



電子證書（伺服器）用戶指南

Microsoft Exchange Server 2010 適用

修訂日期：2022年12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).....	12
D.	安裝中繼 / 交叉證書	17
	安裝授權撤銷清單(ARL)	23
E.	安裝伺服器證書	27
F.	備份密碼匙	31
G.	還原密碼匙	34

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）申請人如何在 Windows 2008 上的 Exchange Sever 2010 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	31
G.	還原密碼匙	34

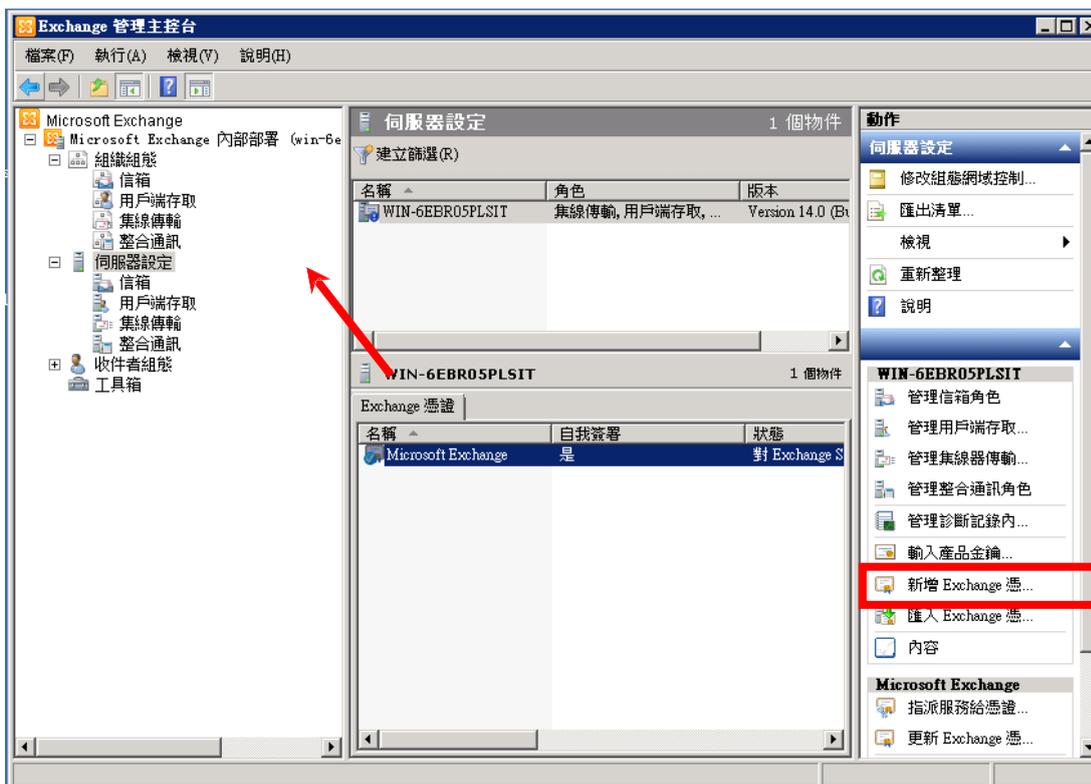
新申請及續期申請

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：

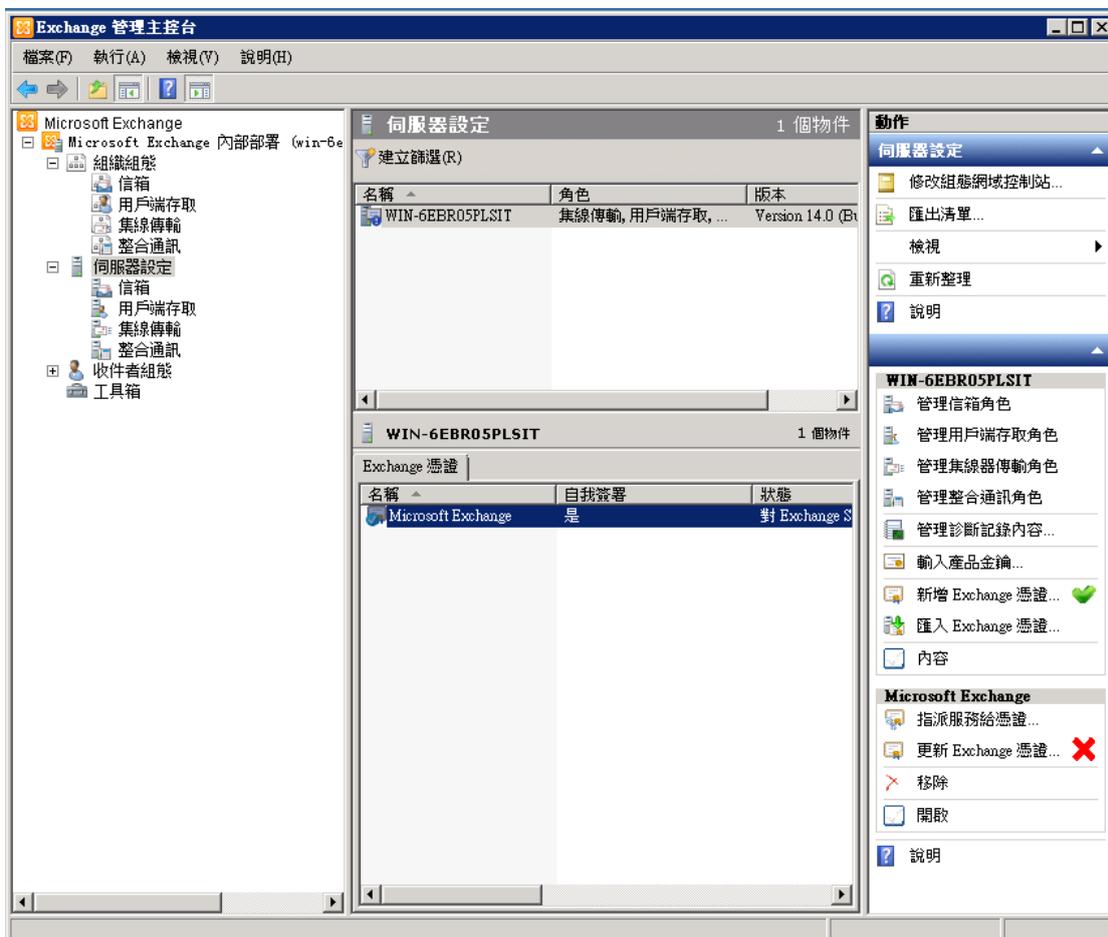
B.	產生證書簽署要求(CSR).....	4
C.	提交證書簽署要求(CSR).....	12
D.	安裝中繼 / 交叉證書	17
	安裝授權撤銷清單(ARL)	23
E.	安裝伺服器證書	27

B. 產生證書簽署要求(CSR)

1. 按[開始]>[所有程式]>[Exchange Sever 2010]>[Exchange 管理主控台]來啟動 Exchange 管理工具。
2. 在 [Exchange 管理主控台] 視窗內，展開 [Microsoft Exchange 內部部署]。
3. 選擇 [伺服器設定]，在右手邊 [動作] 一欄內，按 [新增 Exchange 憑證]。



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Exchange憑證]，要選擇[新增Exchange憑證]。



4. 輸入憑證的易記名稱（如:Hong Kong Post e-cert），並按[下一步]來繼續。

新增 Exchange 憑證

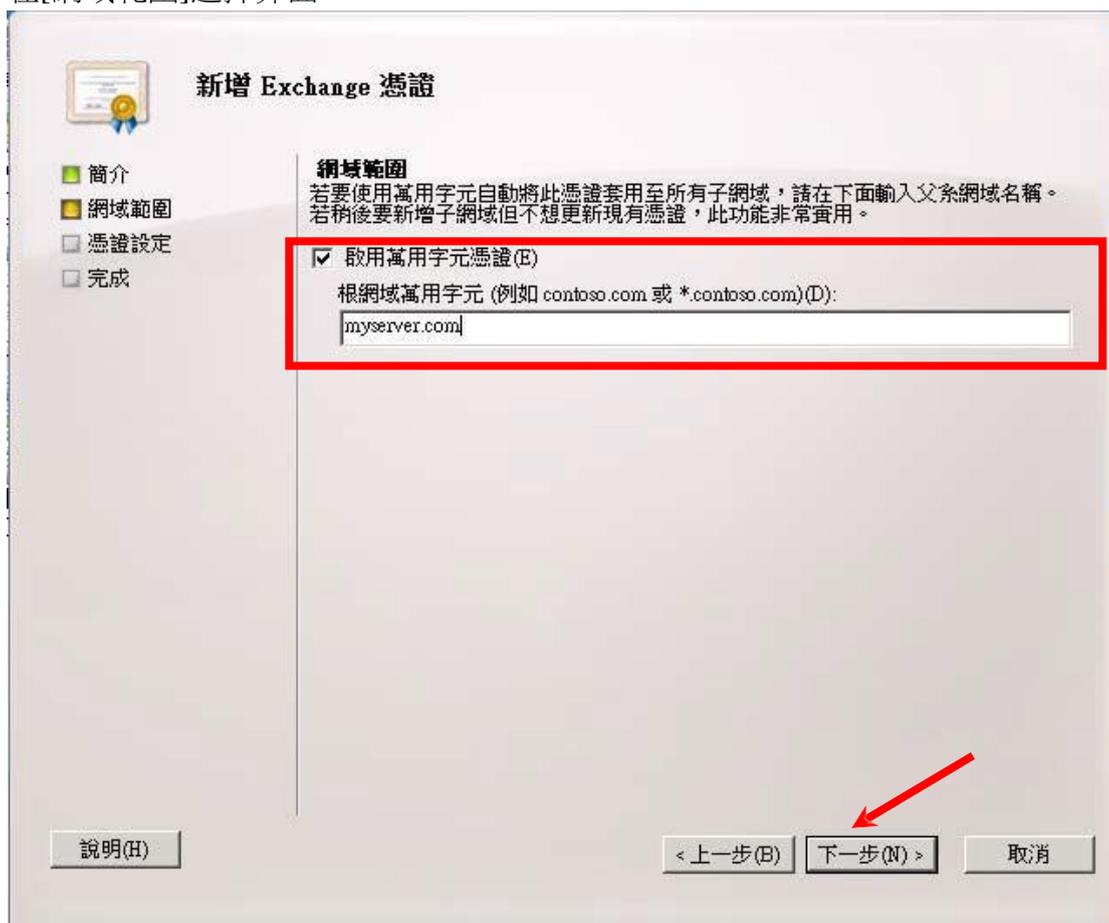
簡介
 網域範圍
 憑證設定
 完成

簡介
此精靈將協助您判斷應用程式正常運作所需的憑證類型。
繼續之前，建議您先閱讀[這些文件](#)，瞭解有關 Exchange Server 服務和憑證需求。

輸入憑證的易記名稱(E):
Hong Kong Post e-cert

說明(H) < 上一步(B) 下一步(N) > 取消

5. 在[網域範圍]選擇界面，



- 如您為電子證書（伺服器）“通用版”的用戶，請鈎選“啟用萬用字元憑證”並與[根網域萬用字元]填入您的伺服器名稱，按[下一步]，並直接進入步驟 6。

注意：請確定[根網域萬用字元]中所填項目與申請表格中‘有通配符的電子證書伺服器名稱’相同，可包括有通配符「*」的部份。

- 如果您為電子證書（伺服器）或電子證書（伺服器）“多域版”的用戶，請直接按“下一步”，並完成步驟 5.1 與 5.2。

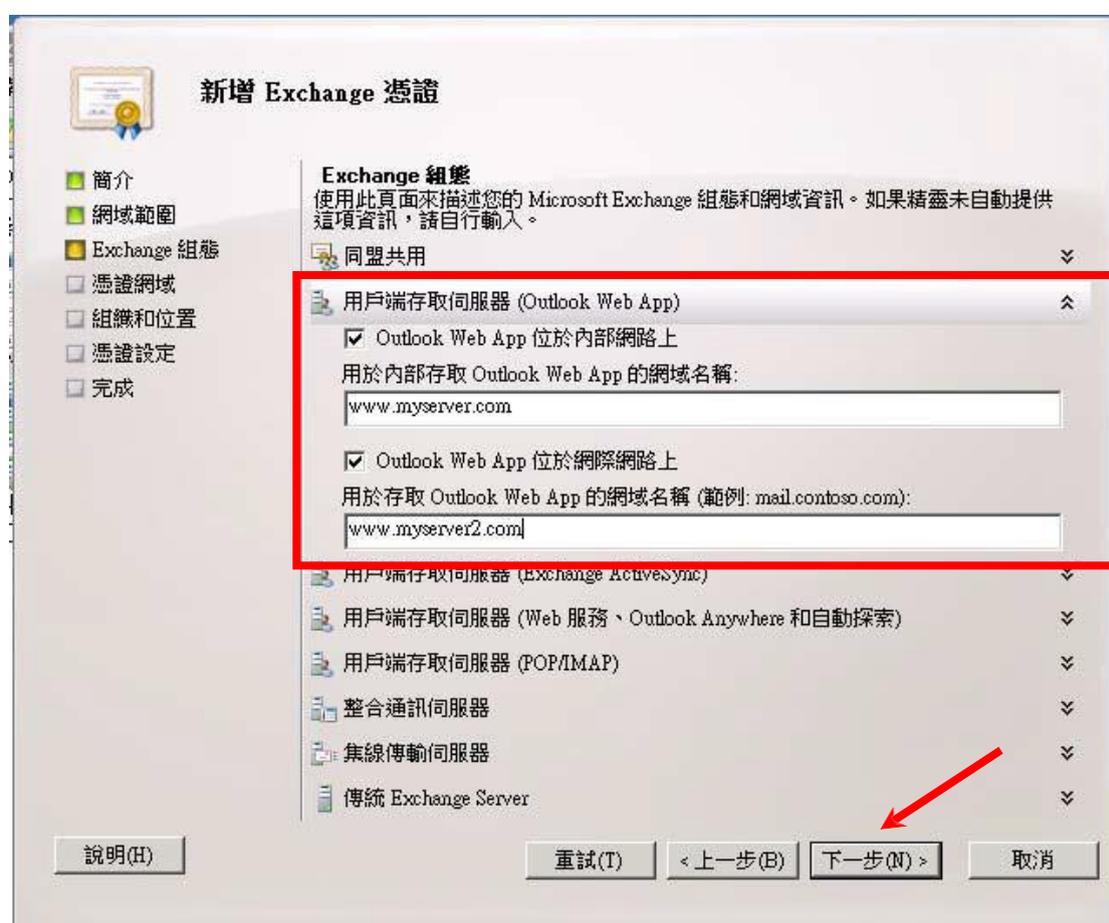
5.1 在 Exchange 組態界面，鈎選您所需要的服務，並按[下一步]來繼續。

