政府機關網站導入HTTPS安全連線暨多網域憑證說明會

國家發展委員會

107年3月

大綱

- 緣由
- 推動時程
- 導入注意事項
- SSL類憑證申請說明
- 多網域憑證申請說明
- SSL類憑證安裝說明
- SSL類憑證常見問題

緣由

- 依據行政院國家資通安全會報第31次委員會議決議辦理，各機關應配合推動期程依限完成網站導入HTTPS
- 依據「行政院及所屬機關資訊安全管理規範」、「行政院及所屬各機關資訊安全管理要點」，敏感性資料於傳輸或儲存時應加密保護
- 國際瀏覽器大廠對於瀏覽器安全發展規範及隱私要求日趨嚴格
  1. Google自2017年1月起，Chrome瀏覽器開始把**收集密碼或信用卡數據的HTTP頁面**標記為“不安全”
  2. Google自2017年10月起，Chrome瀏覽器開始把帶有**輸入數據的HTTP頁面**和所有以**無痕模式瀏覽的HTTP頁面**都會被標記為“不安全”
  3. Google自2018年7月起，Chrome瀏覽器的地址欄將把**所有HTTP標示**為不安全網站

為何導入

- 保護敏感性資料傳輸
- 避免釣魚網站
- 與國際趨勢接軌
- 提升民眾對政府網站安全性觀感

推動時程

- 行政院所屬二、三級機關應於106年 12月底前完成全球資訊網導入HTTPS協定**(已完成)**
- 政府機關對外服務網站應於107年6月底 前完成導入HTTPS傳輸協定。

導入注意事項

如何導入HTTPS安全連線

1.申請SSL憑證

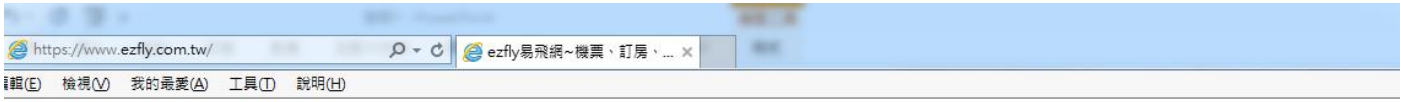
2.安裝SSL憑證及設定憑證串鍊

網站導入注意事項

1. 確認網站是否有內嵌網頁(非https連線)，否則將會產生混合內容的警告(https mixed content)
2. 安裝之憑證主體需與網域相符
3. 依照安裝說明手冊進行憑證5層串鍊設定(參閱附錄一)
4. 進行網站自我檢測
5. 導入後網站須針對SSL相關弱點不定期進行修補

網站Mixed Content(1/3)

