政府機關網站導入HTTPS暨SSL類憑證應用實務說明會

國家發展委員會

108年9月

大綱

- 國際規範及憑證中心發展方向
- SSL憑證申請及管理注意事項
- SSL憑證申請說明
- SSL憑證安裝說明
- SSL憑證安裝及使用常見問題
- SSL憑證相關資訊安全介紹

SSL憑證與資訊安全

網路通訊的資訊安全問題

竊聽

冒名傳送

竄改

否認傳送

網際網路

小明

小華

釣魚網站的手法

- **偽裝：**網路釣客常會仿冒知名公司網站，製作類似的假網頁或使用變形的 網址（例如 www.yahoo.com.tw 可能變成 www.yhaoo.com.tw），再 用電子郵件或即時通訊軟體發送連結，通知你需要登入網站與修改 資料等訊息，一旦按下此連結連到該假網站的同時，你的電腦可能就會自動下載並安裝惡意軟體，且開始記錄你的登入資訊並回傳給釣客，用來獲取不當利益。

- 政府網站如何防範?

  透過可靠的憑證中心取得SSL憑證並安裝於網站上，可讓用戶有效識別政府網站，同時透過SSL憑證加密通道，可防止資料傳輸時被竊取。

可靠CA的重要性

CA須遵循國際規範及各瀏覽器之信賴根憑證計畫之規定執行憑證審驗及簽發作業

- Mozilla與Google的聲明指出，哈薩克政府並非可靠的CA，也未遵循任何發行憑證的規則，代表該國政府可以將任何網站的憑證授予任何人，進而監控網站的加密流量，哈薩克民眾一旦安裝政府的根憑證，政府便能解密與讀取人民所輸入或張貼的內容，也能攔截帳號資訊及密碼。(https://www.ithome.com.tw/news/132557)

- 賽門鐵克（Symantec）坦承旗下的Thawte憑證機構在網域擁有者不知情的狀況下發行了誤發了76個網域的164個憑證，以及未註冊網域的2456個憑證。(https://www.ithome.com.tw/news/99633)

最新國際規範及發展趨勢

■ 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。
   - ➢ 政府機關網站導入HTTPS安全連線

2. Google於CA/Broswer Forum會議中提案於2020年3月1日起，將SSL憑證效期縮減為397天。
   - ➢ 憑證管理中心配合縮短SSL憑證有效期限

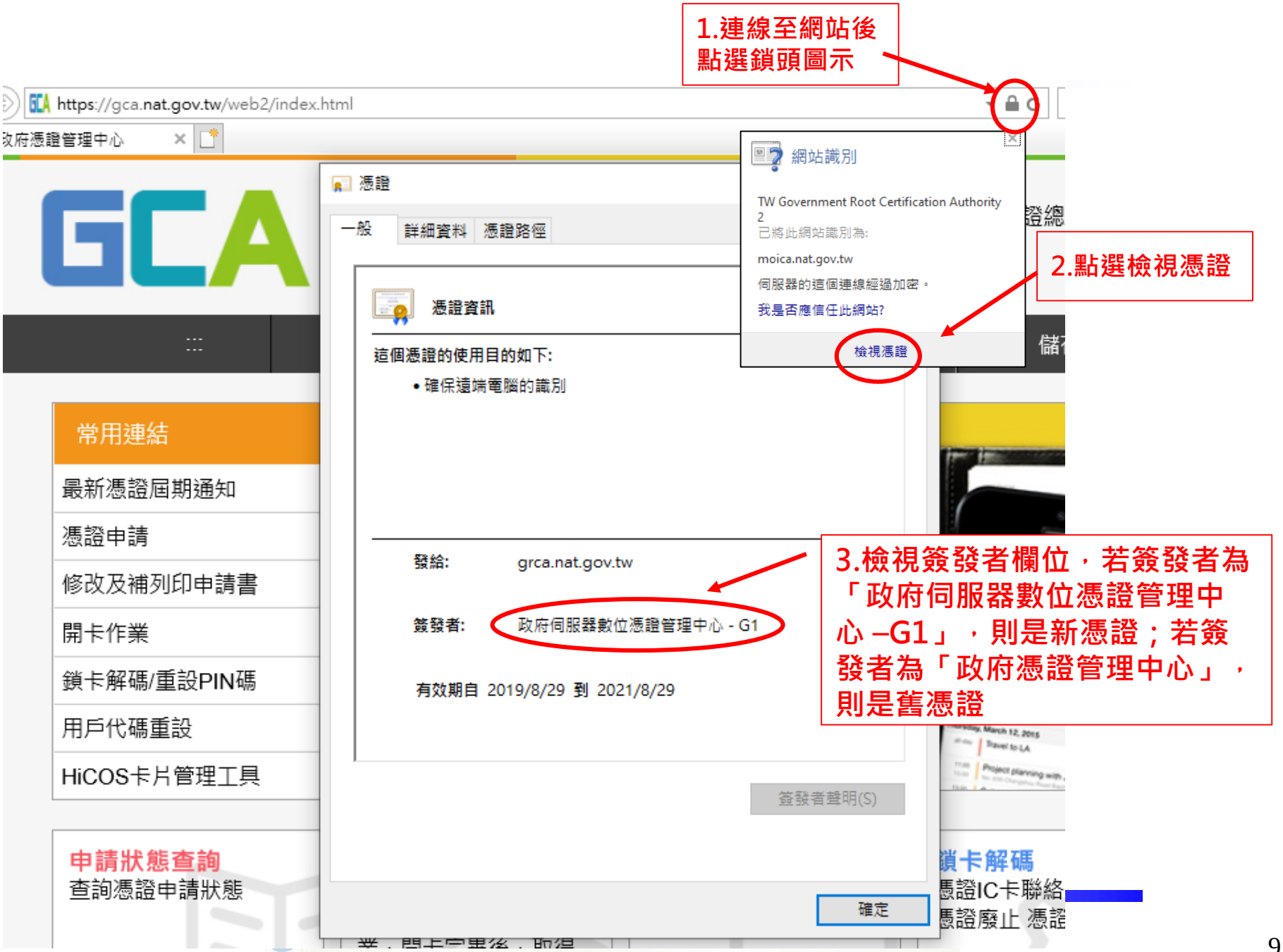
3. 國際瀏覽器大廠要求TLS/SSL憑證、SMIE憑證、Code sign憑證以及Time Stamp憑證必須為獨立之CA所簽發
   - ➢ 配合國際規範及憑證發展趨勢，國發會建置了政府伺服器數位憑證管理中心(GTLSCA)專職簽發SSL憑證。

