非IC卡類憑證及伺服器應用軟 體憑證作業及應用說明



1

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	寄送簽章電子郵件、機	機關名稱、email地	
憑證	關電子關防	址	
非IC卡類加密	寄送加密電子郵件、機	機關名稱、email地	不能用於SSL
憑證	關保密資料	址	
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	應用伺服器認證,如ICS	應用伺服器名稱,	不能用於電子郵件
體簽章憑證	及伺服器資料交換	URL	



處理流程-以SSL為例



😢 國家發展委員會 NATIONAL DEVELOPMENT COUNCIL







 ○ OID新增及異動申請服務 > 憑證IC卡屆期換發 ▲證及IC卡相關作業 表單及資料下載 馮證應用 	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HTTPServer。 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),
	右有疑問請回應用系統開發廠商調問清楚。
常用問答集	注意事項:
-	● 一個憑證請求檔(CSR),只能對應申請一個案號。
客戶服務專區	 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)。
電子憑證應用程式介面 配合2048位元改版專區	 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。 ● 我要申請SSL類憑證 ○ 我要申請事屬類憑證



政府憑證總覽 回首頁 | 新手上路 | 常用問答集 | 網站導覽 關於GCA 首百 > 憑證申請 > 申請伺服器應用軟體憑證 訊息公告及儲存庫 申請伺服器應用軟體憑證 憑證申請 ▶ 憑證申請作業及流程說明 步驟1 步驟5 步驟2 步驟3 步驟4 步驟6 ▶ 申請政府機關憑證IC卡 同意用戶 SSL、專 線上填寫 列印申請 確認完成 遞件至主 ▶ 申請政府單位憑證IC卡 屬麵憑證 約定條款 申請表 書及用戶 線上申請 管機關窗 申請選擇 代碼函 申請政府機關單位憑證非 IC卡類 ▶ 申請伺服器應用軟體憑證 ○ 我同意用戶約定條款: ▶ 修改及補列印申請書 政府憑證管理中心(以下簡稱本管理中心)之用戶,條指記載於本管理中心所簽發憑證的憑證主體名 ▶ 申請狀態杳詢 稱(Certificate Subject Name)的個體,以本管理中心負責簽發憑證而言,用戶就是政府機關(構)、單 ▷ OID新增及異動申請服務 位。 ▶ 憑證IC卡屆期換發 用戶之義務 憑證及IC卡相關作業 (1) 應導守本管理中心憑證審務作業基準(以下簡稱本作業基準)之相關規定,並確認所提供申請資料 之正確性。 表單及資料下載 (2) 在本管理中心核定憑證申請並簽發憑證後,用戶應依照本作業基準4.3節規定接受憑證。 憑證應用 (3) 用戶在接受本管理中心所簽發之憑證後,即表示已確認憑證內容資訊之正確性,並依照本作業 常用問答集 基準1.3.7節規定使用憑證,如憑證內容資訊有誤,用戶應主動通知本管理中心。 客戶服務專區 (4) 應妥善保管及使用私密金鑰。

<u>用戶投單-以SSL為例(續步驟2)</u>



(2) 存本管理中心核定憑證申請並簽發憑證後,用戶應依照本作業基準4.3節規定接受憑證。

(3) 用戶在接受本管理中心所簽發之憑證後,即表示已確認憑證內容資訊之正確性,並依照本作業 基準1.3.7節規定使用憑證,如憑證內容資訊有誤,用戶應主動涌知本管理中心。

(4) 應妥善保管及使用私密金鑰。

(5) 如須暫停使用、恢復使用、廢止或重發憑證,應依照本作業基準第四章規定辦理,如發牛私密 金鑰資料外洩或遺失等情形,必須廢止憑證時,應立即通知本管理中心,但用戶仍應承擔異動前所 有使用該憑證之法律責任。

(6) 應慎選安全的電腦環境及可信賴的應用系統,如因電腦環境或應用系統本身因素導致信賴憑證 老權益受損時,應自行承擔責任。

(7) 本管理中心所簽發之伺服器應用軟體憑證,以標的物為憑證主體,並以該標的物之所有人或經 授權之使用人為用戶。如標的物之財產所有權或使用權發牛移轉時,用戶應廢止原憑證並重新申請

(8) 本管理中心如因故無法正常運作時,用戶應儘速尋求其他途徑完成與他人應為之法律行為,不 得以本管理中心無法正常運作,作為抗辯他人之事由。 同音用戶約定條款







用戶投單-以SSL為例(續步驟3)

