[五、如何產生 CSR 文件]

依據伺服器環境不同，產生 CSR 的方式亦不相同，以下依據常用之伺服器軟體分別列出產生說明教學，若在操作上有任何問題，請直接聯繫亞太客服或您的伺服器環境提供商。

➔ 前導說明 - 產生 CSR 時常見問題

- **不要出現特殊字元**

  在申請伺服器憑證時，不要出現某些特殊字元，否則在您提交 CSR 後，會出現"105"的錯誤代碼。這個錯誤是由於在您產生 CSR 時，輸入的資訊中包含一些特殊字元，如：(@,#,&,!,等等，例如：您可以將"&"用"and"代替)。

- **什麼是公用名 Common Name？**

  在您產生 CSR 時，公用名 (Common Name) 是必須填寫的，但許多客戶填寫這一項時，經常填錯或不符合標準。

  公用名 (Common Name) 是您的主機名稱 + 網域名稱，比如：www.myssl.com.tw 的伺服器憑證是頒發給某一台主機的，而不是一個域名，您的公用名 (Common Name) 必須與您要使用伺服器憑證的主機的全名完全相同，因為 www.domain.com 與 domain.com 是不同的。

  註：用戶在產生 CSR 的時候，若 Domain 為 yourdomain.com 請產出 CSR 為 www.yourdomain.com ，憑證中心所頒發的憑證將在額外自動配額 yourdomain.com

- **保管好私鑰**

  要產生 CSR 檔，你必須為伺服器建立一對密鑰對，密鑰對和憑證是不可分開的，一旦您遺失了公鑰、私鑰或密碼，重新產生密鑰對後，和原來的憑證就不相同了。如果您申請的是 Geotrust SSL 憑證，可以重新提交 CSR 免費重發憑證；如果您申請的是 RapidSSL 憑證，就必須重新付費申請憑證。

  (注意：您必須同時保存.key 和.csr 文件)

- **CSR 檔產生加密長度必須為 2048 bit**

  為加強憑證安全強度，憑證中心已經不頒發低於 2048 bit 的 CSR 憑證提交資訊，請務必在 CSR 產生時候選擇使用 2048 bit 產生。

➔ CSR 產生說明

■ ApacheSSL

" OpenSSL " 工具被用來產生 CSR 和密鑰，它來自于 OpenSSL 包，一般被安裝在/usr/local/ssl/bin 目錄下，如果您安裝在其他目錄下，請做相應調整，你也可以自行下載 OpenSSL，

1. 如果是 Unix 或者 Linux 版本，請在命令行中執行：
   - 更改目錄到 SSL KEY 目錄，請輸入：cd/usr/local/ssl/private
   - 輸入下列命令產生密鑰對： openssl genrsa -des3 2048 > //server.key
   - 更改目錄到 SSL Certificate：cd /usr/local/ssl/cr
   - 使用下列命令產生 CSR 文件：openssl req -new -key //ssl.key >server.csr

2. 如果是 Win32 版本，請運行 cmd.exe 進入命令視窗，執行：
   set OPENSSL_CONF=openssl.cnf
   openssl req -new -nodes -keyout server.key -out server.csr

3. 於是當前目錄下將產生兩個檔：server.key 和 server.csr。請妥善保存這兩個檔，請不要洩露 server.key 私鑰文件。
4. 在這一命令執行的過程中，系統會要求您填寫如下資訊：

Country Name (2 letter code)	使用國際標準組織(ISO)國碼格式，填寫 2 個字母的國家代號台灣請填寫 TW。
State or Province Name (full name)	省份，比如填寫 Taipei
Locality Name (eg, city)	城市，比如填寫 Taipei
Organization Name (eg, company)	組織單位，比如填寫公司名稱的拼音
Organizational Unit Name (eg, section)	比如填寫 IT Dept
Common Name (eg, your websites domain name):	使用 SSL 加密的網站地址。請注意這裡並不是單指您的網域名稱，而是直接使用 SSL 的網站名稱 例如:pay.abc.com。 一個網站這裡定義是： abc.com 是一個網站； www.abc.com 是另外一個網站； pay.abc.com 又是另外一個網站。
Email Address	郵件位址，可以不填
A challenge password	可以不填
An optional company name	可以不填