注意：您應將依據您的伺服器的服務類別進行相應的配置，以下所示範例為電子證書（伺服器）“多域版”。

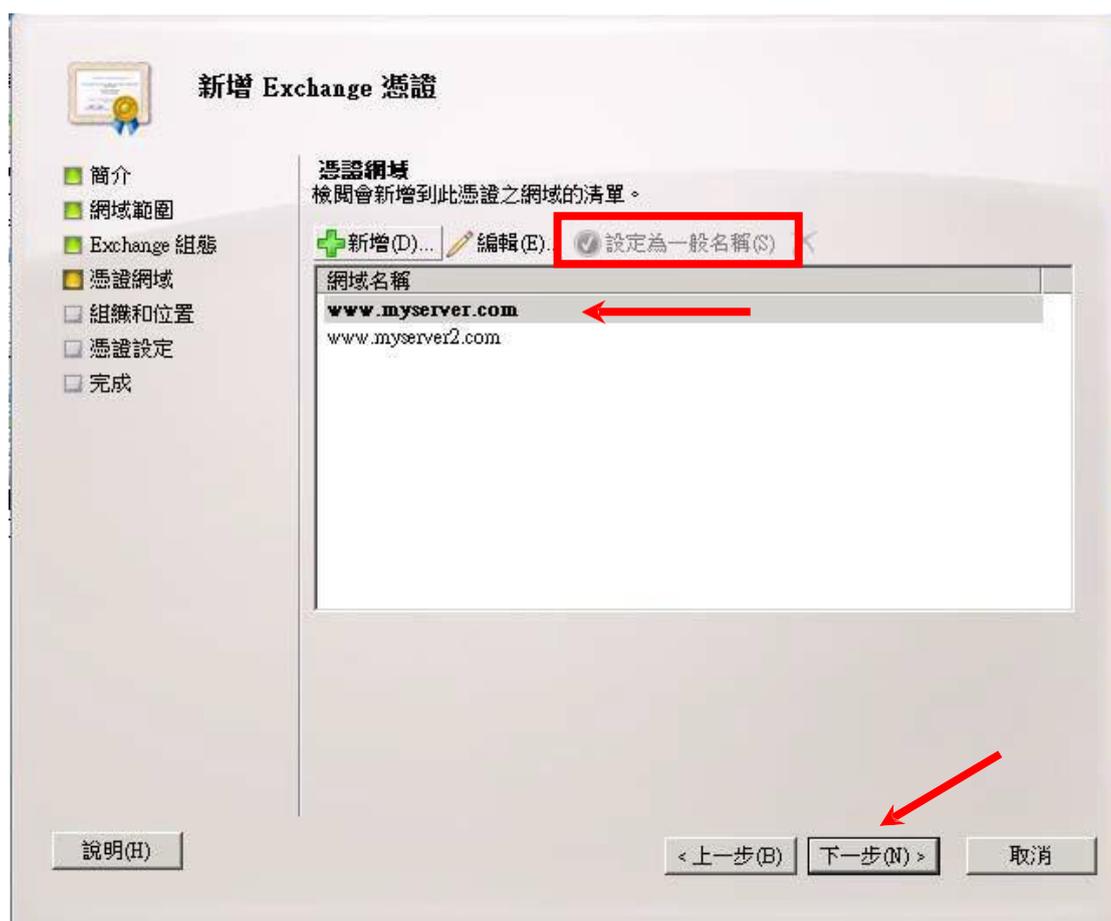
注意：若申請中文伺服器名稱的電子證書（伺服器）

選項 1：請在網域名稱一欄中，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，並可以在網域名稱一欄中輸入轉換後的名稱。



5.2 選擇「一般名稱」設定為一般名稱，並按[下一步]來繼續。



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。

6. 輸入您的組織及組織單位，及選擇“香港特別行政區”作為[國家/地區]，輸入“Hong Kong”作為[城市/位置]及[縣/市]，選擇您的 CSR 存放路徑，然後按[下一步]來繼續。

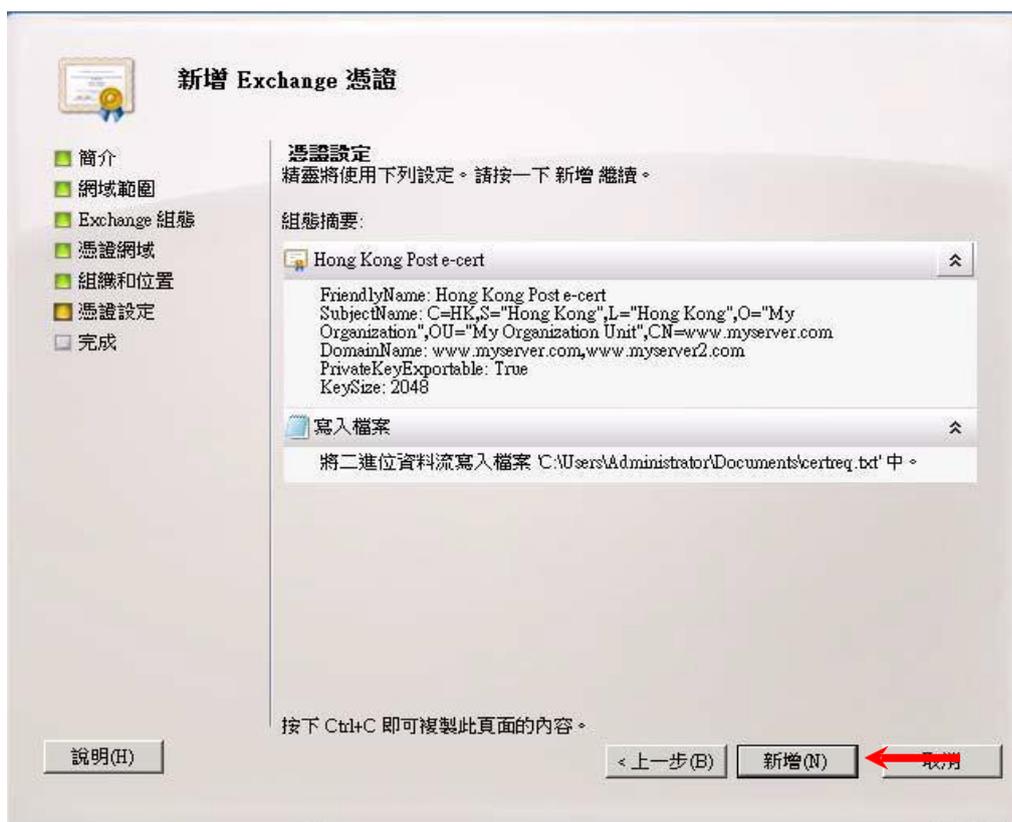
注意：請確保「國家/地區」一欄輸入「香港特別行政區」。

The screenshot shows the 'New Exchange Certificate' wizard in Chinese. The title is '新增 Exchange 憑證'. On the left, there is a navigation pane with the following items: '簡介' (Introduction), '網域範圍' (Domain Scope), 'Exchange 組態' (Exchange Configuration), '憑證網域' (Certificate Domain), '組織和位置' (Organization and Location), '憑證設定' (Certificate Settings), and '完成' (Finish). The '組織和位置' step is currently selected and highlighted in yellow. The main area is titled '組織和位置' and contains the following fields and instructions:

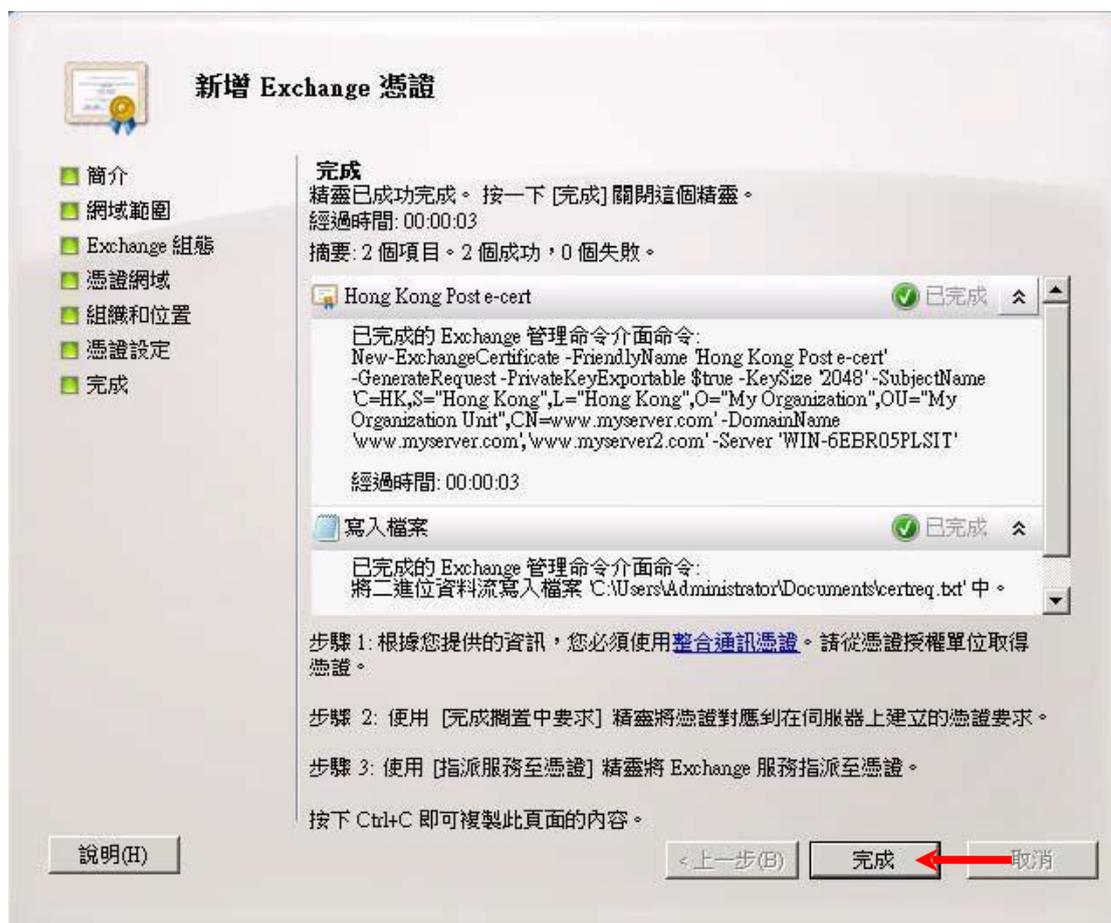
- Instructions: 使用此頁面來輸入您組織的名稱、組織單位、位置，以及憑證要求檔案路徑。
- 組織(O): My Organization
- 組織單位(U): My Organization Unit
- 位置: (empty)
- 國家/地區(C): 香港特別行政區 (dropdown menu)
- 城市/位置(T): Hong Kong
- 縣/市(S): Hong Kong
- 憑證要求檔案路徑: C:\Users\Administrator\Documents\certreq.txt (with a '瀏覽(R)...' button)
- Additional instruction: 在下面的文字方塊中指定要求檔案的名稱。請使用 [瀏覽] 按鈕來選取要在其中建立要求檔案的資料夾。要求檔案的副檔名必須是 ".req"(F)。

At the bottom, there are three buttons: '說明(H)', '< 上一步(B)', and '下一步(N) >', along with a '取消' (Cancel) button.

