

匯智資訊股份有限公司

SSL 數位憑證
IIS6 憑證安裝說明

【版權及商標聲明】

本文件由 Cloudmax 匯智製作，並保留所有權利。

文件提供之安裝步驟僅供參考，詳細狀況依伺服器版本或所在網路環境、架構而有些微差別，請依實際狀況或系統提供商資訊為準，若於安裝上有任何問題可與我們聯繫，將有專員引導您排除障礙。

本文件所引用之各商標及商品名稱分屬其合法註冊公司所有，絕無侵權之意，特此聲明。

【有限擔保責任聲明】

Cloudmax 匯智盡力製作本說明文件其正確性，但不擔保本文件無任何瑕疵，亦不為使用本說明文件而引起之衍生利益損失或意外損毀之損失擔保責任。若對本文件有任何疑問與建議，可利用下方資訊與我們聯繫：

電話：+886-2-2718-7200

傳真：+886-2-2718-1922

信箱：service@cloudmax.com.tw

目錄

一、選擇產生 CSR 檔案方式.....	1
1. 使用 OpenSSL 或透過線上生成工具產生 (申請 GeoTrust 使用).....	1
2. 透過 IIS 伺服器產生 (申請 GlobalSign 使用).....	2
二、安裝前注意事項.....	6
三、數位憑證安裝前準備確認事項.....	7
四、選擇安裝方式.....	9
1. CSR 透過線上 OpenSSL 生成 (操作僅限申請 GeoTrust).....	9
2. CSR 透過 IIS 伺服器產生.....	13
3. 匯入中繼憑證檔案.....	15
五、檢查憑證安裝是否正確.....	21
六、備份數位憑證.....	21

一、選擇產生 CSR 檔案方式

CSR 檔案為提供給憑證中心驗證的檔案，透過此 CSR 檔案憑證中心將會簽發 CER 檔案；

而產生 CSR 檔案的同時會一併會產出 KEY 檔案，而這三個檔案為互相匹配憑證才可正常運行。

1. 使用 OpenSSL 或透過線上生成工具產生 (申請 GeoTrust 使用)

若您為申請 GeoTrust 的憑證，我們建議您可以直接使用我們的 OpenSSL 線上產生工具，來快速產生 CSR 檔，並且將所產生出來的 CSR 檔案提交給匯智，一併產出的 KRY 檔案請您務必儲存，以利後續憑證安裝過程順利。

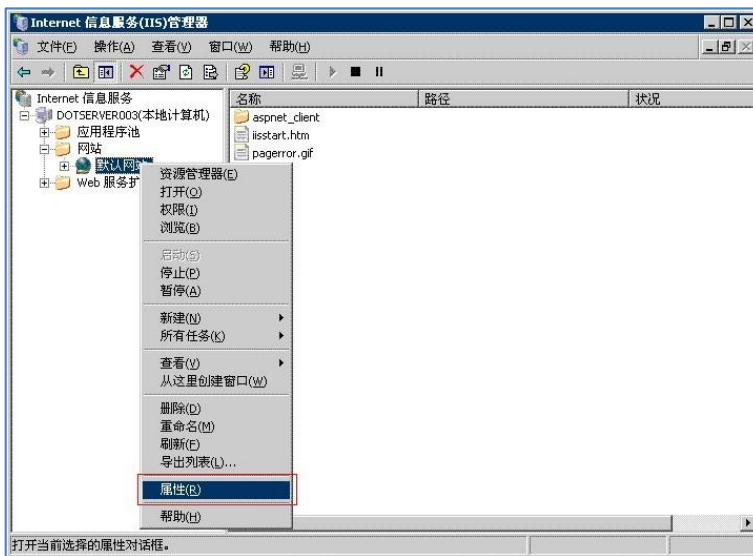
GeoTrust 線上生成 CSR 工具：

<http://geotrust.cloudmax.com.tw/OpenSSL/CreateCSR.asp>

2. 透過 IIS 伺服器產生 (申請 GlobalSign 使用)

