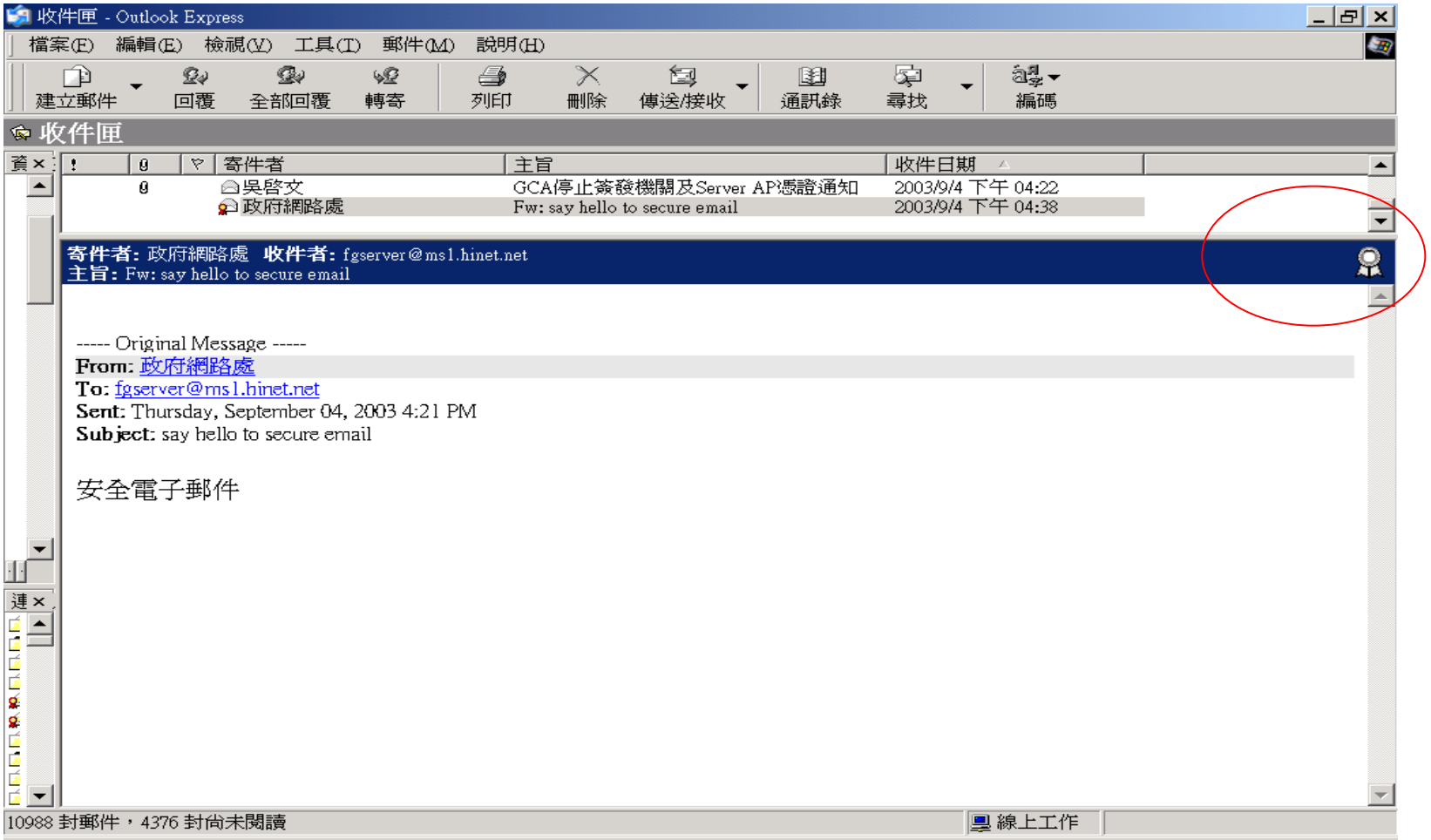
收取安全電子郵件管道

收件者可藉由[郵件安全性內容]確認電子文件