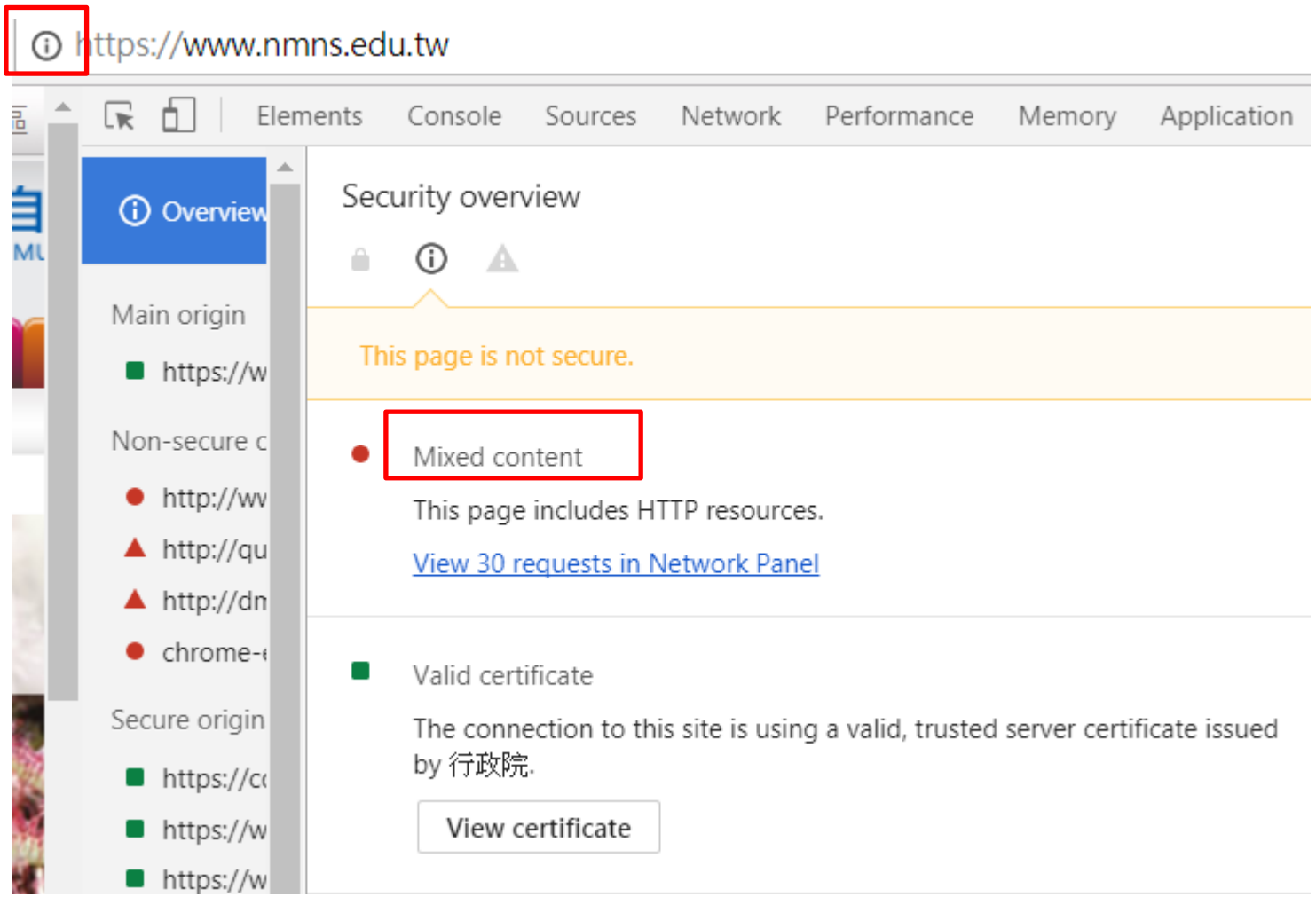
- 網頁的內容必須是https連線，否則會出現混合內容的警告(https mixed content)



