

---

# 政府機關網站導入HTTPS安全連線說明

國家發展委員會  
106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
- SSL類憑證安裝說明
- SSL類憑證常見問題

# 緣由

---

- 行政院資安政策整體規劃
- 立法委員持續關注政府網站資料傳輸之安全
- 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，如Google自2017年1月起，當Chrome使用者瀏覽到低安全性的HTTP網站時，網址列將出現「不安全」的警告標示  
([http://www.bnext.com.tw/article/view/id/40891?utm\\_source=dailyedm\\_bn&utm\\_medium=content&utm\\_campaign=dailyedm](http://www.bnext.com.tw/article/view/id/40891?utm_source=dailyedm_bn&utm_medium=content&utm_campaign=dailyedm))

# 推動時程

---

- 行政院所屬二、三級機關應於本(106)年12月底前完成全球資訊網使用HTTPS傳輸協定
- 政府機關重要對外服務網站於107年12月前完成使用HTTPS傳輸協定
- 本會將依各機關提報IPv6對外服務網站進行檢核

# 導入https優點及面臨問題

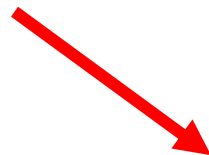
優點	面臨問題
<ul style="list-style-type: none"><li>✓ 確保用戶資料傳輸安全</li><li>✓ 增加民眾對政府網站信賴</li><li>✓ 避免機關網站被假冒的風險</li></ul>	<ol style="list-style-type: none"><li>1. 各機關<ul style="list-style-type: none"><li>✓ Mixed Content問題</li><li>✓ 現有提供API服務須更新</li></ul></li><li>2. 使用者<ul style="list-style-type: none"><li>✓ 太舊瀏覽器版本無法支援</li></ul></li></ol>

# 網站的Mixed Content問題

- 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



# 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也將於今年不再支援WinXP，  
可參考<http://technews.tw/2016/12/26/xp-vista-browser/>

# 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. 確認網站主機作業系統版本是否支援SHA256演算法簽發之憑證
2. 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)
3. 導入後網站須針對SSL相關弱點不定期進行修補



---

# 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

(<http://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**，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)

## ■ 注意事項

1. 僅提供單一網域之申請(未提供萬用網域及多網域憑證)
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. 目前未開放大專院校、學校網站申請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  
<http://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，私密金鑰會同步產生於產製CSR檔的主機**
- 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) Base64編碼