   以上所有欄位必須用英文或拼音形式輸入。

5. 用一個文字編輯器（Notepad 或 VI），打開 " server.csr " ，把裡面的內容全部複製到信件中提供給亞太客服即可。

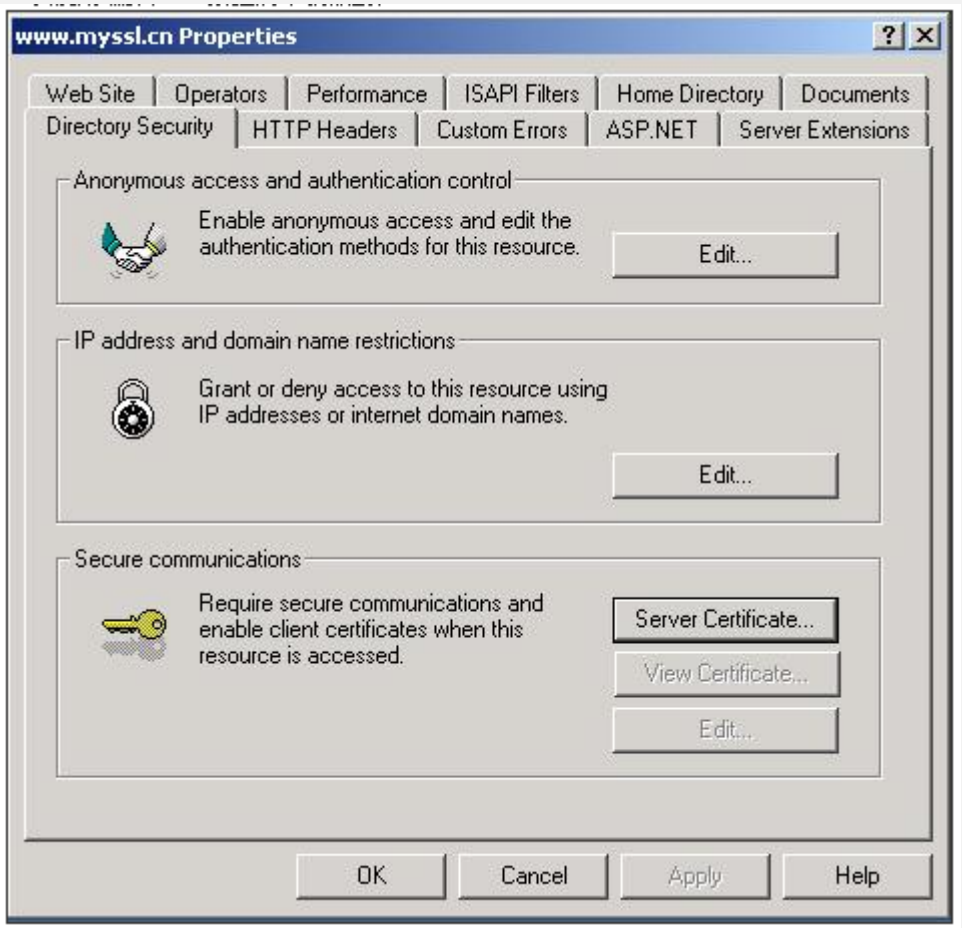
■ Lotus Domino

1. 運行 Domino 的管理用戶端。
2. 通過 “File - Open Server” ，選擇您要管理的 Domino 伺服器。
3. 按 file 標籤。
4. 雙擊伺服器憑證管理資料庫 Server Certificate Administration Database(certsrv.nsf)。
5. 通過管理員面板，按系統資料庫 System Database 並選擇在本地打開 Domino 伺服器憑證管理 Domino Server Certificate Administration (Certsrv.nsf)。
6. 按 “Create Key Ring” 。
7. 輸入密鑰對檔的名稱在 “Key Ring File Name” 欄。
8. 在 “Key Ring Password” 欄輸入一個密碼，這個密碼以數位和字母構成，並區分大小寫。它將用來保護這個密鑰檔不被未授權人使用，密碼長度至少在 12 位元以上。
9. 指定伺服器專用名稱 Distinguished Name 的內容。

10. 按“Create Key Ring”。
11. 當你看到關於“Key Ring ”和“Distinguished server name”的資訊時，按“ok”。
12. 按“Create Certificate Request”。
13. 如果要對在伺服器憑證管理器上提交這個請求做日誌，請在“Log Certificate Request”欄“Yes”，否則，選擇“No”.
14. 按“Create Certificate Request”。
15. 輸入你在第 4 步中指定的密碼。
16. 至此，已經產生了密鑰對和 CSR。
17. 用一個文字編輯器（Notepad 或 VI），打開 " Certificate Request "，把裡面的內容全部複製到信件中提供給亞太客服即可。

