



電子證書（伺服器）用戶指南

Microsoft IIS 10.0 適用

修訂日期：2026 年 1 月

目錄

A.	電子證書（伺服器）申請人指引	2
	新申請及續期申請	3
B.	產生證書簽署要求(CSR).....	4
C.	提交證書簽署要求(CSR).....	9
D.	安裝中繼 / 交叉證書	15
	移除舊有中繼證書（如適用）	17
	安裝中繼 / 交叉證書	18
E.	安裝伺服器證書	22
F.	備份密碼匙	26
G.	還原密碼匙	33

A. 電子證書（伺服器）申請人指引

香港郵政核證機關在收到及批核電子證書（伺服器）申請後，會向獲授權代表發出主旨為“Submission of Certificate Signing Request (CSR)”的電郵，要求獲授權代表到香港郵政核證機關的網站提交 CSR。

本用戶指南旨在提供參考給電子證書（伺服器）申請人如何使用 Microsoft Internet Information Server (IIS) 10.0 產生配對密碼匙和證書簽署要求(CSR)的詳細步驟。包含公匙的 CSR 將會提交到香港郵政核證機關以作證書簽署。

如閣下在證書簽發後遺失密碼匙，您將不能安裝或使用該證書。因此強烈建議閣下於**提交證書簽署要求(CSR)前及完成安裝伺服器證書後**均為密碼匙進行備份。有關備份及還原密碼匙的方法，請參閱以下部分的詳細步驟：

F. 備份密碼匙.....	26
G. 還原密碼匙.....	33

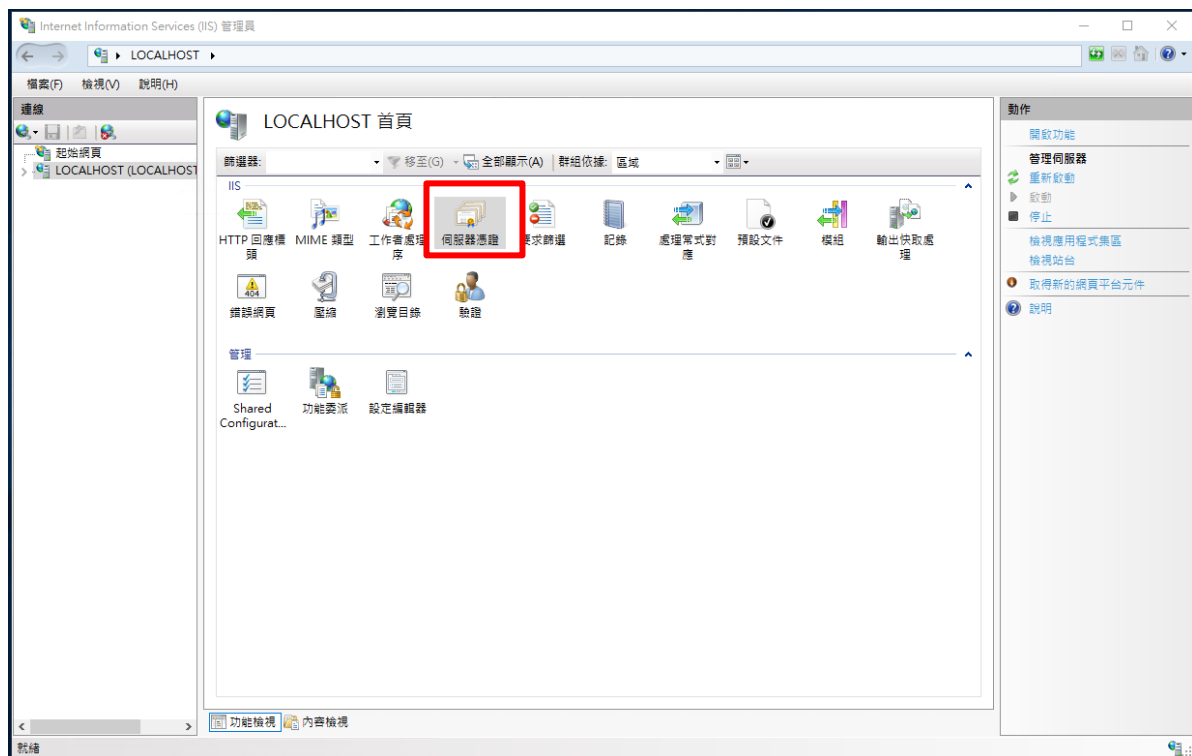
新申請及續期申請

首次及續期申請電子證書（伺服器），請參閱以下部分的詳細步驟：

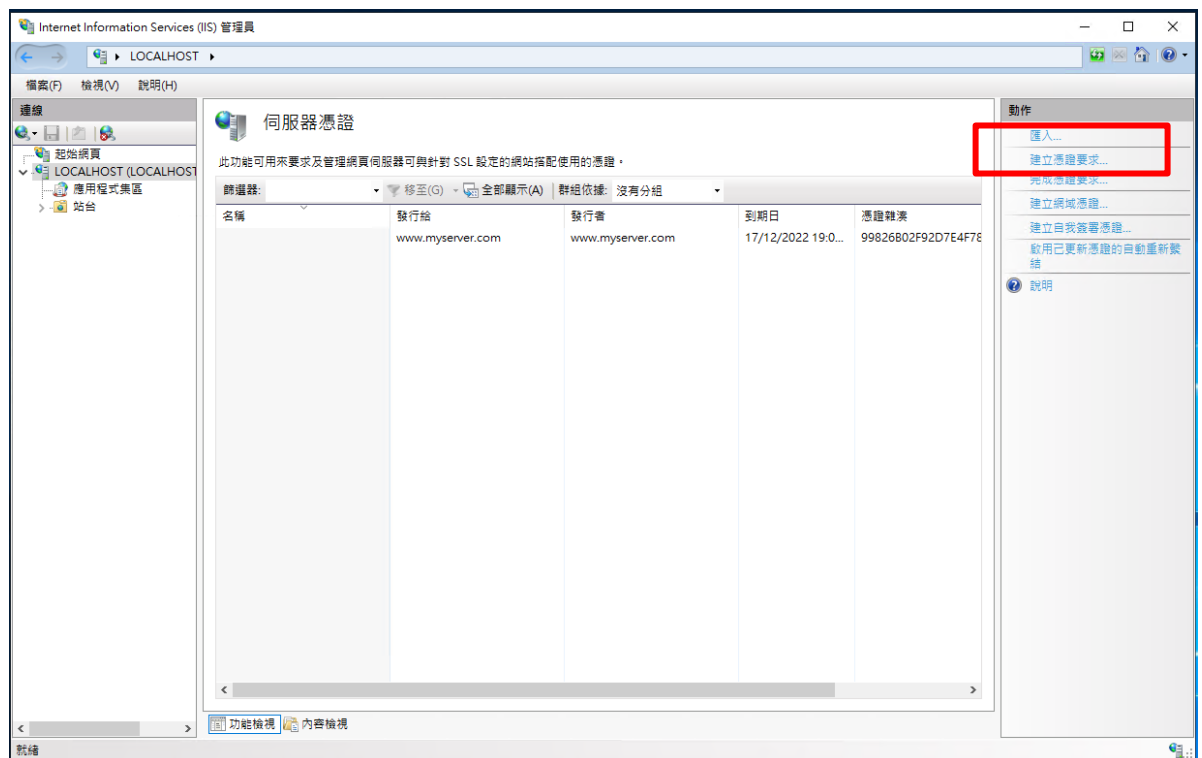
B.	產生證書簽署要求(CSR).....	4
C.	提交證書簽署要求(CSR).....	9
D.	安裝中繼 / 交叉證書	15
	移除舊有中繼證書（如適用）	17
	安裝中繼 / 交叉證書	18
E.	安裝伺服器證書	22

B. 產生證書簽署要求(CSR)

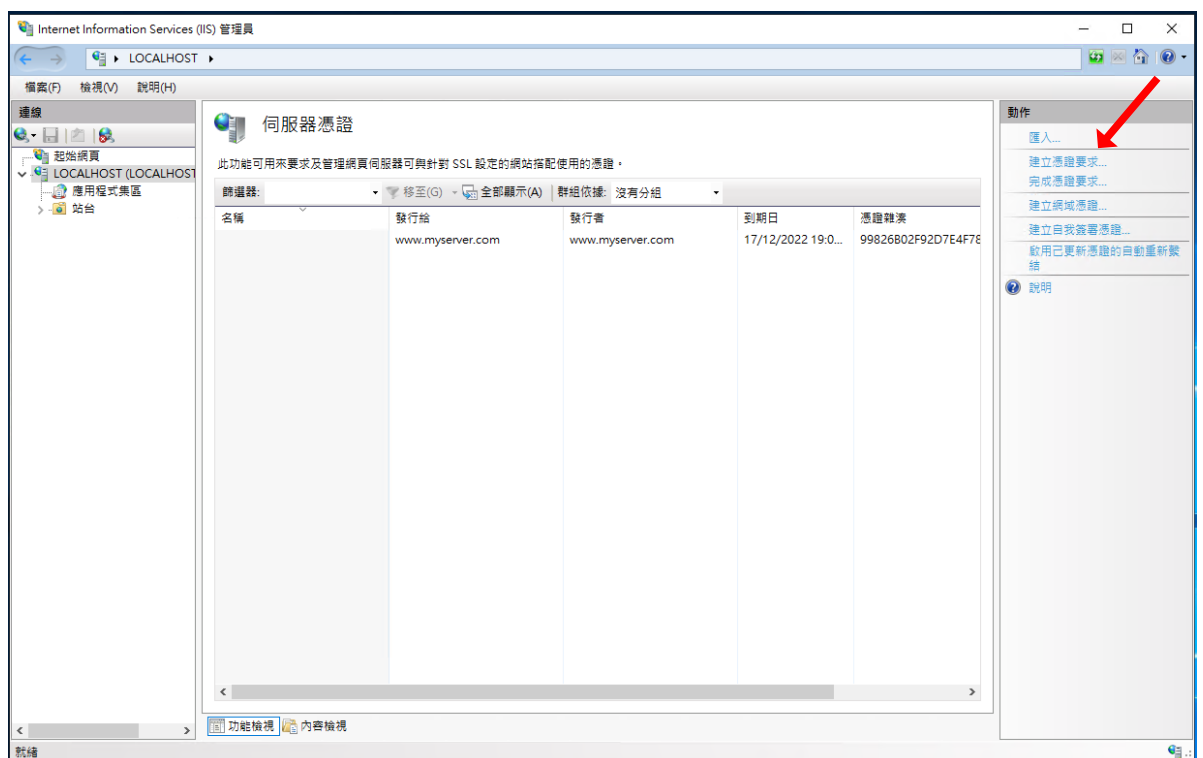
1. 按[開始]>[系統管理工具]>[Internet Information Services (IIS) 管理員]來啟動網際網路資訊服務 (IIS) 管理員。
2. 在[Internet Information Services (IIS) 管理員]視窗內，展開[網站]及選擇您的網站，然後按[伺服器憑證]。



3. 在右手邊[動作]一欄內，按[建立憑證要求]。



注意：新申請及續期申請電子證書（伺服器）的步驟相同，即使是續期電子證書，請不要使用[更新]，要選擇[建立憑證要求]。



4. 輸入您的一般名稱和組織，以及組織單位，並選擇“HK”作為[國家(地區)]，輸入“Hong Kong”作為[縣市/位置]及[省份]，然後按[下一步]。

注意：請確定於「發給」一欄顯示正確的登記域名(即伺服器名稱)及「國家(地區)」一欄顯示「HK」。

注意：若申請電子證書（伺服器）“多域版”或延伸認證電子證書（伺服器）“多域版”，請在「一般名稱」一欄中，輸入與申請表格中所填寫的「用作電子證書主體名稱的伺服器名稱」相同的登記伺服器名稱。而「電子證書主體別名內的額外伺服器名稱」，則無需在產生證書簽署要求(CSR)過程中輸入，香港郵政核證機關系統在簽發證書時，會根據申請表格所申請的資料自動填寫。