若網站含有內嵌的網頁，其連線不是https的話，該網頁的顯示就會變的殘缺

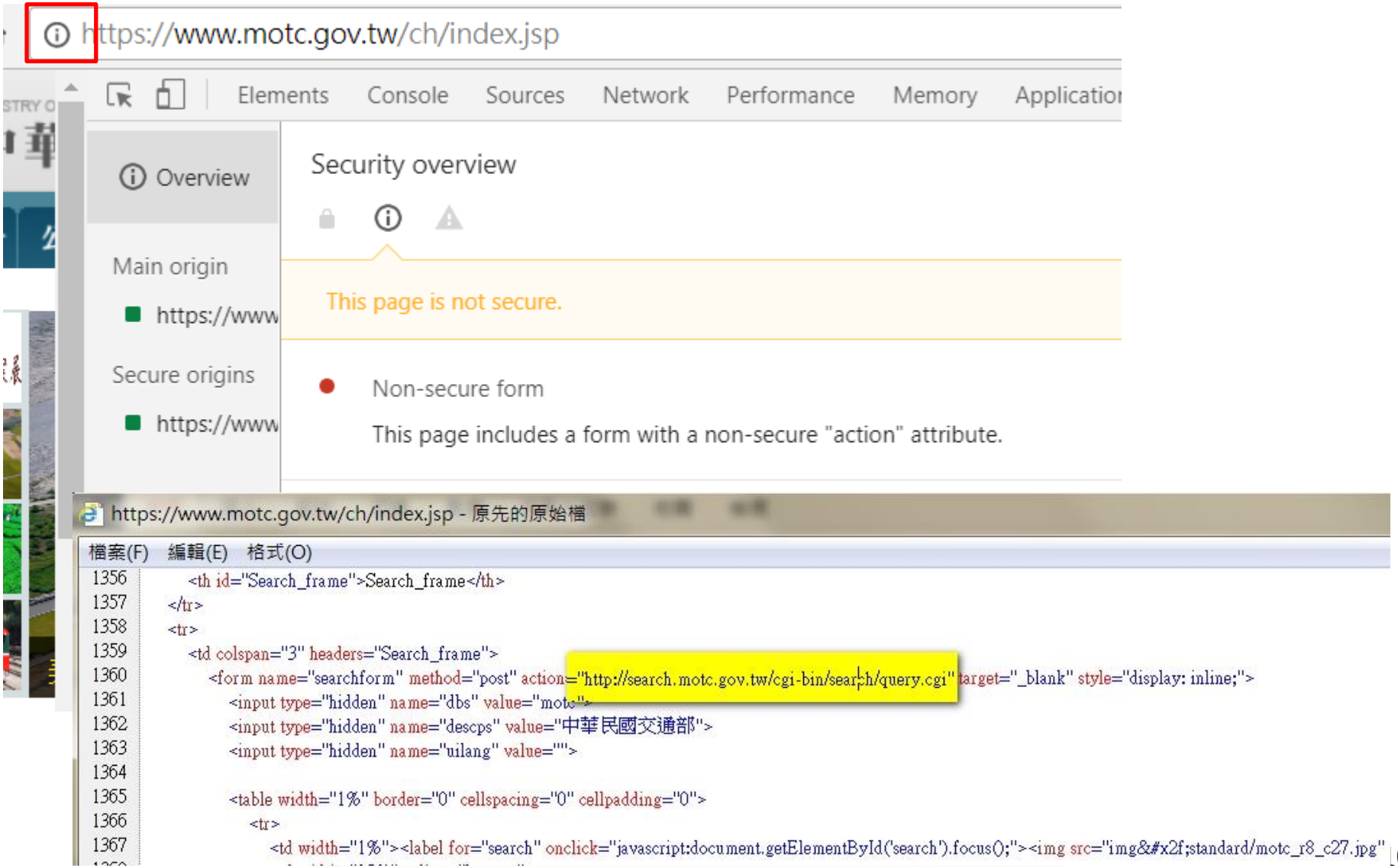
網站Mixed Content(2/3)

- Mixed Content(如網頁圖片未使用https)



網站Mixed Content(3/3)

- 用戶網頁中的form action使用了非https的超連結



SSL憑證主體與網域不符

安裝憑證時，請確認申請憑證之網域與主機網域相同

用戶瀏覽器支援HTTPS憑證版本

瀏覽器	支援HTTPS最低要求版本
Google Chrome	26+
Microsoft Internet Explorer	6+ (須搭配使用XP SP3+)
Firefox	1.5+
Apple Safari	Safari 3+ (OS X 10.5)

註1：Chrome 50以上版本已經不支援WinXP，只能安裝49以下之版本，
可參考http://www.ithome.com.tw/news/105317

註2：Firefox 53以上版本不再支援WinXP，
可參考http://technews.tw/2016/12/26/xp-vista-browser/

SSL類憑證申請說明

申請SSL憑證步驟

- 申請流程請參考GCA網站說明
  (https://gca.nat.gov.tw/web2/apply01.html)

1. 至OID網站查詢機關(構)之單位識別碼(OID)，如無則須新申請
2. 至GCA網站選擇**申請伺服器應用軟體憑證，選擇申請SSL類憑證(也可選擇線上插卡申請)**，線上填寫申請表，並製作憑證請求檔(CSR檔)，完成後上傳申請資料(CSR檔之產製請參考下頁說明)
3. 上傳資料成功之後，列印憑證申請書及附件，以公文或郵寄至國發會
   - 公文範例參考GCA網站說明
   - 若選擇線上插GCA IC卡申請SSL憑證則無須發文

- 注意事項

1. 提供單一網域及**多網域憑證(一張至多20個網域)**之申請(**目前未提供萬用網域**)
2. 申請憑證之網域須為來文申請機關註冊之網域。例如：新北市政府地政局來文申請網域為xxx.ntpc.gov.tw，此網域之註冊單位必須為新北市政府。(若網站委外開發營運，應由網站主管單位註冊網域並提出SSL憑證申請)
3. 若以IP提出申請，請先至http://whois.twnic.net.tw/確認該IP之註冊是否為提出申請之機關所屬，私人IP(Private IP)無法申請
4. **教育部所屬國立高中職以下可申請GCA SSL憑證**