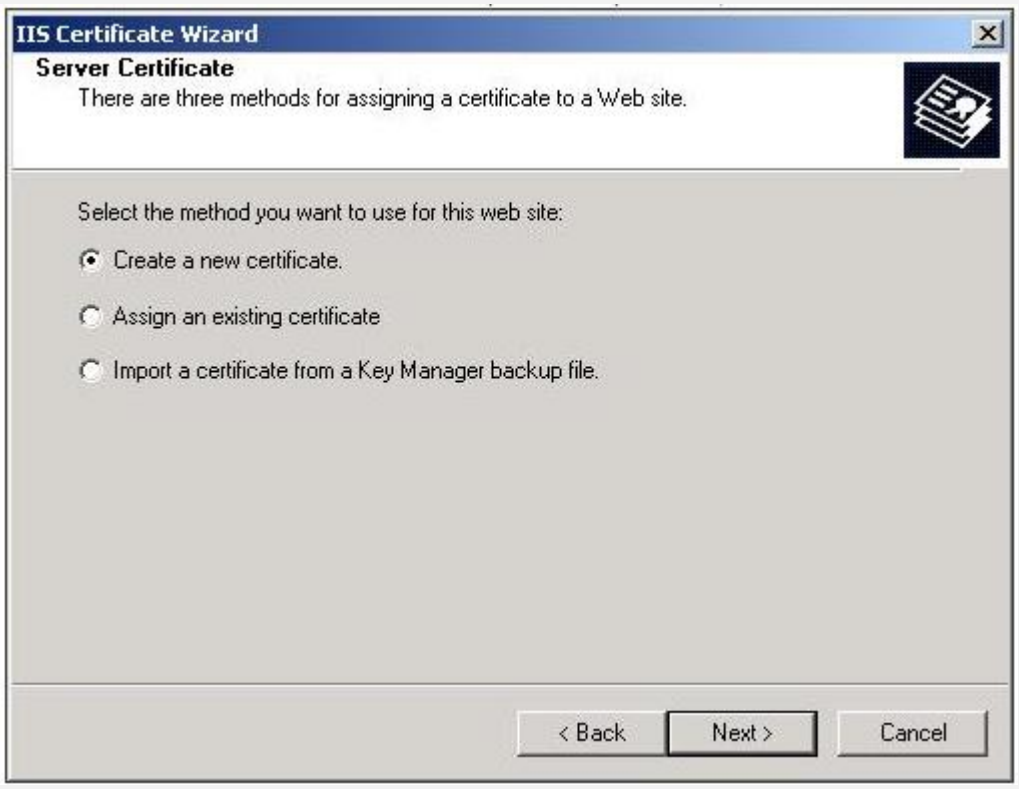
- Windows 2000 - IIS 5.0

1. 在管理員工具 Administrative Tools 下，打開 Internet Services Manager。
2. 滑鼠右鍵按你要加密的網站名，然後按“屬性” Properties。
3. 按“目錄安全性” Directory Security 。
4. 在“安全通信” Secure communications 中按“伺服器憑證” Server Certificate。(注意如果是第一次使用“編輯” Edit 按鈕將未被啟動)



5. 選擇“建立新憑證” Create a new certificate

6. 選擇“現在準備憑證請求，但稍後發送”Prepare the request now, but send it later。

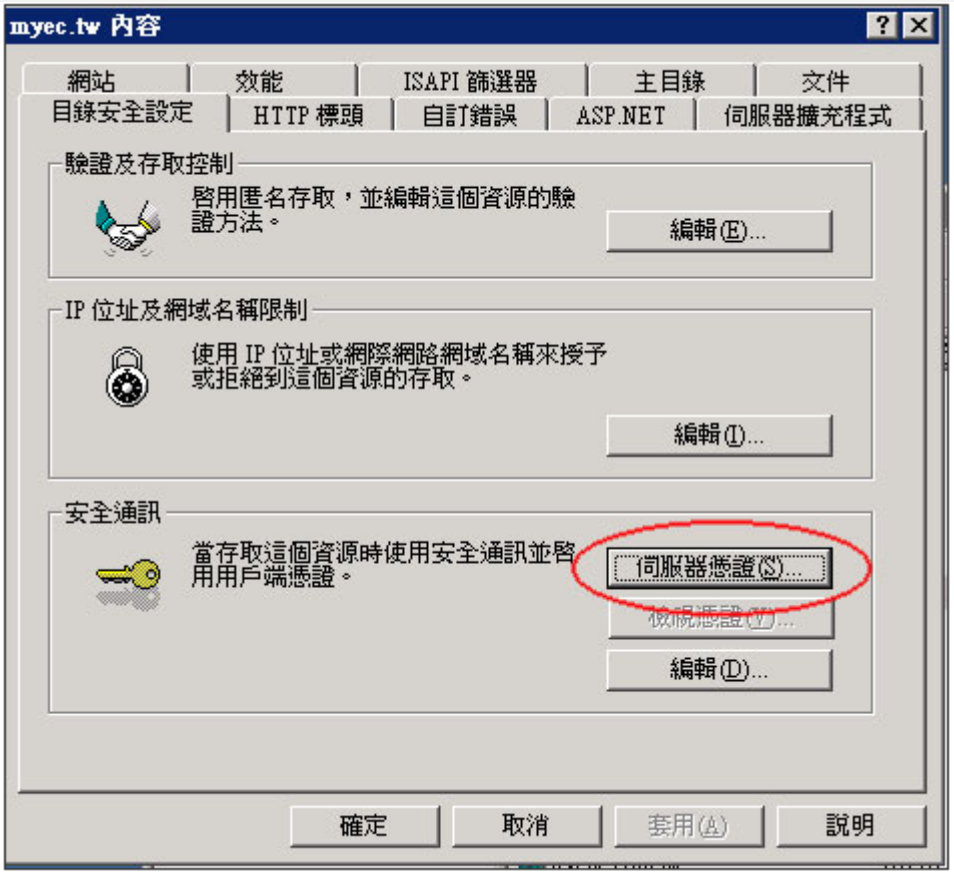


7. 通過 IIS 憑證嚮導完成請求資訊並建立的私鑰將保存在伺服器本地，而建立的公鑰（The Certificate Signing Request）將被用於憑證的申請過程，保存在指定的 TXT 文件中。