政府SSL憑證現況說明

- (舊憑證)GCA簽發之SSL憑證效期皆限制109年7月18日到期，並於108年9月1日起停止簽發SSL憑證。

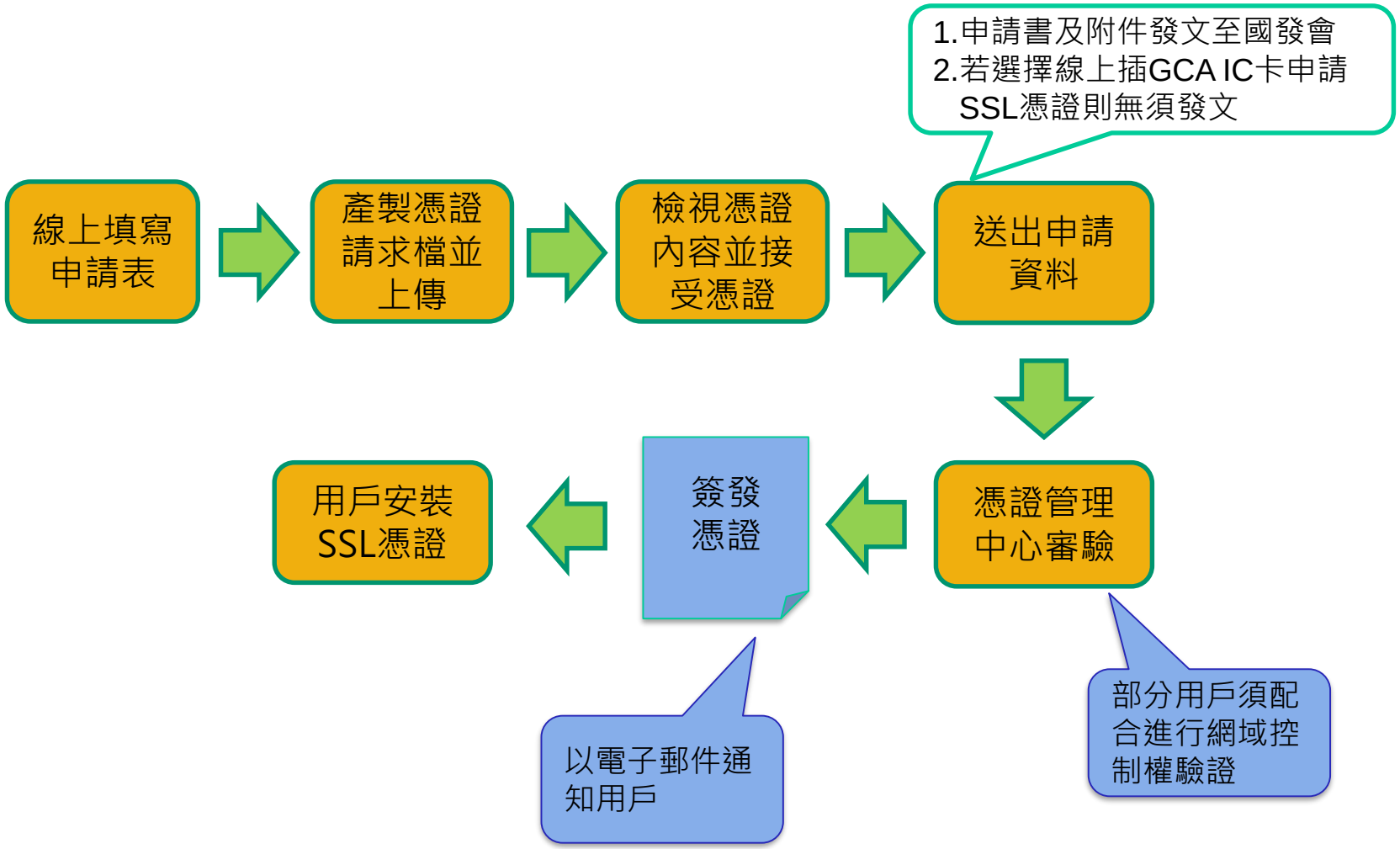
- (新憑證) **GTLSCA簽發之SSL憑證效期為2年**， GTLSCA於108年 9月上線，建議舊用戶(GCA簽發之SSL憑證)於109年4月1日前重新申請SSL憑證。

- 如何判定是GCA簽發之憑證或GTLSCA簽發之憑證??(見下頁說明)


