



電子證書（伺服器）用戶指南

Microsoft Exchange Server 2010 適用

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	18
	移除舊有中繼證書（如適用）	20
	安裝中繼 / 交叉證書	21
	安裝授權撤銷清單(ARL)	25
E.	安裝伺服器證書	29
F.	備份密碼匙	33
G.	還原密碼匙	36

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	33
G. 還原密碼匙	36

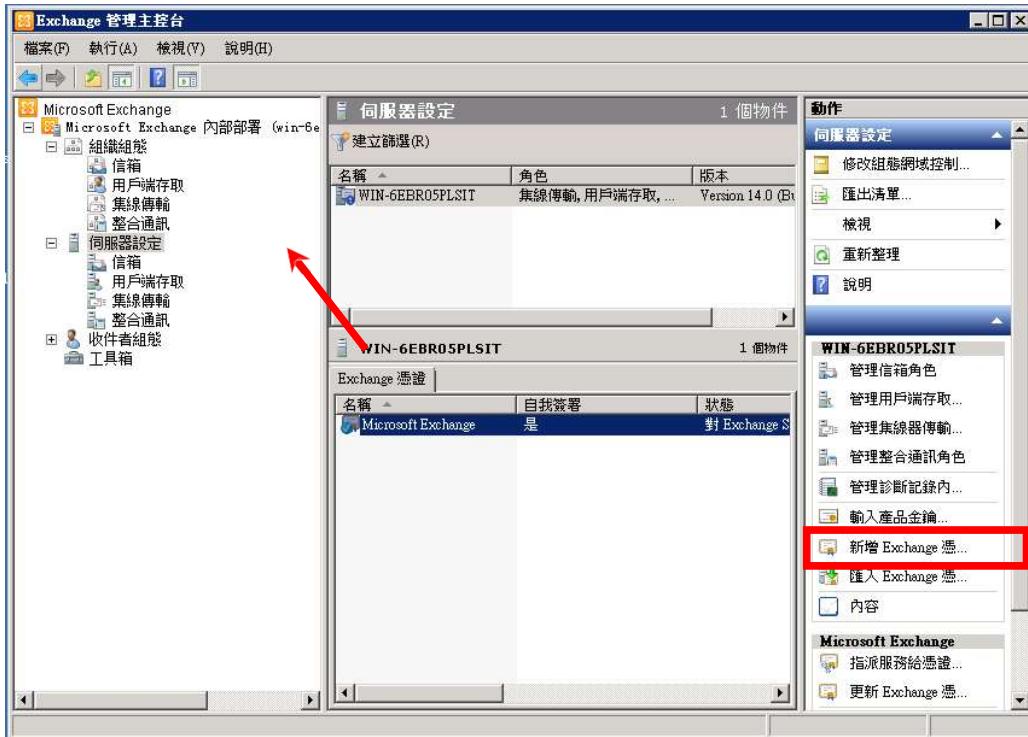
新申請及續期申請

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：

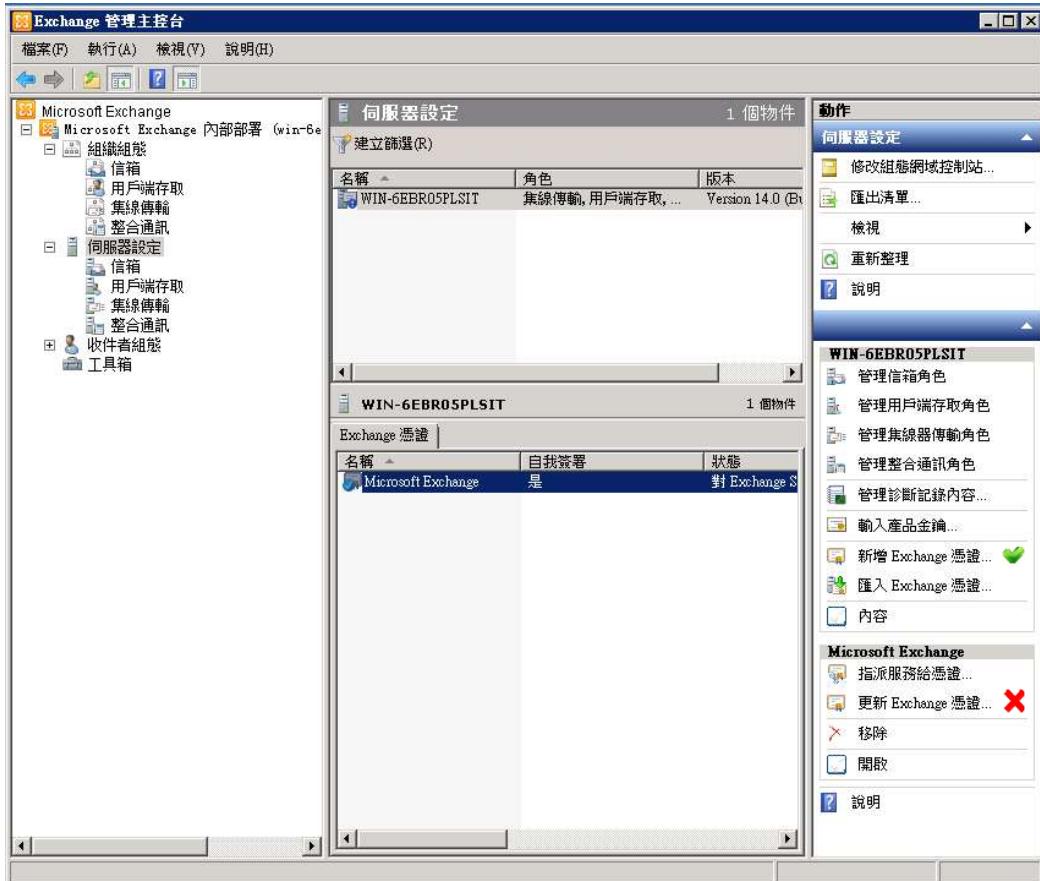
B.	產生證書簽署要求(CSR).....	4
C.	提交證書簽署要求(CSR).....	12
D.	安裝中繼 / 交叉證書	18
	移除舊有中繼證書（如適用）	20
	安裝中繼 / 交叉證書.....	21
	安裝授權撤銷清單(ARL)	25
E.	安裝伺服器證書	29