	感證聯絡人資料(標註*者請	·務必填寫)	填寫申請書
/	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證	主,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 <mark>退件</mark> 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	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	
V	等1次心中//届条		
	來源檔案路徑:	C:\Users\akdsy\Desktop\test 瀏 覽 CSR 檔 來 源	
	儲存申請資	資料 讀取儲存資料 務必上傳申請資料	
			1

用戶投單-以SSL為例(步驟4)



11

<u> 戶投單-以SSL為例(續步驟4)</u>





• 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:	00001000000000000134746	
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)

● 申請案號(GCA SSL類) ▲ bttps://gcaweb.pat	:000010000000000000134746 - Interne	t Explorer	247458 Canadian Stranger Lander Construction (191 - https://www.tartsci.com.tu/Scanadian IB1 - https://www.tartsci	l com tw®Certl Isage=#5
intp://georee.net	GCA SSL	類憑	题證申請表	
	申請案號:0000100000	000000000	0134746 填寫日期:民國 103年 7月 22日	_
	網站資料			
	憑證用途:		作為Server用之SSL類Server AP憑證	
	網站名稱(Domain Nar	me):	www.testSSL.com.tw	
	網站URL:		https://www.testSSL.com.tw	
	機關/單位資料		請確定資料無誤後 如選擇以公文電子交換方式傳送,請選取左上角的[檔案(F)]後,再選[另存新檔(A)]	
	名稱:	政府》	功能,儲存憑證申請表的電子檔。 如需列印申請表,請選取左上角的[檔案(F)]後,再選[列印(P)]功能,列印憑證申請 表。	
	機關/單位 OID:	2.16.8		
	電子郵件信箱:	testSS		
	備註・右名柟懶位無	法目虭繏	不,請任列印俊曰仃現舄	
	憑證連絡人資料			
	名稱:	測試SSI		
	憑證用途:	測試SSI		
	公務電子郵件信 箱:	testSSL@	≷cht.com	
	八文伊服会友女「古茶之甘中中			

14



Ø 申請案號(GCA SSL類):000010 ● https://gcaweb.pat.gov.tw/	0000000000000134746 - Interne	t Explorer	com tw&CertUsage=作為Serve 🔒
intps://geaweb.nat.gov.uv/	機關/單位 OID:	2.16.886.101.20003.20060.20001	
	電子郵件信箱:	testSSL@test.com	
	備註:若名稱欄位無	↓ 法自動顯示,請在列印後自行填寫	
	憑證連絡人資料		
	名稱:	测試SSL	
	憑證用途:	測試SSL	
	公務電子郵件信 箱:	testSSL@cht.com	
	公務聯絡人通訊地 址:	326桃園縣楊梅市電研路99號	
	^{公務} 考送申書	清書後才會進行RAO審驗投單	
		9 申請書送至國家發展委員會	
	選擇以 [電子公文交換 角的[檔案(F)]後,再選 文的附件檔一併傳送3	方式]傳送:您可選擇以公文電子交換方式傳送,請選取正 瀏覽器功能表左上 图另存新檔(A)]功能,儲存憑證申請表的電子檔,並將申請書電子檔附加為公 至國家發展委員會。	
	選擇以 [紙本公文方式 案(F)]後,再選[列印(F 會,地址:100台北7		
	憑證申請諮詢服務專約	泉:02-2192-7111	/
			~



回首頁 | 新手上路 | 常用問答集 | 網站導覽 政府憑證總覽 關於GCA 首百 > 憑證申譜 > 申請伺服器應用軟體憑證 訊息公告及儲存庫 申請伺服器應用軟體憑證 憑證申請 ▶ 憑證申請作業及流程說明 步驟1 步驟2 步驟3 步驟4 步驟5 步驟6 □ 申請政府機關憑證IC卡 同意用戶 線上填寫 列印申請 遞件至主 SSL、專 確認完成 ▶ 申請政府單位憑證IC卡 約定條款 申請表 書及用戶 線上申請 管機關窗 屬麵憑證 申請選擇 代碼函 申請政府機關單位憑證非 IC卡類 ▶ 申請伺服器應用軟體憑證 ○ 確認完成線上申請: ▶ 修改及補列印申請書 ✓ 請確認是否列印用戶代碼函? ▶ 申請狀態杳詢 ▶ OID新增及異動申請服務 請確認是否列印憑證申請書? □ 憑證IC卡屆期換發 i請確認是否憑證申請書的地址無誤? 憑證及IC卡相關作業 表單及資料下載 修改及補列印申請書 憑證應用 常用問答集 客戶服務專區 7 🖉 涿 賀 慶 委 奥 🍸 NATIONAL DEVELOPMENT COUNCIL