若您為申請 GlobalSign 的憑證，我們建議您直接於 IIS 伺服器上產生 CSR 的資訊，產生的步驟如下表：

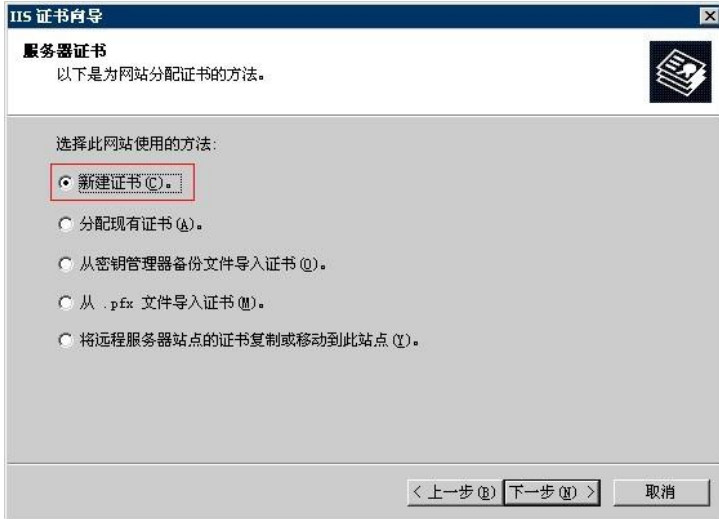
1. 進入 IIS 系統，針對要置入憑證的網站點選滑鼠右鍵/屬性



- 2 於目錄安全性中點選伺服器憑證

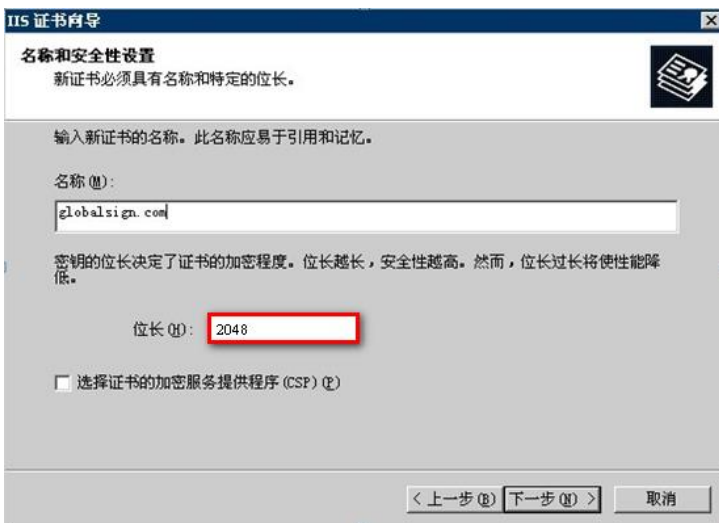


3 選擇新建憑證



4 輸入您容易記憶的名稱(建議直接輸入網域)

特別留意：密鑰長度目前憑證中心僅頒發 2048 的憑證資訊。



5 依照您的實際狀況，填入申請單位與部門名稱



IIS 证书向导

单位信息

证书必须包含您单位的相关信息，以便与其他单位的证书区分开。

选择或输入您的单位和部门名称。通常是指您的合法单位名称及部门名称。

如需详细信息，请参阅证书颁发机构的网站。

单位 (O):
GlobalSign China Co., Ltd.

部门 (O):
IT Dept.

< 上一步 (B) 下一步 (N) > 取消

6 憑證申請的網域名稱



IIS 证书向导

站点公用名称

站点公用名称是其完全合格的域名。

输入站点的公用名称。如果服务器位于 Internet 上，应使用有效的 DNS 名。如果服务器位于 Intranet 上，可以使用计算机的 NetBIOS 名。

如果公用名称发生变化，则需要获取新证书。

公用名称 (C):
cn.globalsign.com

< 上一步 (B) 下一步 (N) > 取消

7 依照您的伺服器所在地而填寫資訊



The screenshot shows the 'IIS 证书向导' (IIS Certificate Wizard) window at the '地理信息' (Geographic Information) step. The title bar reads 'IIS 证书向导'. The main text says '证书颁发机构要求下列地理信息。' (The certificate authority requires the following geographic information). Below this, there are three dropdown menus: '国家(地区) (C):' (Country/Region) set to 'CN (中国)', '省/自治区 (S):' (Province/Autonomous Region) set to 'Shanghai', and '市县 (L):' (City/County) set to 'Shanghai'. A note below the dropdowns states: '省/自治区和市县必须是完整的官方名称，且不能包含缩写。' (Province/Autonomous Region and City/County must be the complete official name, and cannot contain abbreviations). At the bottom, there are three buttons: '< 上一步 (B)' (Previous Step), '下一步 (N) >' (Next Step), and '取消' (Cancel).

8 確認 CSR 產出位置



The screenshot shows the 'IIS 证书向导' (IIS Certificate Wizard) window at the '证书请求文件名' (Certificate Request File Name) step. The title bar reads 'IIS 证书向导'. The main text says '以指定的文件名将证书请求保存为文本文件。' (Save the certificate request as a text file with the specified filename). Below this, there is a text input field for '文件名 (F):' (Filename) containing 'c:\certreq.txt'. To the right of the input field is a '浏览 (B)...' (Browse...) button. At the bottom, there are three buttons: '< 上一步 (B)' (Previous Step), '下一步 (N) >' (Next Step), and '取消' (Cancel).

*若透過 IIS 產生 CSR 檔案，KEY 檔案將會直接儲存於此 IIS 伺服器中。

二、安裝前注意事項

數位憑證是由私密金鑰 (private key) 與公開金鑰 (public key) 兩個部分組成，在進行安裝及使用數位憑證前，須將私密金鑰與公開金鑰檔案放置於伺服器可讀取之儲存區中。

依伺服器網路環境不同而實際需求各異，以下列出安裝時常見忽略的狀況：

- 伺服器是否正常連上 Internet ？
- HTTPS 協定之通訊埠是否開啟¹ ？
- 部分狀況下，伺服器需要額外的固定 IP² 支援；此時需調整網址之 A 紀錄³ 。
- 與伺服器串連的網路設備通訊埠的狀態是否設定完成⁴ ？