之完整性以及簽名者之身分。



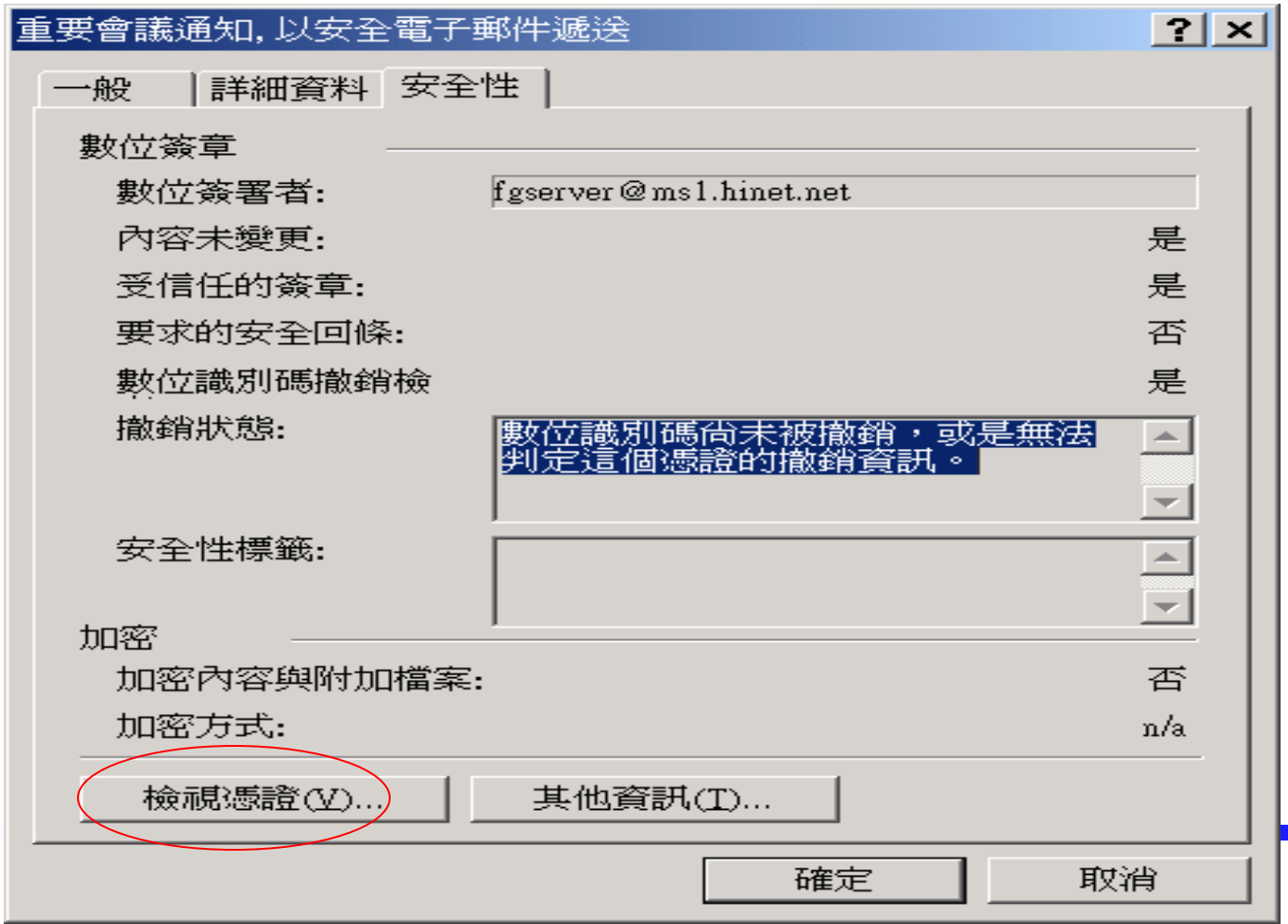
建立安全電子郵件管道(3)