若申請電子證書（伺服器）“通用版”，請在「通用名稱」一欄中，輸入與申請表格中所填寫的「有通配符的電子證書伺服器名稱」相同的登記伺服器名稱(伺服器名稱的最左部份需包括有通配符「*」的部份)。例如 *.myserver.com。

注意：若申請中文伺服器名稱的電子證書（伺服器）

選項 1：請在「通用名稱」一欄中，輸入與申請表格中所填寫的「用作電子證書主體名稱的伺服器名稱」相同的登記伺服器名稱。

選項 2：請使用國際網域名稱轉換工具把中文網域名稱轉換成 ASCII 字元，並可以在“通用名稱”一欄中輸入轉換後的名稱。

要求憑證

分辦名稱屬性

指定憑證的必要資訊。省份及縣市/位置必須指定成正式名稱，而且不能包含縮寫。

一般名稱(M):

組織(O):

組織單位(U):

縣市/位置(L):

省份(S):

國家/地區(R):

上一步(P) 下一步(N) 完成(F) 取消

5. 選擇 “Microsoft RSA SChannel Cryptographic Provider” 作為[密碼編譯服務提供者]及 “2048” 作為密碼匙的[位元長度]，然後按[下一步]。

注意：小於 2048 位元的密碼匙或未能提供足夠保密程度，相反大於 2048 位元有可能與某些瀏覽器不兼容。建議選擇長度為 2048 位元的密碼匙，從而提供較佳的保密程度。

要求憑證

密碼編譯服務提供者內容

選取密碼編譯服務提供者及位元長度。加密金鑰的位元長度會決定憑證的加密強度。位元長度越大，安全性就越高。不過，位元長度較大可能會降低效能。

密碼編譯服務提供者(S):

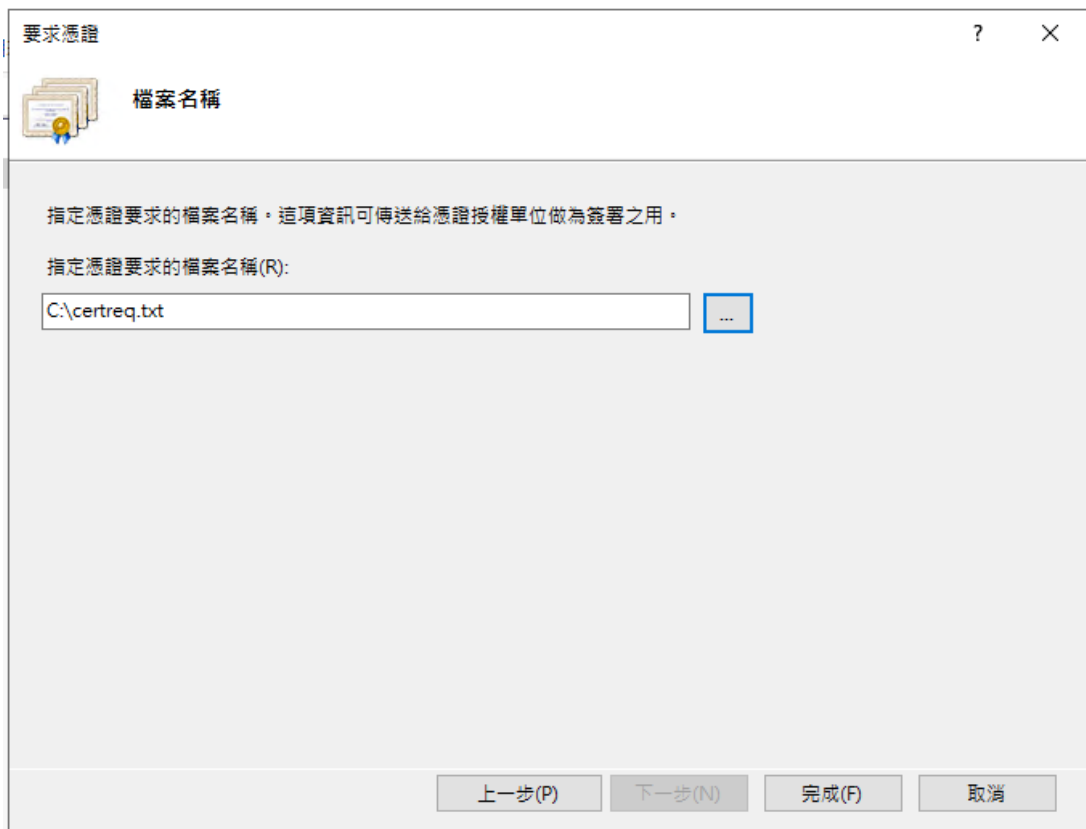
Microsoft RSA SChannel Cryptographic Provider

位元長度(B):

2048

上一步(P) 下一步(N) 完成(F) 取消

6. 輸入新憑證名稱（或接受預設）及按[完成]來關閉精靈。



要求憑證

檔案名稱

指定憑證要求的檔案名稱。這項資訊可傳送給憑證授權單位做為簽署之用。

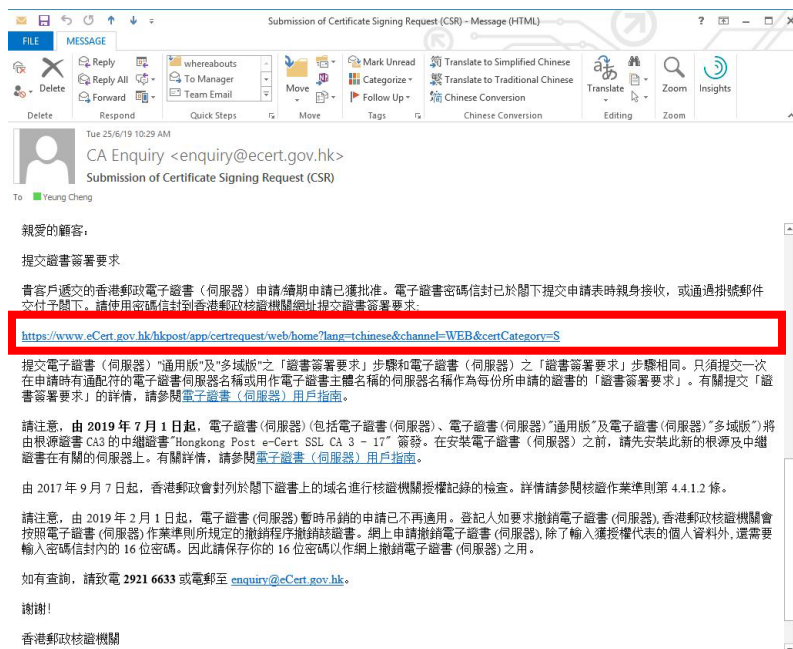
指定憑證要求的檔案名稱(R):

C:\certreq.txt

上一步(P) 下一步(N) 完成(F) 取消

C. 提交證書簽署要求(CSR)

1. 在香港郵政核證機關發出主旨為“Submission of Certificate Signing Request (CSR)”的電郵內按一下超連結以連線至香港郵政核證機關的網站。



2. 輸入[伺服器名稱]、印於密碼信封面的[參考編號](九位數字)及印於密碼信封內的[電子證書密碼](十六位數字)，然後按[提交]。

The solution for e-Security

提交「簽發證書要求」- 電子證書（伺服器）

你在此申請表格所填報的個人資料，香港郵政及其電子核證服務之營運商會用作為你提供電子證書服務的事宜。除非所用途為法例容許又或屬法例規定，否則我們不會用足以辨識你身分的方式，向他人披露你的資料。你向我們提供你的個人資料，全屬自願性質。如未能提供有關資料，可能會影響處理你的電子證書申請。根據《個人資料（私隱）條例》，你有權查閱或更改香港郵政保存有關你的個人資料。如需查閱或更改資料，請填妥《查閱資料要求表格》(Pos736) 或《改正個人資料要求表格》(Pos736A)，然後交回任何一間郵政局或寄交香港郵政個人資料私隱主任。《查閱資料要求表格》和《改正個人資料要求表格》亦可於各郵政局索取。

伺服器資料：

伺服器名稱：

電子證書密碼信封資料：

參考編號：
(印於密碼信封面；九位數字)

電子證書密碼：
(十六位數字密碼內的空白地方無須填寫)

請注意，由2025年5月1日起，電子證書（伺服器）會以新中繼證書簽發。為確保順利過渡，請：

1. 從你的伺服器中移除舊有中繼證書（如適用）。
2. 下載並安裝新中繼證書（標示為「自2025年5月1日起生效」）。
3. 安裝於2025年5月1日或之後簽發的電子證書（伺服器）。

有關詳情，請參閱電子證書（伺服器）用戶指南。

不包含EKU屬位的舊有中繼證書將於2026年6月15日之前被撤銷。

2007 © | 重要告示 | 私隱政策

3. 按[提交]確認申請資料。(如發現資料不正確，請電郵至 enquiry@eCert.gov.hk 聯絡香港郵政核證機關。)

The screenshot shows the '提交「簽發證書要求」- 電子證書（伺服器）」 (Submit 'Certificate Issuance Request' - Electronic Certificate (Server)) page. The left sidebar contains the Hong Kong Post e-Cert logo and navigation icons. The main content area is divided into two columns for registration details.

登記人資料	
伺服器名稱:	www.ecert.gov.hk
機構名稱:	Hong Kong SAR Government 香港特別行政區政府
分行/部門名稱:	HKPO-Business Development Branch 香港郵政
商業登記證編號:	
公司註冊證編號 / 公司登記證編號:	
其他註冊證明文件:	HKPO-BDB

有關所申請的電子證書的資料	
證書類型:	電子證書（伺服器）
登記期:	1年

此頁用以確認申請資料，如以上資料正確，請按[確認]鍵繼續：
如選擇在電子證書內顯示「中文機構名稱」，請按[確認使用中文]鍵繼續：

*如使用中文域名註冊，請務必確認清楚字元正確性，註冊後即不能修改。

2007 © | 重要告示 | 私隱政策

注意：若電子證書申請表格上提供了機構中文名稱和/或分部中文名稱，如要發出一張主體名為機構中文名稱的電子證書(伺服器)，請按[確認使用中文]鍵。

4. （自 2026 年 3 月 15 日起生效，且僅適用於非政府登記人）請從適用於您的電子證書（伺服器）的網域控制驗證 (DCV) 方法清單中選擇您所需的方法，並按照螢幕上的指示進行操作。確認後，系統將自動驗證並確認您對電子證書（伺服器）所包含域名的控制權。如果 DCV 驗證成功，您將可以提交 CSR。

（請注意，系統只會顯示適用於您的電子證書（伺服器）類型的驗證方法供您選擇。）

- A. 如選擇「網站變更」網域控制驗證 (DCV) 方法，請下載驗證檔案“fileauth.txt”，並將其上傳到您電子證書（伺服器）所包含的每個域名對應的網站上的指定位置。上傳檔案並確認檔案可公開存取後，按「確認」繼續。請注意，此方法不適用於電子證書（伺服器）“通用版”。

The screenshot shows the Hongkong Post e-Cert website interface. The main heading is "提交「簽發證書要求」 - 電子證書（伺服器）". Below it, the "網域控制驗證 (DCV) 方法：" (Domain Control Validation (DCV) Method) is set to "網站變更 (建議)" (Website Change (Recommended)).

指示：

- 下載驗證檔案：**
下載包含驗證碼的驗證檔案 (fileauth.txt)。
- 將驗證檔案上傳到您的網頁伺服器：**
將檔案上傳到您的電子證書（伺服器）所包含的每個域名對應的網站上的指定位置。該檔案應透過以下任一網址存取。
 - [http://\[域名\]/well-known/pki-validation/fileauth.txt](http://[域名]/well-known/pki-validation/fileauth.txt)
 - [https://\[域名\]/well-known/pki-validation/fileauth.txt](https://[域名]/well-known/pki-validation/fileauth.txt)
- 檢查檔案：**
上傳檔案後，請確保可以透過瀏覽器存取任一網址來確認其是否已可公開存取。您應該可以看到驗證檔案內的驗證碼。
- 確認：**
確認檔案可公開存取後，請按「確認」繼續。您可以稍後返回此頁面完成網域控制驗證 (DCV) 程序，但請務必在30天內完成。否則，您需要使用新的驗證碼完成驗證程序。

Buttons at the bottom: 確認 (Confirm), 返回上頁 (Return to Previous Page).