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC0TCCAbkCAQAwYsxCzAJBgNVBAYTA1RXMRMwEQYDVQQIDApTb211LVN0YXR1
MQ8wDQYDVQQHDAZUYWlwZWkxDDAKBgNVBAoMA0NIVDEMMAoGA1UECwwDR0NBMRgw
FgYDVQQDDA93d3cudGVzdC5jb20udHcxIDAeBgkqhkiG9w0BCQEWERjb25hbkbBj
aHQuY29tLnR3MIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2EfQVlvU
eIuMoChRXb/EA6iznr+0S/y1lSqNEPNelDem+KwATmTpSxNmFXSUu92orKwL+crw
RwRvIV49JJoYELegtw/1aasOYrDmjMFmOBOr9HT1ql/csc0b1AntjHJKBRD2gtOE
nVPzOAY7nL4E6ZaBABRMs0QwB6Z3uH0FsZWR2X/ewTri16PAYy3D1GZ6NSnAt6oJ
qh9FEENYWY1i+awUtcYBYiul9GYdMAAtBQAnwLPPD+dzYh7BhrJh7F9g9ucyfKkX
PDkzETRBffroZe0RKcZob/M6fzXqsZjIhXzbGjHk+qsiKgegSmHl/pCXKkHwDWfC
cOF8LSi3Kfb21QIDAQABAAAwDQYJKoZIhvcNAQELBQADggEBAI9NSDOx2ceZYTOTV
CKUA+8dGUf1d6K4CKiLMnJuRhB7MNzCGCWEdwq/M3NS0J8TGo6V+P1dbMg0rkruw
LPyNr2juZMHwG+5CvpKCBC5jQb64JGMZqy5KGejunHtYmA1NN6ixDPiheXz6jmSi
y+OSjw9BwgYVI4FJv26GhmmYi0ModvXYuotqiRQUTyUD963R1U1bEOR7uOT+1laP
Mhs95jG3jrTUDszBEKLue6NxnBDWFGiE0lmkDR5bbZPDDtO4DeGqhSd3c+IQ2f2q
DbqAnJKp3uYZujsQuFIet1Czmwi3PMOXJcxaYbnio6DSirRbckvHylAWpcmvaiz
bOzTSbA=
-----END CERTIFICATE REQUEST-----
```

---

# 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「憑證接受通知信」，請依照通知信說明接受憑證
2. 完成憑證接受後請至GCA網站「憑證查詢及下載」下載該憑證
3. 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
  - GRCA2.cer
  - new\_with\_old.cer
  - GCA2.cer
4. 設定憑證串鍊

## SSL憑證安裝注意事項(1/2)

---

- 如多台網站伺服器只要網站Domain Name相同，則只需要申請一張憑證即可，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、NewWithOld\_GCA2.crt到另一台主機
  - Tomcat：複製.keystore檔案到另一台主機

## SSL憑證安裝注意事項(2/2)

- 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CSR檔及重新申請憑證。
- 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)
- 建議網頁伺服器啟用OCSP Stapling機制
- 建議關閉不安全的通訊協定
  1. 關閉SSLv2  
<https://www.nccst.nat.gov.tw/NewInfoDetail?lang=zh&seq=1471>
  2. 關閉SSLv3  
<http://mickey-tang.blogspot.tw/2016/09/windows-iissslv3rc4.html>  
<https://ssorc.tw/5390>  
<https://access.redhat.com/solutions/1232233>
  3. 檢測與修補是否存有不安全的金鑰交換加密演算法  
<http://download.icst.org.tw/attachfilenew/EXPORT檢測與修補方式.docx>



# 憑證串鍊自我檢測

- 非IIS之網頁伺服器可以透過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

✓ The hostname (gca.nat.gov.tw) is correctly listed in the certificate.



Common name: gca.nat.gov.tw  
SANs: gca.nat.gov.tw  
Organization: 行政院  
Location: TW  
Valid from June 26, 2015 to June 26, 2018  
Serial Number: 6e80cf4dac90ff49ef5583748c2f3d4f  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: 行政院



Organization: 行政院  
Location: TW  
Valid from January 30, 2013 to January 30, 2033  
Serial Number: 088dd2963b8b629c194e3200da77ce2c  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: Government Root Certification Authority



Organization: Government Root Certification Authority  
Location: TW  
Valid from September 28, 2012 to December 5, 2032  