憑證請求檔(CSR)產製 (1/2)

- 詳細產製步驟請參考GCA網站手冊
  https://gca.nat.gov.tw/web2/form02.html
- 請產製長度RSA 2048位元金鑰對
- 產製憑證請求檔(Certificate Signing Request)後至GCA網站進行申請作業，該CSR內只含公鑰，私密金鑰只會產生於產製CSR檔的主機中
- IIS
  - 利用IIS管理員產製
  - 私密金鑰會自動產生在IIS主機內，可利用mmc工具匯出備份
- Apache (Nginx)
  - 使用OpenSSL產製
  - 產生的server.key檔案即為私密金鑰，建議備份避免遺失
- Tomcat (JBoss、WebLogic等JAVA Based Web Server)
  - 使用JAVA keytool產製
  - 產生的.keystore檔案內含私密金鑰，建議備份避免遺失

憑證請求檔(CSR)產製 (2/2)

- 憑證請求檔內容(Certificate Signing Request, CSR)

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC0TCCAbkCAQAwgYsxCzAJBgNVBAYTAlRXMRMwEQYDVQQIDApTb211LVN0YXRl
MQ8wDQYDVQQHDAZUYWlwZWkxDDAKBgNVBAoMA0NIVDEMMAoGA1UECwwDR0NBMRgw
FgYDVQQDDA93d3cudGVzdC5jb20udHcxIDAeBgkqhkiG9w0BCQEWEWRjb25hbkBj
aHQuY29tLnR3MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2EfQVlvU
eIuMoChRXb/EA6iznr+0S/yllSqNEPNelDem+KwATmTpSxNmfXSUu92orKwL+crw
RwRvIV49JJoYELegtw/1aasOYrDmjMFmOBOr9HT1ql/csc0b1AntjHJKBRD2gtOE
nVPzOAy7nL4E6ZaBABRMs0QwB6Z3uH0FsZWR2X/ewTri16PAYy3D1GZ6NSnAt6oJ
qh9FEENYWY1i+awUtcYBYiu1d9GYdMAtBQAnwLPPD+dzYh7BhrJh7F9g9ucyfkKx
PDkzETRBffroZe0RKCZob/M6fzXqsZjIhXzbGjHk+qsiKgegSmHl/pCXKkHwDWfC
cOF8LSi3KFb21QIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAIgNSDOxceZYTOTV
CKUA+8dGUf1d6K4CKiLMnJuRhB7MNzCGCWEdwq/M3NS0J8TGo6V+P1dbMg0rkruw
LPyNr2juZMHwG+5CvpKCBC5jQb64JGMZqy5KGejunHtYmA1NN6ixDPiheXz6jmSi
y+OSjw9BwgYVI4FJv26GhmmYi0MOdvXYuotqiRQUTyUD963R1U1bEOR7uOT+1laP
Mhs95jG3jrTUDszBEKLue6NxnBDWFGiE0lmkDR5bbZPDDtO4DeGqhSd3c+IQ2f2q
DbqAnJKp3uYZujsQuFIEt1Czmwi3PMOXJcxaYbnio6DSirRbckvHylAWpcmvaiyz
bOzTSbA=
-----END CERTIFICATE REQUEST-----
```

- 申請多網域憑證只需產製1次CSR檔案並投單申請1張憑證

多網域憑證申請說明

申請方式選擇

提供以下兩種申請方式：

一. 我要申請SSL憑證」

使用時機:機關未申請GCA IC卡，填寫申請表後須發文至國發會。

二. 我要使用IC卡申請SSL類憑證

使用時機:機關已申請GCA IC卡，線上插卡申請，不須發文

※教育部所屬高中職及國中小，填寫申請表後請發文至教育部國民及學前教育署進行初審

網站申請書填寫

- 申請多網域憑證，請點選+來新增填寫網站名稱，申請上限為20個。
- 僅需上傳一個憑證請求檔(CSR)。