Footer: 2007 © | 重要告示 | 私隱政策

- B. 如選擇「網域名稱系統變更」網域控制驗證 (DCV) 方法，請為您的電子證書（伺服器）所包含的**每個**域名新增包含驗證碼的 DNS TXT 記錄。新增 DNS 記錄並確保可公開解析後，按「確認」繼續。

The screenshot shows the '提交「簽發證書要求」- 電子證書（伺服器）' (Submit Certificate Request - Electronic Certificate (Server)) page. The '網域控制驗證 (DCV) 方法' (Domain Control Validation (DCV) Method) is set to '網域名稱系統變更 (建議)' (Domain Name System Change (Recommended)). The instructions state: '1. 新增 DNS 記錄：請為您的電子證書（伺服器）所包含的**每個**域名新增 DNS TXT 記錄。' (1. Add DNS Record: Please add a DNS TXT record for **each** domain name included in your electronic certificate (server)). The record details are: '記錄類型: TXT' (Record Type: TXT), '主機: [域名]' (Host: [Domain Name]), '記錄值: [驗證碼]' (Record Value: [Verification Code]), and 'TTL: 3600'. A '複製驗證碼' (Copy Verification Code) button is provided. The next step is '2. 檢查 DNS 記錄：確保 DNS 記錄是可公開解析的。' (2. Check DNS Record: Ensure the DNS record is publicly resolvable). The final step is '3. 確認：新增 DNS 記錄並確認可公開解析後，請按「確認」繼續。您可以稍後返回此頁面完成網域控制驗證 (DCV) 程序，但請務必在30天內完成。否則，您需要使用新的驗證碼完成驗證程序。' (3. Confirm: After adding the DNS record and confirming it is publicly resolvable, please click 'Confirm' to continue. You can return to this page later to complete the DCV process, but you must complete it within 30 days. Otherwise, you will need to use a new verification code to complete the process). '確認' (Confirm) and '返回上頁' (Return to Previous Page) buttons are at the bottom.

- C. 如選擇「構建電郵」網域控制驗證 (DCV) 方法，請選擇指定的電子郵件地址，然後按「發送驗證碼」。收到電子郵件後，在網頁中輸入驗證碼，然後按「確認」繼續。**請注意，此方法不適用於電子證書（伺服器）“多域版”。**

The screenshot shows the same '提交「簽發證書要求」- 電子證書（伺服器）' (Submit Certificate Request - Electronic Certificate (Server)) page. The '網域控制驗證 (DCV) 方法' (Domain Control Validation (DCV) Method) is set to '構建電郵' (Build Email). The instructions state: '1. 接收驗證碼：請選擇指定的電子郵件地址以接收驗證碼。' (1. Receive Verification Code: Please select a specified email address to receive the verification code). There is a dropdown menu for 'admin' and a dropdown for '[域名]' (Domain Name), followed by a '發送驗證碼' (Send Verification Code) button. The next step is '2. 確認：驗證碼：' (2. Confirm: Verification Code:). There is a text input field for the verification code, followed by the instruction '輸入驗證碼，然後按「確認」繼續。' (Enter the verification code, then click 'Confirm' to continue). '確認' (Confirm) and '返回上頁' (Return to Previous Page) buttons are at the bottom.

7. 下載 Hongkong Post e-Cert (Server) 證書。



The screenshot shows the Hongkong Post e-Cert website. The header includes the logo and the tagline "The solution for e-Security". The main content area is titled "提交「簽發證書要求」 - 電子證書（伺服器）" (Submit 'Certificate Issuance Request' - Electronic Certificate (Server)). It lists three steps: 1. Download "Hongkong Post e-Cert (Server)" certificate, 2. Download Hongkong Post Root Certificate, and 3. Download Electronic Certificate (Server) User Guide. A note mentions that users with older versions of the Root CA3 certificate should update to the 2022 version. The footer includes the year 2007 and links to privacy and security policies.

提交「簽發證書要求」 - 電子證書（伺服器）

你現可以：

1. 下載 "Hongkong Post e-Cert (Server)" 證書
2. 下載香港郵政根源證書
3. 下載電子證書（伺服器）用戶指南

提示
為使"未有預載根源證書CA3的舊版本移動/桌面裝置"在根源證書CA1到期後能繼續進入你們已安裝電子證書（伺服器）的網站/伺服器，請謹記在你們的網站/伺服器安裝"Hongkong Post Root CA 3（交叉證書 2022）"。詳情請參閱公告。

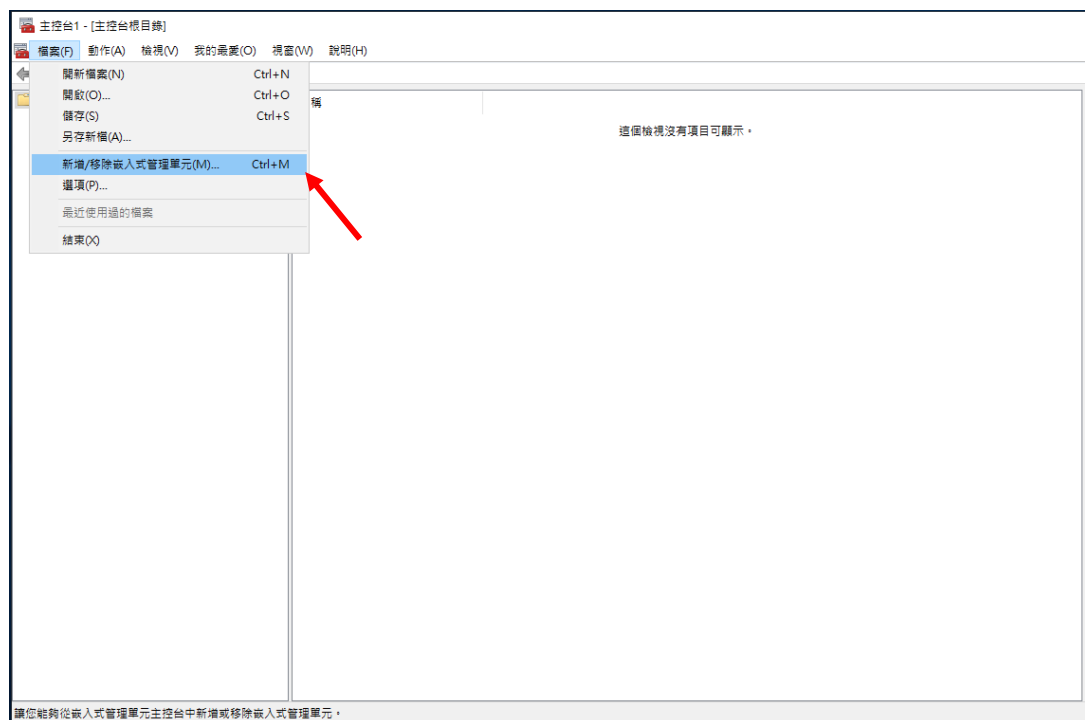
2007 © | 重要告示 | 私隱政策

注意：

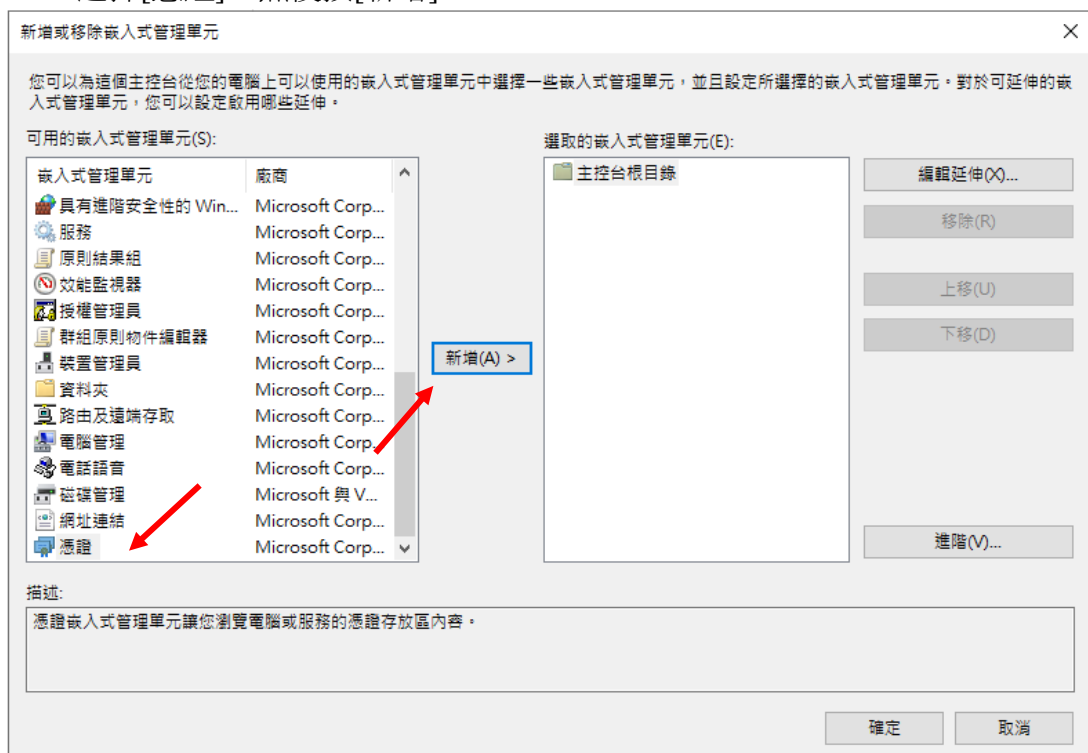
1. 您也可以從搜尋及下載證書網頁下載您的電子證書（伺服器）。
https://www.ecert.gov.hk/tc/sc/index_c.html
2. 安裝由根源證書 Root CA3 簽發的中繼證書"Hongkong Post e-Cert SSL CA 3 - 17"。下載地址如下：
http://www1.ecert.gov.hk/root/ecert_ssl_ca_3-17_pem.crt
安裝由根源證書 GlobalSign Root CA - R3 簽發的交叉證書"Hongkong Post Root CA 3"。
下載地址如下：
http://www1.ecert.gov.hk/root/root_ca_3_x_gscar3_pem.crt
3. 安裝由根源證書 Root CA3 簽發的中繼證書"Hongkong Post e-Cert EV SSL CA 3 - 17"。下載地址如下：
http://www1.ecert.gov.hk/root/ecert_ev_ssl_ca_3-17_pem.crt
安裝由根源證書 GlobalSign Root CA - R3 簽發的交叉證書"Hongkong Post Root CA 3"。
下載地址如下：
http://www1.ecert.gov.hk/root/root_ca_3_x_gscar3_pem.crt