1.連線至網站後
點選鎖頭圖示
https://gca.nat.gov.tw/web2/index.html
政府憑證管理中心
GCA
網站識別
TW Government Root Certification Authority 2
已將此網站識別為:
moica.nat.gov.tw
伺服器的這個連線經過加密。
我是否應信任此網站?
檢視憑證
2.點選檢視憑證
憑證
一般
詳細資料
憑證路徑
憑證資訊
這個憑證的使用目的如下:
• 確保遠端電腦的識別
發給: grca.nat.gov.tw
簽發者: 政府伺服器數位憑證管理中心 - G1
有效期自 2019/8/29 到 2021/8/29
簽發者聲明(S)
確定
3.檢視簽發者欄位，若簽發者為「政府伺服器數位憑證管理中心 –G1」，則是新憑證；若簽發者為「政府憑證管理中心」，則是舊憑證
常用連結
最新憑證屆期通知
憑證申請
修改及補列印申請書
開卡作業
鎖卡解碼/重設PIN碼
用戶代碼重設
HiCOS卡片管理工具
申請狀態查詢
查詢憑證申請狀態
鎖卡解碼
憑證IC卡聯絡
憑證廢止 憑證

SSL憑證申請說明

SSL憑證申請流程


1.申請書及附件發文至國發會
2.若選擇線上插GCA IC卡申請SSL憑證則無須發文
線上填寫申請表
產製憑證請求檔並上傳
檢視憑證內容並接受憑證
送出申請資料
憑證管理中心審驗
部分用戶須配合進行網域控制權驗證
簽發憑證
以電子郵件通知用戶
用戶安裝SSL憑證

開始SSL憑證申請


GCA
政府憑證
管理中心
網站導覽 | 政府憑證總覽 | 關於GCA | 常見問題 | 客服專區
憑證申請
憑證作業
訊息公告
儲存庫
資料下載
常用連結
最新憑證屆期通知
憑證申請
修改及補列印申請書
開卡作業
鎖卡解碼/重設PIN碼
用戶代碼重設
HiCOS卡片管理工具
點選『憑證申請』
採購網
政府標案查詢的好幫手
標案查詢
衛材藥品查詢
優先採購查詢
採購標的分類
申請狀態查詢
查詢憑證申請狀態
進度查詢
開卡作業
當您收到卡片時，為避免被冒用，請進行開卡作業，開卡完畢後，取得PIN碼，才可使用卡片。
我要開卡
屆期換發
查詢目前的憑證有效狀態及憑證詳細資料
我要換發
鎖卡解碼
憑證IC卡聯絡人修改
憑證廢止 憑證停用/復用
我要解碼
屆期通知
最新GCA憑證屆期重新申請通知
我要查詢

1.申請方式選擇

點選『申請伺服器應用軟體憑證』→選擇申請的憑證類別，再按下『下一步』

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。

2.用戶同意條款

正式申請憑證之前，為確保您的權益，請詳細閱讀『用戶約定條款』；再按下『我已閱讀並同意』代表同意條款內容，可繼續下列申請步驟。

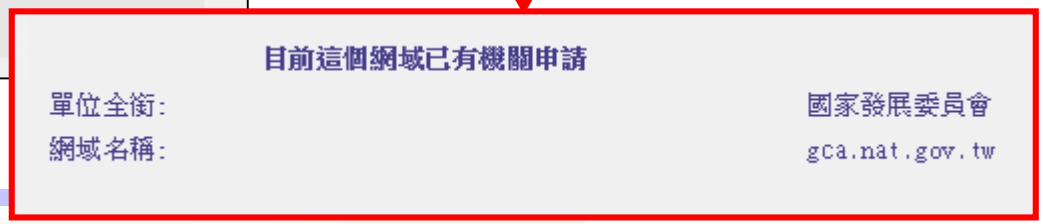
3.申請表填寫(1/2)

將表上所列之各項資訊正確填入。
注意：
*為必填資料。

網域註冊資料確認請至『政府中英文網域名稱註冊系統』(https://rs.gsn.gov.tw/)查詢。

※政府中英文網域名稱註冊系統查詢

查詢結果



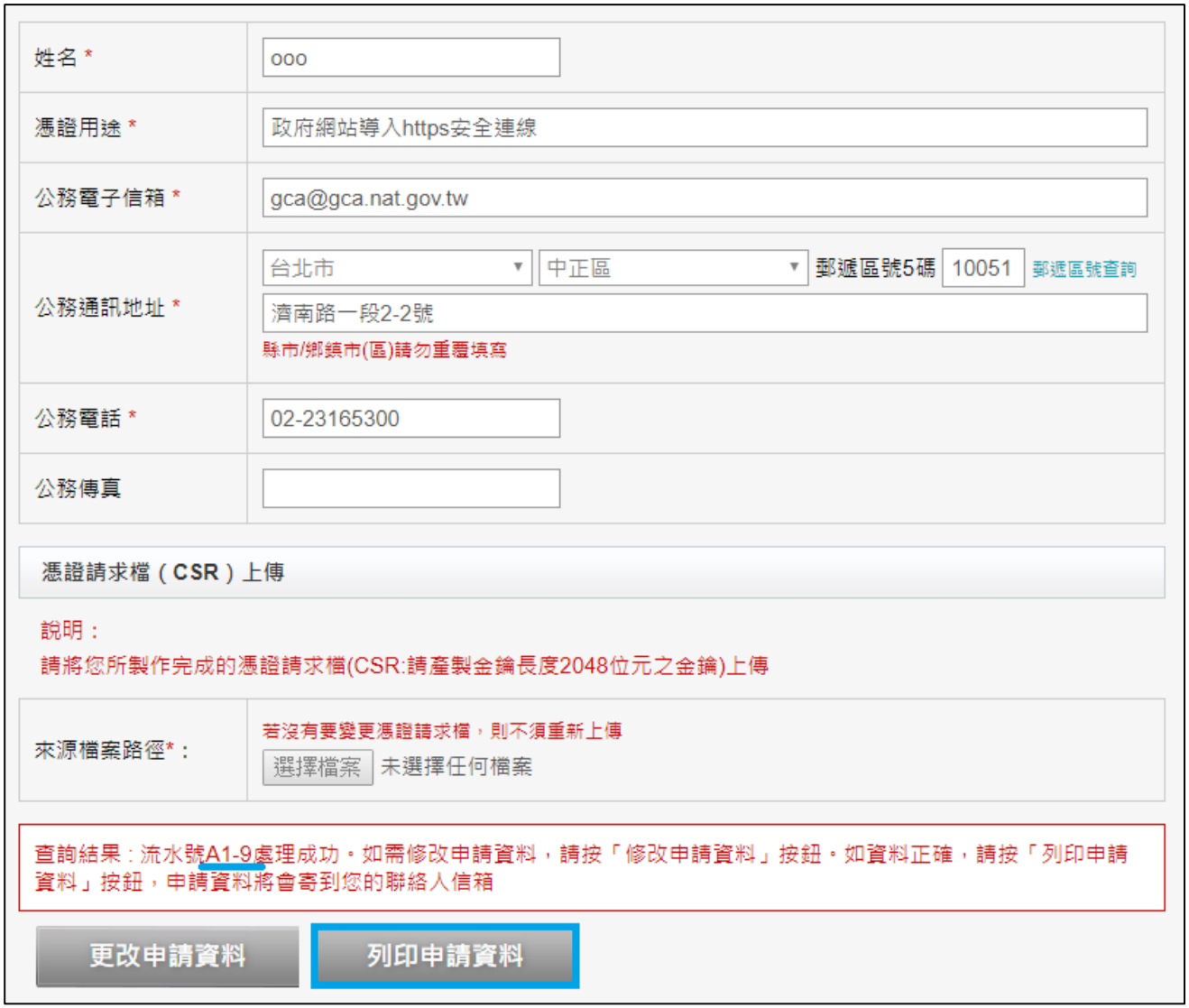
3.申請表填寫(2/2)