(5)下圖為電子郵件之原始內容，使用者可點選信件標頭右側之數位簽章圖示(像徽章)，以檢視此數位簽章之內容



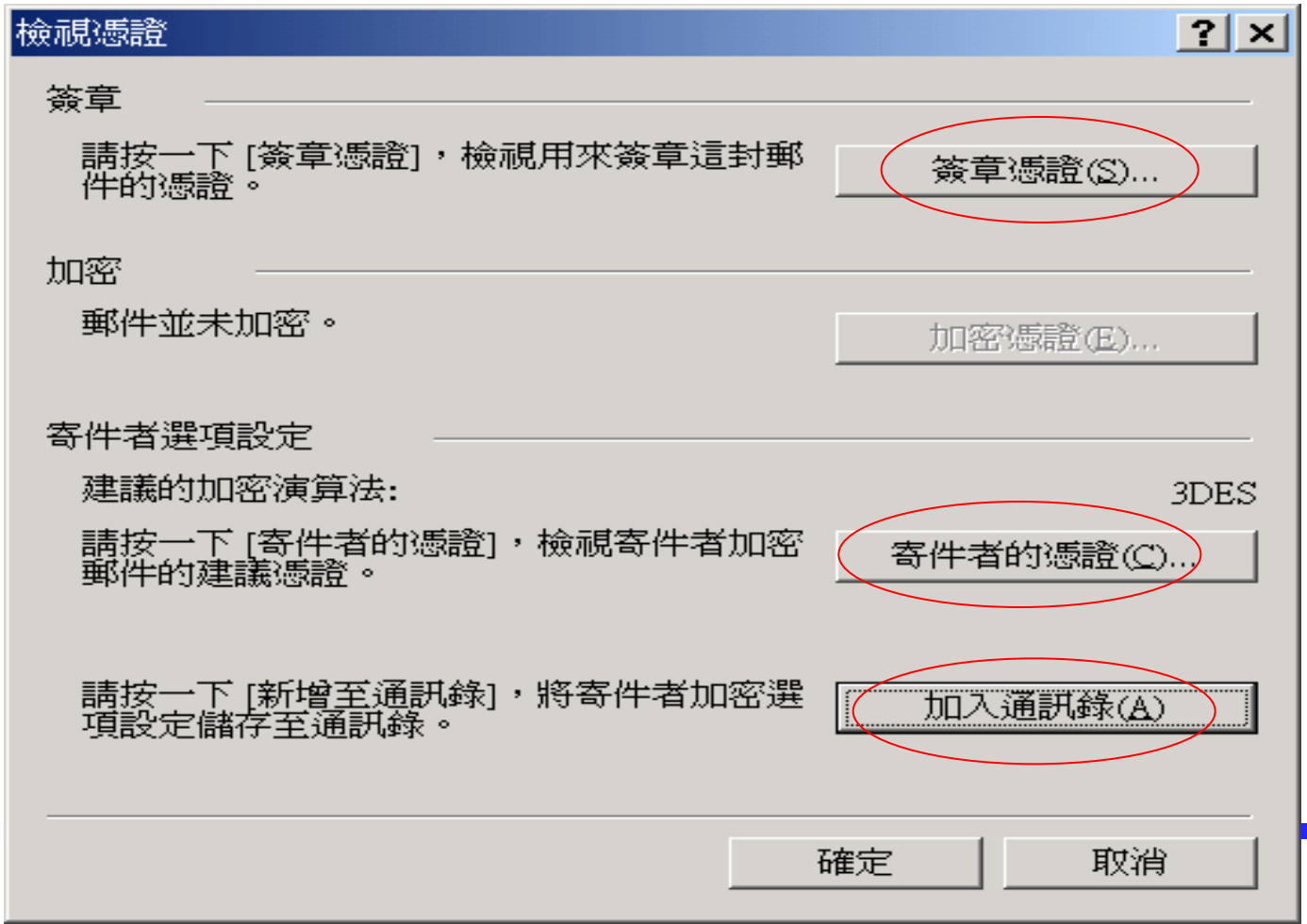
建立安全電子郵件管道(4)