D. 安裝中繼 / 交叉證書

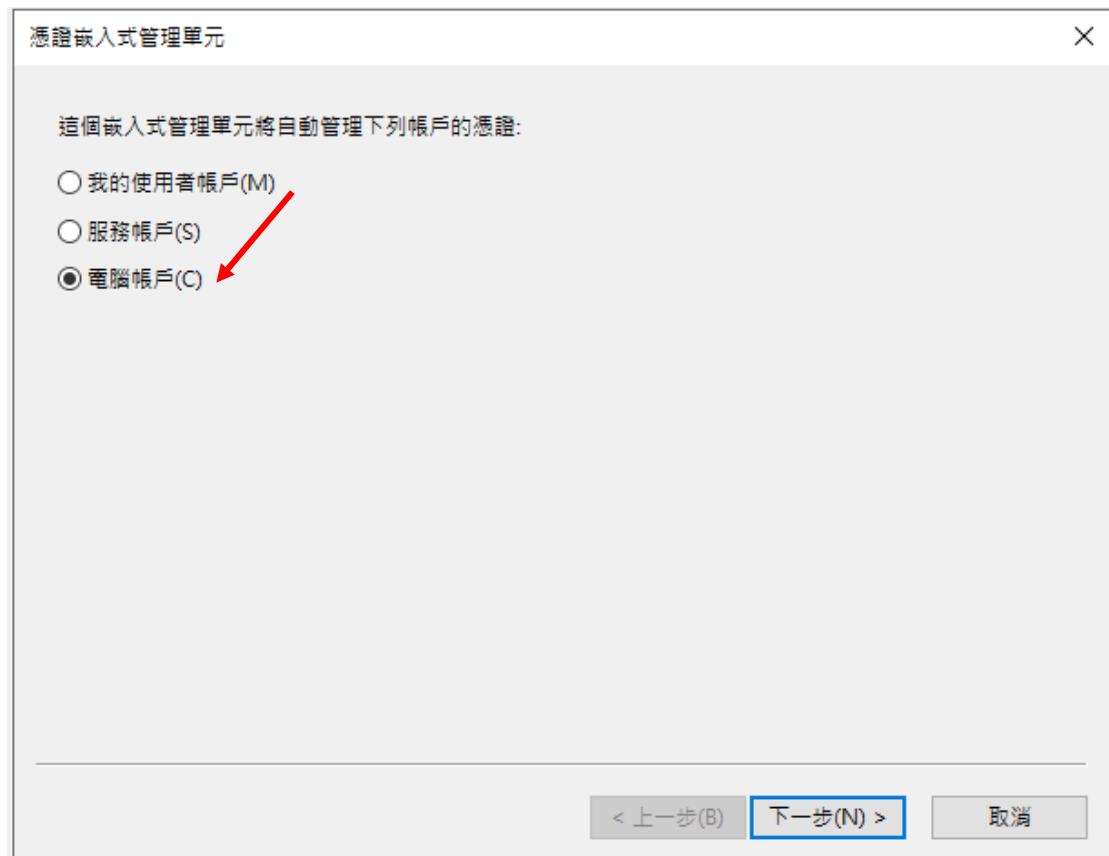
1. 按 [開始] > [執行]，然後輸入“mmc”及按[確定] 來啟動 Microsoft Management Console (MMC)，然後從[檔案]選單中選取[新增/移除嵌入式管理單元]。



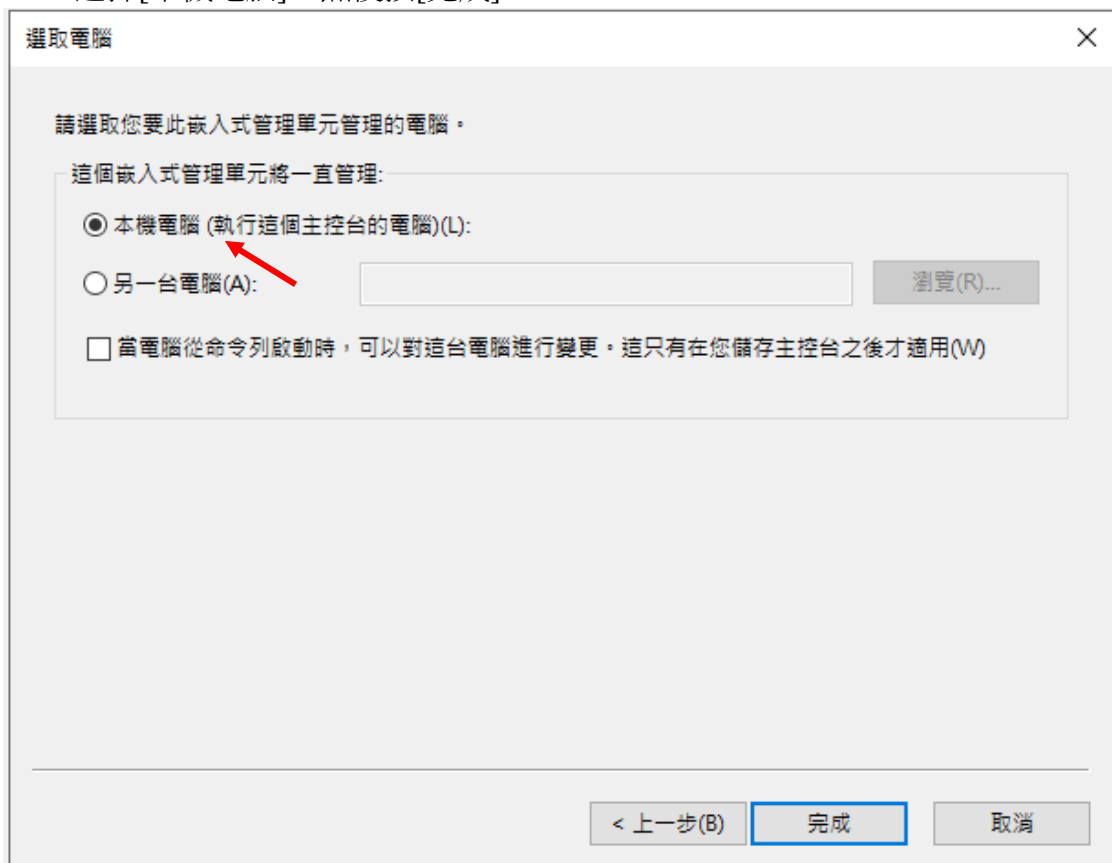
2. 選擇[憑證]，然後按[新增]。



3. 選擇[電腦帳戶]，然後按[下一步]。



4. 選擇[本機電腦]，然後按[完成]。



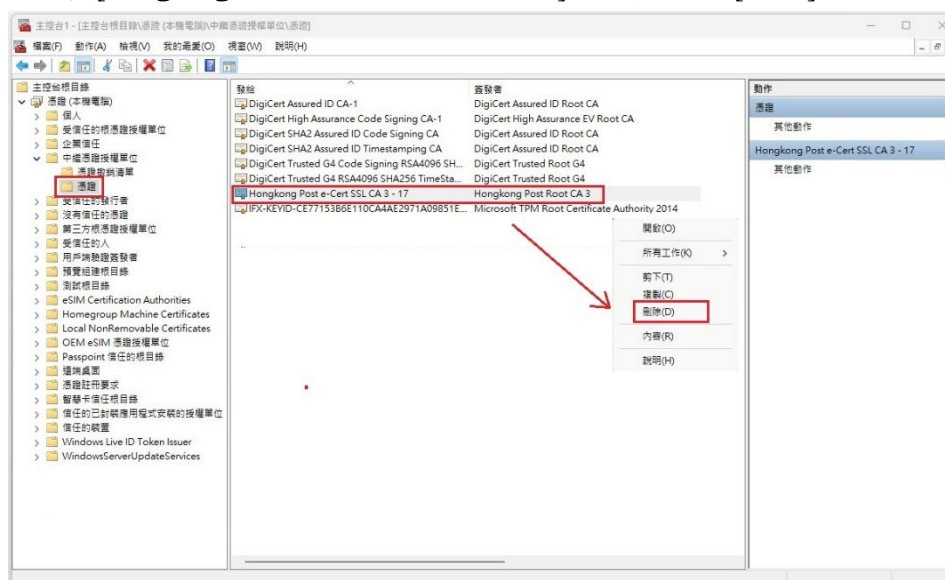
以下內容以“**Hongkong Post e-Cert SSL CA 3 - 17**”中繼證書為例子。

注意：

由 2025 年 5 月 1 日起，電子證書（伺服器）會以新中繼證書簽發。在安裝 2025 年 5 月 1 日或之後發出的電子證書（伺服器）時，**請先移除舊有中繼證書（如適用），然後在相關伺服器上安裝新的中繼證書。**

移除舊有中繼證書（如適用）

展開 [中繼憑證授權單位]，選擇 [憑證]，及以滑鼠右鍵按一下選擇舊有中繼證書[Hongkong Post e-Cert SSL CA 3 - 17]，然後選擇 [刪除]。



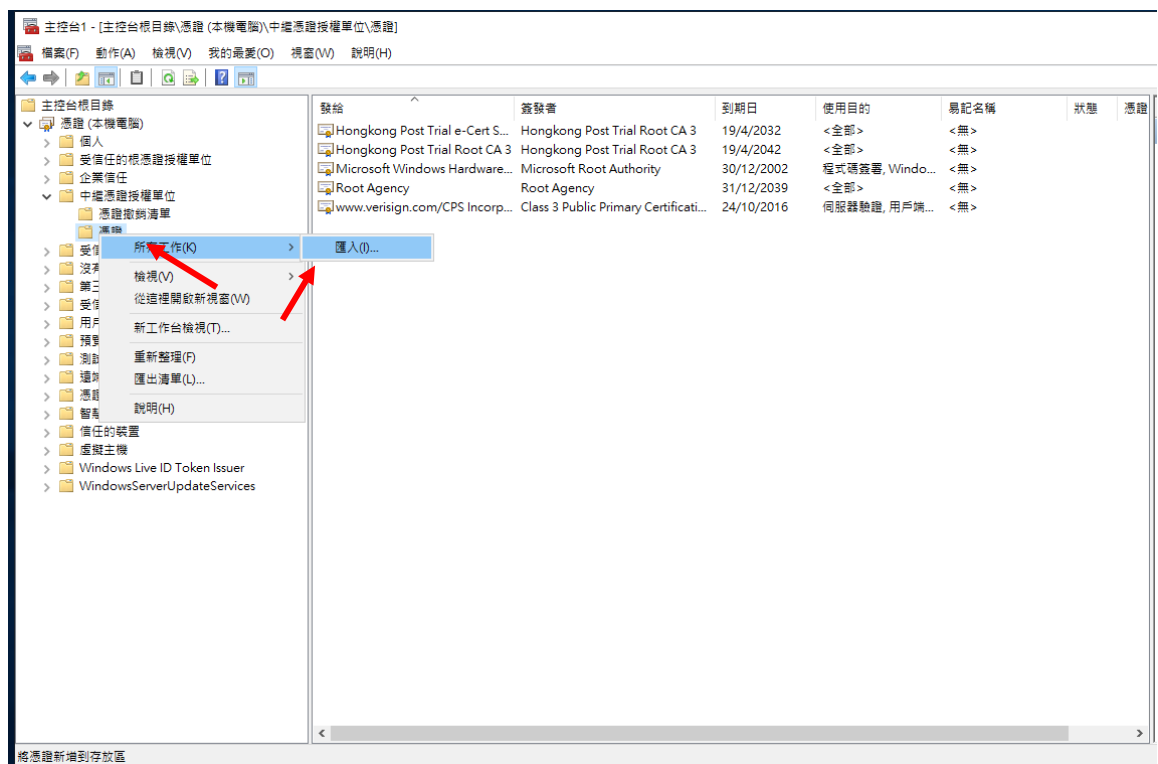
選擇 [是] 確定刪除。



以下內容以“**Hongkong Post e-Cert SSL CA 3 - 17**”中繼證書為例子。

安裝中繼 / 交叉證書

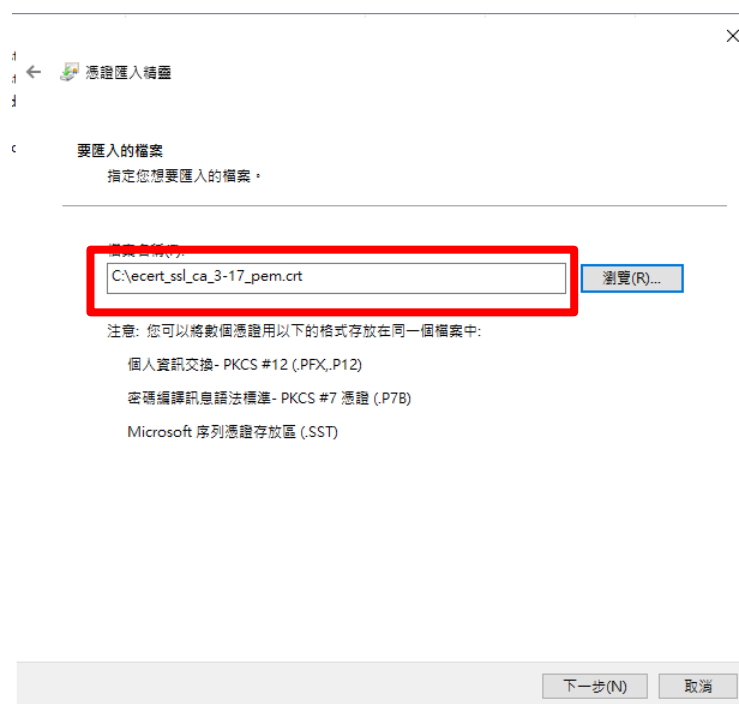
5. 展開[中繼憑證授權]及以滑鼠右鍵按一下[憑證]，然後選擇[所有工作]>[匯入]。