若無法確認網路環境，或您非相關設備或服務的權限擁有者，應與設備、系統所屬管理員或該服務、設備提供商諮詢及確認。

安裝過程中，因操作錯誤或其他不可預期因素，可能導致系統資料異常、毀損，請在系統更動前，將重要系統及資料進行備份。

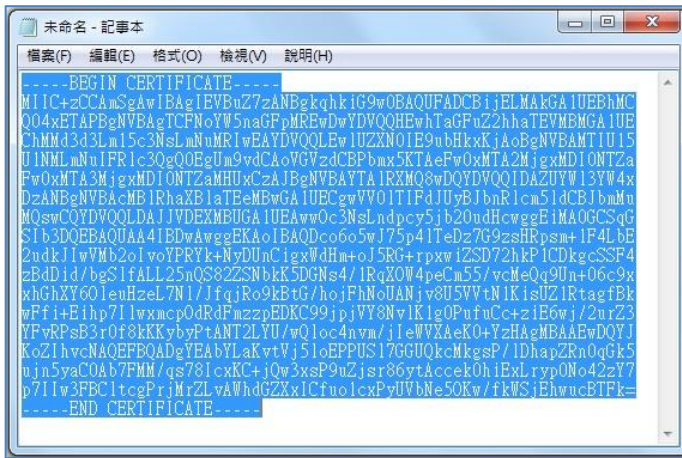
¹ HTTPS 協定預設使用 Port 443，但使用者可依實際狀況進行調整。


² 多個網站共用同一台伺服器的情況下(如虛擬主機)，需要利用額外的固定 IP 以解決通訊埠不足的問題。

³ 須注意您是否擁有修改 DNS(Domain Name Service) Server 權限，且 DNS 紀錄修改需要生效時間。

⁴ 例如防火牆、負載平衡裝置、代理伺服器，可能須調整規則、開啟通訊埠，甚至部分設備也需要安裝、支援數位憑證。

3 開啟純文字檔案，貼上您所複製的資訊



4 將此憑證資訊以另存新檔的方式儲存(儲存為附檔名為.cer)，所見的圖示將會變成 

5 請點擊憑證檔案，確認憑證網域、簽發者單位、有效期間是否為正常資訊

四、選擇安裝方式

上述的憑證資訊確認完畢後，我們即將開始要把憑證安裝於伺服器當中，於第一大項時，我們有介紹兩種因申請不同憑證廠商而建議的生成方式，請參考以下的資訊來完成憑證安裝動作。

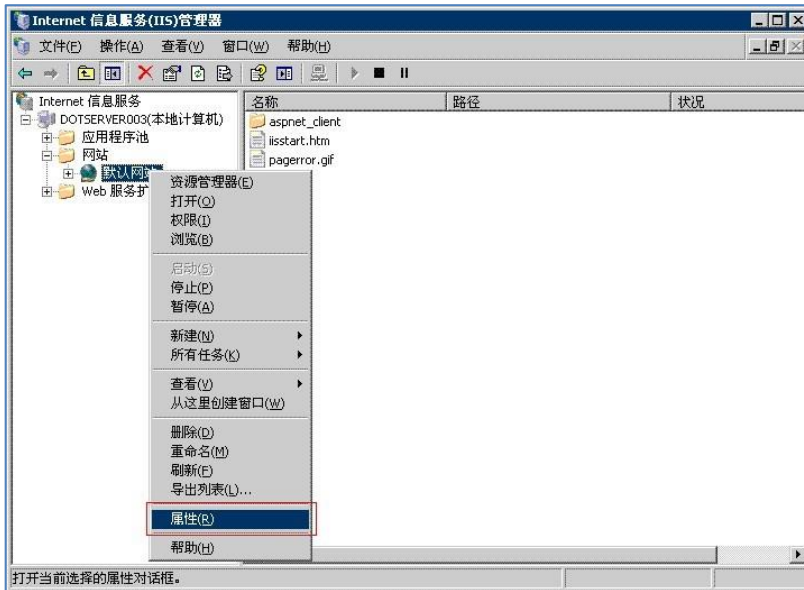
1. CSR 透過線上 OpenSSL 生成 (操作僅限申請 GeoTrust)

目前您的手上有 CER 的文本資訊(我們所提供給您的憑證核發完成信件)以及 KEY 的文本資訊(當時透過 OpenSSL 或是線上生成工具時一併產生的 KEY 檔案)，請準備好兩項的資訊，連入 Geotrust PFX 線上合成工具，並且依照網頁指示完成 PFX 檔案的匯出。