Serial Number: b559e7070725ad626294d512e7771554  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: Government Root Certification Authority



The hostname (gcaweb.nat.gov.tw) is correctly listed in t



The certificate is not trusted in all web browsers. You m  
Intermediate/chain certificate to link it to a trusted root  
this error. The fastest way to fix this problem is to conta



Common name: gcaweb.nat.gov.tw  
SANs: gcaweb.nat.gov.tw  
Organization: 行政院  
Location: TW  
Valid from January 15, 2017 to January 15, 2020  
Serial Number: 60859638810aad4109a402427e96e0e1  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: 行政院



Organization: 行政院  
Location: TW  
Valid from January 30, 2013 to January 30, 2033  
Serial Number: 088dd2963b8b629c194e3200da77ce2c  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: Government Root Certification Authority



串鍊中斷

---

# SSL類憑證常見問題說明

# SSL類憑證常見問題集(1/8)

- 參考網址(<http://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GCA2憑證時會出現憑證不信任的風險，請暫時忽略此風險，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(2/8)

## ■ Microsoft IIS

- 網站於Mozilla Firefox或Android平台瀏覽器瀏覽時出現不信任告警，此為IIS的機制造成(參考附錄說明)
- 針對Firefox之用戶，請用戶連線至GCA首頁(<https://gca.nat.gov.tw>)，瀏覽過一次GCA網站即可解決網站不信任問題
- Android則因為不同版本與使用的瀏覽器會有差異，5.0版以上參考上述Firefox用戶解法處理，較低版本會因使用瀏覽器不同而有差異
- 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>

# SSL類憑證常見問題集(3/8)

## ■ 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(4/8)

---

## ■ 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
- 請注意 Private Key檔案(server.key)的保存

# SSL類憑證常見問題集(5/8)

## ■ 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，請參閱附錄打斷keystore憑證串鍊說明處理



# SSL憑證常見問題集(6/8)

## ■ 手機支援性

	Firefox	Chrome	Safari	Opera	Android原生 Browser
<b>Android Mobile Device</b>	✓ 非IIS架站之網頁，可正常顯示 ✓ IIS架站之網頁瀏覽時可能會顯示不安全網頁*	✓ 非IIS架站之網頁，可正常顯示 ✓ IIS架站之網頁瀏覽時可能會顯示不安全網頁*	/	✓ 非IIS架站之網頁，可正常顯示 ✓ IIS架站之網頁瀏覽時可能會顯示不安全網頁*	✓ 非IIS架站之網頁，可正常顯示 ✓ IIS架站之網頁瀏覽時可能會顯示不安全網頁*
<b>Apple Mobile Device</b>	✓ 非IIS架站之網頁可正常顯示 ✓ IIS架站之網頁瀏覽時可能會顯示不安全網頁*	使用正常	使用正常	使用正常	/

\*註：參考Mozilla Root CA信賴清單



## SSL類憑證常見問題集(7/8)

- 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DN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DN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



## SSL類憑證常見問題集(8/8)

---

- 網站改用https加密連線後，需要整個網頁的內容皆為https安全連線才安全，若網頁中內嵌有http的非安全連線，瀏覽器即會出現混合內容(Mixed Content)的告警或是無法完整顯示網頁內容。
- 建議網頁中所有內嵌之內容都須要是https連線。

---

報告完畢  
謝謝指教

---

## 附錄：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
  1. 將Keystore轉換為pfx檔案  
`keytool -importkeystore -srckeystore %keystoreFile% -destkeystore %pfxFile% -srcstoretype jks -deststoretype PKCS12 -srcalias %aliasName% -destalias %aliasName%`
  2. 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)

- 3) 利用私密金鑰產生CSR檔案