B. 產生證書簽署要求(CSR)

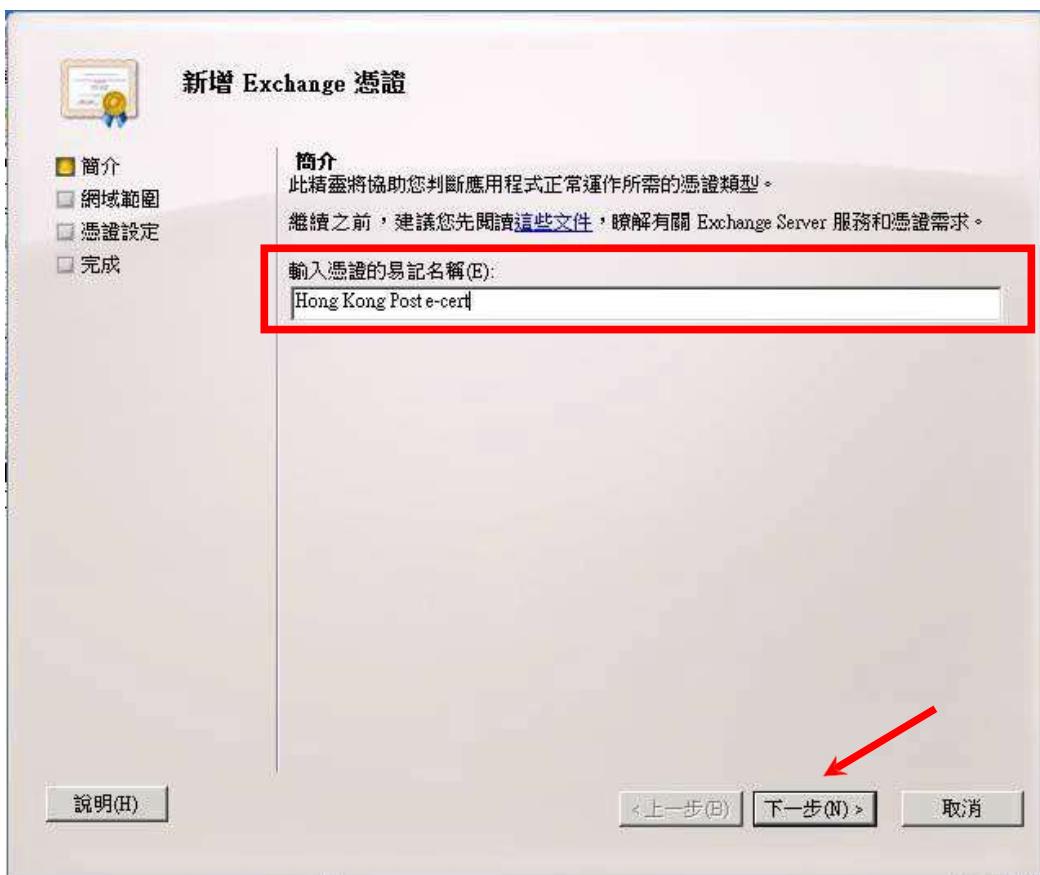
1. 按[開始]>[所有程式]>[Exchange Sever 2010]>[Exchange 管理主控台]來啟動 Exchange 管理工具。
2. 在[Exchange 管理主控台]視窗內，展開[Microsoft Exchange 內部部署]。
3. 選擇[伺服器設定]，在右手邊[動作]一欄內，按[新增 Exchange 憑證]。