SSL類憑證安裝說明

如何安裝SSL憑證

- 憑證簽發後，系統將以電子郵件發送「憑證接受通知信」，請依照通知信說明接受憑證
- 完成憑證接受後請至GCA網站之「憑證查詢及下載」下載該憑證
- 依機關網站伺服器類型(Microsoft IIS、Apache、Tomcat或WebLogic)，至GCA網站之「憑證相關資料下載」專區下載安裝手冊，依手冊指示正確安裝憑證，包括
  - GRCA.cer
  - GRCA1_to_GRCA1_5.cer
  - GRCA1_5_to_GRCA2.cer
  - GCA2.cer
- 設定憑證串鍊

SSL憑證安裝注意事項(1/4)

- 瀏覽器是以網站Domain Name是否相同來認證SSL憑證，因此若有多台網站伺服器，只要網站Domain Name相同，則只需要申請1張SSL憑證即可，完成憑證安裝後可將私密金鑰與憑證搬移到其他主機上使用
  - IIS：參考GCA網站憑證備份與還原手冊，將私密金鑰與憑證匯出成pfx檔案，再複製到另一台主機匯入使用即可
  - Apache：複製.key、.cer/crt、GRCA1_5_GCA2.crt到另一台主機
  - Tomcat：複製.keystore檔案到另一台主機
- 同一台網站伺服器上若有多個不同網站，則可申請多網域憑證進行安裝

SSL憑證安裝注意事項(2/4)

- 憑證管理中心並不會接觸到用戶之私密金鑰，若私密金鑰遺失只能重新產製私密金鑰與CSR檔，之後重新發文申請憑證
- 常見私密金鑰遺失之原因
  - 產製CSR與憑證匯入之主機不同台
  - 產製多個CSR時忘記改私密金鑰或keystore檔名，因而造成檔案覆蓋
  - 產製完CSR後沒有備份私密金鑰，之後發生主機故障毀損，資料無法回復
  - 人為誤刪

SSL憑證安裝注意事項(3/4)

- 憑證串鍊需完整安裝(不可僅安裝SSL憑證)，否則將造成某些瀏覽器瀏覽網站時出現不信任告警(請參考下頁憑證串鍊自我檢測)
- 建議關閉不安全的通訊協定與演算法
  - 關閉SSLv2
    https://www.nccst.nat.gov.tw/VulnerabilityDetail?lang=zh&seq=1037
  - 關閉SSLv3
    https://www.nccst.nat.gov.tw/VulnerabilityDetail?lang=zh&seq=1025
    https://access.redhat.com/solutions/1232233
  - 檢測與修補是否存有不安全的金鑰交換加密演算法
    https://www.nccst.nat.gov.tw/VulnerabilityDetail?lang=zh&seq=1029
    http://download.icst.org.tw/attachfilenew/EXPORT檢測與修補方式.docx

SSL憑證安裝注意事項(4/4)

- 因多網域憑證目前1張只能放20個Domain Name，若同一台Web Server同一個IP上有超過20個網站，則需要使用SNI的技術才能安裝多張多網域憑證
- SNI相關說明請參考附錄三

憑證串鍊自我檢測

- 使用下列網站檢測憑證串鍊是否安裝正確
  https://www.sslshopper.com/ssl-checker.html
- 若檢測發現串鍊有中斷，請依前述憑證安裝手冊，重新設定憑證串鍊

SSL類憑證常見問題說明

SSL類憑證常見問題集(1/6)

- 參考網址(https://gca.nat.gov.tw/web2/faq-05.html)
- 如要在網路設備上安裝SSL憑證，因各家設備廠商介面不同，建議詢問設備廠商安裝方法
- 弱掃軟體Nessus因為參考Mozilla的憑證信賴清單，因此掃描到GCA之SSL憑證時會出現憑證不信任的風險，請忽略此風險或申請豁免，等後續Mozilla植入GRCA2後即可解決
- Microsoft Windows SHA256憑證支援性：
  - Windows 2003之IIS預設並不支援SHA256憑證，須下載微軟更新檔(更新檔編號為KB938397及KB968730) 安裝Patch到Server上即可