GeoTrust PFX 線上合成工具：<http://geotrust.cloudmax.com.tw/OpenSSL/CreatePFX.asp>

** 僅限申請 GeoTrust 憑證適用，因線上合成工具會一併合成 GeoTrust 對應的中繼憑證。*

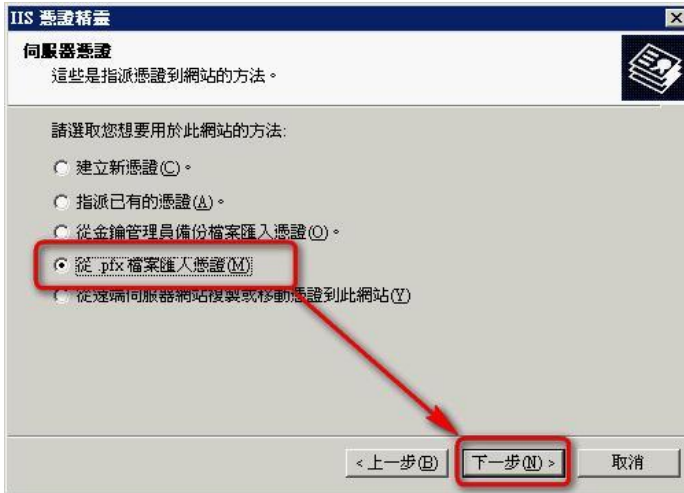
1. 進入 IIS 系統，針對要置入憑證的網站點選滑鼠右鍵/屬性



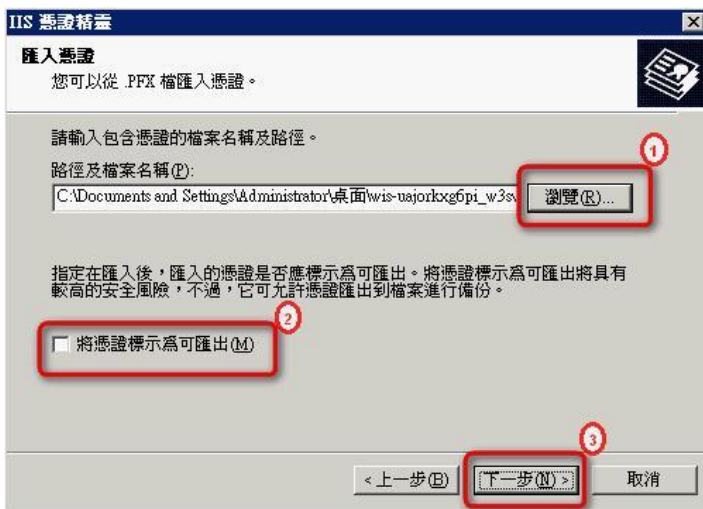
- 2 於目錄安全性中點選伺服器憑證



3 選擇從 .PFX 文件導入憑證



4 選找到剛剛所合成完畢的 PFX 檔案資訊，同時將此 PFX 檔案設定為可匯出



5 HTTPS 預設使用 443 port，請依照實際狀況來進行設定

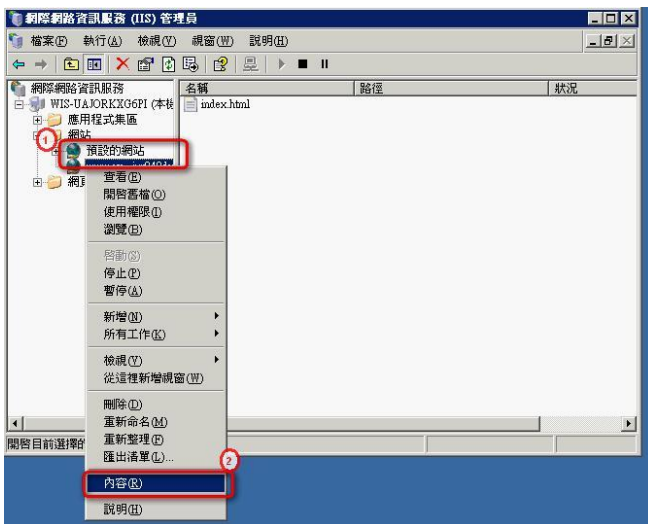


憑證安裝完成，您可以直接跳到 五、檢查憑證安裝是否正確

2. CSR 透過 IIS 伺服器產生

目前您的手上有 CER 的文本資訊(我們所提供給您的憑證核發完成信件)，因您的 CSR 由 IIS 伺服器直接產生，所以 KEY 檔案將會直接保留再 IIS 中，請您依照以下的步驟將簽發下來的 CER 資訊匯入 IIS 伺服器：

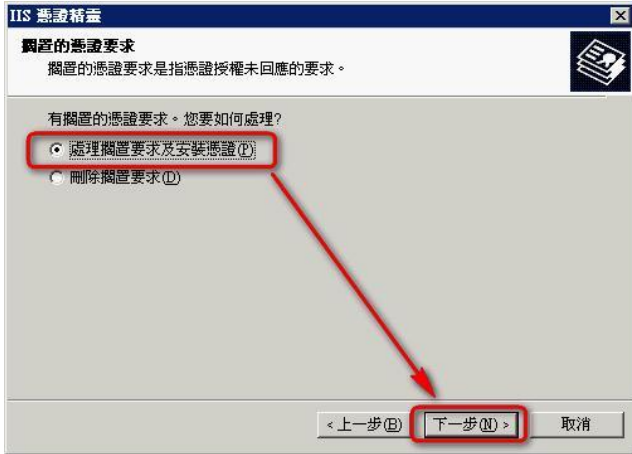
- 1 點選當時執行的站台/內容



- 2 目錄安全設定 / 伺服器憑證



3 處理擱置要求及安裝憑證



4 找尋 3. 數位憑證安裝前準備確認事項 所儲存的 CER 檔案 (副檔名為.cer)