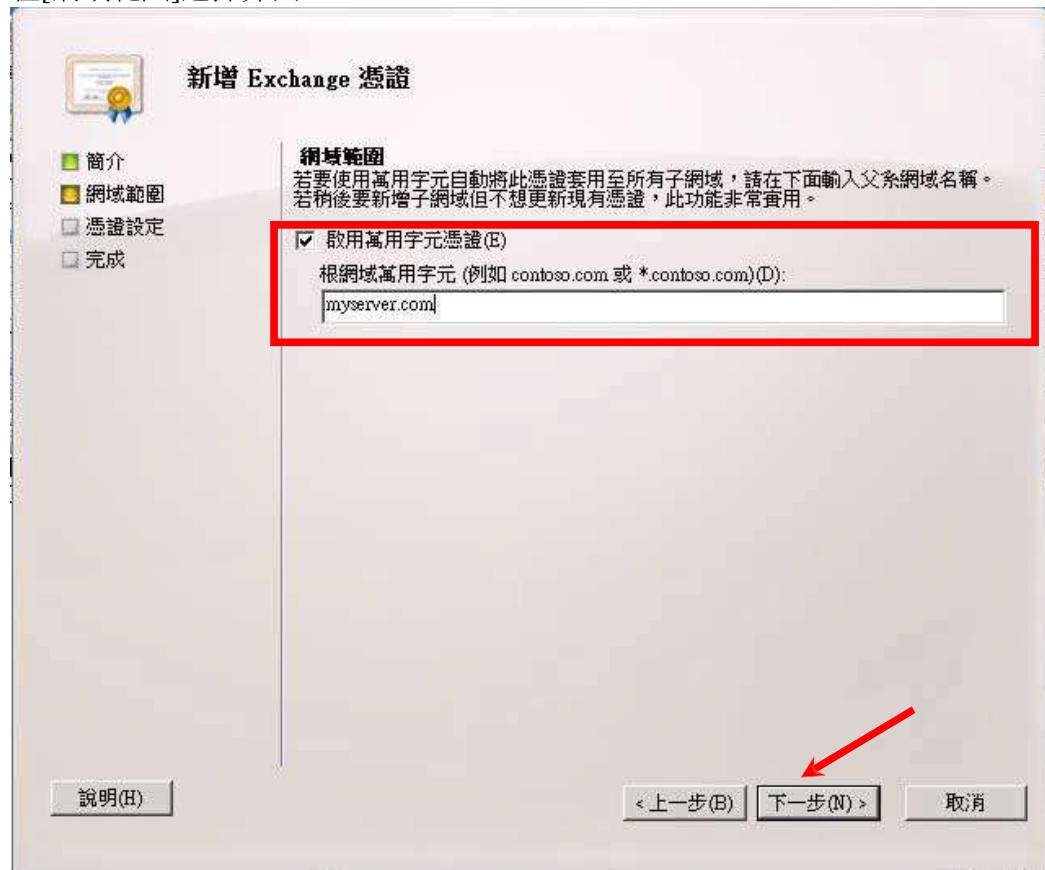
注意：新申請及續期申請電子證書（伺服器）的步驟相同，即使是續期電子證書，請不要使用[更新Exchange憑證]，要選擇[新增Exchange憑證]。