```
openssl req -new -key %server.key% -out  
%server.csr%
```

- 4) 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%
```

- 5) 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%
```

- 6) 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2：SSL類憑證申請流程

# SSL憑證申請



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



政府電子採購網  
政府標案查詢的好幫手

標案查詢  
公開開標查詢  
備材藥品查詢  
優先採購查詢  
採購標的分類  
採購標公告查詢

**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.選擇類別

1.點選『憑證申請』  
2.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』

憑證申請

憑證申請作業流程說明

申請政府機關憑證IC卡

申請政府單位憑證IC卡

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

修改及補列印申請書

申請狀態查詢

OID新增及異動申請服務

憑證IC卡屆期換發服務

首頁 > 憑證申請 > 申請伺服器應用軟體憑證

申請伺服器應用軟體憑證

1

Step 1  
SSL、專屬類憑證申請選擇

2

Step 2  
同意用戶約定條款

3

Step 3  
線上填寫申請表

4

Step 4  
列印申請書及用戶代碼函

5

Step 5  
確認完成線上申請

申請伺服器應用軟體憑證說明

伺服器應用軟體憑證之簽發對象為政府機關（構）及政府單位的伺服器應用軟體，包括SSL伺服器應用軟體與專屬類伺服器應用軟體兩種，其中，SSL類伺服器應用軟體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。  
專屬類伺服器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器應用軟體憑證，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、專屬類伺服器應用軟體憑證為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

1. 一個憑證請求檔(CSR)，只能對應申請一個案號。

2. 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)。

3. 請多利用公文電子交換將憑證申請書於發文時以PDF檔案格式或影像掃描檔附件傳送。

4. 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。

5. 若申請內容資料不符，將Email通知退件處理。

6. 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。

7. 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email補件，如未補件則採退文方式辦理。

8. 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。

9. 一個憑證僅能對應一個網域。

請選擇您要申請的憑證類別

☒ 我要申請SSL類憑證

☐ 我要申請專屬類憑證

下一步

33

## 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『下一步』代表同意條款內容，可繼續下列申請步驟。

憑證申請

憑證申請作業流程說明

申請政府機關憑證IC卡

申請政府單位憑證IC卡

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

修改及補列印申請書

申請狀態查詢

OID新增及異動申請服務

憑證IC卡屆期換發服務

首頁 > 憑證申請 > 申請伺服器應用軟體憑證 (我要申請SSL類憑證) 步驟2

申請伺服器應用軟體憑證 (我要申請SSL類憑證) 步驟2

1

Step 1  
SSL-專屬類憑證申請選擇

2

Step 2  
同意用戶約定條款

3

Step 3  
線上填寫申請表

4

Step 4  
列印申請書及用戶代碼函

5

Step 5  
確認完成線上申請

我同意用戶約定條款

政府憑證管理中心(以下簡稱本管理中心)之用戶，係指記載於本管理中心所簽發憑證的憑證主體名稱(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)、單位。

用戶之義務

- 應遵守本管理中心憑證實務作業基準(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。
- 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。
- 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，用戶應主動通知本管理中心。
- 應妥善保管及使用私密金鑰。
- 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，如發生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。
- 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者權益受損時，應自行承擔責任。
- 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生移轉時，用戶應廢止原憑證並重新申請憑證。
- 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。

下一步

### 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。

#### 申請伺服器應用軟體憑證 (我要申請SSL類憑證) 步驟3

1

2

3

4

5

Step 1  
SSL、專屬類憑證申請選擇

Step 2  
同意用戶約定條款

Step 3  
線上填寫申請表

Step 4  
列印申請書及用戶代碼函

Step 5  
確認完成線上申請

伺服器應用軟體憑證申請表(SSL類)

申請本類憑證必須附上相對的憑證簽發申請檔(CSR)!

註冊資料(標註\*者請務必填寫)

政府機關單位識別碼OID \*

2.16.886.101.20003.20060.20001

請點選查詢、將結果正確填入此欄位。

政府機關單位OID查詢

用戶代碼\*

請自行設定6位到10位之英數字或符號 (大小寫有別)，查詢憑證申請進度、憑證IC卡開卡、解卡鎖碼/重設PIN碼以及憑證暫時停用等作業皆會使用到用戶代碼，請務必牢記！

輸入用戶代碼：●●●●●●

確認用戶代碼：●●●●●●

網站資料(標註\*者請務必填寫)

★網站名稱(Domain Name)\*  
如：www.cht.com.tw

[gca.nat.gov.tw](https://gca.nat.gov.tw) 請確認申請網域為該申請機關註冊之網域。

★網站URL\*  
如：https://www.cht.com.tw

<https://gca.nat.gov.tw> 僅填寫伺服器位址底下之路徑不需填

# ※政府中英文網域名稱註冊系統查詢

政府中英文網域名稱註冊系統

申請同意事項  
申請流程  
網域名稱查詢  
網域名稱申請  
申請表列印  
進度查詢  
密碼異動  
資料查詢/異動  
FAQ  
DNS指定與異動  
回填中文域名  
回首頁

政府網域包括英文網域「GOV.TW」，與中文網域「政府.TW」（別名為「政府.台灣」或「政府」）。