  - Windows 2000本身無法支援SHA256憑證，且微軟已不提供支援，建議更換新版的Windows Server
  - Windows XP需更新到SP3版才支援SHA256憑證

SSL類憑證常見問題集(2/6)

- Microsoft IIS
  - 若匯入憑證後按F5憑證即消失，代表憑證並未與私密金鑰合併，可能是私密金鑰遺失，請確認是否當初是在同一台主機上產製CSR檔
  - 如是，請參考下列網址嘗試回復私密金鑰
    http://www.entrust.net/knowledge-base/technote.cfm?tn=7905

SSL類憑證常見問題集(3/6)

- Microsoft IIS
  - Windows Server 2003容易發生私密金鑰被覆蓋，建議產製完新的請求檔後備份私密金鑰 (Win2003微軟已於2015/7終止支援，建議升版)
  - 可於CSR檔案產製後，使用mmc工具匯出憑證註冊要求(含私密金鑰)進行私密金鑰備份，或於憑證匯入後(完成憑證要求)參考GCA網站之**Windows IIS上SSL憑證備份與復原步驟說明**文件進行備份

SSL類憑證常見問題集(4/6)

- Apache
  - 憑證需轉換為Base64編碼，GCA核發之SSL憑證為DER編碼，轉換步驟可參考安裝手冊
  - httpd-ssl.conf需要設定對應的私密金鑰、SSL憑證與GCA憑證串鍊放置目錄
  - Apache 2.4.8以下版本與以上之憑證串鍊安裝方式有差異，請參考安裝手冊之說明
  - 請注意 Private Key檔案(server.key)之保存及備份

SSL類憑證常見問題集(5/6)

- Tomcat
  - JAVA版本需1.7版以上，1.6版以下有Bug，會造成自發憑證無法匯入
  - 重複執行金鑰產製會導致原本的私密金鑰被後面產製的金鑰覆蓋，因而與實際申請憑證的憑證請求檔(CSR)無法配對(私密金鑰保存在.keystore檔案中)
  - 私密金鑰與憑證不配對的錯誤訊息為
    金鑰工具錯誤: java.lang.Exception: 回覆時的公開金鑰與金鑰儲存庫不符
  - SSL憑證匯入時，請確認使用的.keystore檔與之前產生CSR時是同一個檔案
  - GRCA、GCA憑證請特別注意需依照手冊說明依順序匯入，此階段易產生錯誤而無法建立憑證串鍊，如發生匯入順序錯誤時，請參閱附錄二打斷keystore憑證串鍊說明處理，處理完後即可重新匯入憑證

SSL類憑證常見問題集(6/6)

- 憑證安裝後測試時使用IP連線，瀏覽器如出現告警畫面是正常現象，因為憑證內註記是Domain Name，瀏覽器比對輸入連線網址與憑證內Domain Name不符因而告警
- 因為瀏覽器只認憑證內註記之Domain Name，因此只要Domain Name不變的情況下，憑證可以備份後轉移到任何主機，不需重申請，例如：主機損毀、主機OS重新安裝等

報告完畢
謝謝指教

附錄一：憑證5層憑證串鍊設定

憑證安裝及設定

- GCA SSL最新之憑證串鍊為
  GRCA1 → GRCA1_to_GRCA1_5 → GRCA1_5_to_GRCA2 → GCA2 → SSL
- 憑證安裝手冊請參考GCA網站之文件
  (https://gca.nat.gov.tw/web2/form02.html)
- 若目前網站伺服器之憑證串鍊如非5層串鍊，請參考『SSL憑證重新設定5層串鍊說明』調整
  (http://gca.nat.gov.tw/download/GCA_SSL_Reset_5LayerChain.pdf)

附錄二：打斷keystore憑證串鍊步驟

打斷keystore憑證串鍊步驟(1/2)

- 若留有原本OpenSSL產生的server.key，則請跳到(3)步驟
- 下列%%中包含的內容請依照實際環境填入
  - 將Keystore轉換為pfx檔案
    keytool -importkeystore -srckeystore %keystoreFile% -destkeystore %pfxFile% -srcstoretype jks -deststoretype PKCS12 -srcalias %aliasName% -destalias %aliasName%
  - 從pfx檔案中分離私密金鑰(.key)