(6)在數位簽章內容中之「安全性」分項，可看出此數位簽章簽名者之電子郵件位址及其他關於此憑證的安全資訊，點選「檢視憑證」按鈕，即可檢視更詳細的憑證資訊。



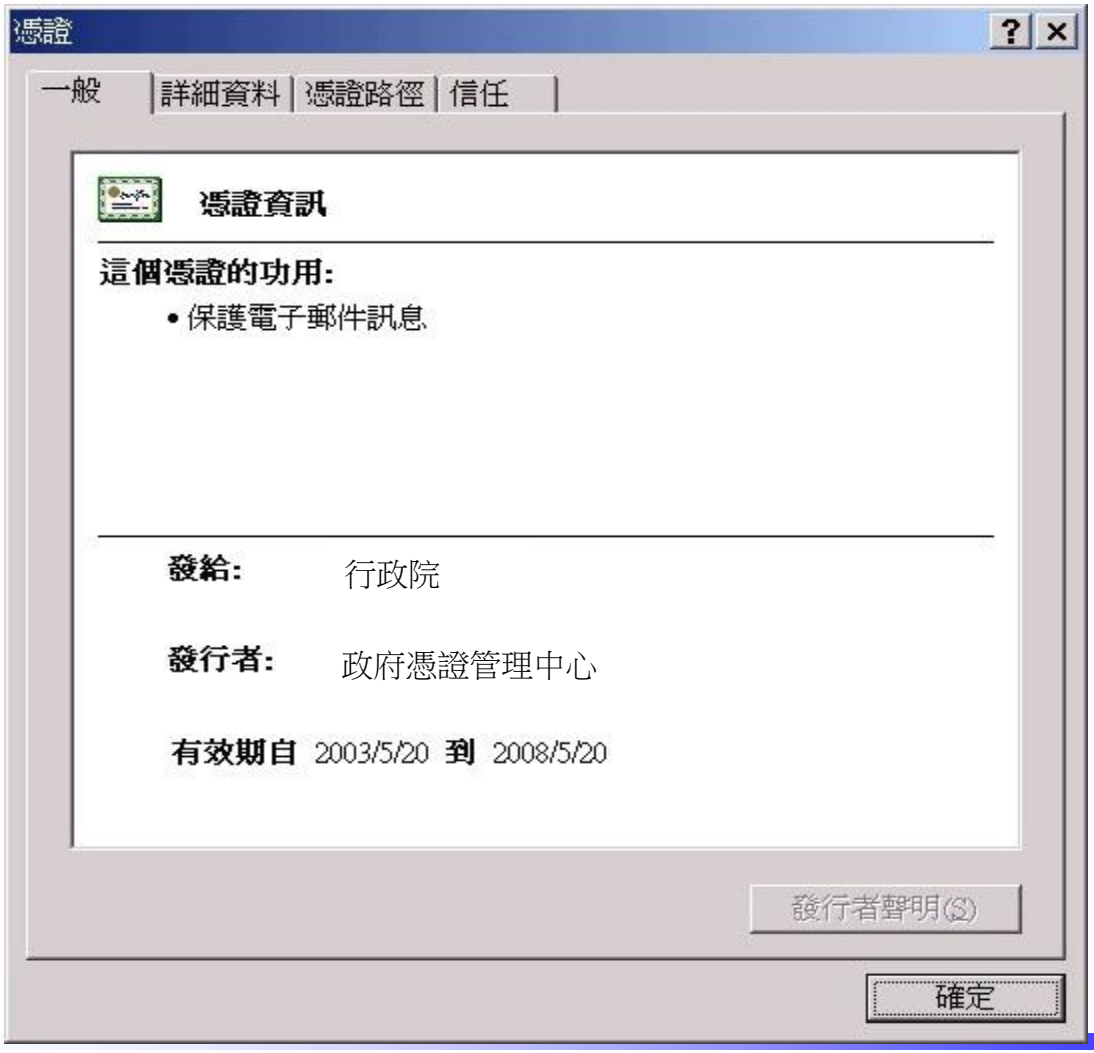
建立安全電子郵件管道(5)

(7)在此畫面中，可點選「簽章憑證」、「寄件者的憑證」按鈕來檢視寄件者所使用的簽章用及加密憑證。 也可將寄件者之加密用憑證存入通訊錄



建立安全電子郵件管道(6)

(8)憑證檢視畫面如圖所示



五、Q & A

1.如何查詢及下載憑證?

gca.nat.gov.tw-→[憑證及IC卡相關作業] →憑證查詢及下載，可憑“機關名稱”或“機關OID”或”電子郵件信箱”或“憑證IC卡號”或“憑證序號”等關鍵詞之一種進行查詢

一般建議選擇電子郵件信箱查尋您所要找尋的憑證。

2.何謂 CSP?

CSP(Cryptographic Service Provider) 是一個動態連結資料庫 (Dynamic Link Library, DLL檔)，你使用的應用程式透過 CryptoAPI 呼叫 CSP 提供的函式。利用這些功能，應用程式可以輕易的達到資料加解密、認証的功能，而不需要知道這些密碼功能的演算法。由於應用程式和 CSP 是分別獨立的個體，當密碼演算法更新時，只需要以新的 CSP 替換，而不用重新改寫或編譯應用程式，減少開發程式的成本。