7. 檢查憑證設定並按[新增]。

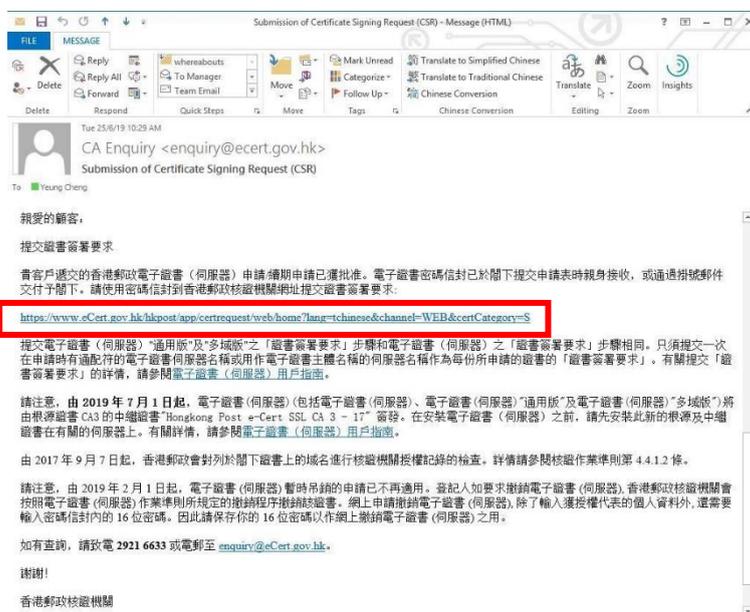


8. 按[完成]來設定。



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 screenshot shows the web form titled "提交「簽發電子證書要求」 - 電子證書（伺服器）". The form contains the following fields and instructions:

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。除非所用途為法律容許又或屬法例規定，否則我們不會用足以辨識你身份的方式，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，你有權獲得及更改個人資料，包括獲得一份此表格上填報資料的副本。如需查閱或更改資料，請致電九龍郵政局信箱60777號，電郵往 enquiry@eCert.gov.hk 或傳真往 2775 9130。

伺服器資料：
伺服器名稱：

請填寫以下有關電子證書密碼信封的資料：
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)

提交 清除

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。）

提交「簽發電子證書要求」- 電子證書（伺服器）

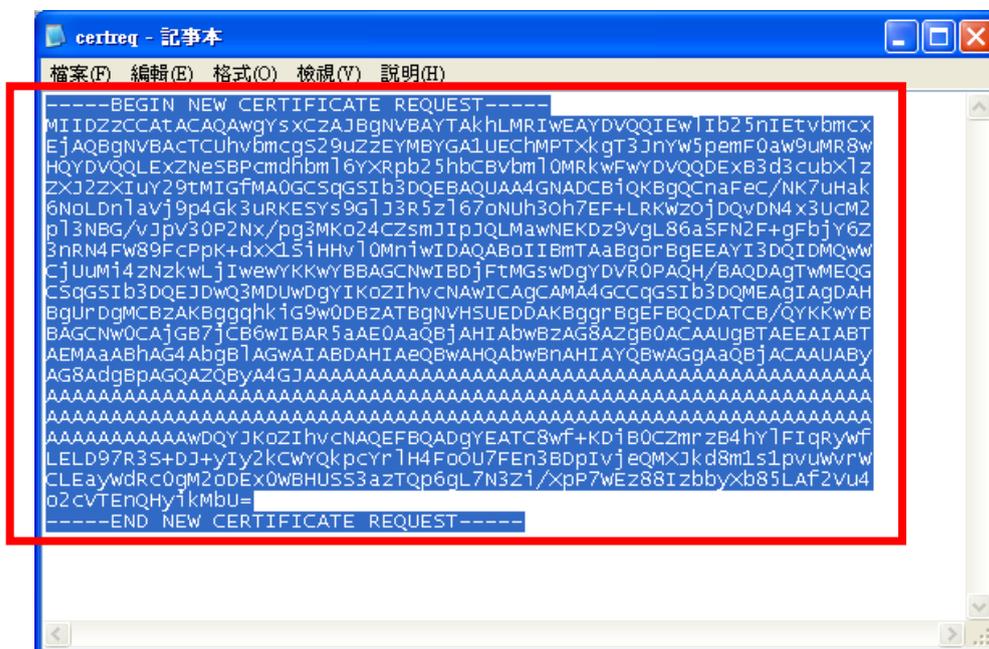
登記人資料	
伺服器名稱：	www.my-organisation.com
額外伺服器名稱：	www.我的組織.com
附加伺服器數量：	1
機構名稱：	My Organisation 我的組織
部門名稱 / 分行名稱：	
商業登記證：	1234567812312121
公司註冊證 / 公司登記證：	12345678
其他註冊證明文件：	
有關所申請的電子證書的資料	
證書類型：	電子證書（伺服器）“多域版”
證書簽章雜湊演算法：	SHA-256
有效期：	2年

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。

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]鍵繼續。

- 用文字編輯器(例如：記事本)開啟早前產生的證書簽署要求(CSR)及複製全部內容包括“-----BEGIN NEW CERTIFICATE REQUEST-----”及“-----END NEW CERTIFICATE REQUEST-----”。(您可參考B 部的步驟 6 的憑證要求檔案的位置。)



- 在方格內貼上內容，然後按[提交]。

6. 按 [接受] 確認接受此證書。

The screenshot shows the Hongkong Post e-Cert website interface. The header includes the logo and the slogan 'The solution for e-Security'. The main heading is '提交「簽發電子證書要求」- 電子證書（伺服器）'. Below this, it lists user information and certificate details. At the bottom, there are instructions and two buttons: '接受' (Accept) and '不接受' (Do Not Accept). A red arrow points to the '接受' button.

提交「簽發電子證書要求」- 電子證書（伺服器）

以下為你的電子證書內的資料：

用戶資料	
伺服器名稱：	www.我的伺服器.com
機構名稱：	My Organization
分行/部門名稱：	My Organization Unit
商業登記證：	1234567890123457
公司註冊證 / 公司登記證：	
其他註冊證明文件：	
其他資料（由香港郵政核證機關系統產生）	
登記人參考編號：	0001397035
證書類型：	Hongkong Post Trial e-Cert (Server)
簽發機關：	Hongkong Post Trial e-Cert SSL CA 3 - 17
證書序號：	21 d3 47 fb 40 69 89 01 b8 89 67 1d 62 29 30 e7 d9 34 16 28
證書簽章雜湊演算法：	SHA-256
證書有效日期：	14/08/2019 - 14/08/2020

如使用中文域名註冊，請務必確認清楚字元正確性，註冊後即不能變更或修改。

請按 [接受] 確認接受上述證書，並同意香港郵政根據電子交易條例的規定將該證書於儲存庫公布。

(注意：香港郵政收集你的個人資料，只會用於處理你的電子證書申請事宜。你有權根據個人資料（私隱）條例的規定，要求查詢及更正你的個人資料。)

2007 © | 重要告示 | 私隱政策

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



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. 就所有類型的電子證書（伺服器）而言：

安裝由根源證書Root CA3 簽發的中繼證書"Hongkong Post e-Cert SSL CA 3-17"。可於以下網址下載：

http://www1.ecert.gov.hk/root/ecert_ssl_ca_3-17_pem.crt

安裝交叉證書"Hongkong Post Root CA 3（交叉證書2022）"。可於以下網址下載：

http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt

3. 就所有類型的延伸認證電子證書（伺服器）而言：

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"。可於以下網址下載：

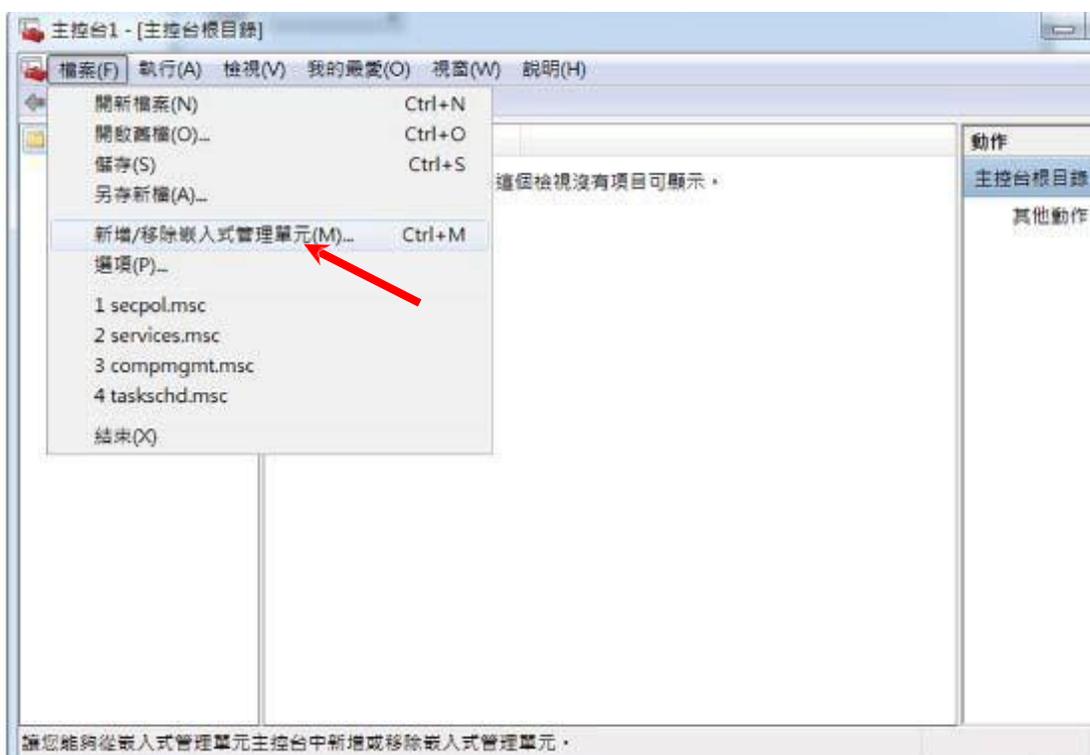
http://www1.ecert.gov.hk/root/ecert_ev_ssl_ca_3-17_pem.crt

安裝交叉證書"Hongkong Post Root CA 3（交叉證書2022）"。可於以下網址下載：

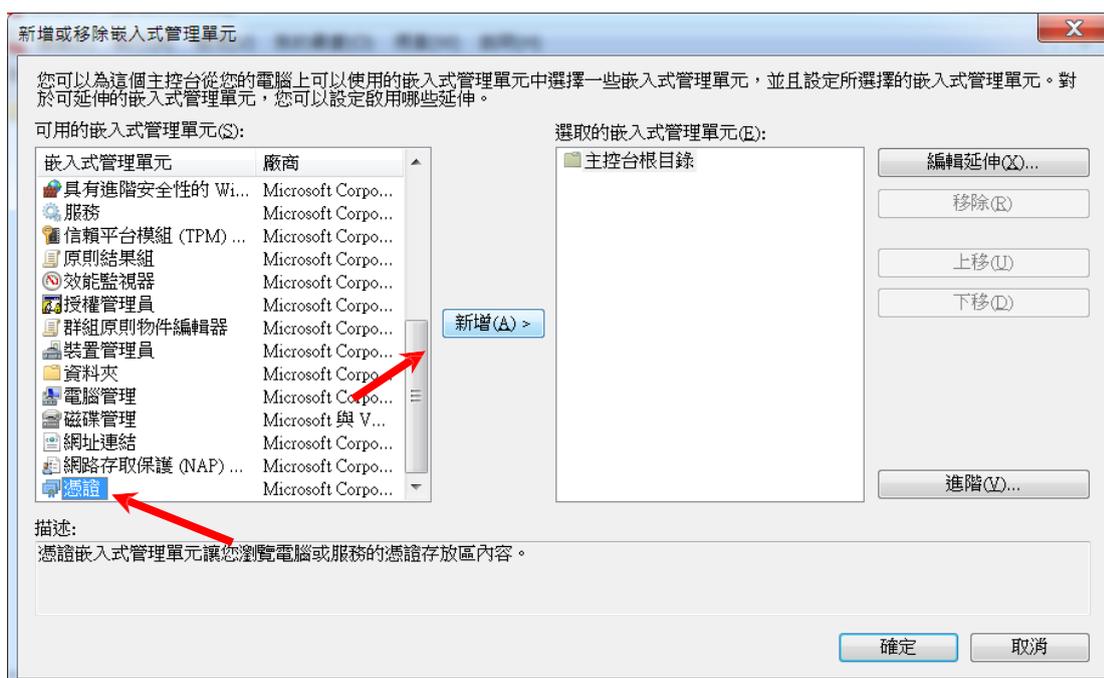
http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt

D. 安裝中繼 / 交叉證書

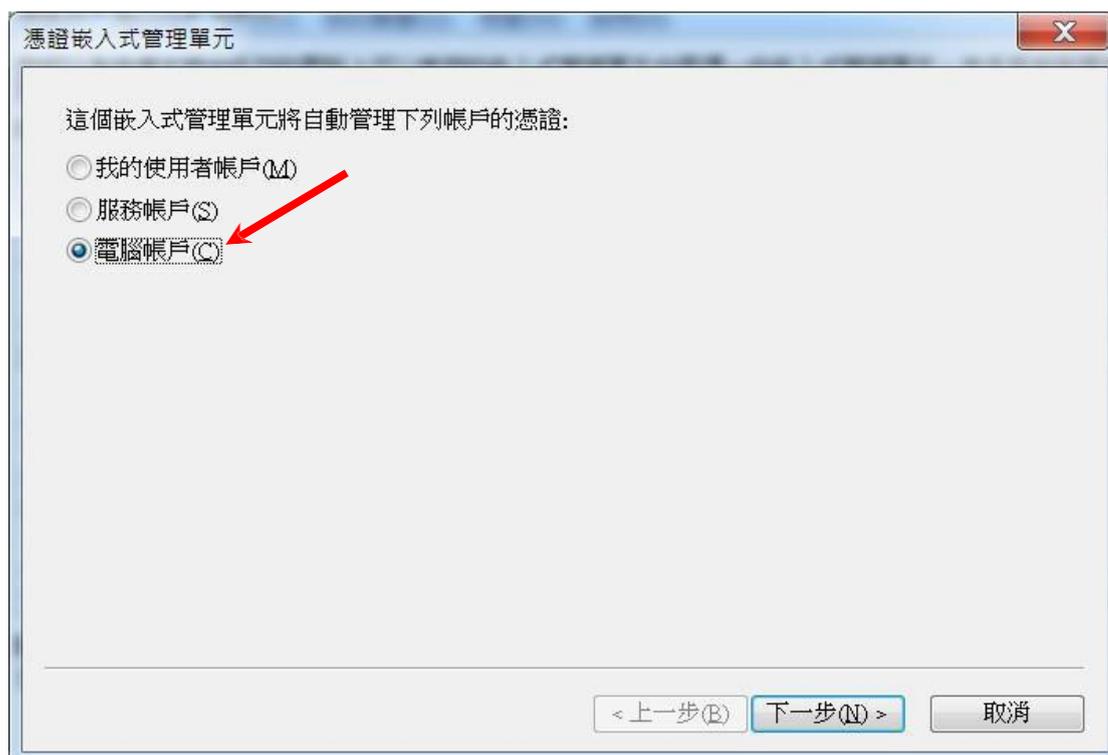
1. 按[開始]>[執行]，然後輸入“mmc”及按[確定]來啟動 Microsoft Management Console (MMC)，然後從[檔案]選單中選取[新增/移除嵌入式管理單元]。