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



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。

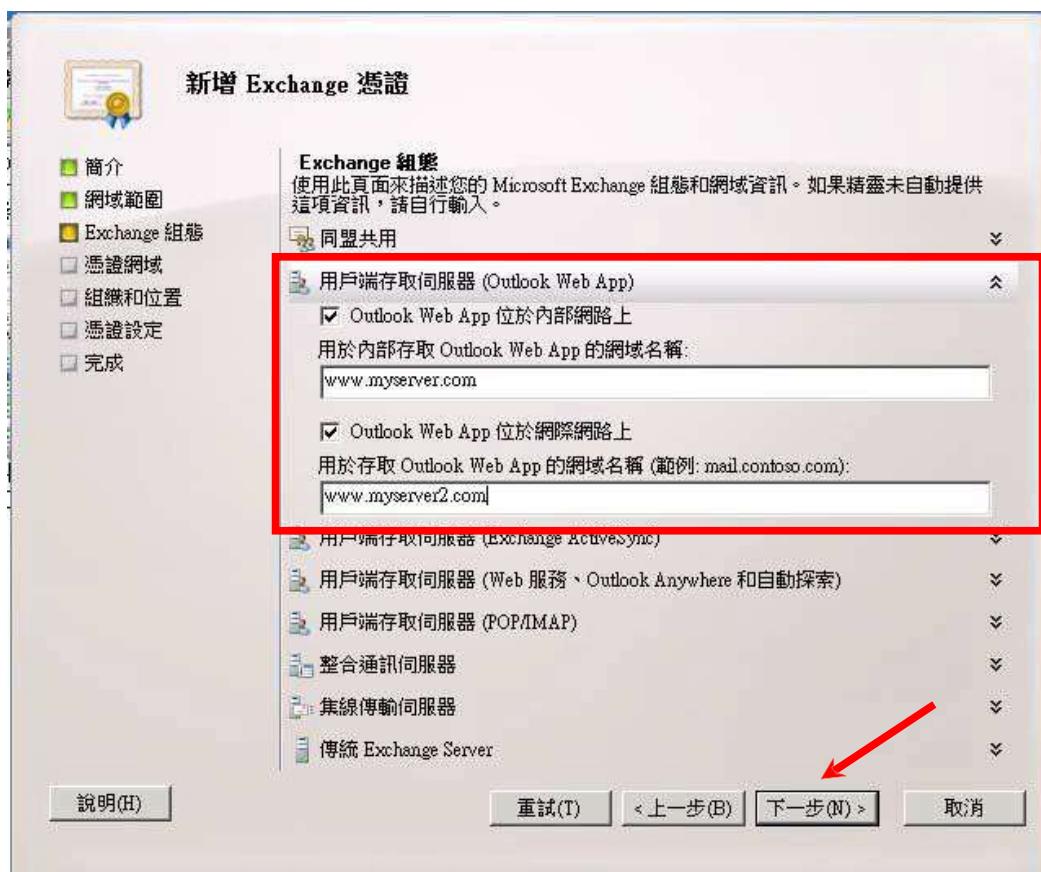
5.1 在 Exchange 組態界面，鈎選您所需要的服務，並按[下一步]來繼續。