每一機關（構）註冊之屬性型英文網域名稱以一個為限，中文網域名稱除機關全稱外，簡稱以二個為限，並應排列優先順序；各機關因業務需要，另於台灣網路資訊中心(TWNIC)註冊泛用型中文網域名稱(.TW或.台灣)，不受此限。

**範例：**行政院英文網域名為「EY.GOV.TW」，中文網域名為「行政院.政府.TW」。

**網域名稱之命名：**  
各機關（構）申請註冊之名稱，應以申請機關（構）之正式中、英文全銜，或與中、英文全銜有關之縮寫、字詞、簡稱為限。

1. 中、英文全銜範例：行政院中、英文全銜為「行政院」與「Executive Yuan」，中文網域名稱可命名為「行政院.政府.TW」，英文網域名稱可命名為「EXECUTIVEYUAN.GOV.TW」。
2. 英文縮寫範例：行政院英文全銜為「Executive Yuan」，縮寫為「EY」，英文網域名稱可命名為「EY.GOV.TW」。
3. 英文字詞範例：行政院英文全銜為「Executive Yuan」，英文網域名稱可命名為「EXECUTIVE.GOV.TW」。
4. 中文簡稱範例：國家發展委員會中文全銜為「國家發展委員會」，簡稱為「國發會」，中文網域名稱可命名為「國發會.政府.TW」。

詳細請參考  
[政府網域名稱申請同意事項](#)

政府中英文網域名稱查詢(可先確認網域名稱是否重覆)

輸入網域名稱  .

查詢結果

目前這個網域已有機關申請

單位全銜：

國家發展委員會

網域名稱：

gCa.nat.gov.tw

### 3.申請表填寫(2/2)

憑證聯絡人資料(標註*者請務必填寫)	
說明： 1. 憑證聯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。	
姓名 *	<input type="text" value="000"/>
憑證用途 *	<input type="text" value="政府網站導入https安全連線"/>
公務電子信箱 *	<input type="text" value="gca@gca.nat.gov.tw"/>
公務通訊地址 *	<div>台北市 <input type="text" value="中正區"/> 郵遞區號5碼 <input type="text" value="10051"/> <a href="#">郵遞區號查詢</a></div> <div>濟南路一段2-2號</div> <div>縣市/鄉鎮市(區)請勿重覆填寫</div>
公務電話 *	<input type="text" value="02-23165300"/>
公務傳真	<input type="text"/>
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，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*：	<input type="text" value="C:\Users\kathy\Desktop\"/> <input type="button" value="瀏覽..."/> <div>點『瀏覽』按鈕，選擇來源檔案路徑。 憑證請求檔需自行製作，一個請求檔核發一張憑證。</div>
查詢結果：	
<input type="button" value="上傳申請資料"/>	

※一定要填寫正確信箱，  
憑證核發後，將以此信箱  
Email通知進行憑證接受。



## 4.列印申請資料(1/2)

姓名 *	<input type="text" value="000"/>
憑證用途 *	<input type="text" value="政府網站導入https安全連線"/>
公務電子信箱 *	<input type="text" value="gca@gca.nat.gov.tw"/>
公務通訊地址 *	<div>台北市 <input type="text" value="中正區"/> 郵遞區號5碼 <input type="text" value="10051"/> <a href="#">郵遞區號查詢</a></div> <div><input type="text" value="濟南路一段2-2號"/></div> <div>縣市/鄉鎮市(區)請勿重覆填寫</div>
公務電話 *	<input type="text" value="02-23165300"/>
公務傳真	<input type="text"/>
憑證請求檔 ( CSR ) 上傳	
<p>說明：</p> <p>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，請輸入檔案所存放之位置，可按"瀏覽"按鈕尋找您的檔案</p>	
來源檔案路徑*：	<input type="text" value="C:\Users\kathy\Desktop\c"/> <input data-bbox="1227 1204 1339 1236" type="button" value="瀏覽..."/>
<div>查詢結果：流水號00001000000000000000160545處理成功。如需修改申請資料，請按「修改申請資料」按鈕。如資料正確，請按「<a href="#">列印申請資料</a>」按鈕，申請資料將會寄到您的聯絡人信箱</div>	
<div><input type="button" value="更改申請資料"/> <input type="button" value="列印申請資料"/></div>	

記下流水號，  
並點『列印  
申請資料』。

## 4.列印申請資料(2/2)

姓名 *	<input type="text" value="□□□"/>
憑證用途 *	<input type="text" value="政府網站導入https安全連線"/>
公務電子信箱 *	<input type="text" value="gca@gca.nat.gov.tw"/>
公務通訊地址 *	<div>台北市 <input type="text" value="中正區"/> 郵遞區號5碼 <input type="text" value="10051"/> <a href="#">郵遞區號查詢</a></div> <div>濟南路一段2-2號</div> <div>縣市/鄉鎮市(區)請勿重複填寫</div>
公務電話 *	<input type="text" value="02-23165300"/>
公務傳真	<input type="text"/>

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，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\*：

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。

## 5.申請表

### GCA SSL類憑證申請表

- 申請案號：0000100000000000000160545

- 填寫日期：民國 106年 2月20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
網站URL	https://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
電子郵件信箱	如需寫入電子郵件信箱，請於收到卡片且完成開卡作業後，再至憑證作業之寫入憑證內安全電子郵件信箱功能進行寫入

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	○○○
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	

請將憑證申請表連同公文一併傳送至國家發展委員會，憑證申請諮詢服務專線：0 2-2192-7111



## 6.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	00001000000000000000160545
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)