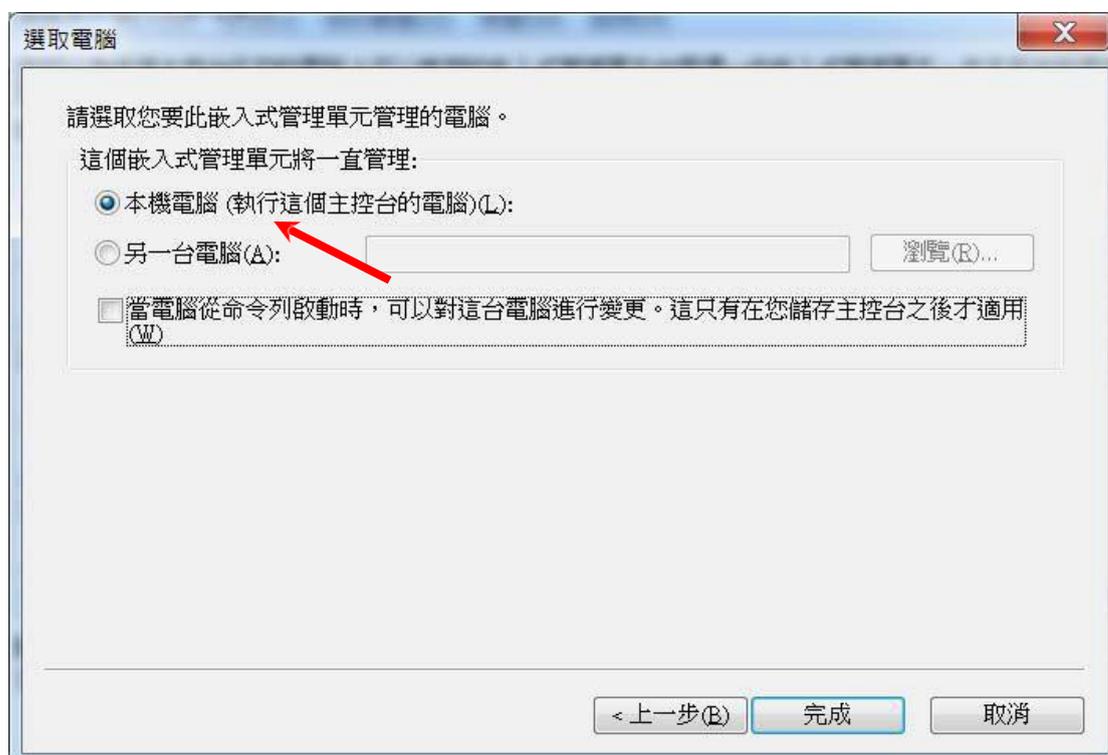
2. 選擇[憑證]，然後按[新增]。



3. 選擇[電腦帳戶]，然後按[下一步]。

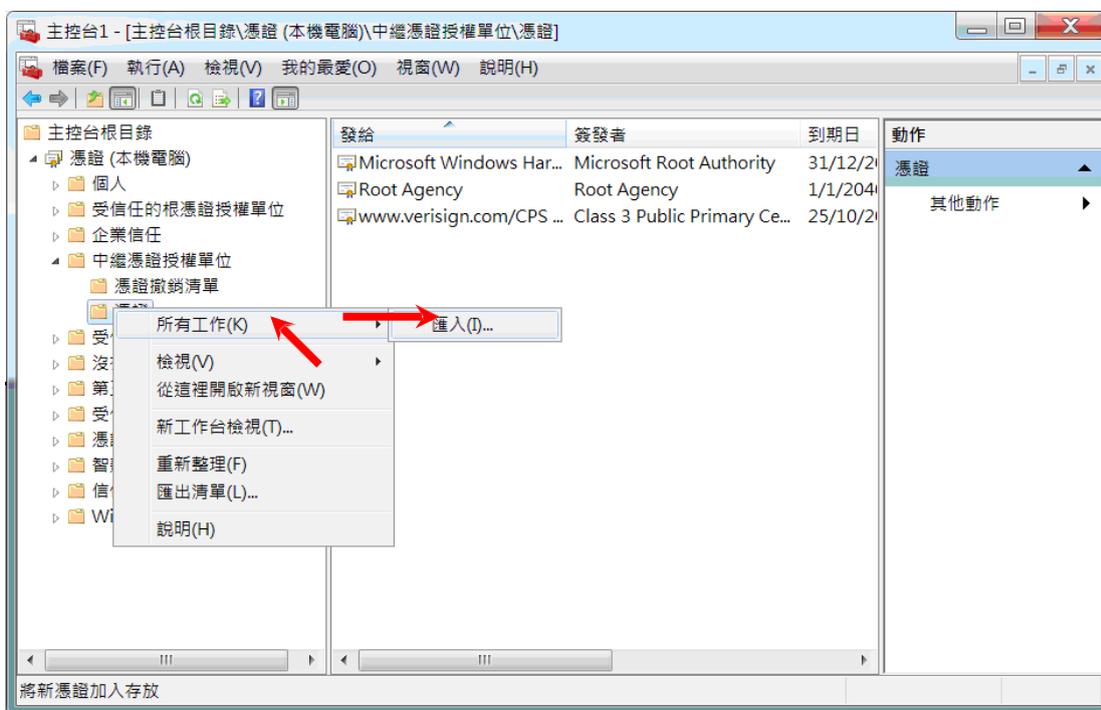


4. 選擇[本機電腦]，然後按[完成]。



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

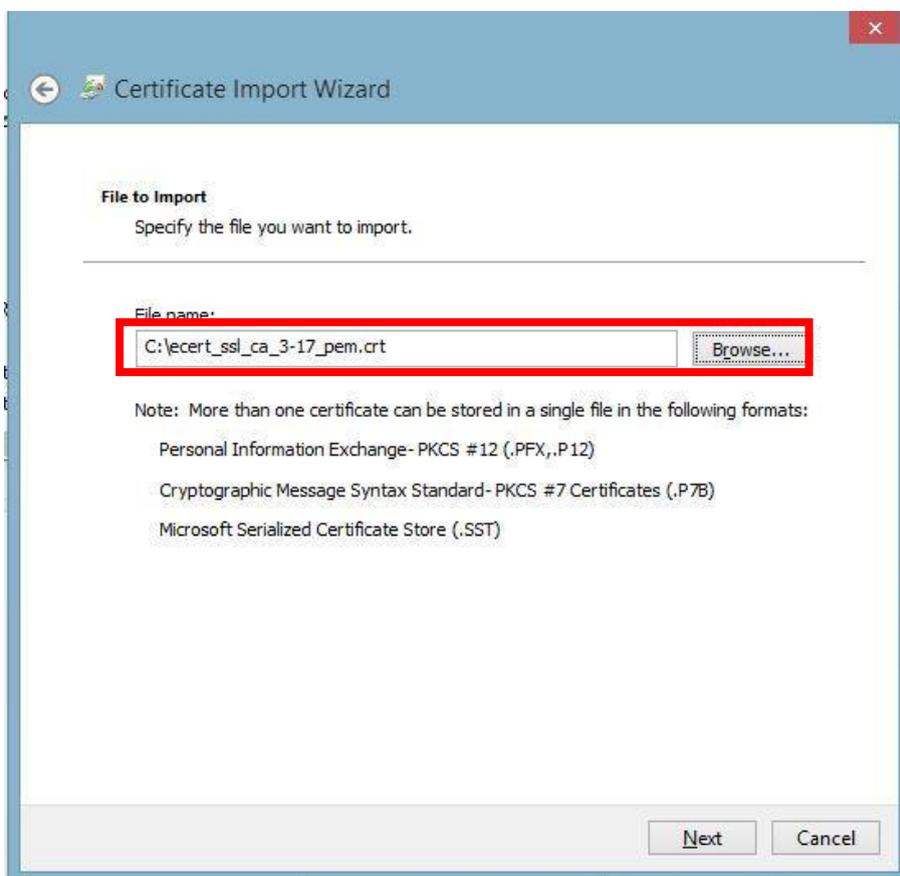
5. 展開[中繼憑證授權單位]及以滑鼠右鍵按一下[憑證]，然後選擇[所有工作]>[匯入]。



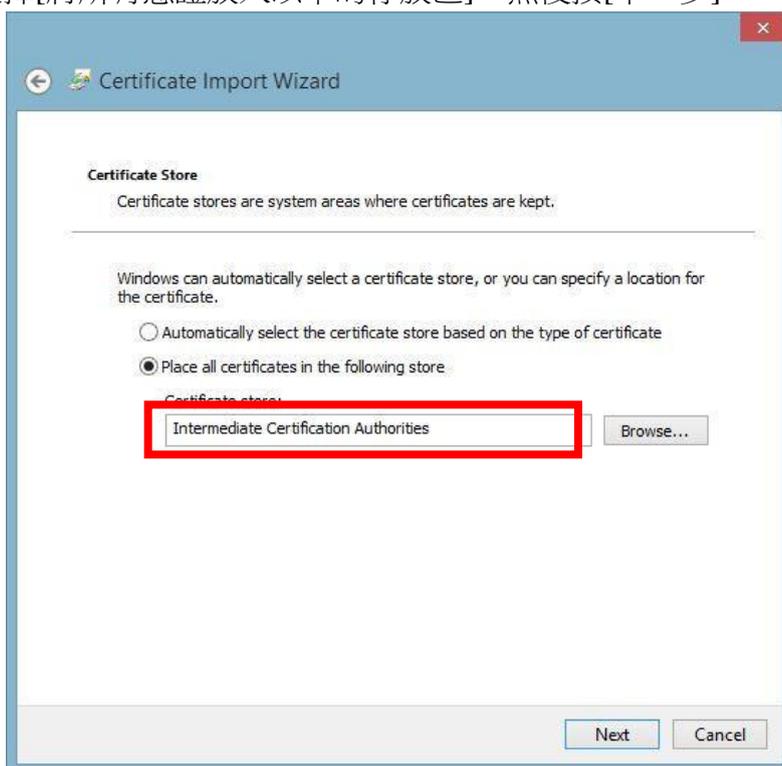
6. 在[憑證匯入精靈]內，按[下一步]繼續。



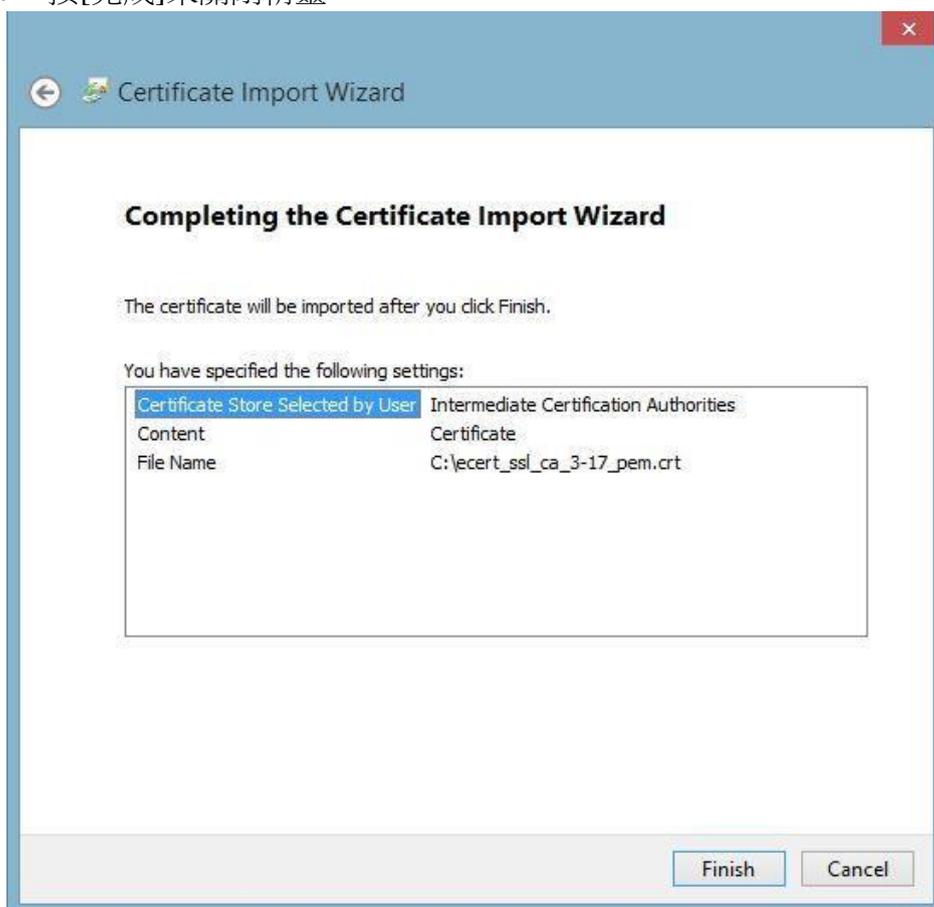
7. 按[瀏覽]指定早前於 C 部的步驟 7 下載的 **Hongkong Post e-Cert SSL CA 3 - 17** 中繼證書 (ecert_ssl_ca_3-17_pem.crt)，然後按[下一步]。