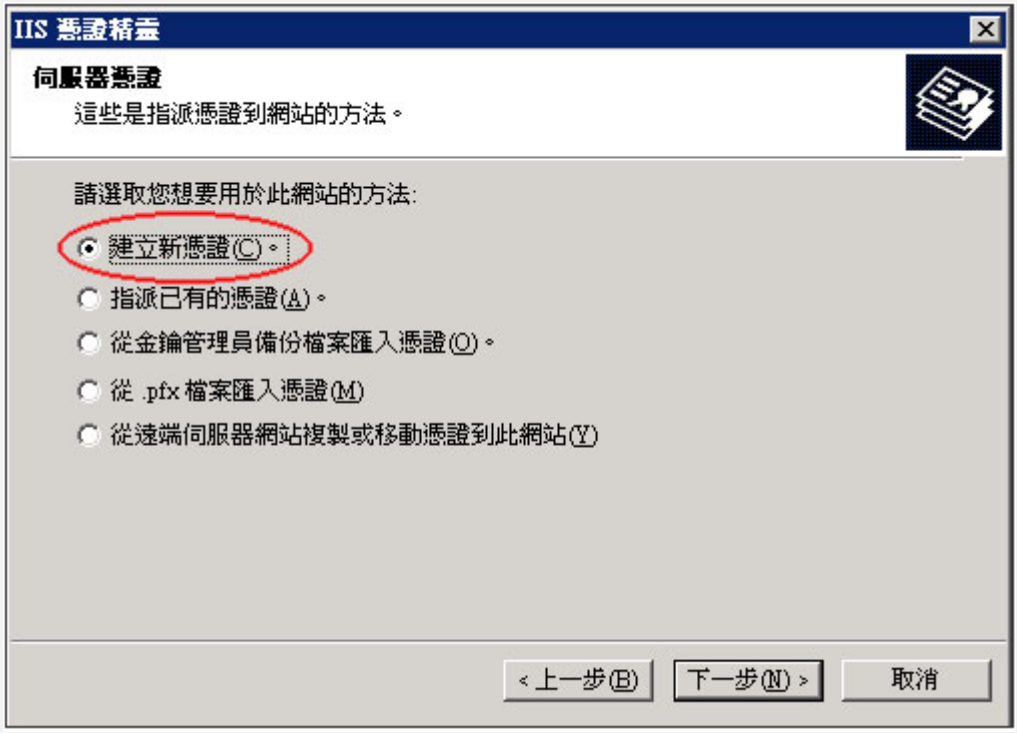
8. 按“完成”退出 IIS 憑證導引，CSR 檔已經被產生好了。
9. 將產生完的 CSR 檔提供給亞太客服即可。

- Windows 2003-IIS 6.0

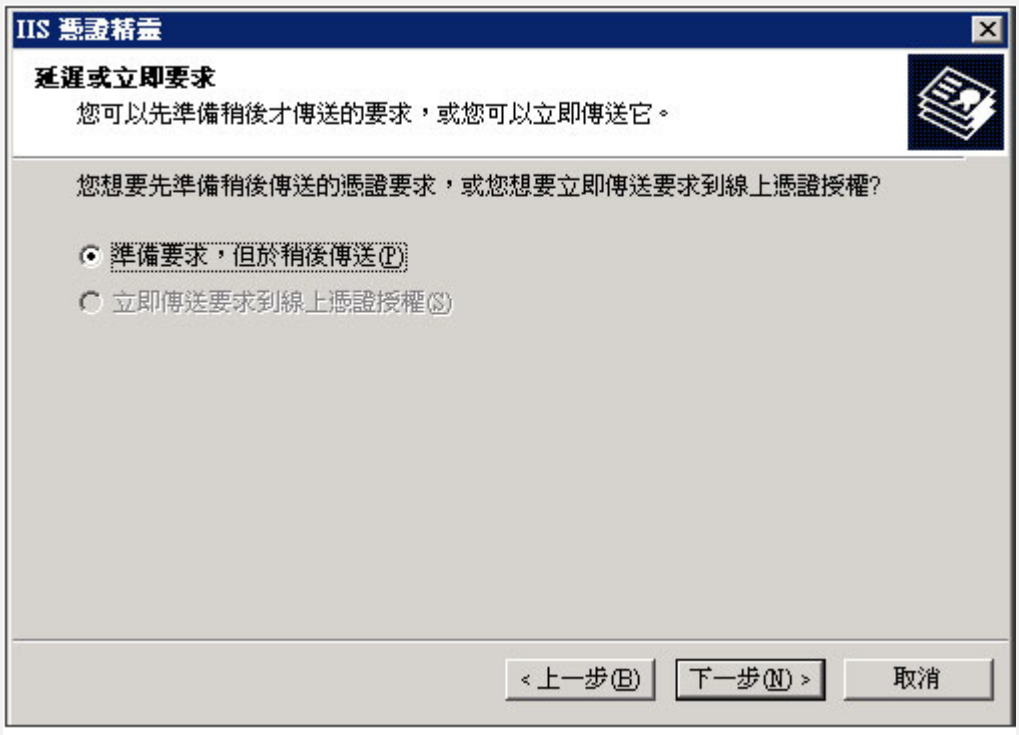
1. 在管理員工具 Administrative Tools 下，打開 Internet Services Manager。
2. 滑鼠右鍵按你要加密的網站名，然後按“屬性” Properties。
3. 按“目錄安全性” Directory Security 。
4. 在“安全通信” Secure communications 中按“伺服器憑證” Server Certificate。