※一定要填寫正確信箱，憑證核發後，將以此信箱Email通知憑證核發。

4.憑證接受

確認憑證內容無誤後，點選接受憑證。

5.列印申請資料(1/2)



記下流水號，並點『列印申請資料』。

5.列印申請資料(2/2)


姓名 *
ooo
憑證用途 *
政府網站導入https安全連線
公務電子信箱 *
gca@gca.nat.gov.tw
公務通訊地址 *
台北市
中正區
郵遞區號5碼
10051
郵遞區號查詢
濟南路一段2-2號
縣市/鄉鎮市(區)請勿重覆填寫
公務電話 *
02-23165300
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:請產製金鑰長度2048位元之金鑰)上傳
來源檔案路徑*：
若沒有要變更憑證請求檔，則不須重新上傳
選擇檔案
未選擇任何檔案
查詢結果：申請書及用戶代碼函已經顯示於新視窗，並且寄送到您的聯絡人電子郵件信箱，請自行儲存與列印。
如尚需修改請按[更改申請資料]，完成請按[離開]按鈕離開。
離開
更改申請資料

6.申請表

GTLSCA SSL類憑證申請書

- 申請案號：A1-9
- 填寫日期：民國 108年 8月29日

網站資料

憑證用途	政府網站導入https安全連線
網站名稱(Domain Name)	gca.nat.gov.tw

政府機關資料

名稱	政府憑證管理中心憑證測試中心
機關/單位 OID	2.16.886.101.20003.20060.20001

備註：名稱欄位若為空白請在列印後自行填寫

憑證聯絡人資料

姓名	ooo
憑證用途	政府網站導入https安全連線
公務電子郵件信箱	gca@gca.nat.gov.tw
公務通訊地址	10051台北市中正區濟南路一段2-2號
公務電話	02-23165300
公務傳真	

機關單位請將申請書連同公文函送至國家發展委員會；國立高中職請函送至教育部國民及學前教育署，憑 證申請諮詢服務專線：02-2192-7111

7.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	A1-9
用戶代碼	12345678

憑證申請諮詢服務專線：02-2192-7111

(開放時間 08:30-18:00，例假日暫停服務)