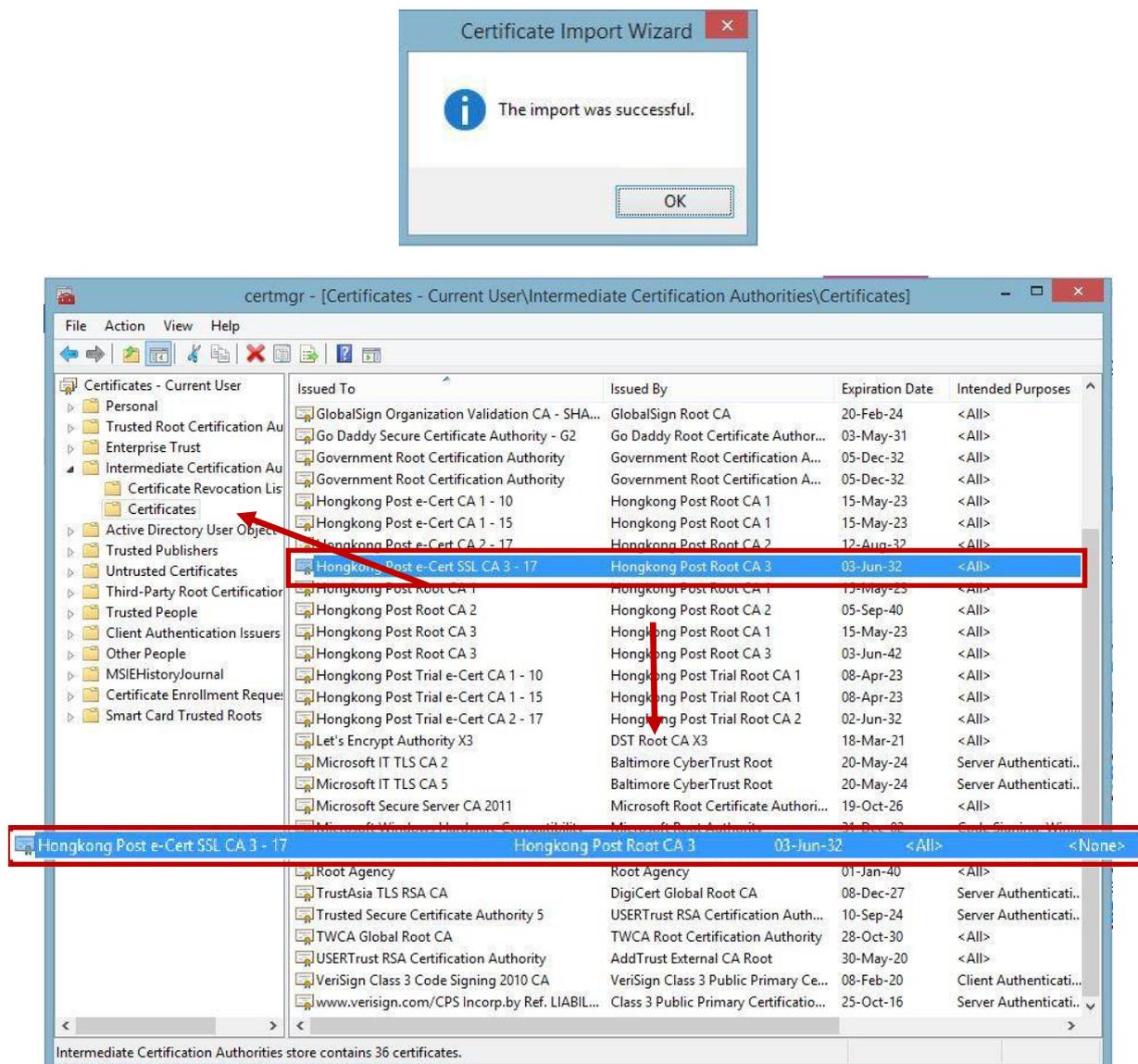
8. 選擇[將所有憑證放入以下的存放區]，然後按[下一步]。



9. 按[完成]來關閉精靈。



10. 按[確定]來完成。

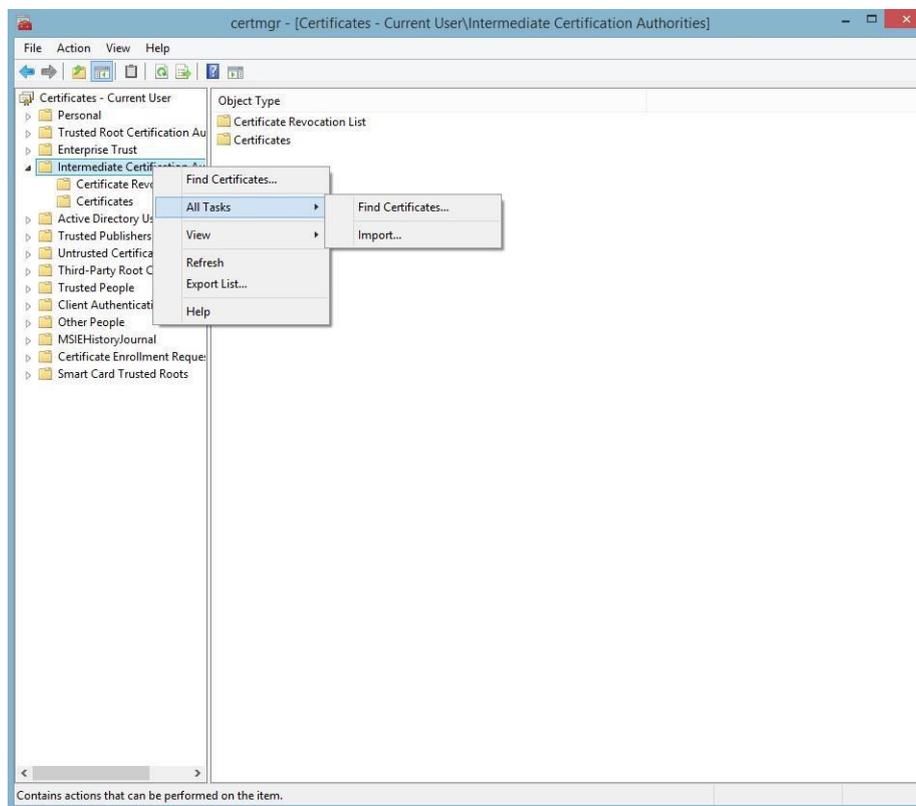


圖表 1: “Hongkong Post e-Cert SSL CA 3 - 17” 中繼證書已成功安裝

11. 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)。

安裝授權撤銷清單(ARL)

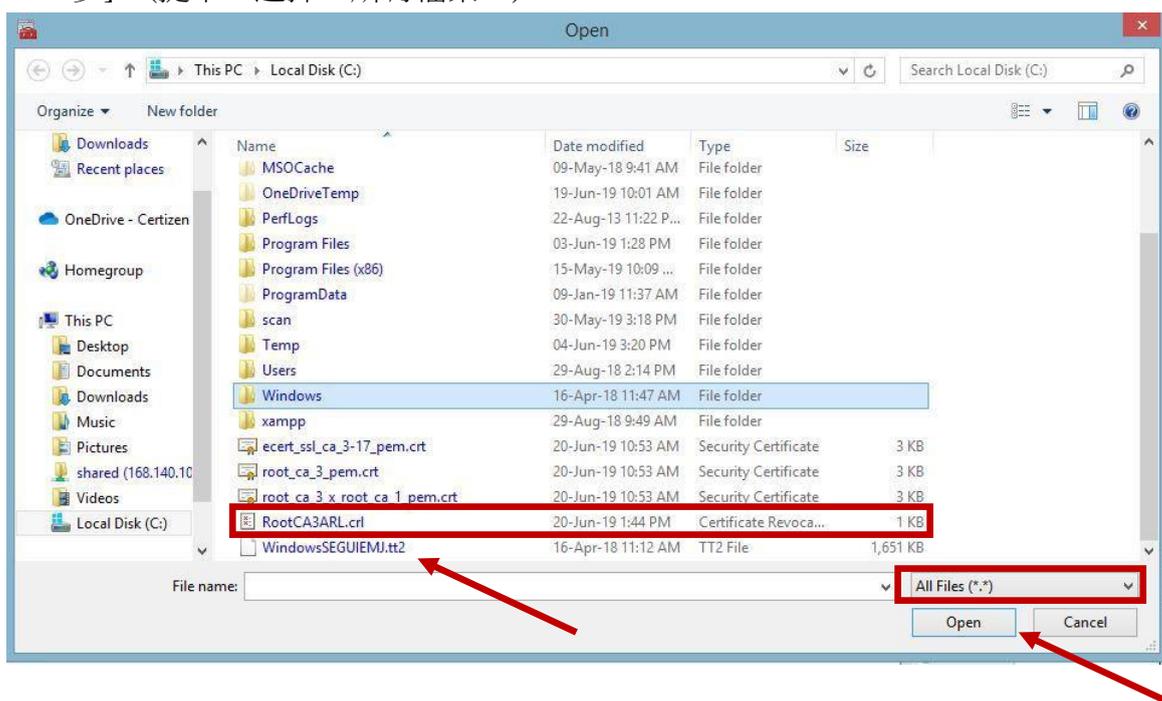
12. 下載授權撤銷清單(ARL)：<http://crl1.eCert.gov.hk/crl/RootCA3ARL.crl>
13. 展開[中繼憑證授權]及以滑鼠右鍵按一下，然後選擇[所有工作]>[匯入]。



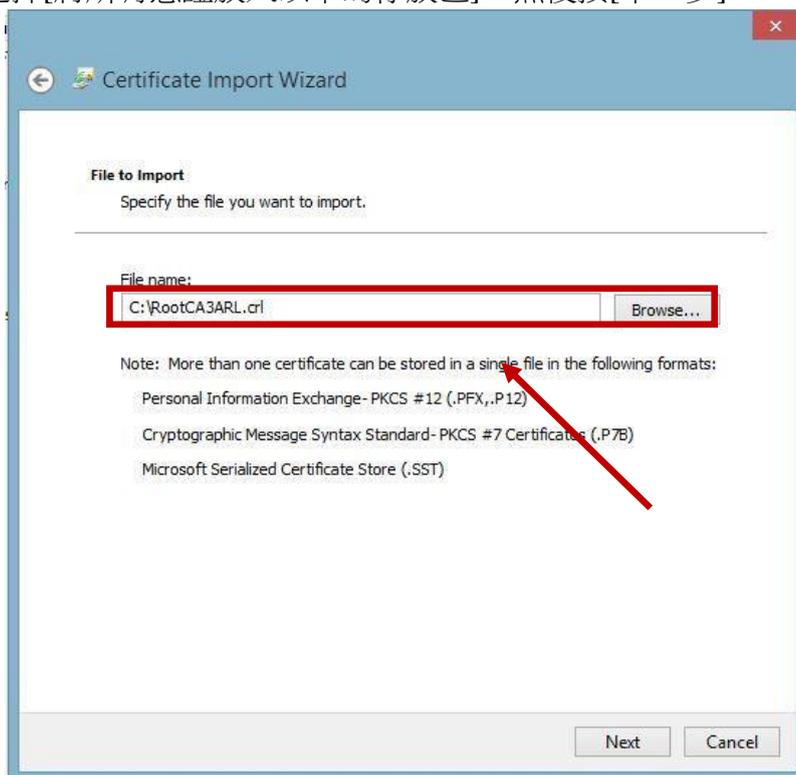
14. 在[憑證匯入精靈]內，按[下一步]繼續。



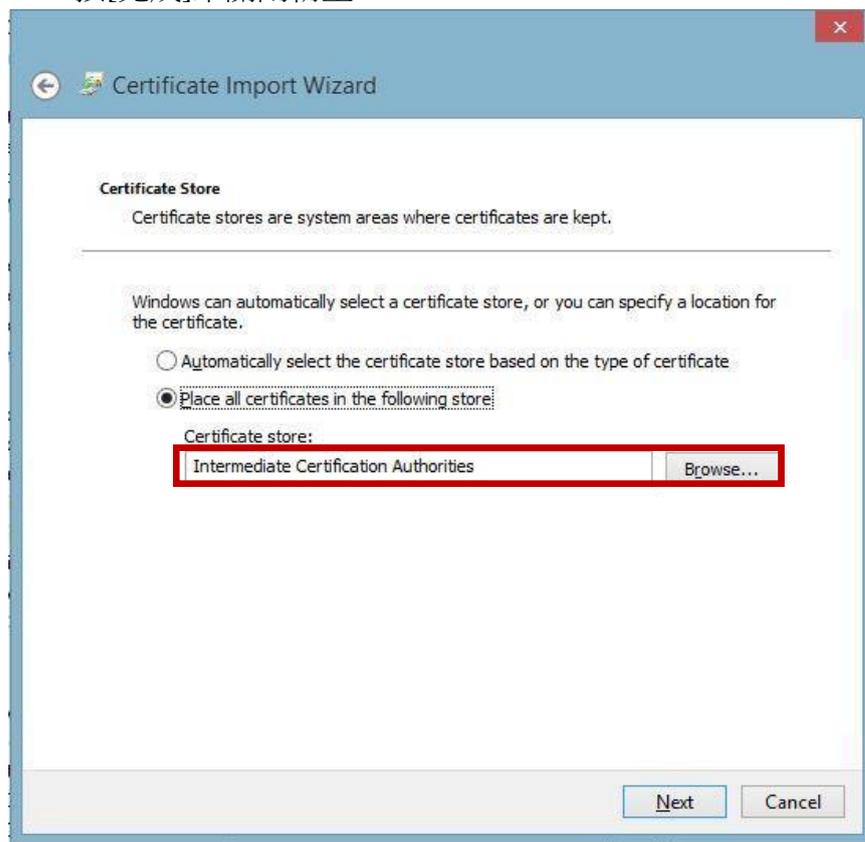
15. 按[瀏覽]選擇早前於步驟 11 下載的“Hongkong Post Authority Revocation List (ARL)”授權撤銷清單 (RootCA3ARL.crl)，然後按[下一步]。(提示：選擇“所有檔案”)