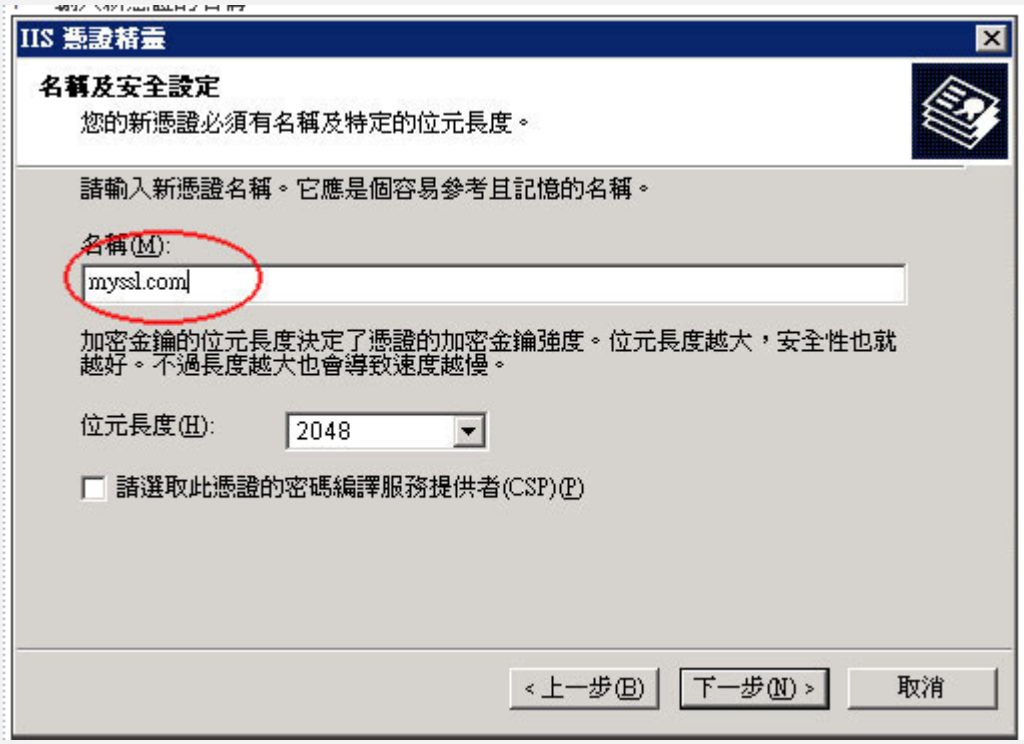
5. 選擇“建立新憑證” Create a new certificate



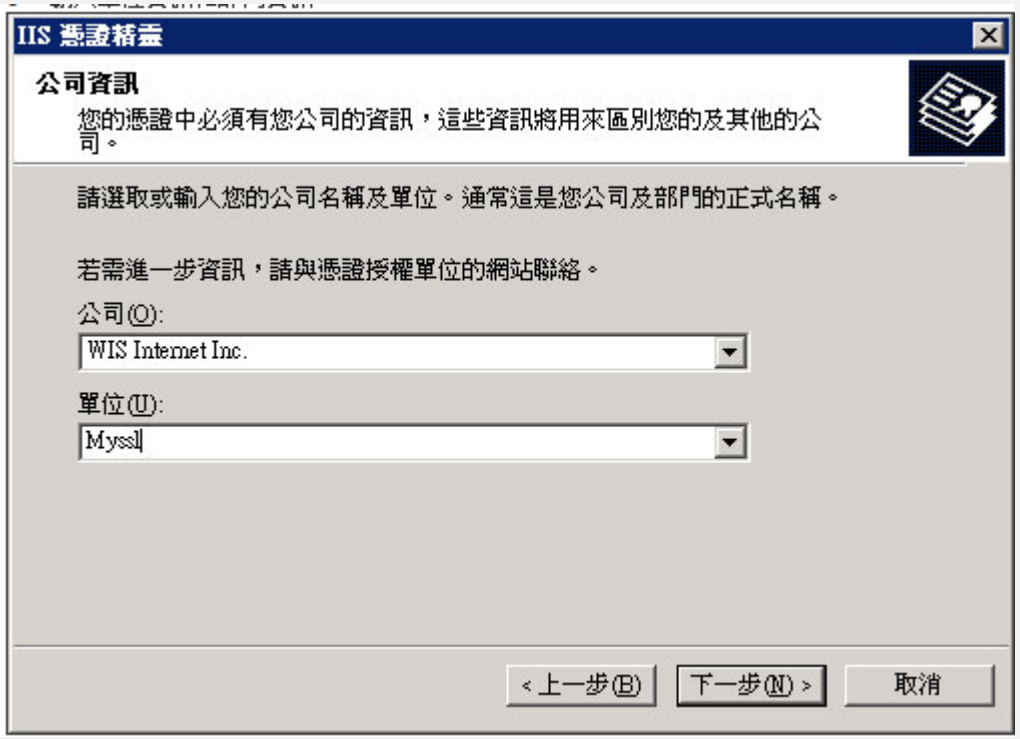
6. 選擇“準備請求，但於稍後發送”Prepare the request now, but send it later。