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。



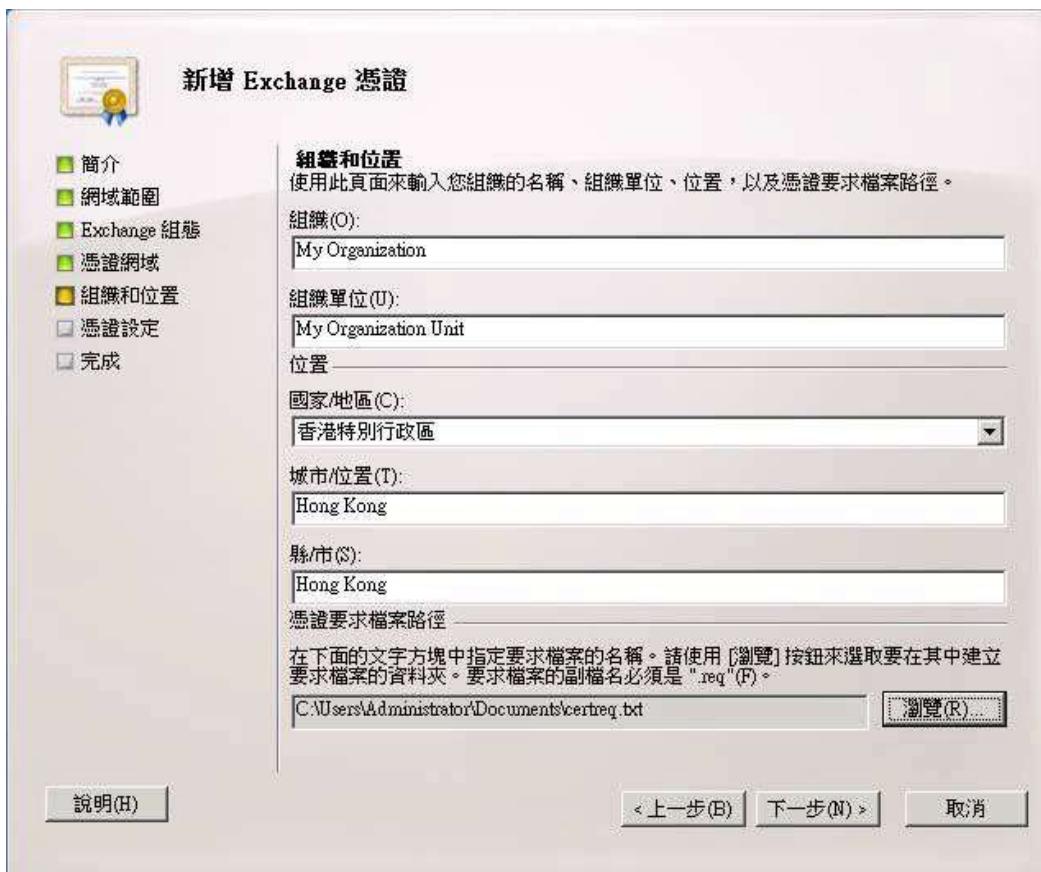
5.2 選擇「一般名稱」設定為一般名稱，並按[下一步]來繼續。



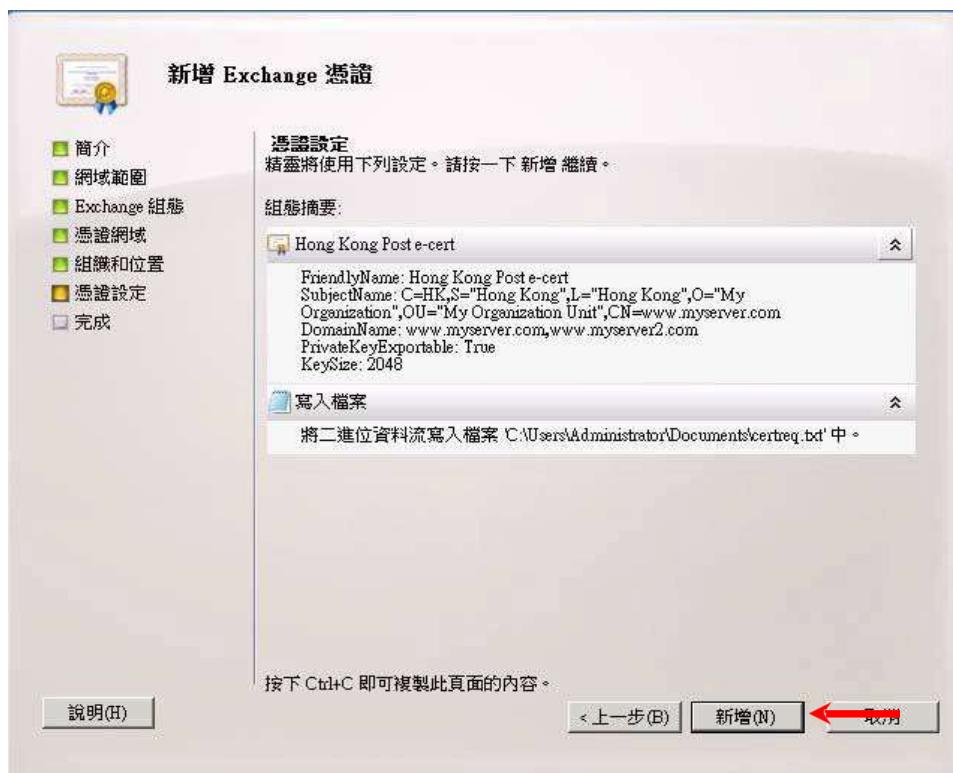
注意：若申請電子證書（伺服器）“多域版”或延伸認證電子證書（伺服器）“多域版”，請在「一般名稱」一欄中，輸入與申請表格中所填寫的「用作電子證書主體名稱的伺服器名稱」相同的登記伺服器名稱。