5 HTTPS 預設使用 443 port，請依照實際狀況來進行設定



3. 匯入中繼憑證檔案

※ 若您的憑證是使用線上合成的方式匯入，可直接跳過此步驟。

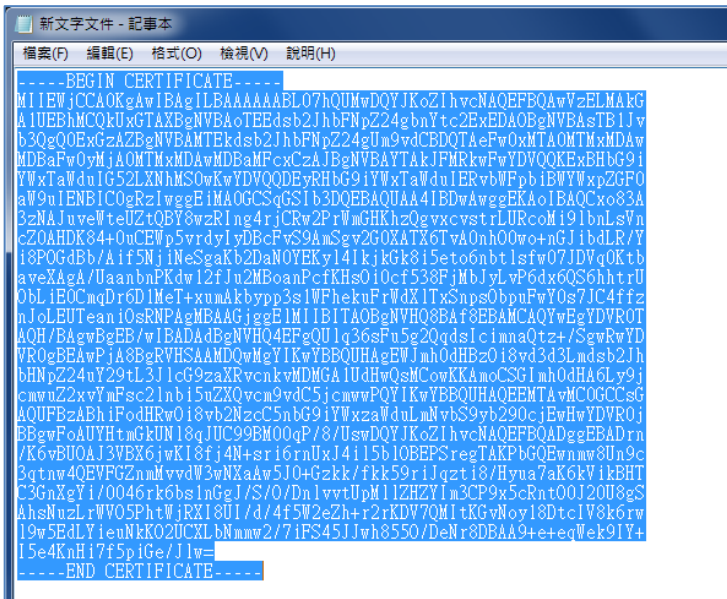
電腦運算能力於近十年內大幅提升，為確保憑證用戶網路資料傳輸安全，各大憑證中心於 2010 年起開始做根憑證 1024 升級為 2048 位元的作業，而舊的瀏覽器因缺少 2048 位元的根憑證資料，所以需要利用中繼憑證來進行交互驗證，確保於舊版本瀏覽器使用 HTTPS 連線時，不會出現錯誤或警告訊息，請您依照以下的步驟來完成中繼憑證匯入動作：

- 1 請協助查看憑證資訊檔案文本資料中「中繼憑證」

```
中繼憑證：
-----BEGIN CERTIFICATE-----
MIIEWjCCA0KgAwIBAgILBAAAAAABL07hQUmWdQYJKoZIhvcNAQEFBQAwwVzELMAkG
A1UEBhMCQkUxGTAxBgNVBAoTEEdsb2JhbFNPZ24gUm9vdCBDQTAEFw0xMTA0MTMxMDAw
MDBAFw0yMjA0MTMxMDAwMDBAFw0xMTA0MTMxMDAwMDBAFw0yMjA0MTMxMDAwMDBA
YwduIG52LXNhMS0wKwYDVQQDEyRhbG9yWwYwduIERvbWVpbiBwYXN0eXZGF0eS08
aW9uENB1C0gRZlwggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCo83A
3zNAJuveWteUzTQBY8wzRIng4rjCRw2PrWmGHKhZQgvxcvstrLURcoM9lbnLsVn
cZ0AHDk84+0uCEWp5vrdYlYDbcFvS9AmSgv2G0XATX6TVA0nh0Owo+nGjIbdLR/Y
i8POGdBb/Aif5NjilNeSgAkB2DaNOYEky14IkJkGk8i5eto6nbtlsfW07jDVq0Ktb
aveXAgA/UaanbnPKdw12fju2MBoanPcfKhs0i0cf538FjMbjyLvP6dx6QS6hhtrU
ObLiE0CmqDr6D1MeT+xumAkbypp3s1WFhekuFrWdXITxSnpsObpuFwY0s7jC4ffz
nJoLEUTeaniOsRNPAGMBAAAGjggEIMIIBITA0BgNVHQ8BAf8EBAMCAQYwEgYDVR0T
AQH/BAgwBgEB/wIBADAdBgNVHQ4EFgQUlq36sFu5g2QqdsIcimnaQtz+/SgwRwYD
VR0gBEAwPjA8BgRVHSAAAMDQwMgYIKwYBBQUHAQEWJmH0dHBzOi8vd3d3Lmdsb2Jh
bHNuZ24uY29lL3JlcG9zaXRvcnkvdMDMGA1UdHwQSMCOWKKAQMoCSGImh0dHA6Ly9l
cmwwZ24uYmFsc2lnbi5uZXQvcn9vdC5jc2VwYXN0eXZGF0eS08aW9uENB1C0gRZlwg
AQUFBzABHIFodHRwOi8vb2NzcC5nbG9yWwYwduLmNvbS9ybz290cjEwHwYDVR0j
BBgwFoAUyHtmGkUNl8fj4N+sri6rnUx4il5l0BEPsregTAKPbGQEWnmw8Un9c
/K6vBU0AJ3VBx6jwKl8fj4N+sri6rnUx4il5l0BEPsregTAKPbGQEWnmw8Un9c
3qtW4QEVFGZnmMvvd3wNxaAw5J0+Gzkk/fk59riqzt8/Hyua7aK6kVikBHT
C3GnuzYi/0046rk6bs1nGgJ/S/O/DnlvtvUpMlIHZYIm3CP9x5cRnt00J20U8gS
AhsNuzLrVVO5PhtWjRXI8Uj/d/4f5W2eZh+r2rKDV7QMItKGVNoy18DtcIV8k6rW
l9w5EdLyeuNkK02UCXLBnmw2/7IFS45Jjwh8550/DeNr8DBAA9+e+eqWek9iy+
I5e4KnH7f5piGe/1lw=
-----END CERTIFICATE-----
```