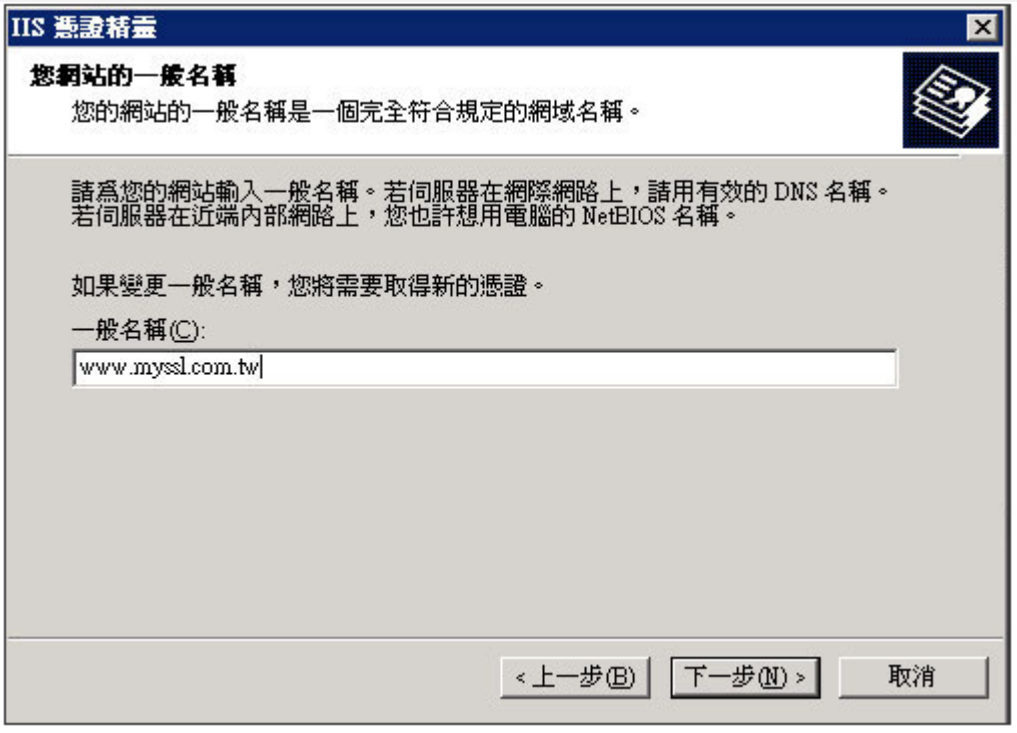
7. 輸入新憑證的名稱：



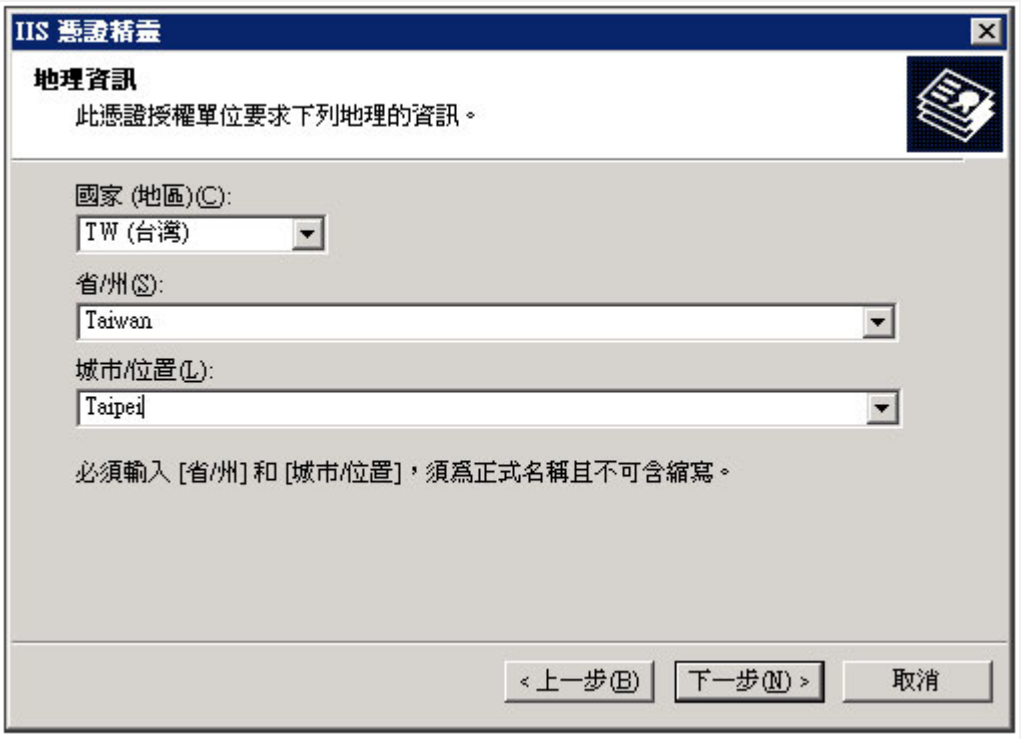
8. 輸入單位資訊和部門資訊：



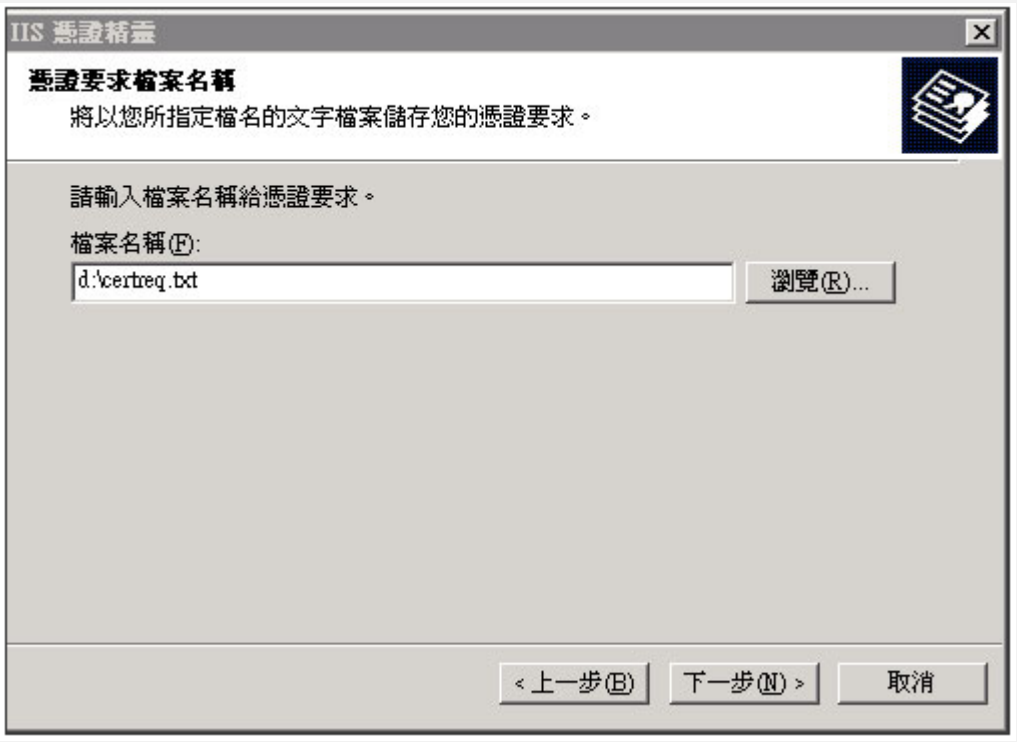
9. 輸入網站的一般名稱(即欲指定加密的網址)