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。

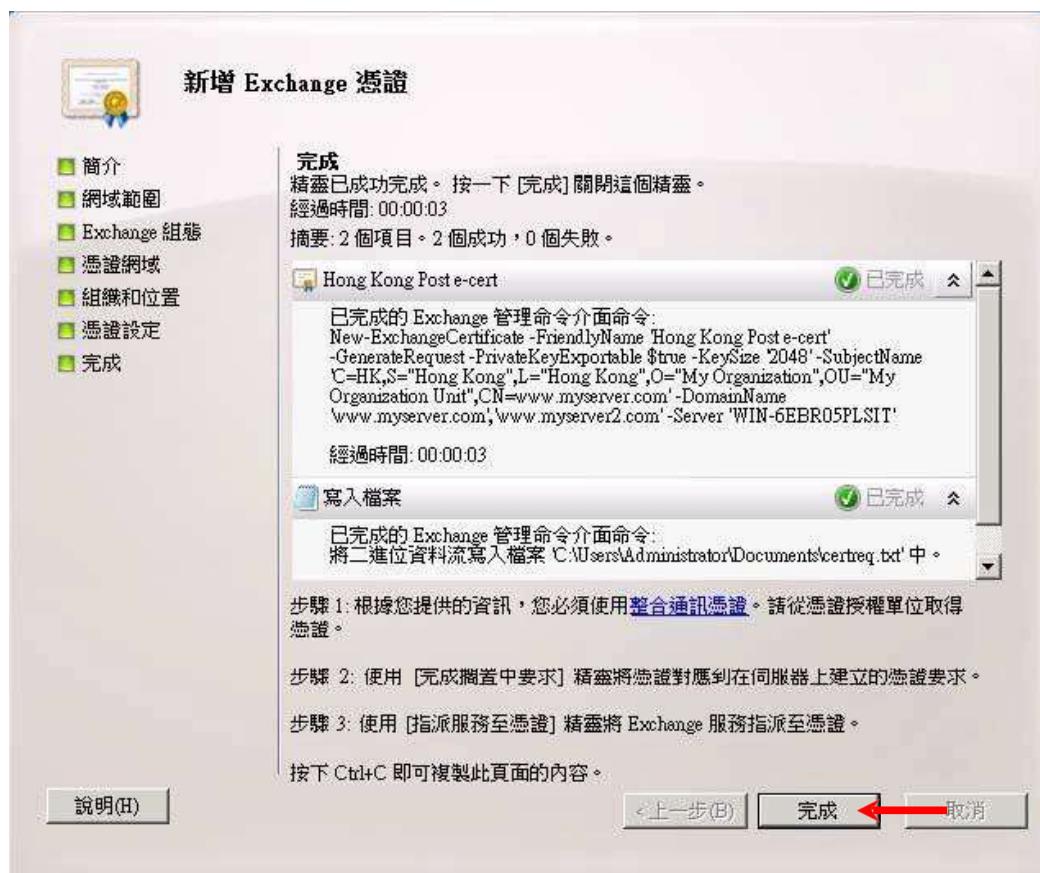
注意：請確保「國家/地區」一欄輸入「香港特別行政區」。



7. 檢查憑證設定並按[新增]。

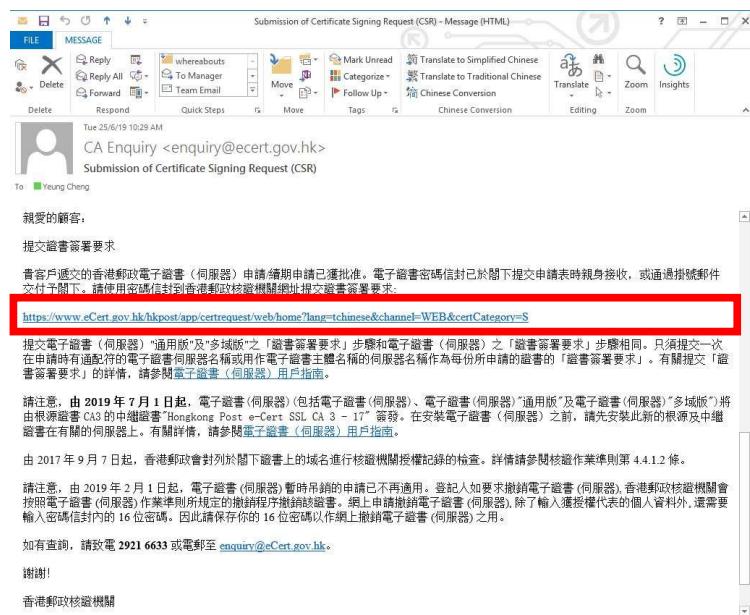


8. 按[完成]來設定。



C. 提交證書簽署要求(CSR)

- 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。



- 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 'Submit Certificate Signing Request - e-Certificate (Server)' page. It includes fields for '伺服器資料': '伺服器名稱' (www.ecert.gov.hk), '電子證書密碼信封資料': '參考編號' (018564144) and '電子證書密碼' (*****), and a note: '請注意，由2025年5月1日起，電子證書（伺服器）會以新中繼證書發放。為確保順利過渡，請：' followed by three steps: 1. 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）。 There is also a note: '有關詳情，請參閱電子證書（伺服器）用戶指南。' and a note at the bottom: '不包含EKU欄位的舊有中繼證書將於2026年6月15日之前被撤銷。'