Q & A

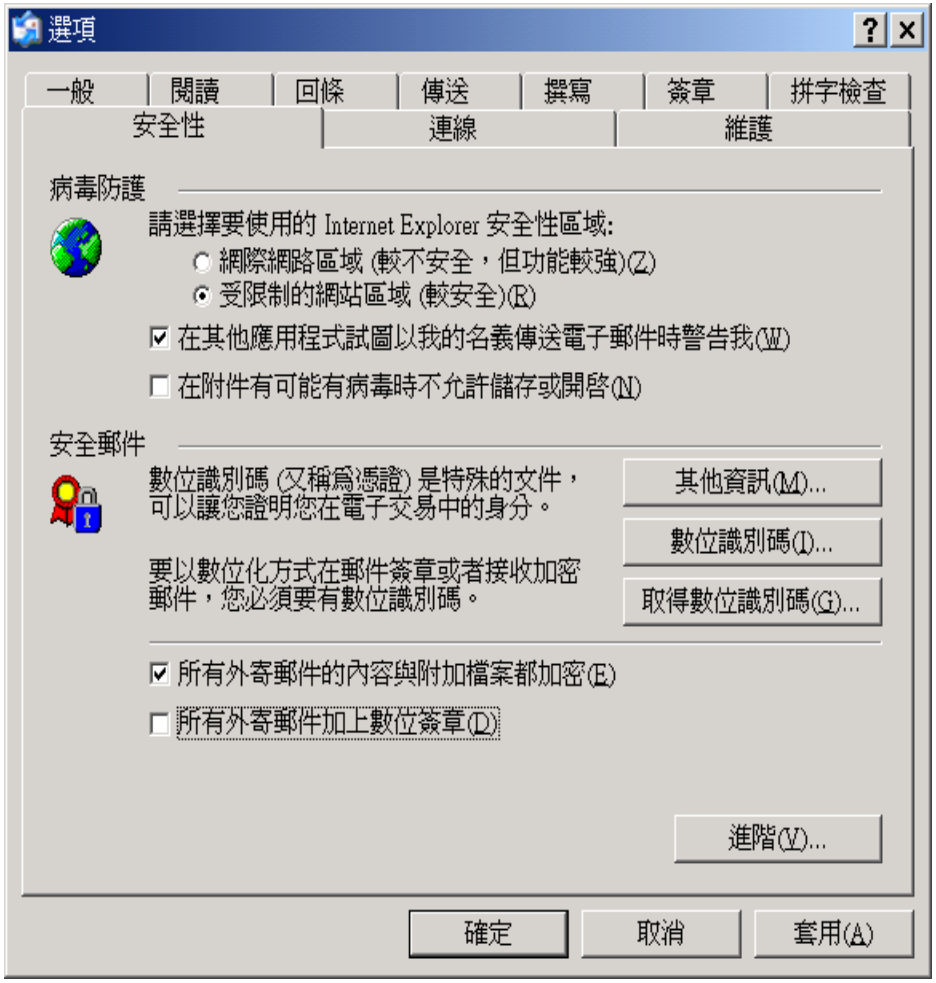
3. 所選擇的加密方法有哪些?

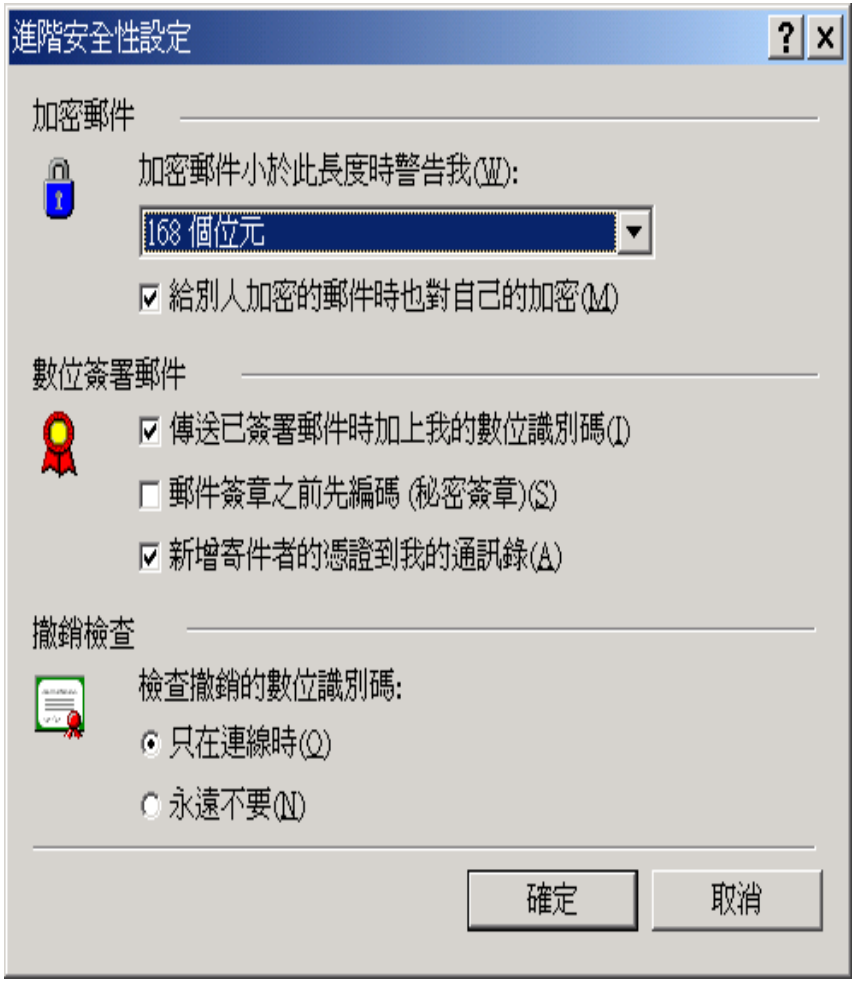
Outlook Express 能解密 RC2 (64-bit) 所加密的郵件，但無法使用此演算法傳送郵件。強烈建議選擇3DES (168-bit)之演算法。