- 2 請複製憑證資訊(包含『-----BEGIN CERTIFICATE-----』至『-----END CERTIFICATE-----』)

- 3 開啟純文字檔案，貼上您所複製的資訊



- 4 將此憑證資訊以另存新檔的方式儲存(儲存為附檔名為.cer) , 所見的圖示將會變成

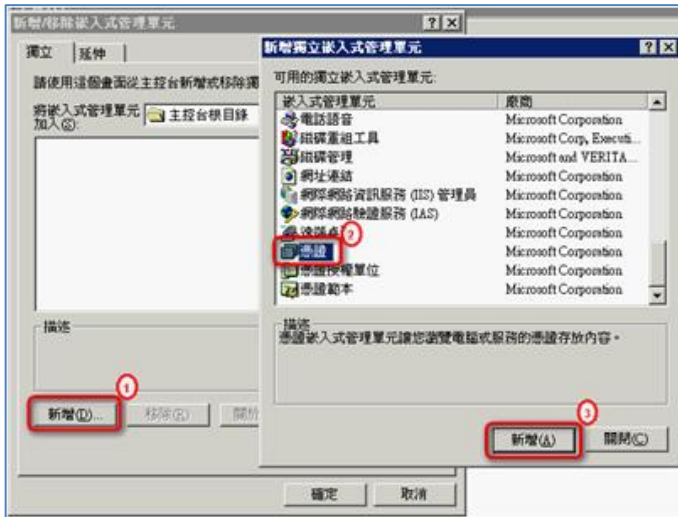


- 5 開始 > 執行(R) , 輸入"mmc"

- 6 於主控台視窗中點選 檔案 / 新增/移除嵌入式管理單元



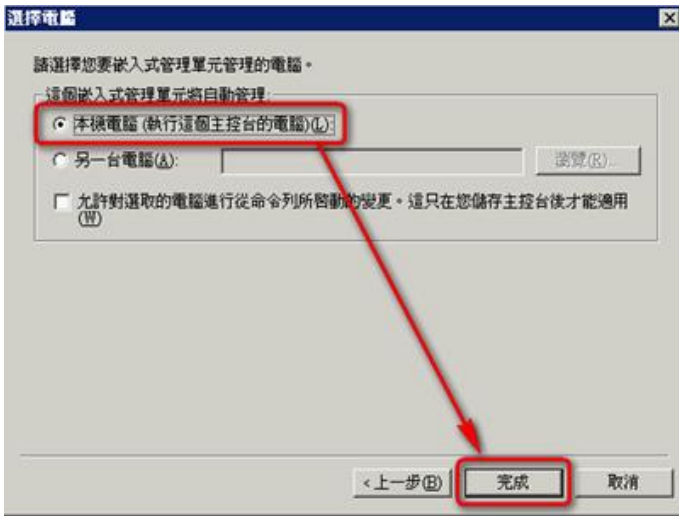
- 7 點選『新增』, 然後在彈跳出來的「新增獨立嵌入式管理單元」視窗中點選 憑證/ 新增