6. 在[憑證匯入精靈]內，按[下一步]繼續。



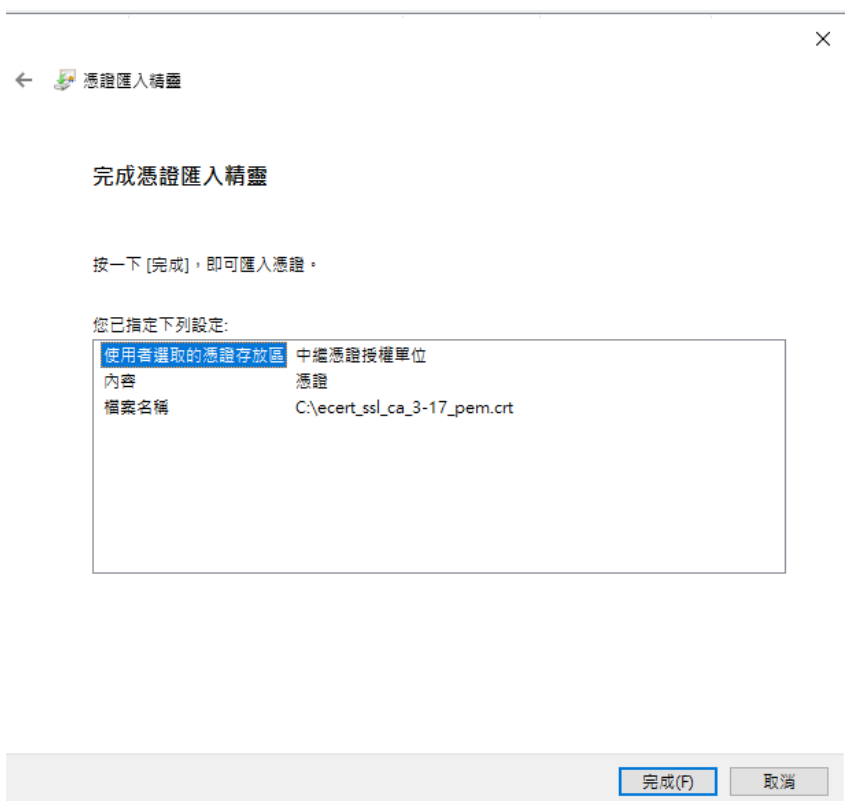
7. 按[瀏覽]指定早前於 C 部的步驟 7 下載的“Hongkong Post e-Cert SSL CA 3 – 17”中繼證書 (ecert_ssl_ca_3-17_pem.crt)，然後按[下一步]。



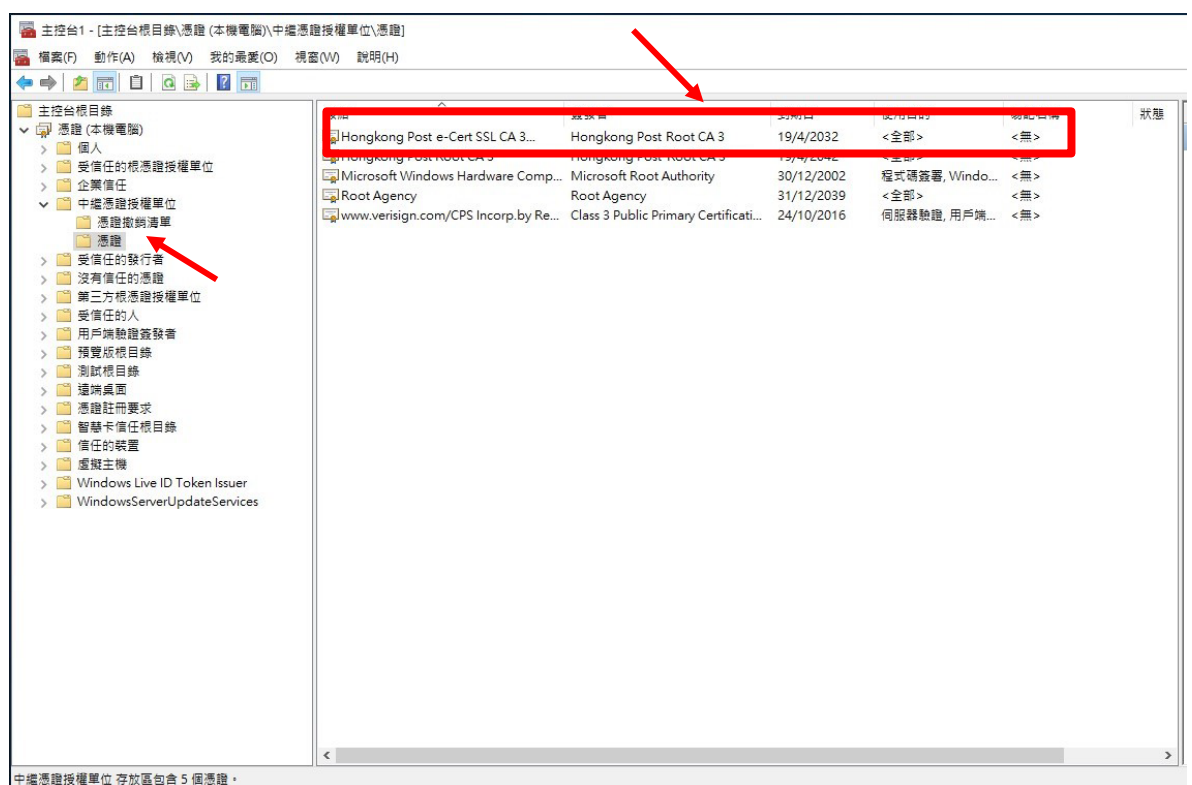
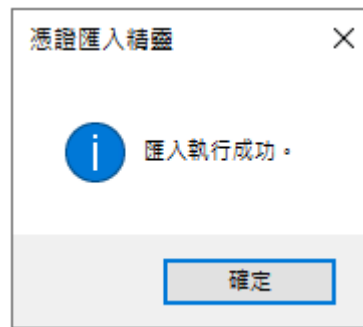
- 選擇[將所有憑證放入以下的存放區]，並選擇中繼憑證授權單位為憑證存放區，然後按[下一步]。



- 按[完成]來關閉精靈。



10. 按[確定]來完成。

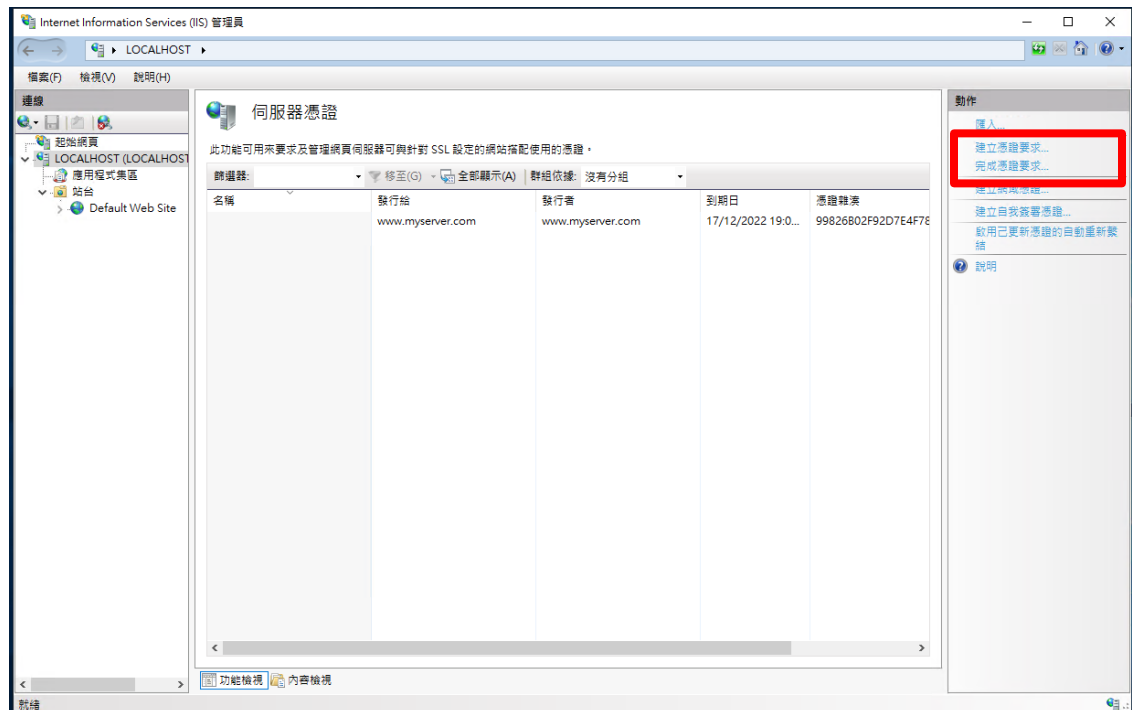


圖表 1: “Hongkong Post e-Cert SSL CA 3 – 17” 已成功安裝

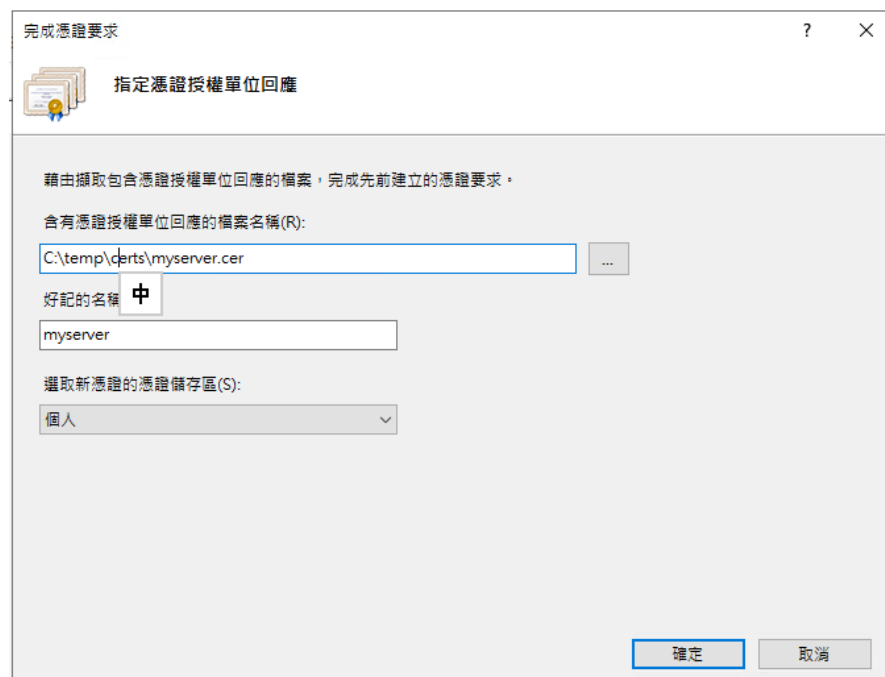
重複步驟 5 到步驟 10 以安裝通過 C 部分步驟 7 下載的交叉證書 (root_ca_3_x_gsca_r3_pem.crt)。