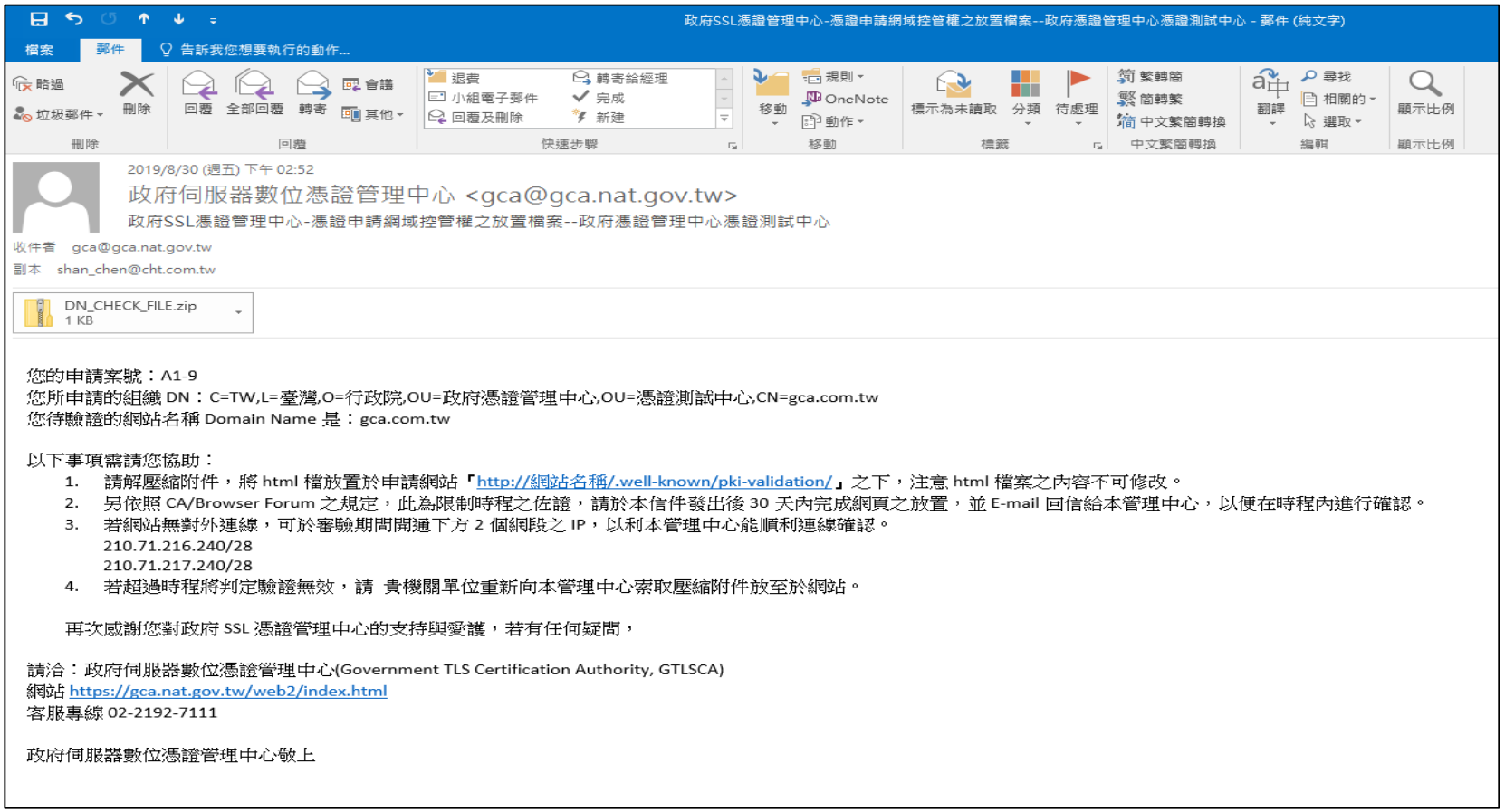
8.配合進行網域驗證

憑證審驗人員依據CA/Browser Forum之Baseline Requirements最新版第3.2.2.4節「Validation of Domain Authorization or Control」之規範，針對不同類型的網域會有不同審驗方式。

1. .gov及.edu的網域直接透過GSN網域註冊系統及學術網域註冊系統進行網域所有權確認。
2. 其他類的網域(如：.com、.org、.taipei、.net……)之驗證，因網域註冊管理者非政府單位，無法直接確認網域控制權，因此用戶須配合進行網域控制權驗證。

網域所有權驗證方式(1/2)

- 憑證管理中心將以電子郵件方式通知用戶配合進行網域控制權驗證，郵件中附帶一內含隨機亂數植的網頁檔案，並請用戶將此網頁放置於該網域指定的目錄，再由憑證管理中心進行驗證。



政府SSL憑證管理中心-憑證申請網域控管權之放置檔案--政府憑證管理中心憑證測試中心 - 郵件 (純文字)

檔案 郵件 告訴我您想要執行的動作...

略過 垃圾郵件 刪除 回覆 全部回覆 轉寄 會議 其他 退費 小組電子郵件 回覆及刪除 轉寄給經理 完成 新建 移動 規則 OneNote 動作 標示為未讀取 分類 待處理 繁轉簡 簡轉繁 中文繁簡轉換 翻譯 尋找 相關的 選取 顯示比例

2019/8/30 (週五) 下午 02:52

政府伺服器數位憑證管理中心 <gca@gca.nat.gov.tw>

政府SSL憑證管理中心-憑證申請網域控管權之放置檔案--政府憑證管理中心憑證測試中心

收件者 gca@gca.nat.gov.tw

副本 shan_chen@cht.com.tw

DN_CHECK_FILE.zip
1 KB

您的申請案號：A1-9
您所申請的組織 DN：C=TW,L=臺灣,O=行政院,OU=政府憑證管理中心,OU=憑證測試中心,CN=gca.com.tw
您待驗證的網站名稱 Domain Name 是：gca.com.tw

以下事項需請您協助：

1. 請解壓縮附件，將 html 檔放置於申請網站「http://網站名稱/.well-known/pki-validation/」之下，注意 html 檔案之內容不可修改。
2. 另依照 CA/Browser Forum 之規定，此為限制時程之佐證，請於本信件發出後 30 天內完成網頁之放置，並 E-mail 回信給本管理中心，以便在時程內進行確認。
3. 若網站無對外連線，可於審驗期間開通下方 2 個網段之 IP，以利本管理中心能順利連線確認。
   210.71.216.240/28
   210.71.217.240/28
4. 若超過時程將判定驗證無效，請 貴機關單位重新向本管理中心索取壓縮附件放至於網站。

再次感謝您對政府 SSL 憑證管理中心的支持與愛護，若有任何疑問，

請洽：政府伺服器數位憑證管理中心(Government TLS Certification Authority, GTLSCA)
網站 https://gca.nat.gov.tw/web2/index.html
客服專線 02-2192-7111