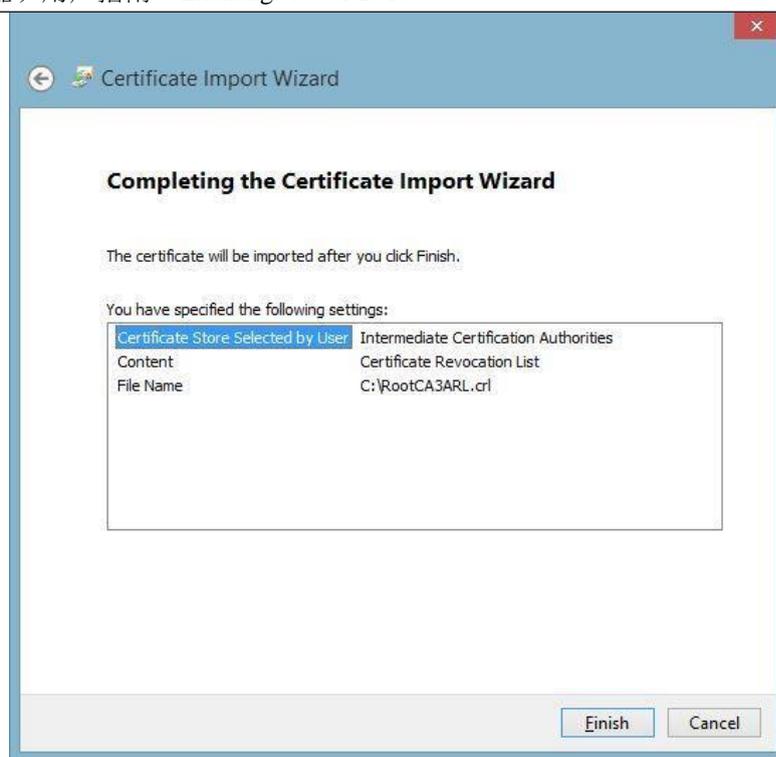


16. 選擇[將所有憑證放入以下的存放區]，然後按[下一步]。



17. 按[完成]來關閉精靈。





18. 按[確定]來完成。

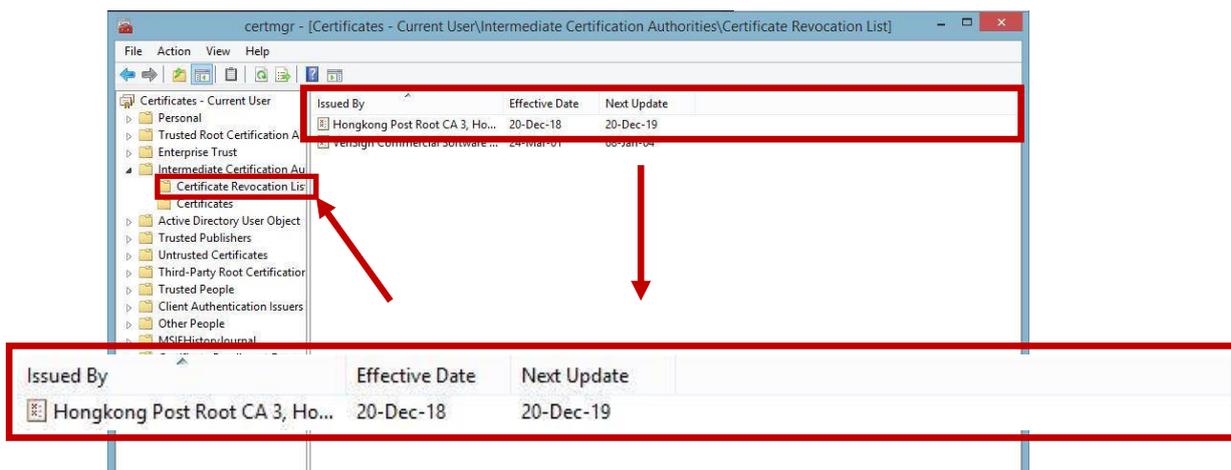
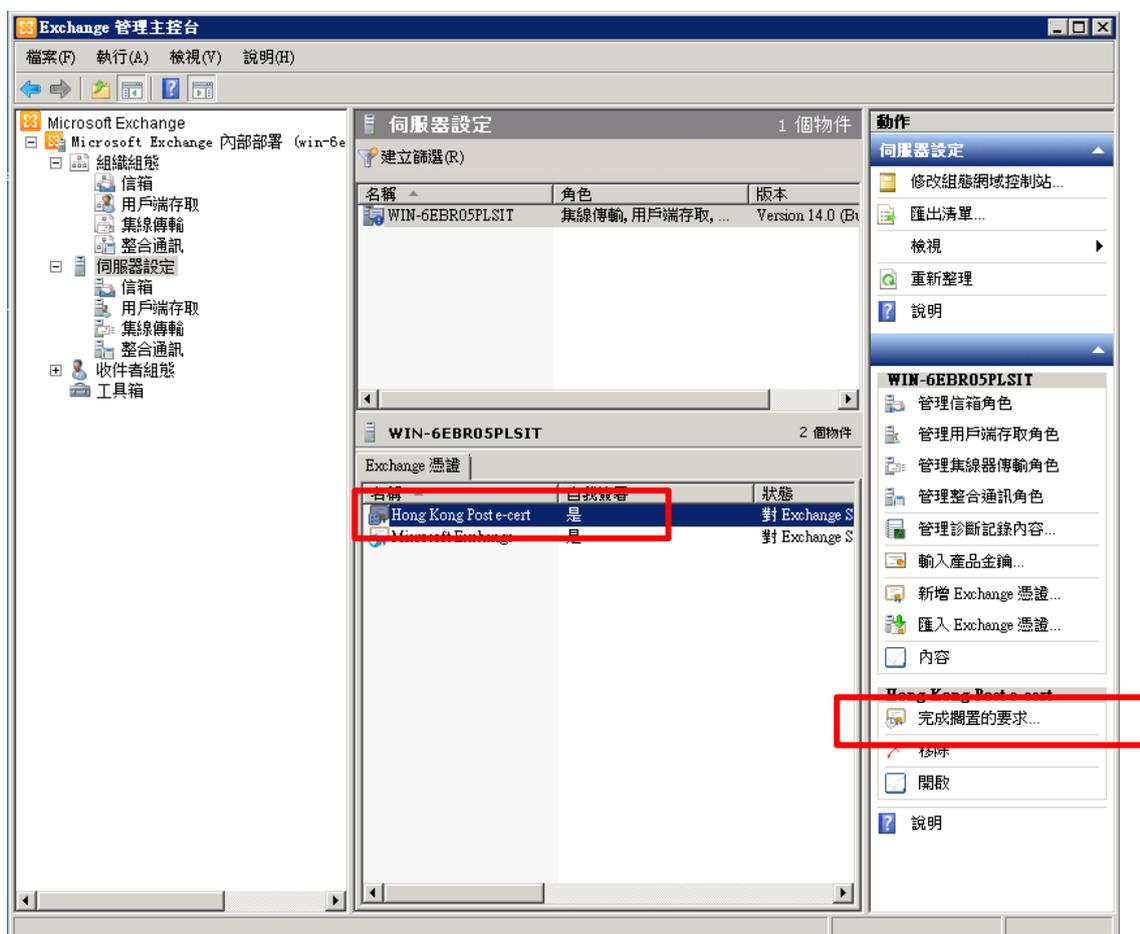


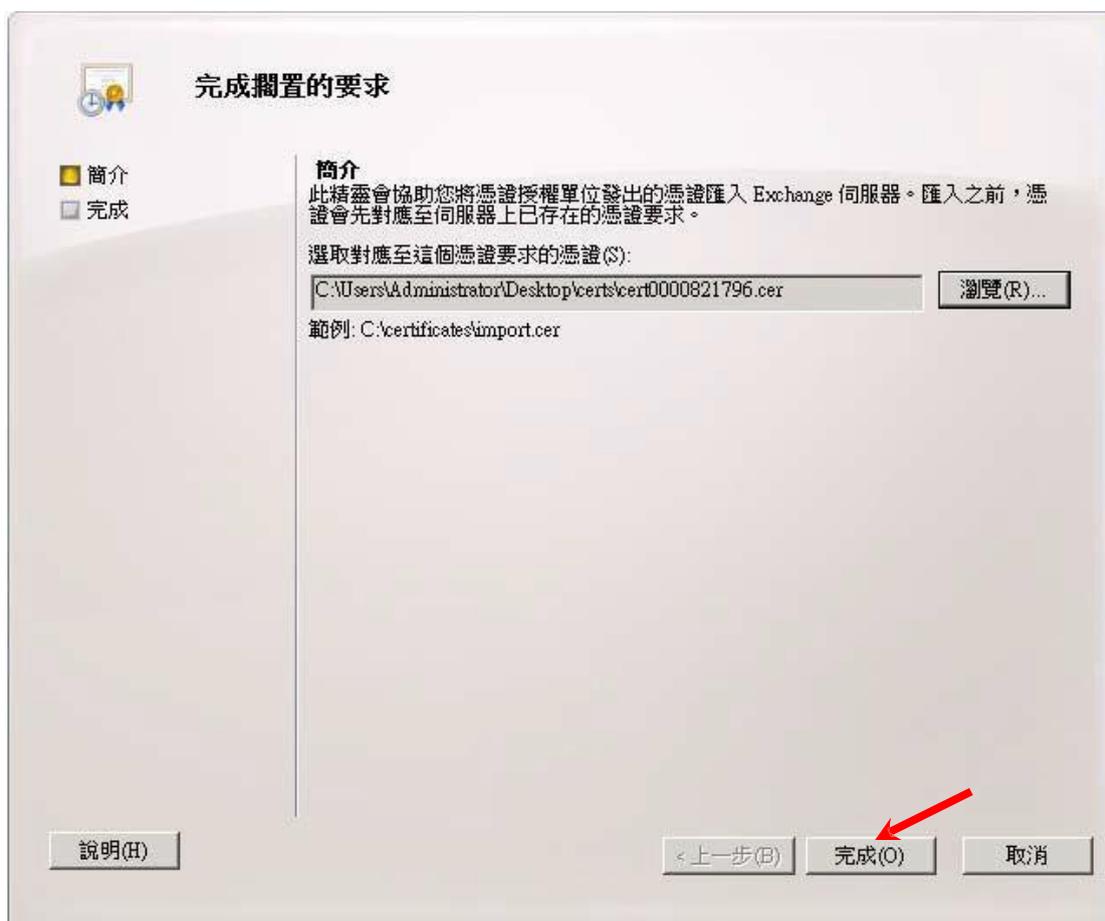
圖 3: “Hongkong Post Authority Revocation List (ARL)” 授權撤銷清單已成功安裝