E. 安裝伺服器證書

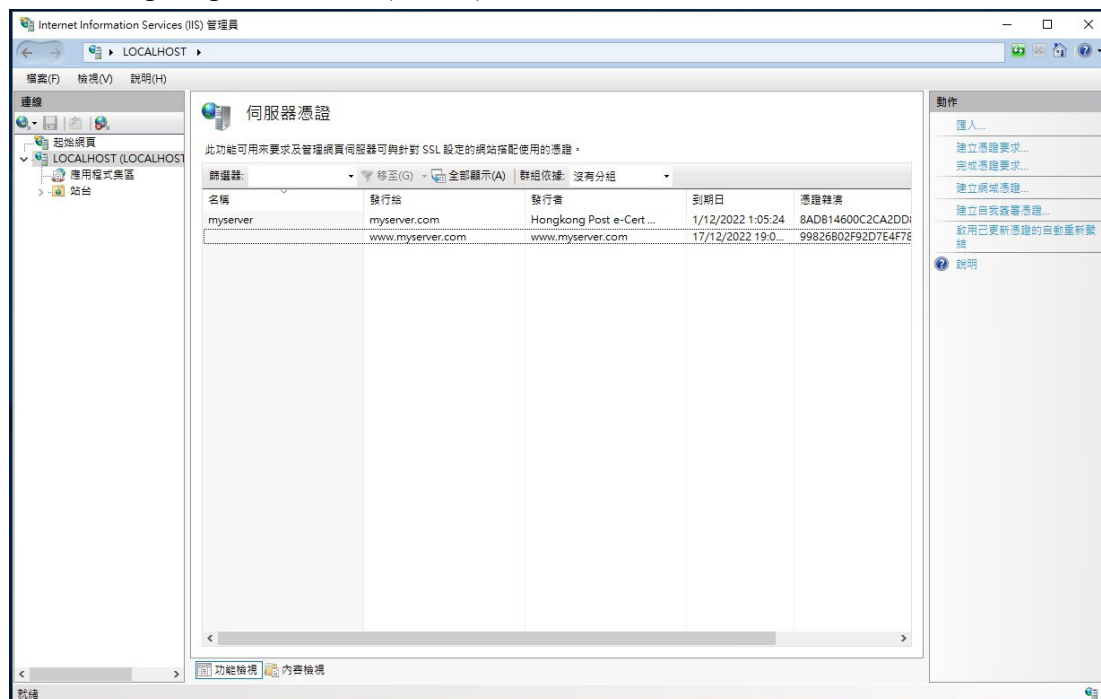
1. 在[Internet Information Services 管理員]視窗內，選擇您的網站，然後按[伺服器憑證]。在右手邊動作一欄內，按[完成憑證要求]。



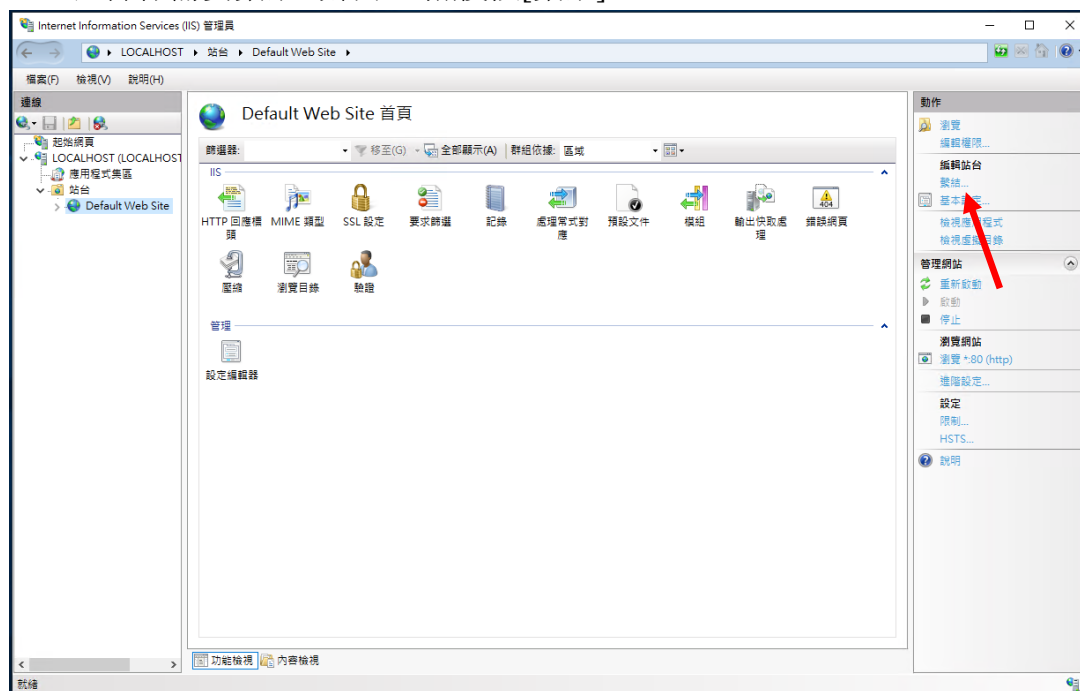
2. 按[瀏覽]指定早前於 C 部的步驟 7 下載的“Hongkong Post e-Cert (Server)”證書及輸入[好記的名稱]，然後按[確定]。



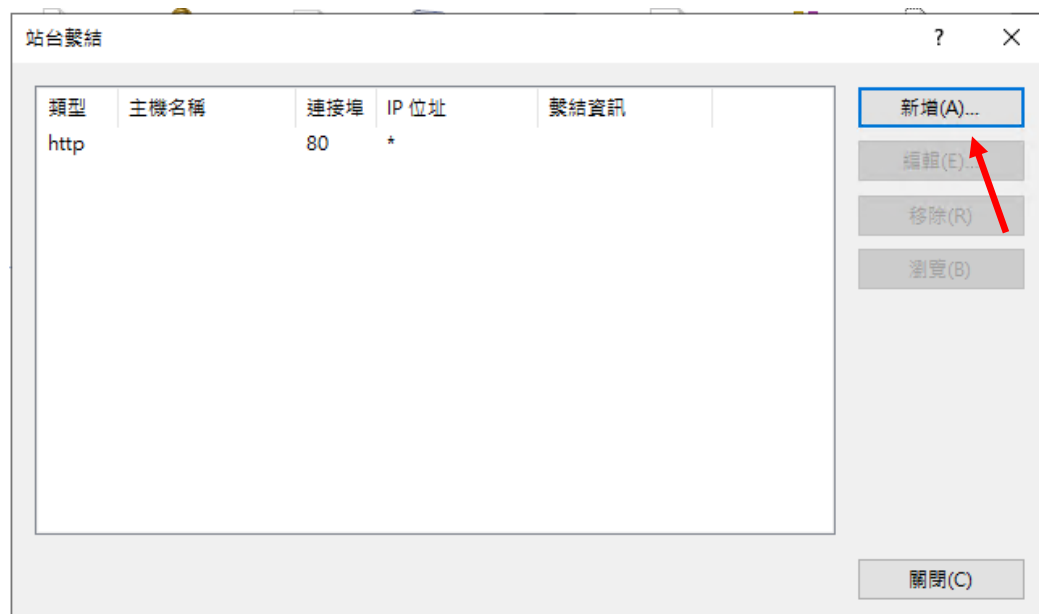
3. “Hongkong Post e-Cert (Server)” 證書已成功安裝。