政府伺服器數位憑證管理中心敬上

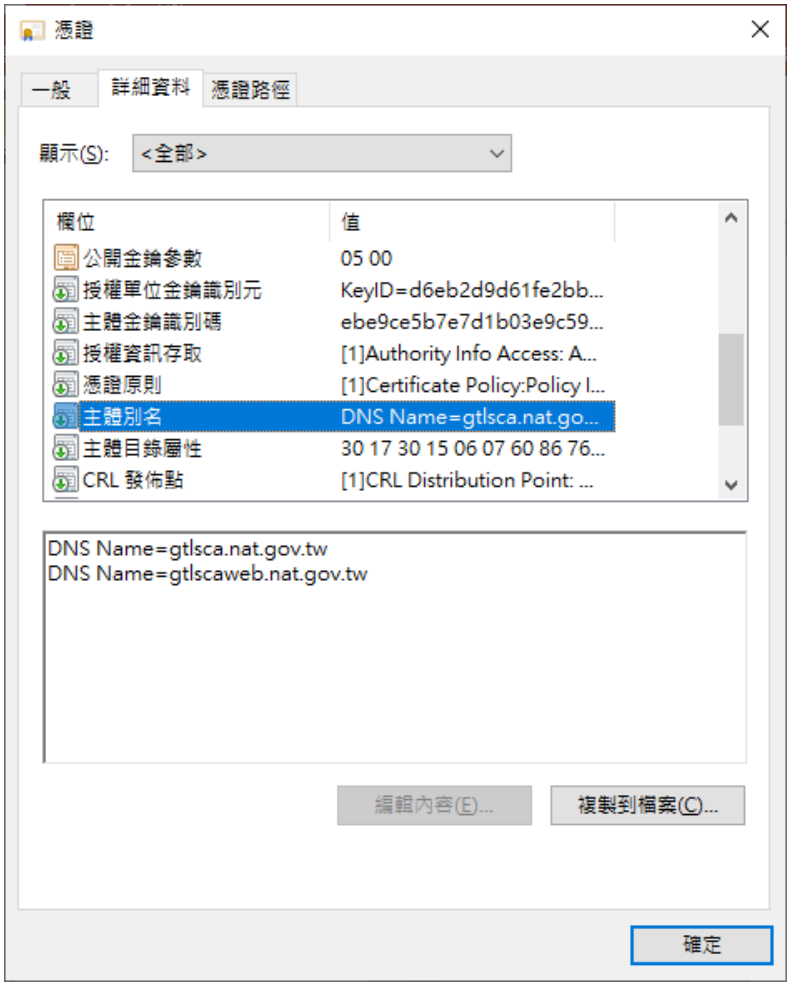
網域所有權驗證方式(2/2)

SSL憑證申請注意事項(1/2)

1. 不提供以IP申請SSL憑證
2. 網域不可含下底線符號「_」
3. 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)
4. 憑證請求檔(CSR檔)內只含公鑰，私密金鑰只會在用戶產製CSR檔的主機中，若私密金鑰遺失只能重新產製私密金鑰與CSR檔，並重新申請憑證。
5. 提供單一網域及多網域憑證之申請(**未提供萬用網域**)
6. 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
7. 申請多網域憑證時，一張多網域憑證所能填寫之網域數量上限為900字元

SSL憑證申請注意事項(2/2)

8. 多網域憑證名稱主體名稱之CN(Command Name)僅能註記一組網域名稱做為代表。



SSL類憑證安裝說明

如何安裝SSL憑證

1. 憑證簽發後，系統將以電子郵件發送「憑證簽發通知信」，請依照通知信說明取得憑證
2. 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
   - ROOTeCA_64.crt
   - eCA1_to_eCA2-New.crt
   - GTLSCA.crt
3. 設定憑證串鍊

SSL憑證安裝注意事項(1/2)

1. 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網站上之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、eCA1_GTLSCA.crt到另一台主機
   - Tomcat
     複製.keystore檔案到另一台主機
2. 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(2/2)

1. 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，之後重新發文或插卡申請憑證。
2. 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)
3. 建議關閉不安全的通訊協定與加密演算法
   - 關閉SSLv3
     https://www.nccst.nat.gov.tw/VulnerabilityDetail?lang=zh&seq=1025
   - 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

憑證串鍊自我檢測

1. 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
2. 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

GTLSCA憑證串鍊

1. GTLSCA SSL之憑證串鍊為
   eCA → eCA1_to_eCA2 → GTLSCA → SSL
2. GTLSCA為全新的CA，所使用之根憑證與中繼憑證皆與原有GCA不同
3. 取得新申請的GTLSCA SSL憑證後，請依照安裝手冊重新安裝新的憑證串鍊，原本GCA SSL憑證串鍊即不再使用

瀏覽器將於2020年終止TLS1.0與1.1

1. 微軟、蘋果、Google及Mozilla四大瀏覽器業者預計將在2020年上半年終止網頁加密驗證協定TLS (Transport Layer Security) 1.0及1.1版的支援
2. TLS 1.2的支援性
   - Web Server

     Windows Server 2008(IIS 7)、Apache 2.2.23、JAVA 7(Tomcat, WebLogic等)(含)以上
   - 瀏覽器

     IE11、Chrome 22、Firefox 27、Safari(Mac OS X: 7, iOS: 5) (含)以上
3. 可透過SSL Labs網站檢測網頁伺服器是否支援TLS 1.2
   https://www.ssllabs.com/ssltest/index.html

TLS1.0與1.1終止後之影響

1. Windows Server 2003 (IIS 6)最高只支援TLS 1.0，明年瀏覽器停止支援TLS 1.0後，將會造成網站無法正常瀏覽，建議盡快升級
2. Web Server本身需支援TLS 1.2，並且調整Web Server之設定啟用TLS 1.2
3. SSL/TLS協定只與Web Server本身支援與設定有關，SSL憑證本身並沒有區分版本，皆為同樣的憑證格式

TLS 1.2設定啟用(IIS)