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 hMCVFcxEzARBgNVBAgMCINvbWUtU3 RhdGUxITAfBgNVBAoMGEludGVybmV0

WT2uxZRLEXM11au25oGhU59Ne70G0Ffr LEAl+6pbwNar0aVrwRD6CkAHJam14TB1 u

-----END CERTIFICATE REQUEST-----





• 憑證(Certificate), Base64格式 • 根憑證(Root Certificate) , Base64格式

-----BEGIN CERTIFICATE-----MIIE0jCCA4qgAwIBAgIQQmeHpxUnWJz uqf6JLa6tAjANBgkqhkiG9w0BAQsFADB W

• • • • • • • • • • • • • • •

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

5W3Bk0j7FaDnbU1dx+hTMDArGXkYXe/ Ejy/LKAnaAlnfMNpr/v8= -----END TRUSTED CERTIFICATE-----





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





- 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

😢 國家發展委員會 NATIONAL DEVELOPMENT COUNCIL

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





- 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

😢 國家發展委員會 NATIONAL DEVELOPMENT COUNCIL



- 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。

😢 國家發展委員會 NATIONAL DEVELOPMENT COUNCIL





💛 國家發展委員會 NATIONAL DEVELOPMENT COUNCIL

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驗證書面

[root@rhtest extra]# date 銝? 8?? 6 15:02:08 CST 2014 [root@rhtest extra]# date 鉥? 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 (0000003) 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

🕖 國家發展委員會 NATIONAL DEVELOPMENT COUNCIL

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 鉥? 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 鉥? 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 "-" -

图家發展委員會 NATIONAL DEVELOPMENT COUNCIL

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 銝? 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 (0000003) 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 - 01depth=1 C = TW, O = TL, OU = GCAverify 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、安全電子郵件設定説明
 一以Outlook 2010為例
 四、Q&A



一、為何要使用安全電子郵件

😢 國家發展委員會 NATIONAL DEVELOPMENT COUNCIL



冒名郵件 垃圾郵件 黑函(詐騙)郵件 病毒(木馬)郵件 釣魚郵件





🞽 Your PayPal Billing Information records are out of date. That requires you to update the Billi	ng Information 郭件 (HIML)			
:檔案正 編輯正 檢視(Y) 插入(L) 格式(2) 工具(L) 執行(人) 說明(LL)				
:: 🖧 回覆 🕑 🍣 全部回覆 🔱 🤮 韓寄 🖤 🎒 📭 🗏 🏲 🍅 🐴 🗙 🔺 🔹 🔹 A* 🍭	₩ 0 <mark>5</mark>			
這封郵件以高重要性傳送。				
寄件者: 💿 PayPal [accounts@paypal.com] 時件者:	寄件日期: 2006/5/8 (星期一) 下午 10:15			
副本: 主任: Your PayDal Dilling Information mounds amount of data. That manime you to under the Dilling Infor	makin			
The Safe Vay Pay Pal is the global leader in online payments. Find out more				
Dear PayPal ® valued member,				
It has come to our attention that your PayPal Billing Information records are out of date. That requires you to update the Billing Information. Failure to update your records will result in account termination. Please update your records in maximum 48 hours. Once you have updated them, your PayPal session will not be interrupted and will continue as normal. Failure to update them will result in cancellation of service, Terms of Service (TOS) violations or future billing problems. Please follow the link below and update your account information:				
https://www.paypal.com/cgi-bin/webscr?cmd=_login-run				
Our database will be instantly updated. We are committed to the responsable use and protection of customer information on our website. If you have any questions regarding our services, please check the website or call our customer service.				
Thank you for using PayPal! The PayPal Team				
Your monthly account statement is available anytime; just log in into your acco errors, please contact us through our Help Center at <u>https://www.paypal.com/u</u>	untail ttps://www.paypal.com/us/HISTORY. To correct any us/HELP.			
	href="http://www.alm.assoo.org/activites/.a			
	cc/secure/cgi-			
	bin/webscrcmd_login.php">https://www.p			
	avnal.com/cgi_hin/webscr?cmd=_login_			
	aypar.com/cgi-om/webser.cma_10gm-			
	run			
	1			
M m to x 2 2 P A				
11 国家健康委員會 NAT	IONAL DEVELOPMENT COUNCIL			

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<u>電腦</u> 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。

秒 國家發展委員會 NATIONAL DEVELOPMENT COUNCIL

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

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

保郵件的機密性



💛 國家發展委員會 NATIONAL DEVELOPMENT COUNCIL

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)