4. 選擇你需要繫結的網站，然後按[繫結]。



5. 按[新增]。

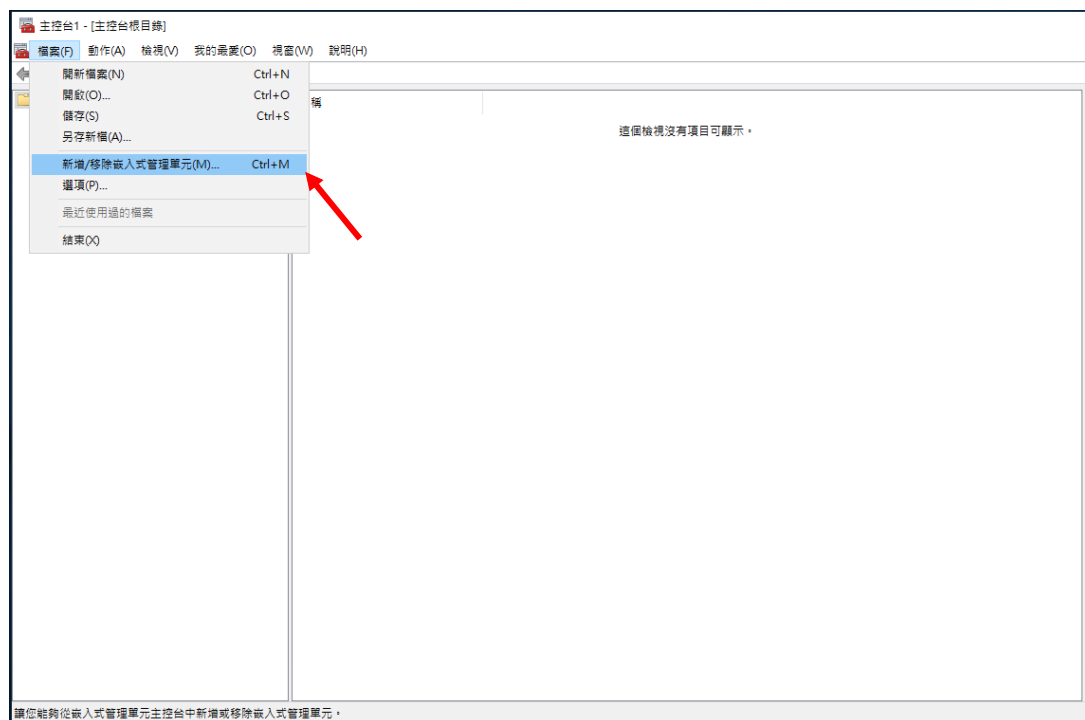


6. 選取[https]及相對應的 SSL 憑證及確定。

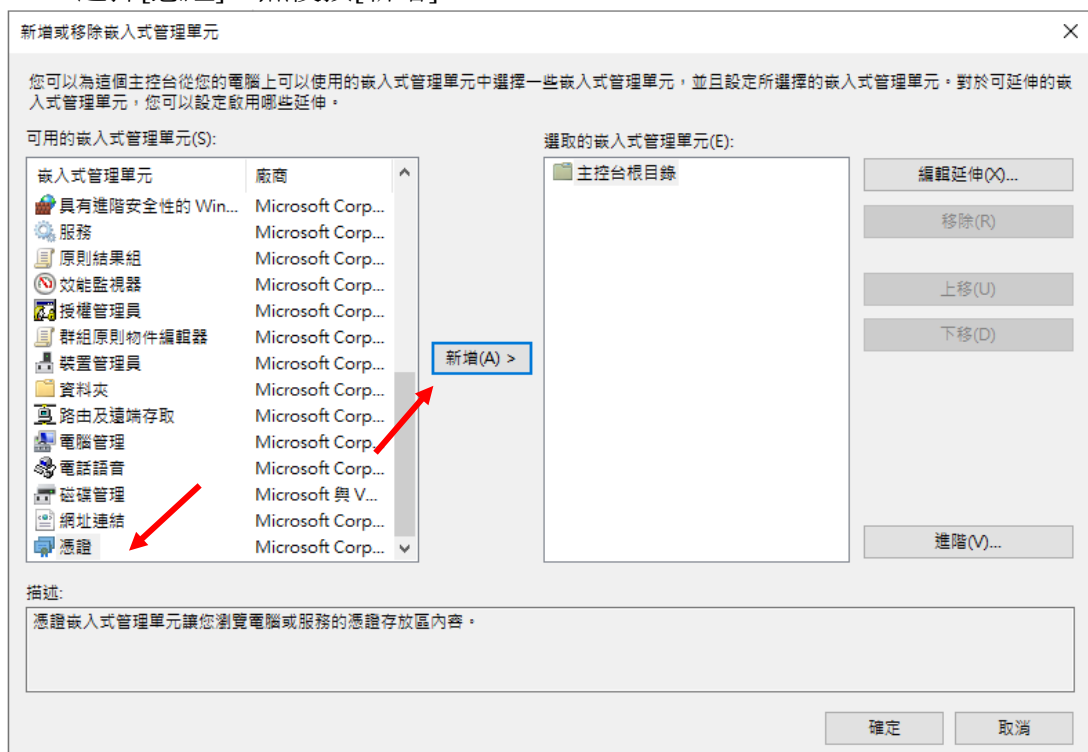


F. 備份密碼匙

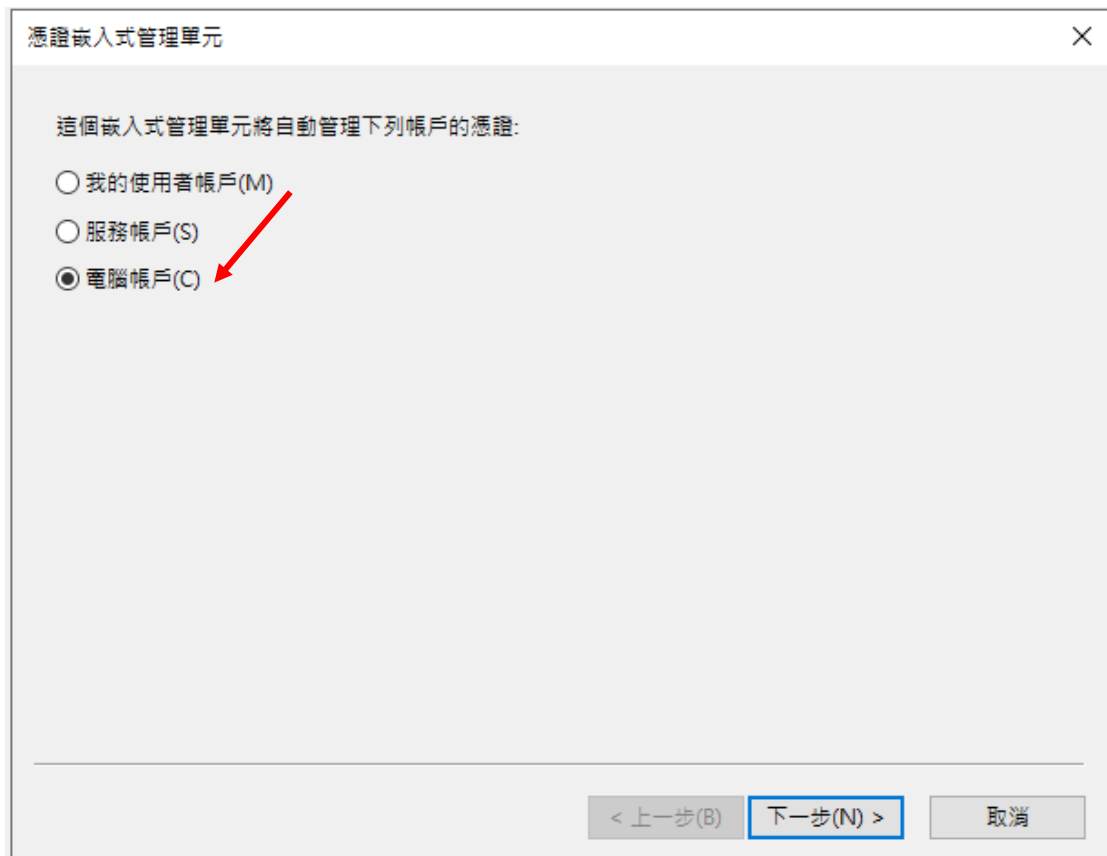
1. 按[開始]>[執行]，然後輸入“mmc”及按[確定]來啟動 Microsoft Management Console (MMC)，然後從[檔案]選單中選取[新增/移除嵌入式管理單元]。