10. 輸入地理資訊



11. 輸入憑證請求檔案名



12. 按“完成”退出 IIS 憑證導引，CSR 檔已經被產生好了。
13. 將產生完的 CSR 檔提供給亞太客服即可。

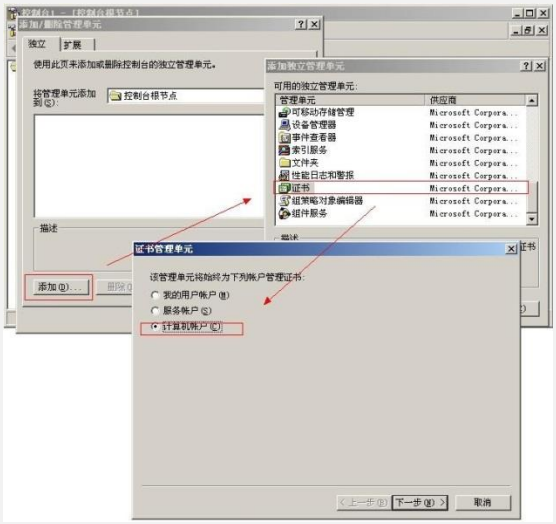
■ IIS 7.0

Step 1：生成數位憑證簽名請求文件(CSR)

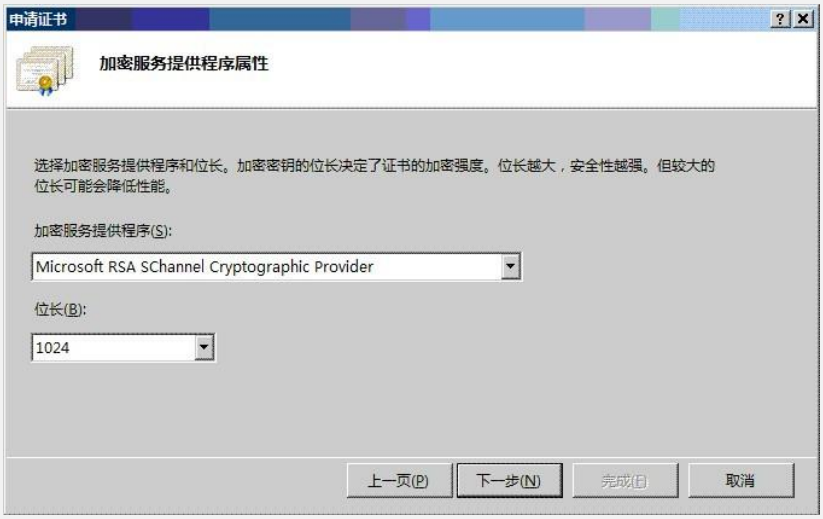
1. 打開 IIS 服務管理器，點擊計算機名稱，雙擊打開右則的伺服器憑證圖標

2. 雙擊打開伺服器憑證後，點擊右則的創建憑證申請

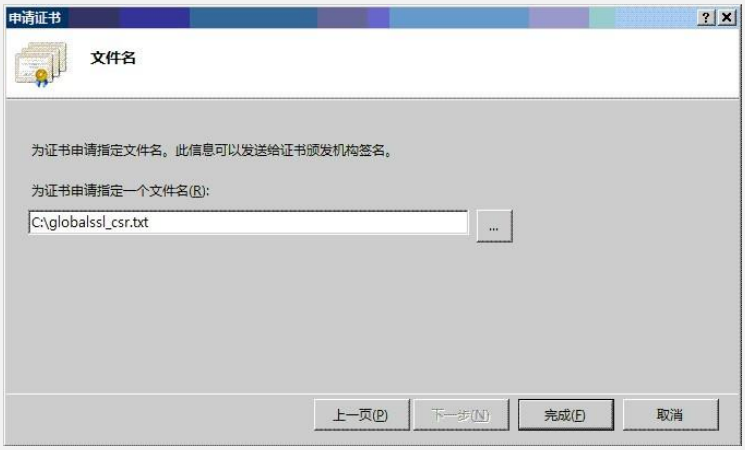
3. 輸入申請數位憑證訊息（必須為英文字符），點擊下一步



4. 選擇加密服務提供程序和加密長度，建議默認，點擊下一步



5. 選擇憑證籤名請求（CSR）文件保存的路徑和文件名，點擊完成



Step 2：提交 CSR，申請數位憑證

遞交憑證申請表及相關資料，並把憑證請求文件（CSR）提交給我們。我們確認資料齊全後，三個工作日內完成憑證頒發。

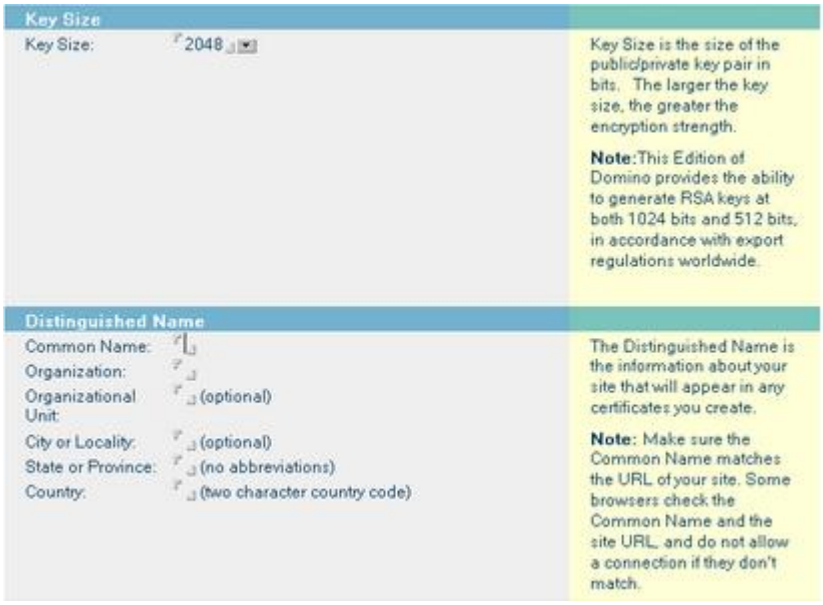
- Tomcat

1. 運行 cmd.exe， 進入命令行視窗
2. 進入 Java_JRE\bin 目錄，如 cd C:\PROGRA~1\Java\jre1.5.0_06\bin
3. 運行 keytool -genkey -alias tomcat -keyalg RSA -keystore c:\server.key
   - 輸入 keystore 密碼： 請輸入保護憑證密鑰的密碼。
   - 您的名字與姓氏是什麼？請輸入網域名稱,例如：www.domain.com
   - 您的組織單位名稱是什麼？請輸入單位名稱，如: APTG
   - 您的組織名稱是什麼？請輸入部門名稱，如： IT Dept
   - 您所在的城市或區域名稱是什麼？輸入城市名稱，如：Taipei
   - 您所在的州或省份名稱是什麼？輸入省份名稱，如：Taipei