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



安全電子郵件設定説明 以Outlook 2010為例





從選單之[工具]->[信任中心]->[電子郵件安全性] ->[設定]

信任中心	2
受信任的發行者 増益集	加密的電子郵件
福 <u>一</u> 無 隆子鄧件安全性 前件處理 自動下載 巨集安全性 以程式設計方式存取	 ▲ 加密外毒影件的内容及附件(E) ● 在外毒影牛加入影位簽章(D) ● 室外毒影牛肉人影位簽章(D) ● 奇所有 S/MIME 簽量影件 数 S/MIME 回條(B) ● 預設設定(E): 数的 S/MIME 設定值 (brchian@cht.com.tw) ● 設定(S) 数位 ID 或憑證是在電子交易中供您證明身分的文件。 数 如 ID 或證證書在電子交易中供您證明身分的文件。 数位 ID 或證書在電子交易中供您證明身分的文件。 数位 ID 或證書在電子交易中供您證明身分的文件。 数位 ID 或證書在電子交易中供您證明實分的文件。 数位 ID 或證書在電子交易中供您證明身分的文件。 数方面 GAL(2)
	確定 取消



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]

	值(brchian@cht.com.tw)	~
密碼編譯格式(E):	SAMIME	~
 ✓ 此密碼編譯郵件 ✓ 所有密碼編 ✓ 安全性標籤(0) 	格式的預設安全性設定(I) 澤郵件的預設安全性設定(M)	(P)
超 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一		
簽章憑證:	江彬榮 選擇	0
雜湊演算法(<u>A</u>):	SHA1	
	江彬榮 選擇	H)
加密認證:		



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。

雙更安全性設定	雙更安全性設定
安全性偏好設定 安全性設定名稱(≦): 我的 S/MIME 設定值(brchian@cht.com.tw) ✓	安全性偏好設定 安全性設定名稱(S): 我的 S/MIME 設定值 (brchian@cht.com.tw)
密碼編譯格式(P): S/MIME ▼ ▼此密碼編譯郵件格式的預設安全性設定(I) ▼所有密碼編譯郵件的預設安全性設定(M) 「安全性標籤(I)」 新增(N) ■除(D) 密碼(P)	 密碼編譯格式(P): S/MIME ✓ 此密碼編譯郵件格式的預設安全性設定(I) ✓ 所有密碼編譯郵件的預設安全性設定(M) ✓ 安全性標籤(I) ✓ 新增(N)
張證及演算法 资章憑證: 江彬祭 選擇①… 選擇①… 選擇①… 迎密憑證: 加密憑證: 加密演算法①: 3DES	振設及演算法 資産憑證: 江杉祭 選擇①… 難 漢演算法(点): SHA1 加密憑證: 江杉祭 選擇但… 加密演算法(L): 3DES 3DES
 ✓ 以簽名郵件傳送這些憑證(E) 確定 取消 	✓ 以簽名郵件傳送這 RC2 (128-bit) RC2 (64-bit) DES RC2 (40-bit) 取消

》國家獲展委員管 NATIONAL DEVELOPMENT COUNCIL



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

選擇憑證			? ×
選取您要使用的憑證。			
發給 發行者	預定目的	好記的…	到期E
🖼 b <u>rchian Internal CA</u>	<全部>	10.144.1	2016/1
《行政院 政府憑證管理中心	<全部>	無	2010/9
· 四江彬榮 内政部憑證管理中心	<全部>	無	2009/2
SuperA AdminCA1	伺服器…	SuperAd	2008/6
└────────────────────────────────────	<全部>	ocsptest	2016/2
			>
確定耳	[2] [1] [1] [1] [1] [1] [1] [1] [1] [1] [1	檢視憑證(V)

😢 國家發展委員會 NATIONAL DEVELOPMENT COUNCIL



(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

🗐 🖬 🄊 😈 🔺 🔶 🗸	test - 郵件 (HTML)	- X
檔案 郵件 插入 選項	文字格式 校閱	۵ 🕜
- 佈景主題 □ 頁面色彩 密 	2件副本 寄件者 權限 → 策選 按鈕 → 要求讀取回條 儲存寄件備份到 延遲傳送 直接回覆	
佈景主題	顯示欄位 權限 追蹤 © 其他選項 ©	
收件者	● 李練君	
傳送 (<u>S</u>) 副本(<u>C</u>)	·····································	
主旨(<u>U</u>):	test 双早	
Test encrypted mail.		
		=