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 Hong Kong Post e-Cert website interface for submitting a certificate application. The top navigation bar includes the Hong Kong Post e-Cert logo, a green banner with the text 'The solution for e-Security', and a photo of three people smiling. The main form area has a blue header '提交「簽發證書要求」 - 電子證書（伺服器）'. It contains several input fields for registration details, such as '登記人資料' (Applicant Information) and '伺服器名稱' (Server Name). On the right side, there are fields for 'www.e-cert.gov.hk', 'Hong Kong SAR Government', 'HKPO-Business Development Branch', and '香港郵政'. Below these, there are fields for '商業登記證編號' (Business Registration Number), '公司註冊證編號 / 公司登記證編號' (Company Registration Number / Company Registration Certificate Number), and '其他註冊證明文件' (Other Registration Proof Document), with 'HKPO-BDB' selected. A section titled '有關所申請的電子證書的資料' (Information about the applied electronic certificate) includes '證書類型' (Certificate Type) set to '電子證書（伺服器）' and '登記期' (Registration Period) set to '1年'. At the bottom of the form, there is a note: '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；' followed by four buttons: '確認' (Confirm), '拒絕' (Reject), '返回上頁' (Return to Previous Page), and '確認使用中文' (Confirm Use Chinese). A small note at the bottom states: '*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稱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”。**



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 'Submit Certificate Request - Electronic Certificate (Server)' page. The top navigation bar includes the Hongkong Post e-Cert logo and the tagline 'The solution for e-Security'. The main content area has a green header '提交「簽發證書要求」- 電子證書（伺服器）'. A dropdown menu for '網域控制驗證 (DCV) 方法' is set to '網域名稱系統變更 (建議)'. Below it, a section titled '指示：' contains three steps:

- 新增 DNS 記錄：** 嘗試為您的電子證書（伺服器）所包含的每個域名新增 DNS TXT 記錄。
- 檢查 DNS 記錄：** 確保 DNS 記錄是可公開解析的。
- 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。

At the bottom right are '確認' (Confirm) and '返回上頁' (Return to Previous Page) buttons.

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 'Submit Certificate Request - Electronic Certificate (Server)' page, but the dropdown menu for '網域控制驗證 (DCV) 方法' is now set to '構建電郵' (Build Email). The '指示：' section contains two steps:

- 接收驗證碼：** 請選擇指定的電子郵件地址以接收驗證碼。
- 確認：** 驗證碼： [input field] 輸入驗證碼，然後按「確認」繼續。

At the bottom right are '確認' (Confirm) and '返回上頁' (Return to Previous Page) buttons.

5. 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----”。在方格內貼上內容，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）

請貼上「簽發證書要求」(Certificate Signing Request, CSR) (已被base64 編碼的PKCS#10) 於下面的方格內，並按[提交]鍵繼續。

```
-----BEGIN CERTIFICATE REQUEST-----
MIICmCgCAQWkOEIMnkGAIUEBhMCSEaxGTAXBgNVBAMMEHd3dy5lY2VydC5n
b3YuaGswggE1MA0GCSqGSIb3DQEBAQUA4IBwAwggEKAoIBAQClRjsYnP5CN1Z
erGydMz/1WI1CN/+Pi+qBTg94m4FzrHcMZDAtEmKFPzavNvUZ8eSJNHe6W
GhL1750WuGu19cWhmAzQnBv1rhKcjeUh1wDuvva+CYIMx8WSQvnJ1XBmuNn
2LAjCCEHh0RyDwgv0vahzctoMnbIJzv7Q/0MN5R5tgcSHSQjaqcCfZK
90xwvhsS09h/huXzgXzXzXzXzXzXzXzXzXzXzXzXzXzXzXzXzXzXzXzXzXzXz
qewvxdhSsPf49yzt5n3zom8/f4cdj115jWheo24slxoyF1ndTMqH-N5H1F0z
r45TxDfApHBDAGojJa8yjghk1O9w0RC04HshdMmsGh1USeQoQMBKEHd3dy5l
Y2VydCSnbh3YuaGswQYJKc2IhvNAGE1RQAQgeESAHIS37X1J7MLNAv2HplpT+9Y
zg5oTz2gUTSSehoy72X/24+/lgeJexFVBykXTANQRECDn16OLFdfK8K2z2nPg/d5
7SE73Nhuyxy5sNOdcjTODlu8z8kwDkrEPkVU-RCEAa+-J5&1sx/4LMOUhudREpY
0/Zm0gH1laTMFHFRBOJ1zFFW1SSddSN9xx37uAe+71JzK4ATBkTRehg5Wb5t
UjITV4s10t8k16IRU78A/0z32U1DUyxob3H6iRcKxhMuIS/kjaihx53Ge8twcnfU
WjNOpelNJdH7yjzzTyrrMB8EcblvLKEk7+7Sa445rxlpA2sy1bZ43yzTE9whdCYA=
```

提交 返回上頁

2007 © | 重要告示 | 私隱政策

6. 按 [接受] 確認接受此證書。

The solution for e-Security

提交「簽發證書要求」 - 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.ecert.gov.hk
機構名稱:	Hong Kong SAR Government
分行/部門名稱:	HKPO-Business Development Branch
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