   - 該單位的兩字母國家代碼是什麼？台灣請輸入 TW
   - CN=www.domain.com, OU=WIS Internet Inc. , O=IT, L=Shanghai, ST=Shanghai, C=TW 正確嗎？輸入 Y
   - 輸入的主密碼（如果和 keystore 密碼相同，按 Enter
4. 運行 keytool -certreq -alias tomcat -keystore c:\server.key -file c:\server.csr
5. 輸入密碼後回存檔案，則 C:\ 產生 server.csr 文件，(請注意，一定要保存好 server.key 和 server.csr 文件)
6. 用一個文字編輯器（Notepad 或 VI），打開 " Certificate Request " ，把裡面的內容全部複製到信件中提供給亞太客服即可

- Domino

1.請先進入憑證管理服務，並且點擊 Create Key Ring.

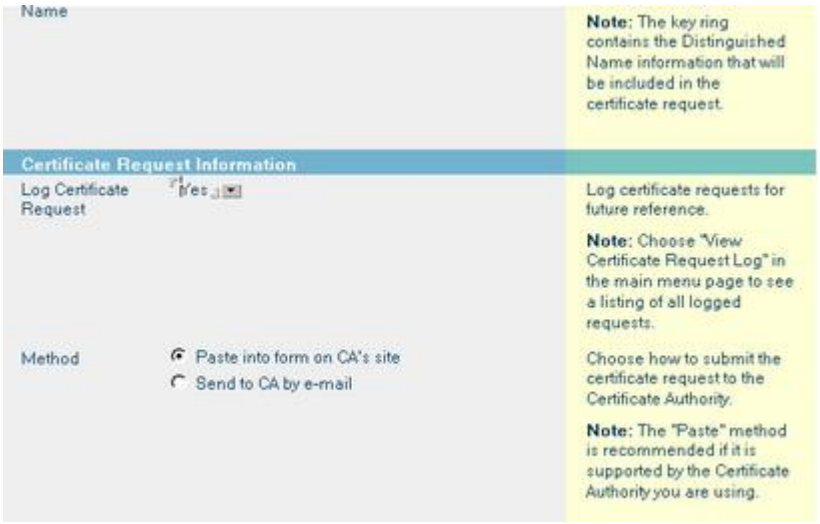
2.請輸入相關憑證資訊



Key Size	2048	加密強度
Common Name	*.pwctw.com.tw	憑證域名
Organization	PricewaterhouseCoopers	單位名稱
Organizational Unit	IT	部門名稱
City or Locality	Taipei	城市
State or Province	Taiwan	省洲
Country	TW	國家簡碼(台灣=TW)

3.點擊繼續，將會請您確認相關資訊的視窗，再次點擊確認將會回到主選單

4.您可以在下方找到 Method 當中的 Paste into form on CA's site.，並且點擊下方的 Create Certificate Request



5.將會開啟新的視窗，上方為您的 CSR 相關資訊，下方為 CSR 編碼，煩請您將下方編碼，以文字檔的方式保存好提供給亞太客服即可。