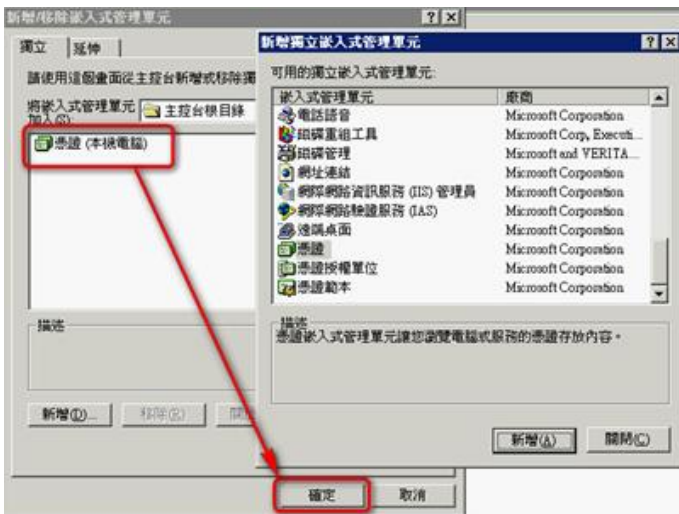
8 選擇『電腦帳戶』，然後『下一步』



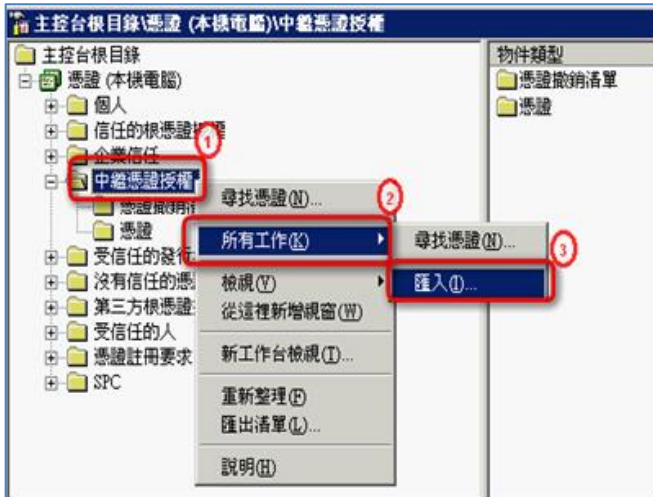
9 選擇『本機電腦(執行這個主控台的電腦)』，然後完成



10 完成後，在「新增/移除嵌入式管理單元」視窗中將出現「憑證(本機電腦)」圖示，點選『確定』完成憑證管理單元新增程序



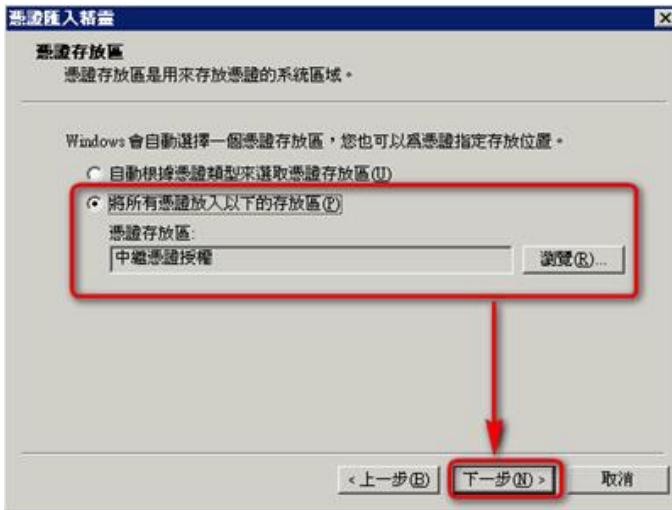
- 11 開啟憑證主控台，在『中繼憑證授權』點選右鍵，『所有工作 > 匯入』。系統執行憑證匯入精靈歡迎畫面後，『下一步』



- 12 用『瀏覽』選擇下載的中繼憑證檔案位置，然後點選『下一步』



- 13 選擇『將所有憑證放入以下的存放區』，憑證存放區為預設的『中繼憑證授權』，然後『下一步』



憑證安裝完成，您可以直接跳到 五、檢查憑證安裝是否正確

五、檢查憑證安裝是否正確

您可以透過此驗證工具來確認憑證是否已經正確掛載：

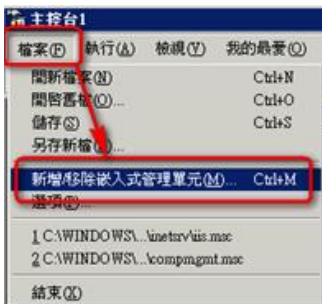
GeoTrust：<http://geotrust.cloudmax.com.tw/OpenSSL/checkservercert.asp>

GlobalSign：<https://globalsign.sslabs.com/>

六、備份數位憑證

匯智數位憑證在憑證有效期間內，提供憑證重置(Reissue)與更新的服務。不過重置過程需與新申請憑證時相同，必須再次產生私密金鑰與 CSR、驗證、簽發公開金鑰等程序後，才可再取得憑證。將可能耽誤寶貴的系統復原時間。基於資安考量，建議系統管理者將數位憑證進行備份。備份的方式如下：

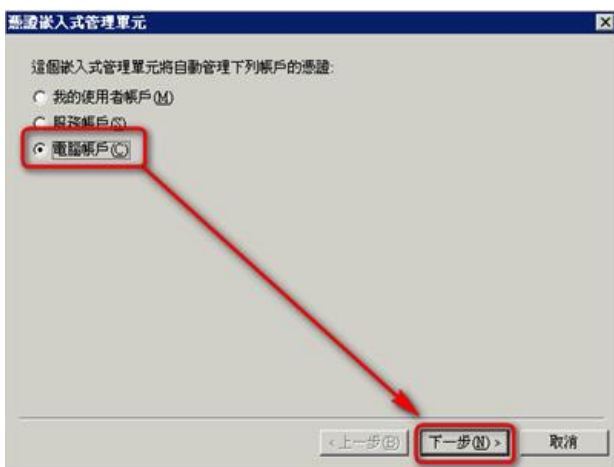
- 1 開始 > 執行(R)，輸入"mmc"
 - * 若已經有看到憑證項目請直接跳到本步驟 7
- 2 於主控台視窗中點選 檔案 / 新增/移除嵌入式管理單元



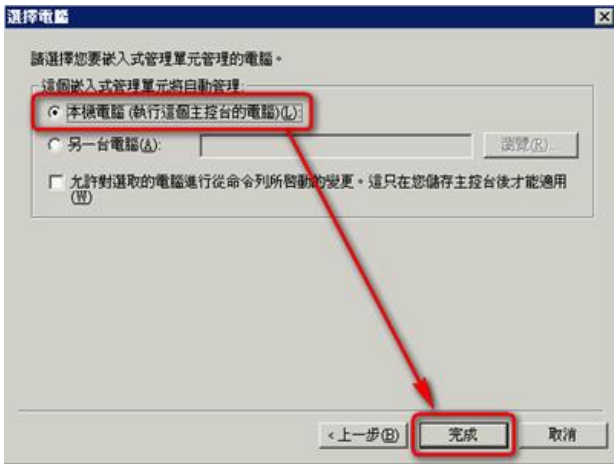
- 3 點選『新增』，然後在彈跳出來的「新增獨立嵌入式管理單元」視窗中點選 憑證/ 新增