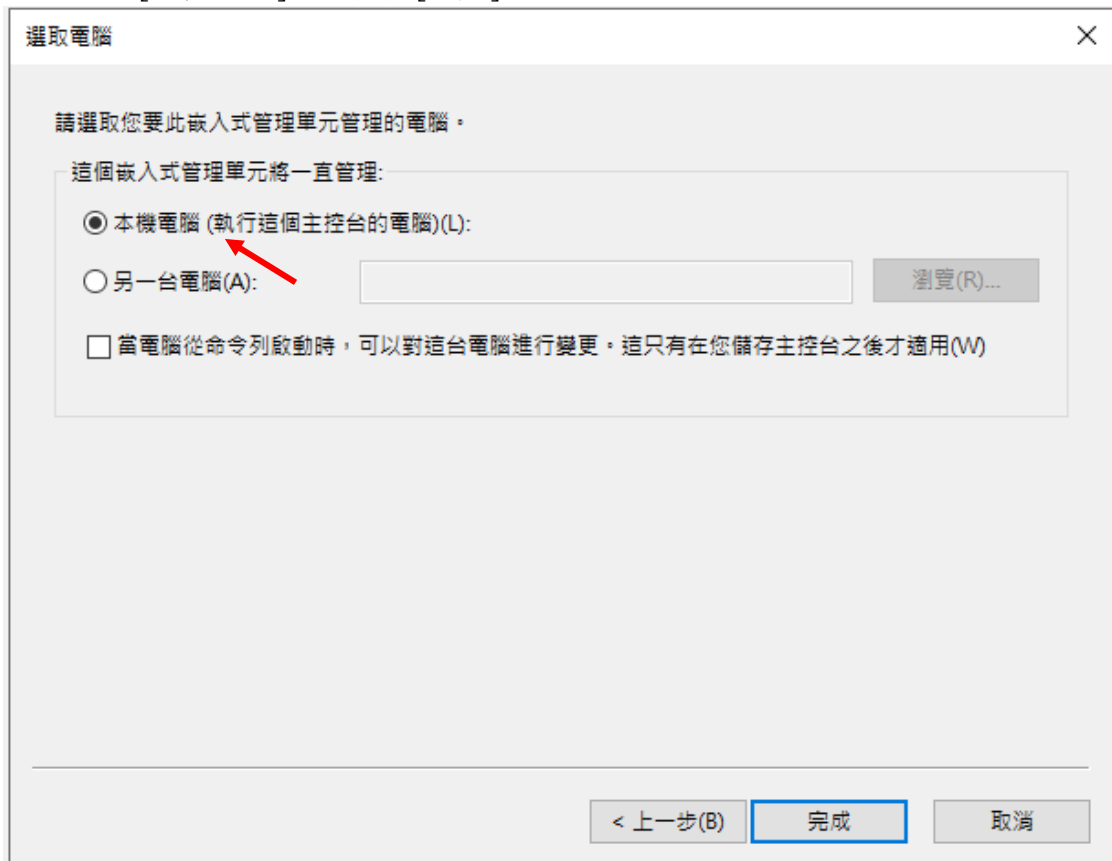
2. 選擇[憑證]，然後按[新增]。



3. 選擇[電腦帳戶]，然後按[下一步]。

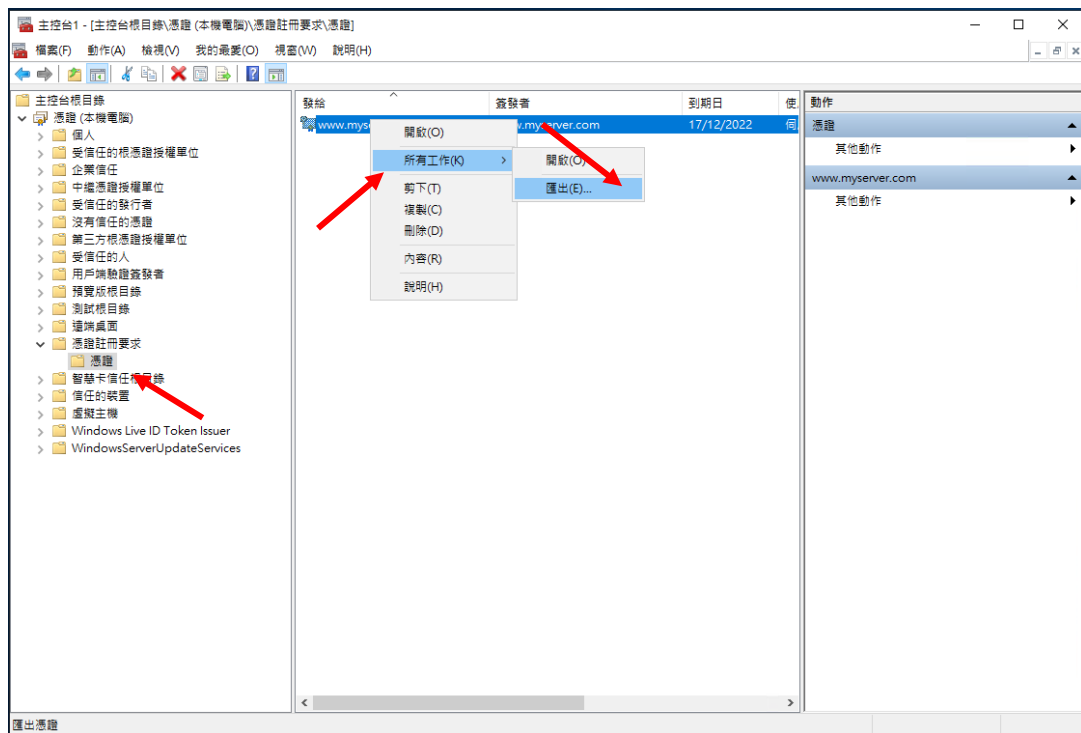


4. 選擇[本機電腦]，然後按[完成]。

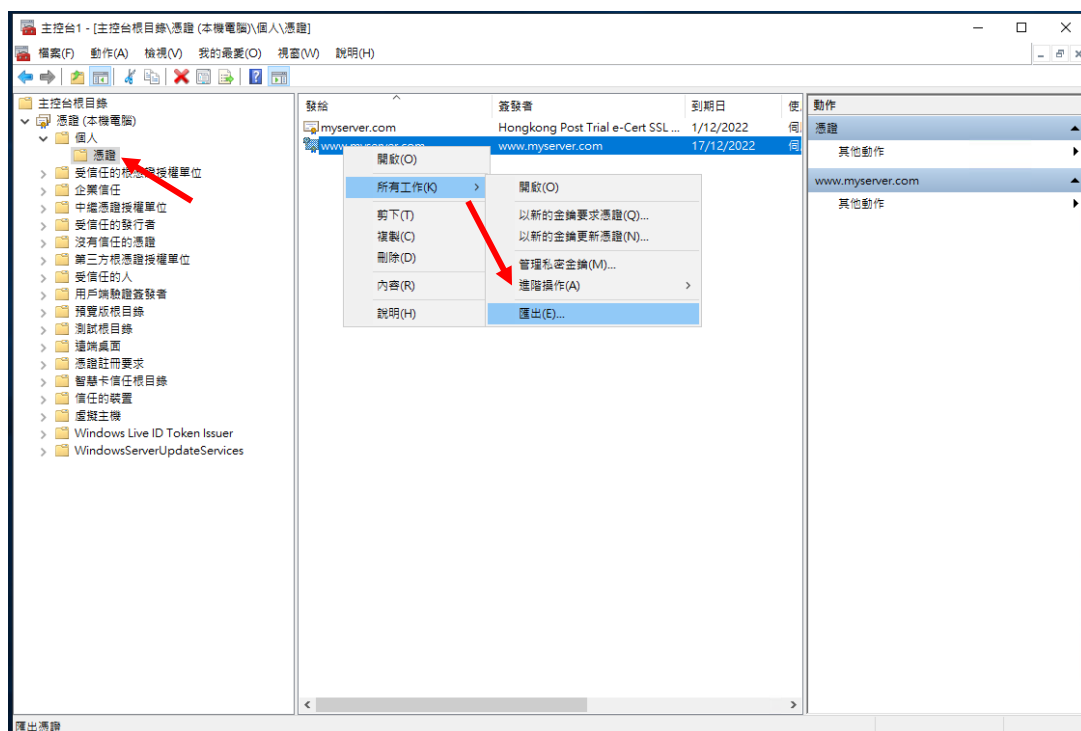


5. 備份密碼匙

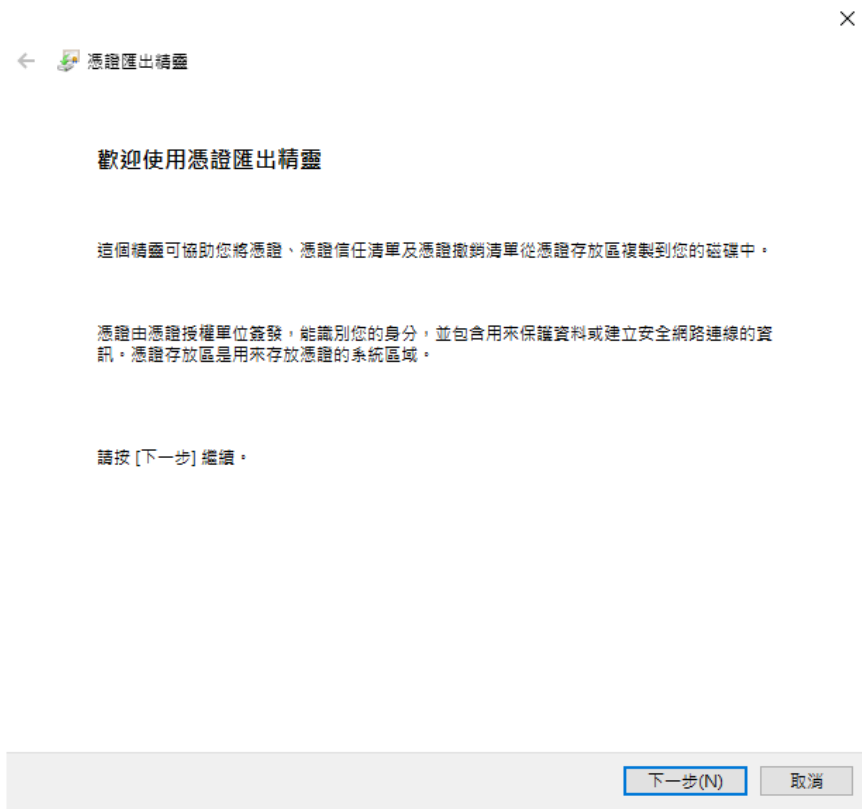
- 備份憑證註冊要求的密碼匙，請展開[憑證註冊要求](或於某些系統稱為[REQUESTS])。按一下[憑證]，選擇你剛建立的憑證註冊要求，然後以滑鼠右鍵選擇[所有工作]>[匯出]。



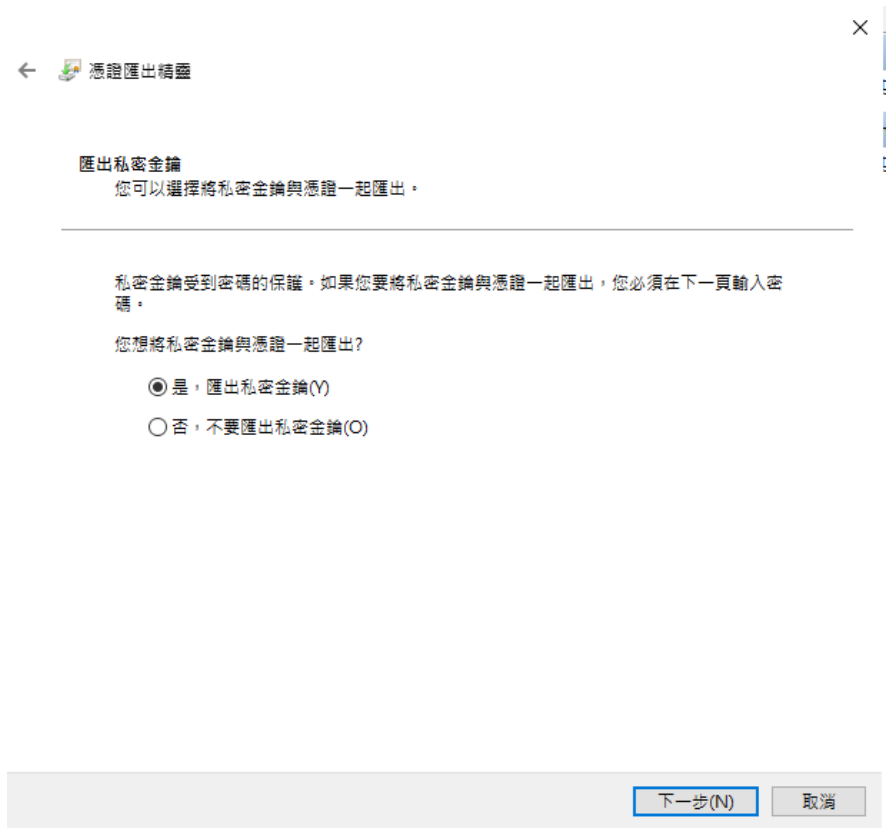
- 備份現有證書的密碼匙，展開[個人]及以滑鼠右鍵按一下[憑證]，選擇你需要備份的證書，然後以滑鼠右鍵按一下[所有工作]>[匯出]。



6. 在[憑證匯出精靈]內，按[下一步]繼續。



7. 選擇[是，匯出私密金鑰]，按[下一步]繼續。



8. 選擇[個人資訊交換 - PKCS #12 (.PFX)(P)]，只選取[如果可能的話，包含憑證路徑中的所有憑證(U)]及[啟用憑證隱私權(E)]，然後按[下一步]。



9. 輸入密碼匙的密碼，然後按[下一步]。

注意：請緊記這個重要的密碼。如果您忘記這密碼，您將不能還原您的密碼匙。

×

← 憑證匯出精靈

安全性
為維護安全性，您必須保護安全性主體的私密金鑰，或透過密碼保護。

☐ 群組或使用者名稱 (建議選項)(G)

新增(A)
 移除(R)

☒ 密碼(P):

●●●●

確認密碼(C):

●●●●

加密: TripleDES-SHA1 ▼

下一步(N) 取消

10. 按[瀏覽]指定密碼匙的備份檔案，然後按[下一步]。（此檔案的副檔名預設值為 pfx）。

×

← 憑證匯出精靈

要匯出的檔案
請指定您要匯出的檔案名稱

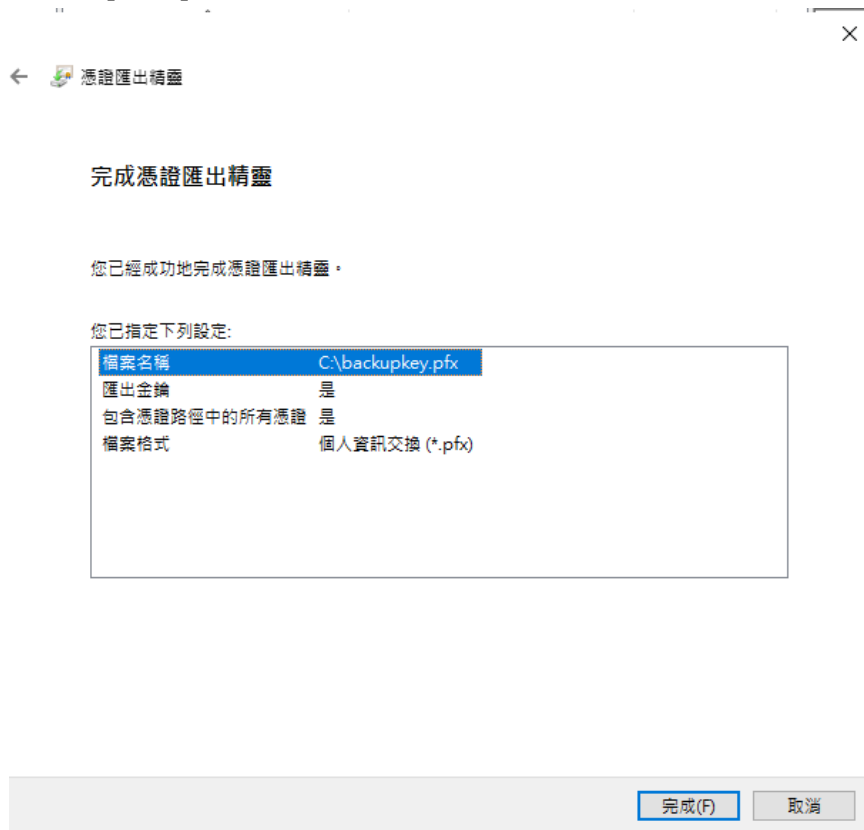
檔案名稱(F):

C:\backupkey.pfx

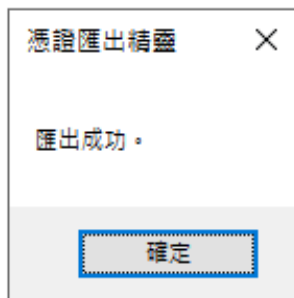
瀏覽(R)...

下一步(N) 取消

11. 按[完成]來關閉精靈。

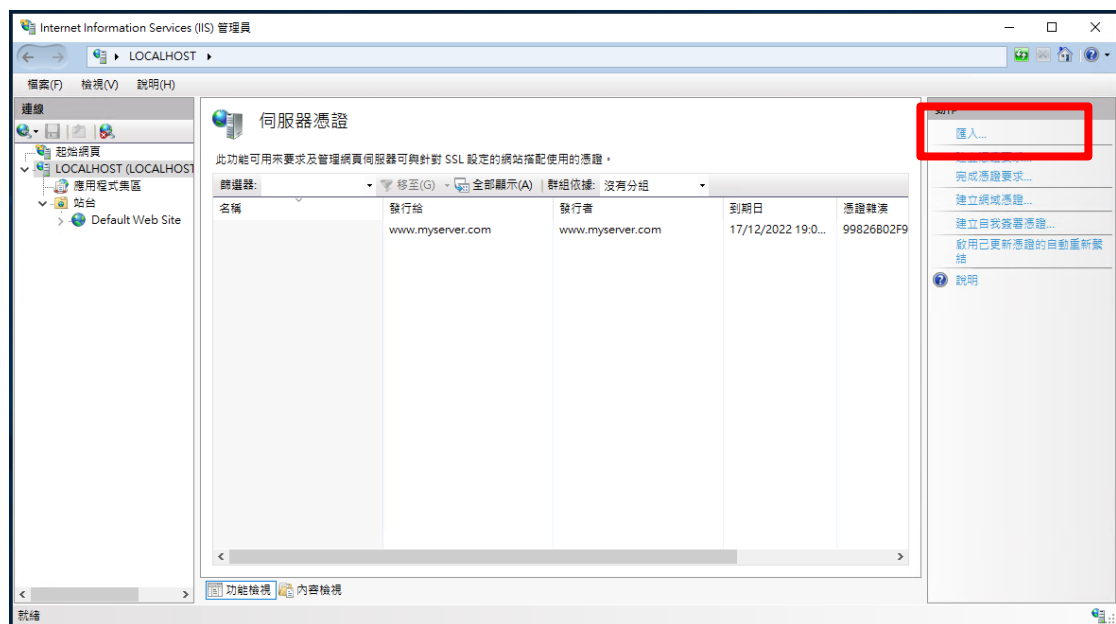


12. 按[確定]來完成。



G. 還原密碼匙

1. 按[開始]>[控制台]>[所有控制台項目]>[系統管理工具]>[Internet Information Services (IIS) 管理員]來啟動網際網路資訊服務 (IIS) 管理員。
。
2. 選擇你的網站，然後按[伺服器憑證]。
3. 在右手邊動作一欄內，按[匯入]。



4. 輸入包含憑證的檔案名稱及路徑及憑證的密碼，然後按[確定]。

注意：你可以取消選取[允許匯出此憑證]使不允許匯出憑證。或為使您將來可以進行備份或傳輸您的憑證，可選取[允許匯出此憑證]使憑證可匯出。

匯入憑證

憑證檔案 (.pfx)(C):
C:\backupkey.pfx

密碼(P):
●●●●●

選取憑證儲存區(S):
個人

☒ 允許匯出此憑證(A)

確定 取消

5. 電子證書（伺服器）証書已成功匯入。