4.如何強制每封信都產生簽章與加密,副本寄給自己的信件能否也加密?

於outlook 中找<工具>-→<選項>-→<安全性>

Q & A


選項
一般
閱讀
回條
傳送
撰寫
簽章
拼字檢查
安全性
連線
維護
病毒防護
請選擇要使用的 Internet Explorer 安全性區域:
網際網路區域 (較不安全，但功能較強)(Z)
受限制的網站區域 (較安全)(R)
在其他應用程式試圖以我的名義傳送電子郵件時警告我(W)
在附件有可能有病毒時不允許儲存或開啓(N)
安全郵件
數位識別碼 (又稱爲憑證) 是特殊的文件，可以讓您證明您在電子交易中的身分。
其他資訊(M)...
數位識別碼(I)...
要以數位化方式在郵件簽章或者接收加密郵件，您必須要有數位識別碼。
取得數位識別碼(G)...
所有外寄郵件的內容與附加檔案都加密(E)
所有外寄郵件加上數位簽章(D)
進階(V)...
確定
取消
套用(A)


進階安全性設定
加密郵件
加密郵件小於此長度時警告我(W):
168 個位元
給別人加密的郵件時也對自己的加密(M)
數位簽署郵件
傳送已簽署郵件時加上我的數位識別碼(I)
郵件簽章之前先編碼 (秘密簽章)(S)
新增寄件者的憑證到我的通訊錄(A)
撤銷檢查
檢查撤銷的數位識別碼:
只在連線時(O)
永遠不要(N)
確定
取消

Q & A

5.為什麼電子郵件地址要記載於憑證內？不記載會有什麼影響?

若憑證中沒有記載用戶的Email Address，則用戶所申請的IC卡將無法用來收發加密或簽章的安全電子郵件(Secure Email)，也就是說用戶所申請的IC卡將無法與Outlook或Outlook Express等支援安全電子郵件的軟體來搭配使用。所以申請人在勾選Email要不要記載在憑證中時，主要的考慮因素是申請人要不要使用安全電子郵件，如果申請人覺得自己並不需要安全電子郵件的功能則可以勾選不要將E-mail記載在憑證中。但是除了考量安全電子郵件的功能，個人隱私的保護也是需要考量的重要因素。

Email Address的洩露對於不同的人可能造成不同的影響，對於那些原本就將Email Address公佈在網路上(例如其個人網頁)的人，其Email Address本來就是網路上公開的資料，沒有洩不洩漏的疑慮。但對於某些人而言，Email Address是屬於個人隱私資料的，只跟親朋好友秘密通信，或是怕收到廣告信，因此希望盡量不要在網路上任意流傳，但是安全電子郵件的國際標準為提高電子郵件的安全度，規定憑證中必須記載E-mail Address以便確認電子郵件發文者及收文者的身分，這當中當然是有所衝突的。

MOICA所提供的折衷做法是讓申請者在戶政事務所進行憑證IC卡接受確認階段，選擇是否公佈憑證。

Q & A

6.無法使用安全性電子郵件原因分析

1.憑證中SubjectDirectoryAttribute中並沒有放置email位址。

2. 憑證中email位址和收發信的mail帳號不一致。

希望各位以後能多利用安全電子郵件，以確認郵件之寄件者，內容之完整性及資料之機密性

報告完畢
敬請指教