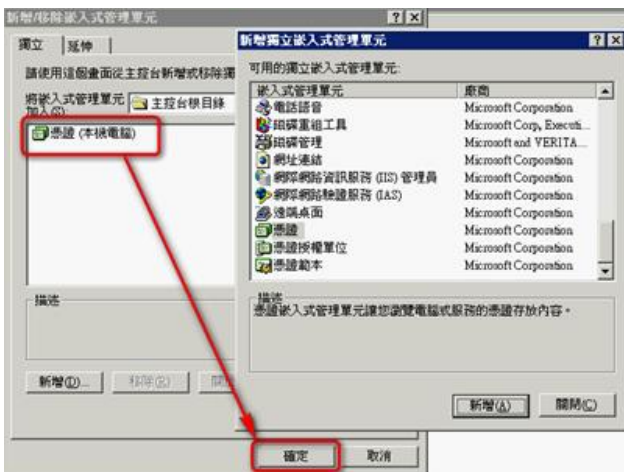
- 4 選擇『電腦帳戶』，然後『下一步』



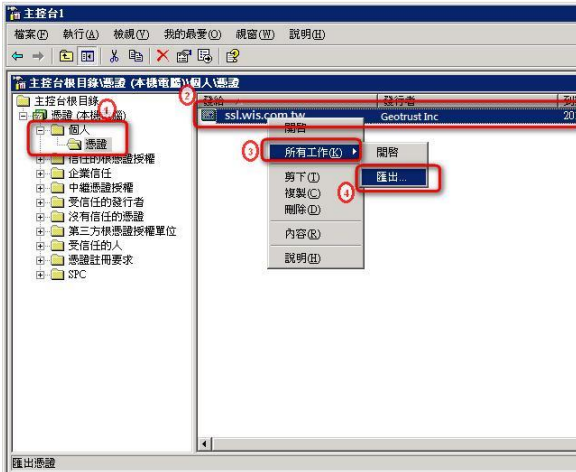
5 選擇『本機電腦(執行這個主控台的電腦)』，然後完成



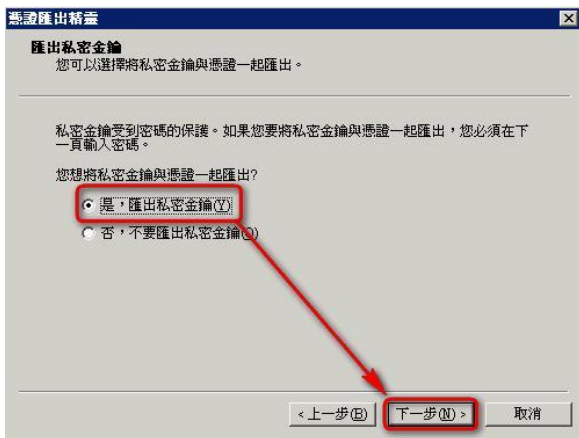
6 完成後，在「新增/移除嵌入式管理單元」視窗中將出現「憑證(本機電腦)」圖示，點選『確定』完成憑證管理單元新增程序



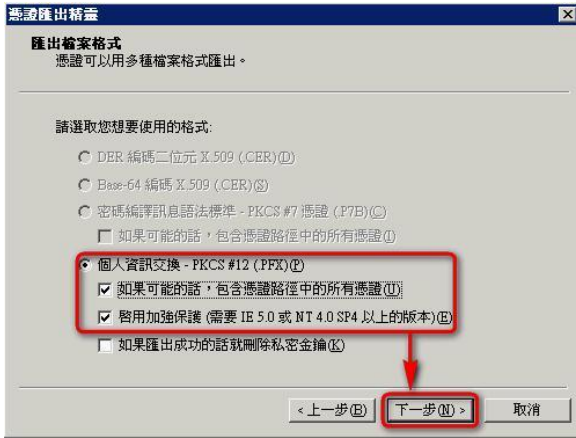
- 7 開啟憑證主控台，點選『個人 > 憑證』，於工作室窗選定欲備份的憑證後，右鍵，
『所有工作 > 匯出』



- 8 於憑證精靈歡迎畫面點選『下一步>』後，選擇『是，匯出私密金鑰』，然後『下一步』



- 9 「匯出檔案格式」預設為「個人資訊交換-PKCS#12(.PFX)(P)」，請將『如果可能的話，包含憑證路徑中的所有憑證』
- 話，包含憑證路徑中的所有憑證』



- 10 用『瀏覽』指定檔案匯出位置及名稱，然後『下一步(N)』



11 在憑證匯出精靈中自行設定設定 6 碼以上之保護密碼，『密碼(P)』及『確認密碼

(C)』欄位需相同



12 憑證精靈最後將顯示匯出資訊，點選『完成』。在匯出成功訊息點選『確認』關閉工

作視窗