1. 需修改Windows Registry (HKey_Local_Machine\System\CurrentControlSet\Control\Security Providers \SCHANNEL\Protocols)
2. 可直接於GTLSCA網站下載已經製作好之.reg檔案，解壓縮後點兩下即可進行設定，可免除手動修改Registry之麻煩
   https://gtlsca.nat.gov.tw/download/Disable_Protocols.zip
3. 本.reg檔案會開啟TLS 1.2 Server端協定，並關閉SSLv2、SSLv3、TLS 1.0和TLS 1.1之Server端協定
4. 此調整可能會影響微軟其他產品或功能之連線(ex: SQL Server、遠端桌面等)，建議先於測試主機測試確認後，再調整正式主機之設定

TLS 1.2設定啟用(Apache)

- 修改SSL設定檔(一般為httpd-ssl.conf)

```
#   SSL Protocol support:
#   List the protocol versions which clients are allowed to
#   connect with. Disable SSLv2 by default (cf. RFC 6176).
SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1

#   SSL Cipher Suite:
#   List the ciphers that the client is permitted to negotiate.
#   See the mod_ssl documentation for a complete list.
SSLCipherSuite EECDH+AES128:EECDH+AES256:EECDH+CAMELLIA:!ECDSA:!MD5
```

TLS 1.2設定啟用(Tomcat-1)

- 修改server.xml設定檔(Http11NioProtocol)

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
           connectionTimeout="8000"
           maxThreads="150"
           URIEncoding="UTF-8"
           enableLookups="false"
           SSLEnabled="true"
           scheme="https"
           secure="true"
           keystoreFile=
           keystorePass=
           clientAuth="false"
           sslProtocol="TLSv1.2"
           ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
                    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
                    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
                    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
                    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
                    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384" />
```

TLS 1.2設定啟用(Tomcat-2)

- 修改server.xml設定檔(Http11AprProtocol)

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11AprProtocol"
           connectionTimeout="8000" maxThreads="150" SSLEnabled="true"
           scheme="https" secure="true">
    <UpgradeProtocol className="org.apache.coyote.http2.Http2Protocol" />
    <SSLHostConfig honorCipherOrder="true" protocols="TLSv1.2"
                   ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
                            TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
                            TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
                            TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
                            TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
                            TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384">
        <Certificate certificateKeyFile="                    "
                     certificateFile="                    "
                     certificateChainFile="                    "
                     type="RSA" />
    </SSLHostConfig>
</Connector>
```

SSL類憑證安裝及使用常見問題

SSL類憑證常見問題集(1/6)

1. 參考網址(https://gca.nat.gov.tw/web2/faq-05.html)
2. 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

SSL類憑證常見問題集(2/6)

3. 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請求檔，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
- cer檔案無法直接轉換成pfx格式，需先依照安裝手冊完成註冊要求後，再參考GCA網站憑證備份與還原手冊把憑證與私密金鑰匯出即為pfx格式

SSL類憑證常見問題集(3/6)

3. Microsoft IIS

- 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)

4. Apache

- 憑證需轉換為Base64編碼，GTLSCA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GTLSCA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)

5. Tomcat
   - 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
   - 匯入憑證時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

SSL類憑證常見問題集(6/6)

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
7. 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

TLS/SSL協定相關網路威脅

TLS/SSL協定相關威脅及攻擊方式

1. Padding Oracle On Downgraded Legacy Encryption (POODLE)

2. Browser Exploit Against SSL/TLS (BEAST)

3. Compression Ratio Info-leak Made Easy (CRIME)

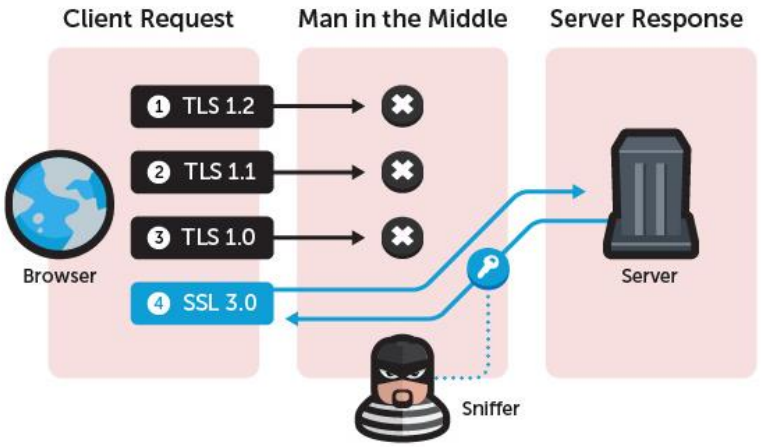
4. Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext (BREACH)

5. Heartbleed

POODLE攻擊

- POODLE(Padding Oracle On Downgraded Legacy Encryption)屬於一種中間人攻擊方式，因為SSL 3.0的密文區塊並沒有驗證填充資料，讓那些能劫持使用者和網站伺服器連線的攻擊者，有辦法去修改SSL密文的最後一個區塊，導致攻擊者能解密他們所截取的加密流量。

- 雖然SSL 3.0已經由TLS所取代，但如果連線有任一方不支援最新版本的話，TLS用戶端和伺服器將降級到較早版本的協定，使得POODLE攻擊得以進行。



POODLE對策

- 禁用SSL 3.0協定:
  - 伺服端設定Web Server
  - 用戶設定瀏覽器

- 當仍需要用到舊式系統時，OpenSSL.org的安全公告建議網頁伺服器使用TLS_FALLBACK_SCSV機制，以確保僅在必要時使用SSL 3.0，讓攻擊者不能再強制協定的降級。

BEAST攻擊

- BEAST(Browser Exploit Against SSL/TLS)攻擊法是透過**監聽封包**與**操控客戶端傳送某些特製的資料**，攻擊者就可能在SSL 3.0和TLS 1.0以前的版本破解出其中的某塊明文。