E. 安裝伺服器證書

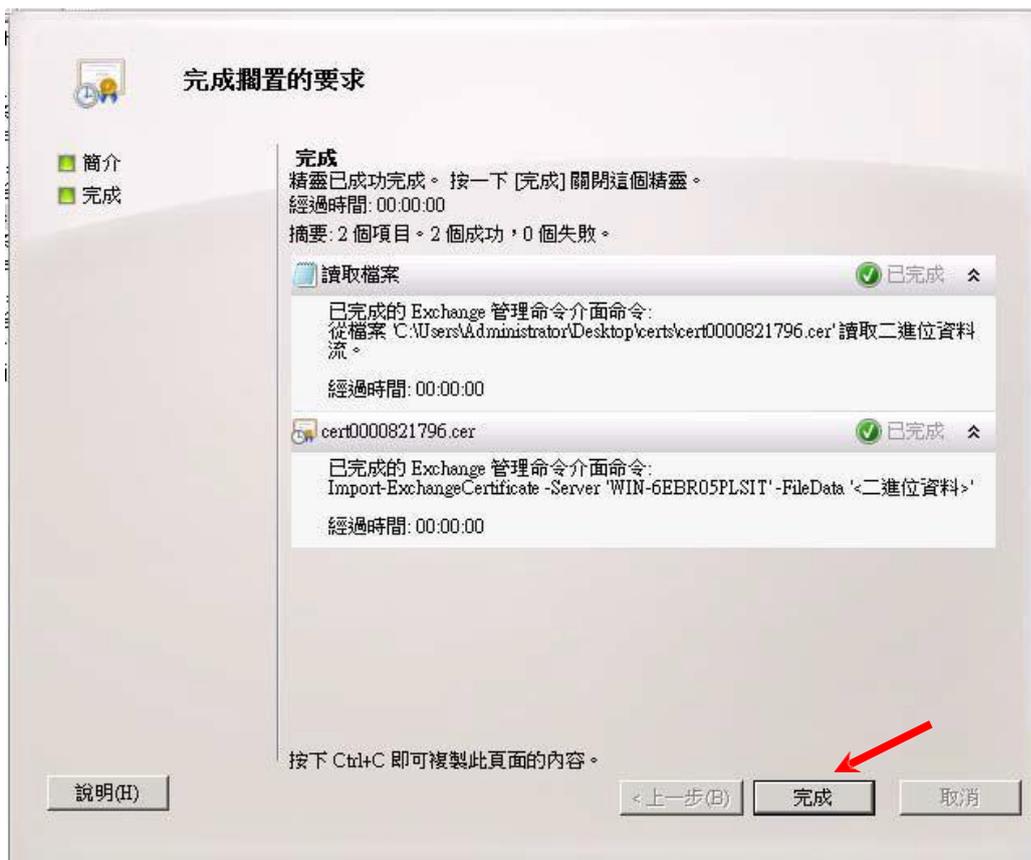
1. 在 [Exchange 管理主控台] 視窗內，選擇 [伺服器設定]，然後選擇您於步驟 B 中所申請的 Exchange 憑證。在右手邊動作一欄內，按 [完成擱置的要求]。



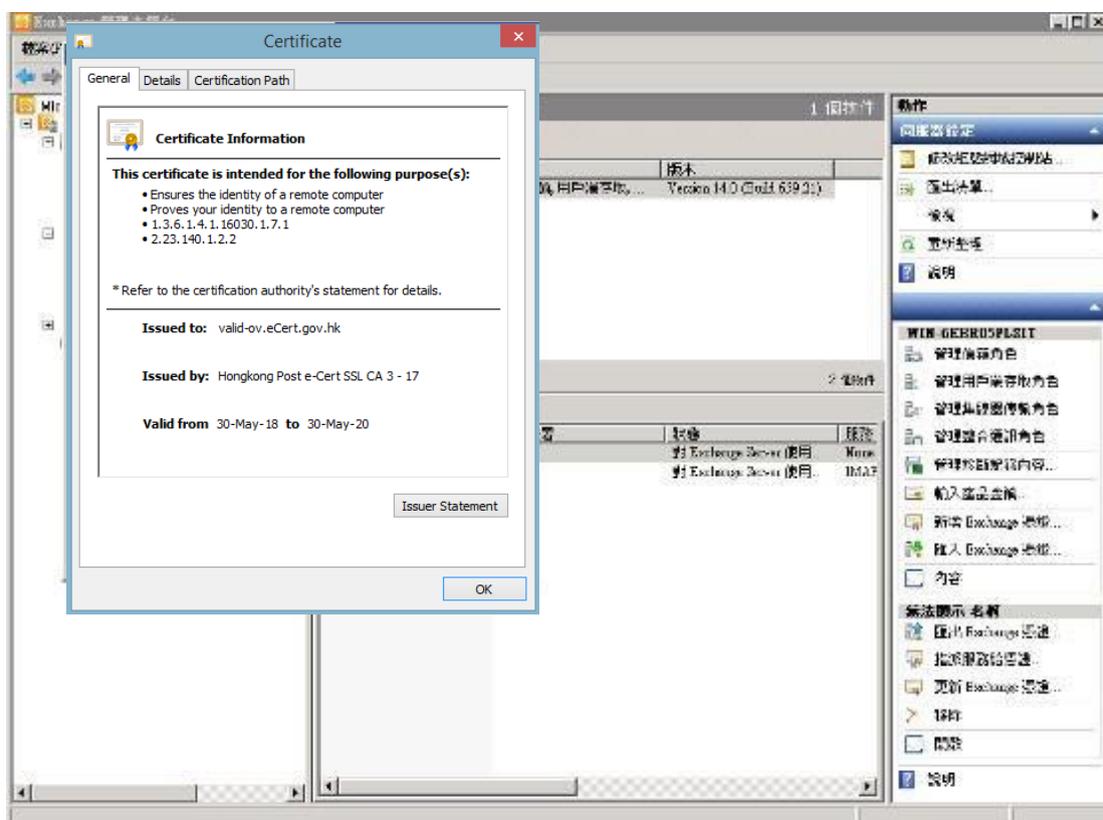
- 按[瀏覽] 選擇早前於 C 部的步驟 7 下載的“Hongkong Post e-Cert (Server)” 證書，然後按[完成]。



3. 按[完成]來結束憑證安裝。

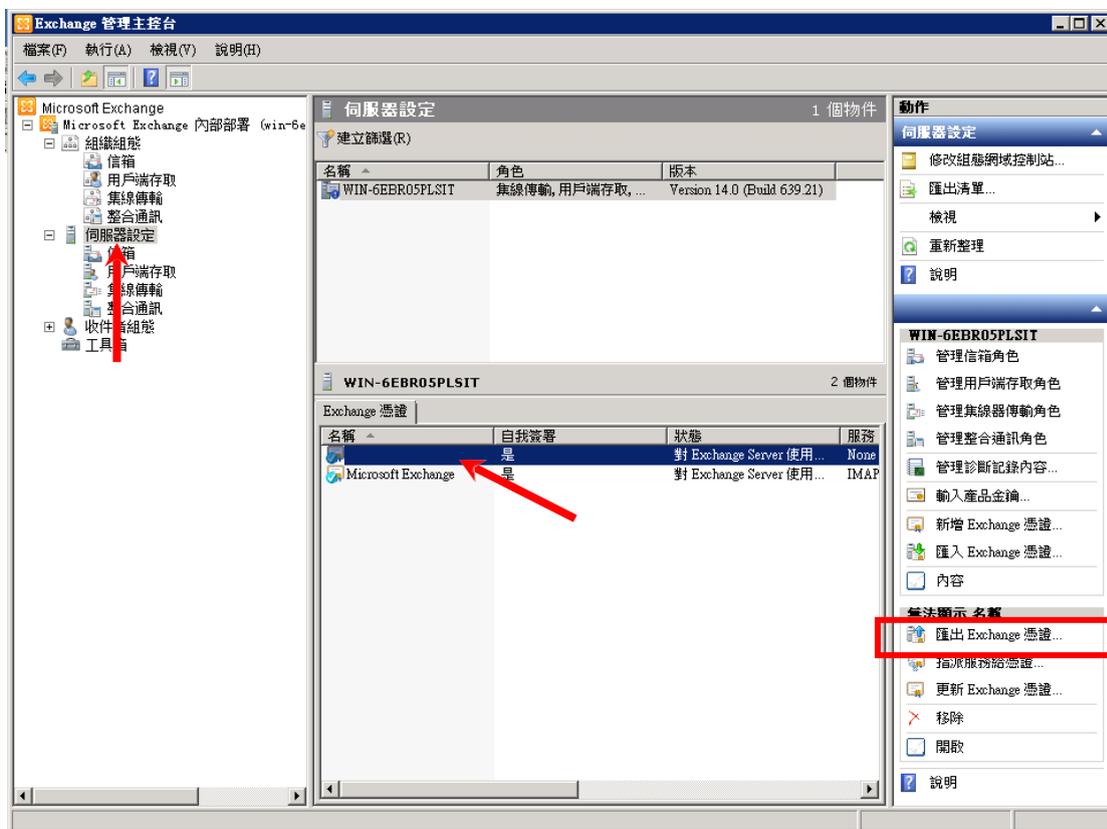


4. Hongkong Post 伺服器證書已經成功安裝，你可以雙擊證書以察看證書資訊。

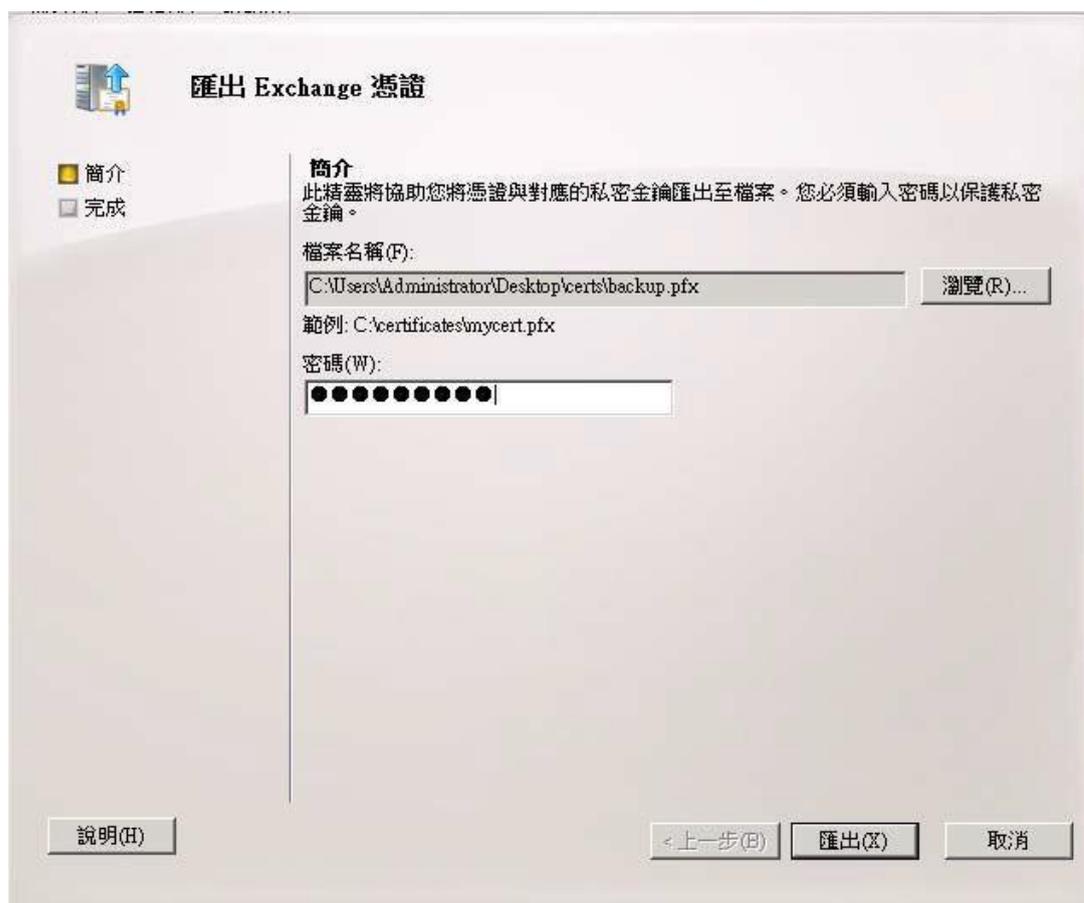


F. 備份密碼匙

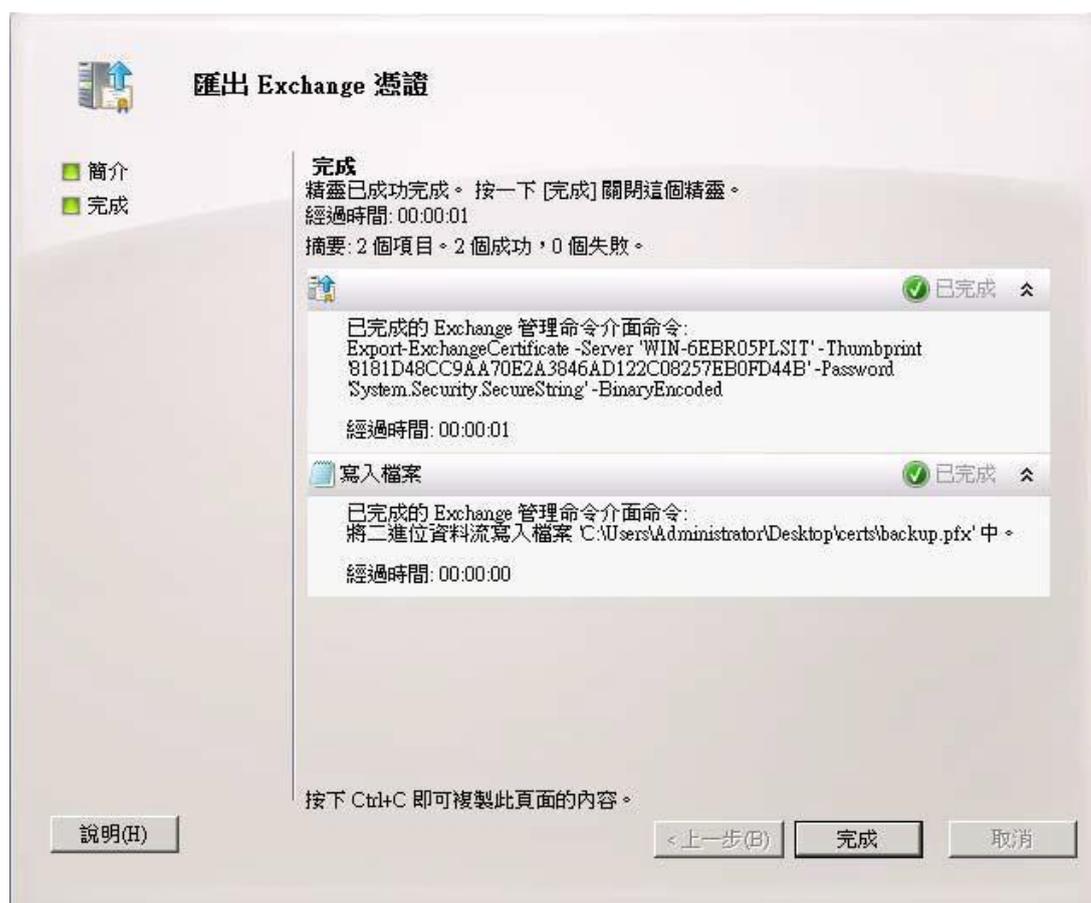
1. 在“Exchange 管理主控台”界面，按“伺服器設定”，選擇您想要備份的密碼匙。於右手邊選項，選擇“匯出 Exchange 憑證”。