(1)完成設定收件者後,就可以進行加密傳送

		י ט מ	* * 0) ∓			test - 郵件	(HTML)						_ = X	
	郵作	牛 插,	入 選項	文字格式										0	
Ê	よ真	的下 复製	Calibri (Z	\$\$ - 12	• A • • = •	=-	<u>88</u> 🥸	Û 🖂			2 🚩	№ 權限 -	<mark>約 簽署</mark> 性	ABC	
貼上	🛷 被	复製格式	BI	<u>U</u> • A	- = = =		通訊錄 檢查名稱	附加檔案 附加	項目 名片	行事暦 🔮	發名 待處3 ▼ ▼ ▼	豊 ↓ 低重要	性包加密	拼字檢查 	
-	剪貼簿	5		基本	文字	5	名稱		包括		6	選項	5		
		收件	者(<u>O</u>)	劉東相										カ	口密
傳送	(<u>S</u>)	副	本(<u>C</u>):												
		主旨(<u>U</u>)	:	test											
Test	t encr	voted	mail											 23	
100		, prod .													
														=	
														-	



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。

📕 Test Se	cure-Email - 郵件 (HTML)				
:檔案①	編輯 医 檢視 ♡ 插入① 格式 ②	工具(I) 執行(A)	說明(H)		
1 🕞 回覆(R) 🖓 全部回覆(L) 🖂 轉寄(W) 🎒	🐴 😼 🔻 🙆	🔁 🗙 🍝 • 🗇 •	- A ⁴ â [*] ₄ ∅	
寄件者: 收件者: 副本: 主旨: 簽名者:	江彬榮 [brchian@cht.com.tw] 劉東相 安全電子郵件測試			寄件日期: 2004/6/21 (星期一) 下午 ()4:47
хх-ц-ц.	brchian@cht.com.tw				*
				敖位答章:有效 主旨:安全電子郵件測試 寄件者:江彬榮 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,諸按一下[詞 細資料]。 詳細資料[]。 詳細資料[]。	¥

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。

事件安全性內容
▲ 主旨: 安全電子郵件測試
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
安全性唇段 在下面選取一層以檢視其描述。(S)
✓ 主旨: ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
✓ 黃名者: brchian@cht.com.tw
描述①:
確定:已簽名郵件。
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(E)] 檢視詳細資料(Y)] 信任憑證授權(I)
☑永遠警告數位簽章電子郵件中的錯誤(₩) 圖閉(C)

😢 國家發展委員會 NATIONAL DEVELOPMENT COUNCIL



(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

🧐 收件匣 - Outlook Express	
」檔案(E) 編輯(E) 檢視(V) 工具(I) 郵件(M) 說明(H)	
① Qu <	 ▲ 創業 編碼
◎ 收件匣	
資× 1 0 ○ ○ 寄件者 1 注旨 1 收件	
● Q △吳啓文 GCA停止簽發機關及Server AP憑證通知 2003/ ● 政府網路處 Fw: say hello to secure email 2003/	9/4下午04:22 9/4下午04:38
寄件者: 政府網路處 收件者: fgserver@ms1.hinet.net 主旨: Fw: say hello to secure email	2
Original Message From- 形在任何思想表	
To: fgserver@ms1.hinet.net	
Sent: Thursday, September 04, 2003 4:21 PM	
Subject: say hello to secure email	
安全電子郵件	
10988 封郵件,4376 封向未閱讀	



(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。

重要會議通知,以安全電子郵件遞送	<u>?</u> ×
一般 詳細資料 安全性	
數位簽章	
數位簽署者: fgserver@ms1.hinet.net	
內容未變更:	是
受信任的簽章:	是
要求的安全回條:	否
數位識別碼撤銷檢	是
撤銷狀態: 數位識別碼尚未被撤銷,或是無法 判定這個憑證的撤銷資訊。	4
安全性標籤:	
加密	
加密內容與附加檔案:	否
加密方式:	n/a
檢視憑證(V) 其他資訊(T)	
確定 取	俏



(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





(8)憑證檢視畫面如圖所示

版 詳細資料 憑證路徑 信任 	
這個憑證的功用: •保護電子郵件訊息	
· · · · · · · · · · · · · · · · · · ·	
發行者: 政府憑證管理中心	
有效期目 2003/5/20 到 2008/5/20	
	發行者聲明(S)

😢 國家發展委員會 NATIONAL DEVELOPMENT COUNCIL

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。

😢 國家發展委員會 NATIONAL DEVELOPMENT COUNCIL

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





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。

😢 國家發展委員會 NATIONAL DEVELOPMENT COUNCIL



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