- 雖然在 TLS 1.1 以後將此問題修正了，可是攻擊者仍能在握手傳輸的中間，插入一個 TCP FIN或RST來降級協定，改用TLS 1.0進行攻擊。

BEAST對策

- 伺服端設定Web Server
  - 優先執行TLS 1.1和1.2協定
- 客戶端設定瀏覽器
  - 優先執行TLS 1.1和1.2協定
  - 在internet和intranet區阻止ActiveX Controls和Active Scripting

CRIME攻擊

- CRIME(Compression Ratio Info-leak Made Easy)是基於選擇明文攻擊法配合資料壓縮偶爾造成的資訊泄露。

- CRIME可竊取啟用資料壓縮的SSL/TLS協定所傳輸的私密Web Cookie。在成功解讀身分驗證Cookie後，攻擊者就能實行連線劫持和發動進一步攻擊。

CRIME對策

- 可藉由**禁用壓縮**而避免CRIME，無論是在用戶端的瀏覽器中禁用壓縮，還是由網站根據TLS的協商特性阻止使用資料壓縮。
  - 最新版本的Chrome和Firefox已處理此問題，IE則因不支援TLS壓縮而不受影響。
  - 使用TLS 1.2，因TLS 1.2預設是不使用任何壓縮。

BREACH攻擊

- BREACH(Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext)是一種CRIME攻擊法的變體，通過自適應超文字壓縮做瀏覽器偵聽和滲透，攻擊網頁伺服器內建的HTTP資料壓縮而解讀HTTPS私密資訊。

- 與CRIME攻擊一樣，BREACH也要能：1. 監聽密文。2. 操弄使用者送出某種 HTTP request。不同的地方是，BREACH 需觀察 server response 來達到攻擊目的。

BREACH對策

- **BREACH 與 SSL/TLS 版本無關**，與金鑰長度也無關，只要符合前面所說的假設前提，即有可能破解 SSL/TLS 加密保護的資料，進而作到 session hijacking，或是取得重要資料。

- 因此目前要防範BREACH只能注意：
  - **1. Server 不使用 HTTP 壓縮。**
  - **2. Server 不要將 client request 中的部份資料反映在 response 裡。**
  - **3. Server response 中不要包含重要的資料。**

Heartbleed漏洞與對策

- Heartbleed漏洞存在OpenSSL的TLS/DTLS 傳輸安全層的Heartbeat（心跳）擴充功能中，該漏洞受到攻擊時會造成記憶體內容的外洩，讓駭客可以讀取到系統記憶體內原本應該由OpenSSL軟體所保護的機密資料，例如帳號密碼，甚至信用卡交易的資料。這個漏洞並不是SSL/TLS協定的問題，而是OpenSSL函式庫在處理TLS擴充協定的錯誤。

- 對策：受影響的OpenSSL版本為1.0.1~1.0.1f版和 1.0.2-beta~1.0.2-beta1版，只要更新至1.0.1g及1.0.2-beta2以後的版本即可。

報告完畢
謝謝指教

附錄1：Server Name Indication (SNI)說明

SNI (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

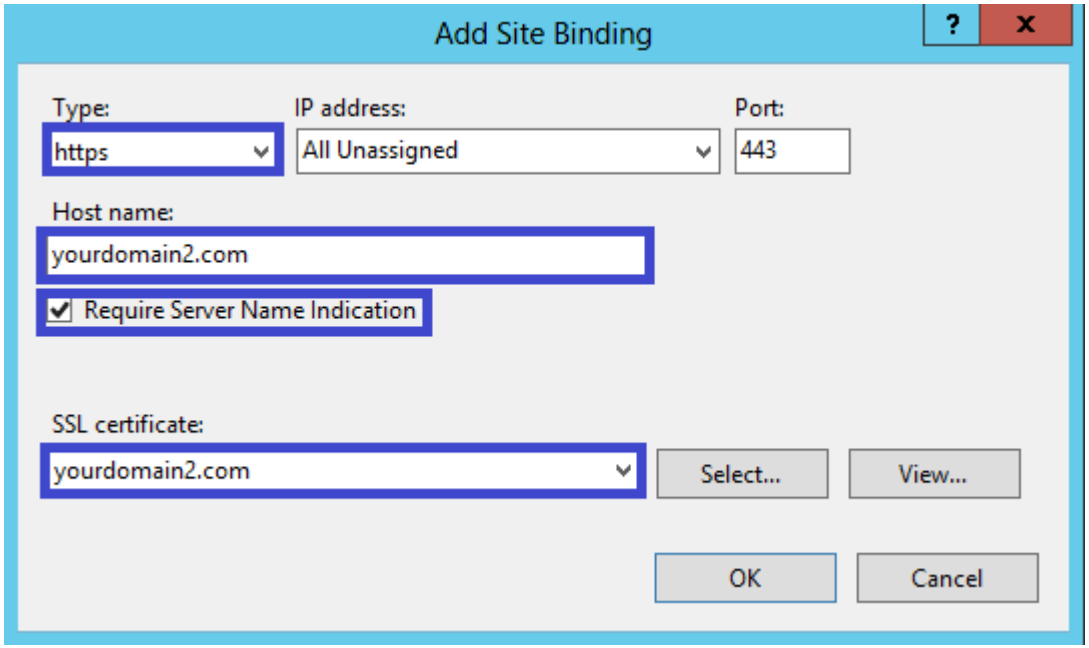
- Internet Explorer 7 and later on Windows Vista and later
  Internet Explorer (any version) on Windows XP does not support SNI
- Mozilla Firefox 2.0 and later
- Opera 8.0 (2005) and later
  TLS 1.1 protocol must be enabled
- Google Chrome:
  Supported on Windows Vista and later
  Supported on Windows 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 (2/2)

- IIS設定方法



- Apache設定方法：使用VirtualHost
- Tomcat設定方法：使用SSLHostConfig