2. 選擇存放名稱及路徑並輸入密碼（默認匯出文檔格式為.PFX）。按[匯出]。

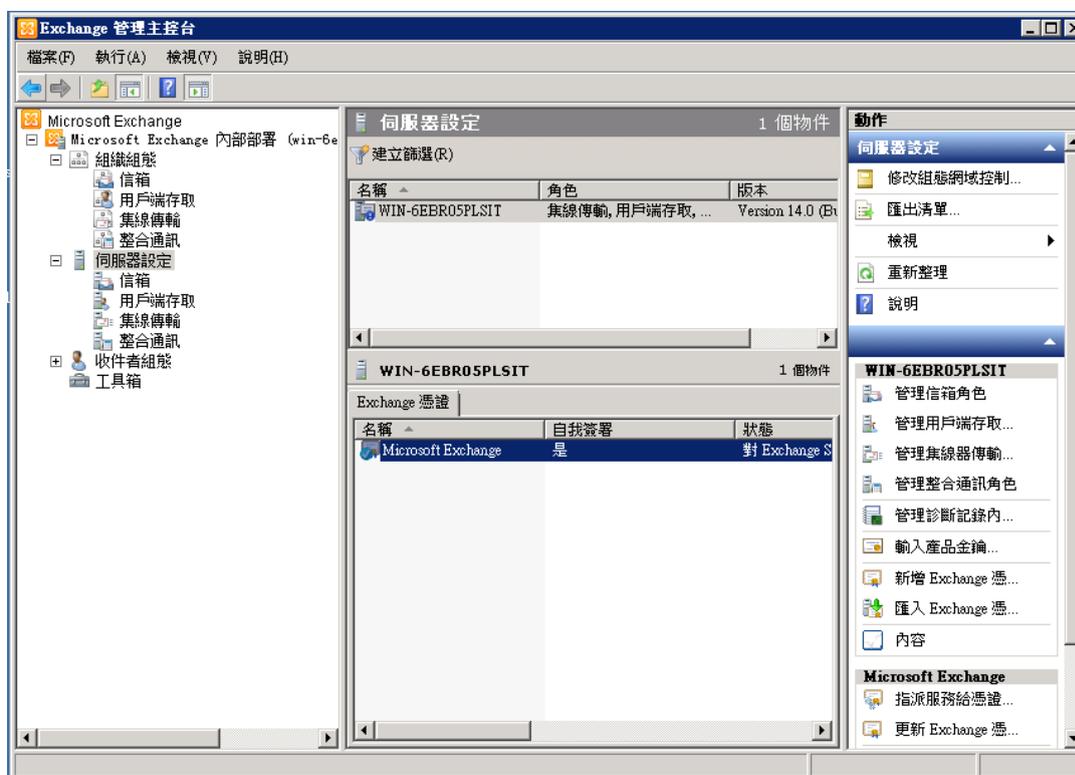


- 按[完成]來結束匯出憑證，Hongkong Post e-cert 伺服器憑證已經成功匯出。

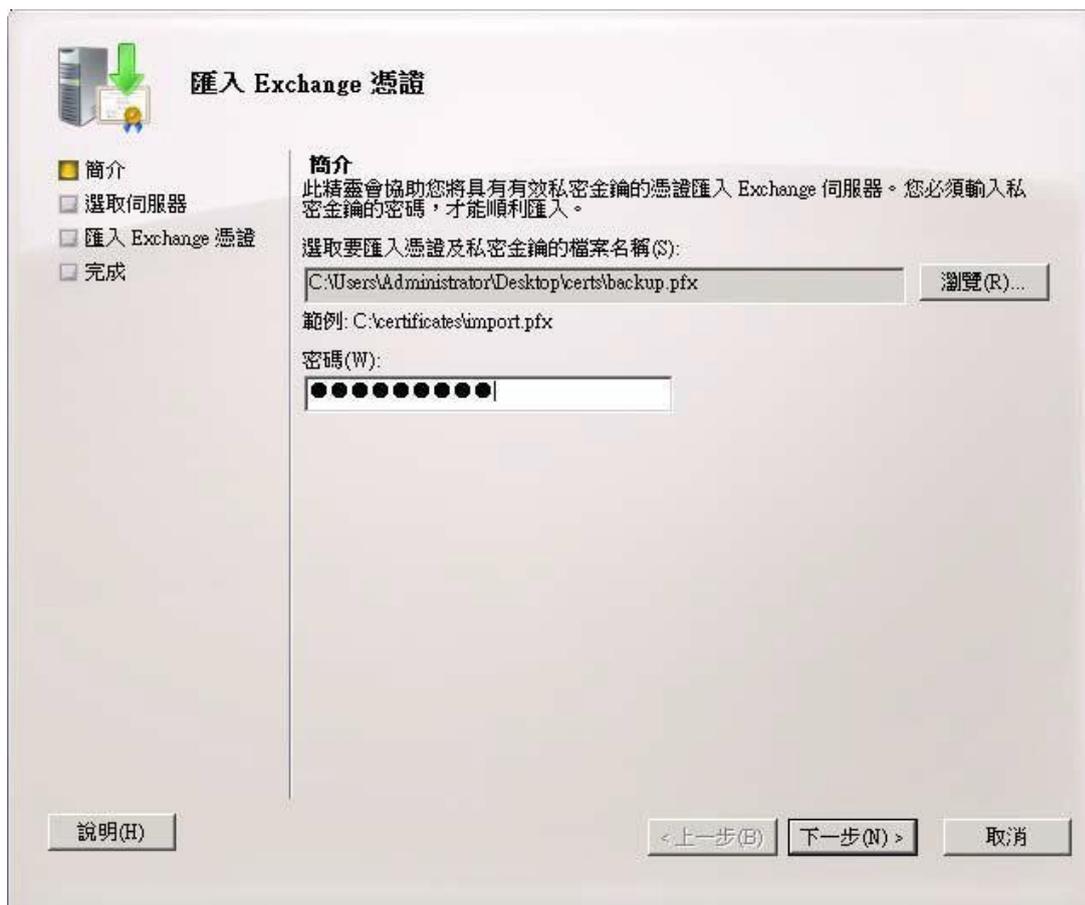


G. 還原密碼匙

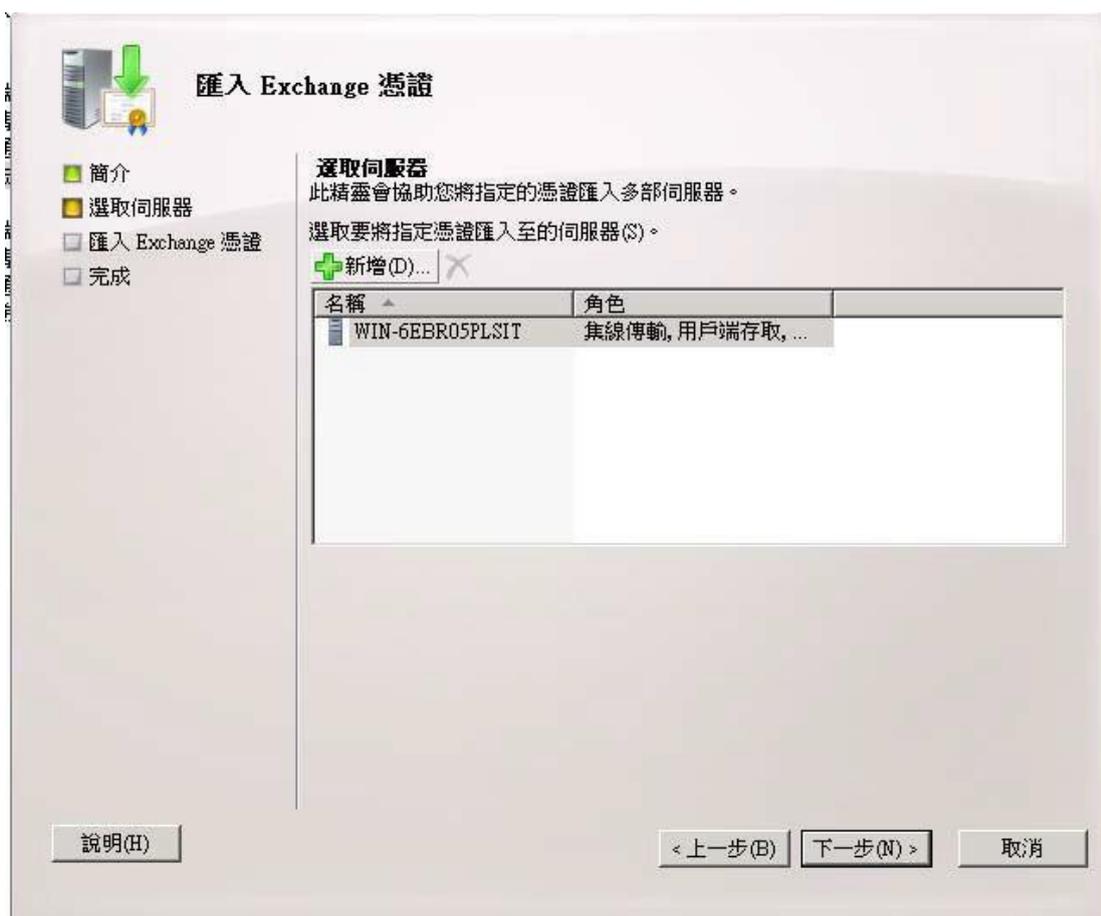
1. 在“Exchange 管理主控台”界面，按“伺服器設定”，於右手邊選項，選擇“匯入 Exchange 憑證”。



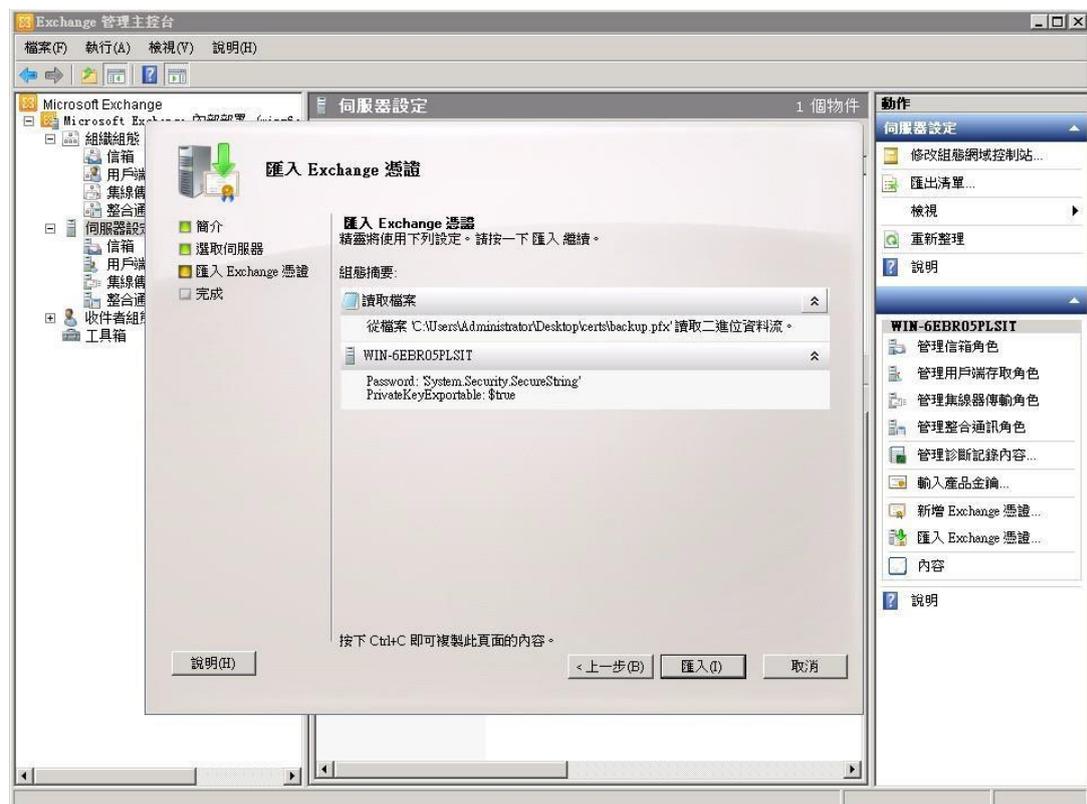
2. 在“匯入 Exchange 憑證”界面中，選擇包含輸入包含憑證的檔案名稱及路徑及憑證的密碼，然後按[下一步]來繼續。



3. 選擇相應的伺服器，並按[下一步]來繼續。



4. 檢查憑證相關資訊，並按[匯入]。



- 按[完成]來結束匯入憑證，電子證書（伺服器）證書已成功匯入。