    openssl pkcs12 -in %pfxFile% -nocerts -nodes -out %server.key%

打斷keystore憑證串鍊步驟(2/2)

- 利用私密金鑰產生CSR檔案
  openssl req -new -key %server.key% -out %server.csr%
- 利用OpenSSL與私密金鑰產生自簽憑證
  openssl x509 -req -days 7305 -sha1 -extfile openssl.cfg -extensions v3_ca -signkey %server.key% -in %server.csr% -out %server.cer%
- 將自簽憑證匯入原本的keystore中，以打斷內部的憑證串鍊
  keytool -import -keystore %keystoreFile% -alias %private key entry% -file %server.cer%
- 經由上述動作後已經為乾淨的keystore，之後請參考GCA網站上的Tomcat憑證安裝手冊進行憑證匯入即可

附錄三：Server Name Indication (SNI)說明

SNI說明 (1/2)

- 讓單一IP主機可以安裝多張SSL憑證
- 支援的Web Server與Browser版本如下

Servers that Support SNI

- Microsoft Internet Information Server IIS 8 or higher
- Apache 2.2.12 or higher, must use mod_ssl
- Apache Tomcat on Java 7 or higher
- All versions of lighttpd 1.4.x and 1.5.x with patch, or 1.4.24 or higher without patch
- Nginx with implemented OpenSSL with SNI support

Desktop Browsers

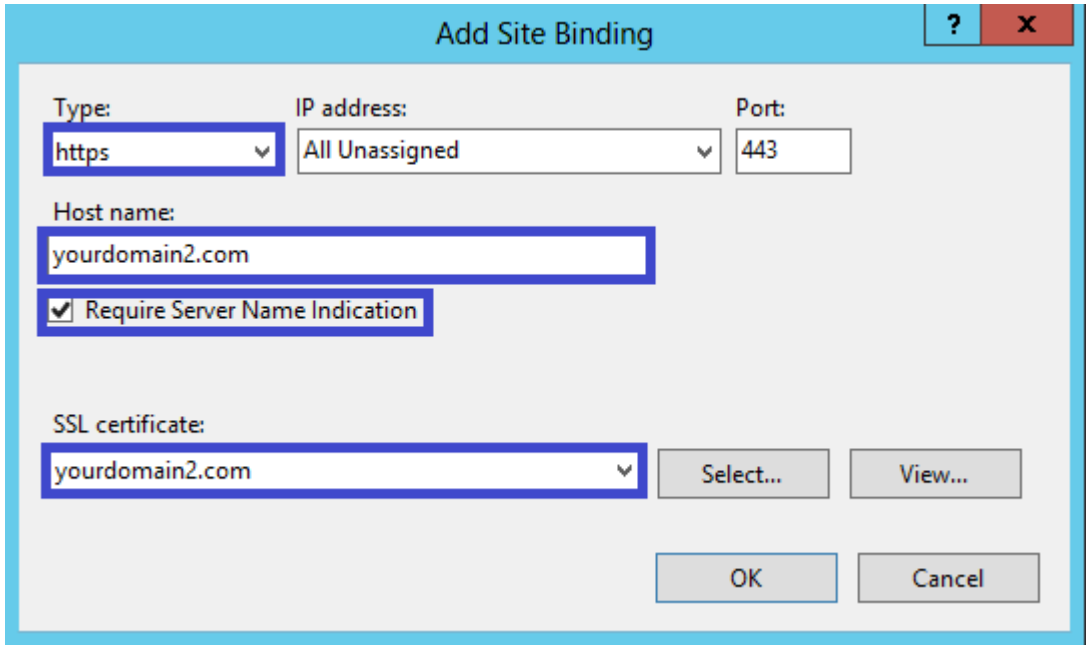
- Internet Explorer 7 and later on Windows Vista and later
  Internet Explorer (any version) on Windows XP does not support SNI
- Mozilla Firefox 2.0 and later
- Opera 8.0 (2005) and later
  TLS 1.1 protocol must be enabled
- Google Chrome:
  Supported on Windows Vista and later
  Supported on Windows XP on Chrome 6 and later
  Supported on OS X 10.5.7 on Chrome v5.0.342.1 and later
- Safari 2.1 and later
  Supported on OS X 10.5.6 and later
  Supported on Windows Vista and later

Mobile Browsers

- Mobile Safari for iOS 4. and later
- Android default browser on Honeycomb (v3.x) and later
- Windows Phone 7

SNI說明 (2/2)

- IIS設定方法



- Apache設定方法：使用VirtualHost
  - 可參考 https://www.digicert.com/ssl-support/apache-multiple-ssl-certificates-using-sni.htm
- Tomcat設定方法：使用SSLHostConfig
  - 可參考 http://www.studytrails.com/java/tomcat-multiple-ssl-certificates-host-using-sni/