其他資料 (由香港郵政核證機關系統產生)

登記人參考編號:	
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:	45 b9 30 00 2d 44 89 87 4c 74 c4 88 35 4b d1 92 08 b8 6c 20
證書有效日期:	13/01/2026 - 31/07/2026 (199日)

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。)

接受 不接受

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. 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_gsca_r3.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

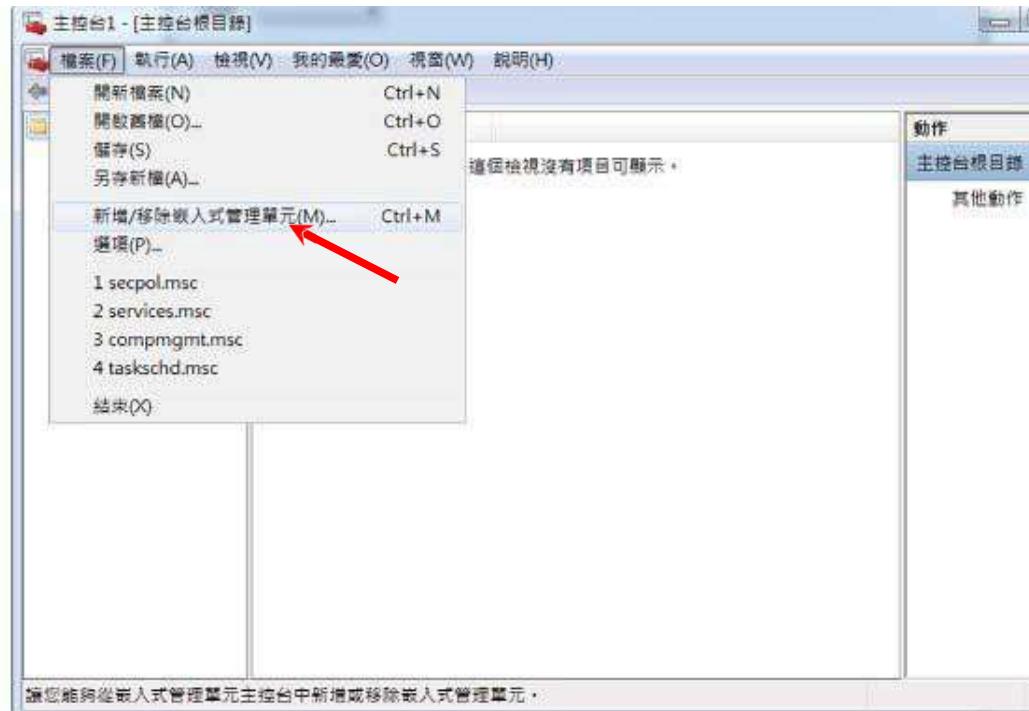
安裝由根源證書 GlobalSign Root CA - R3 簽發的交叉證書 "Hongkong Post Root CA 3"。

下載地址如下：

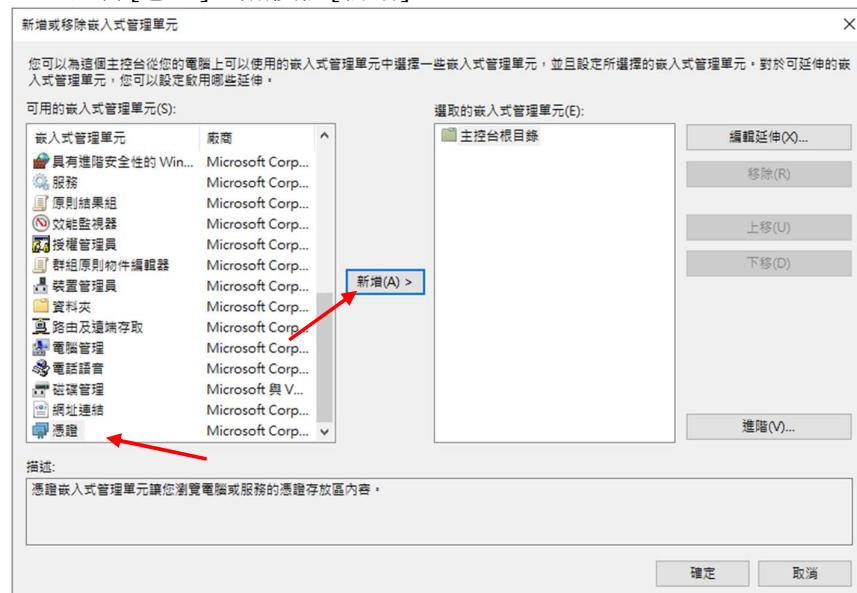
http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3.pem.crt

D. 安裝中繼 / 交叉證書

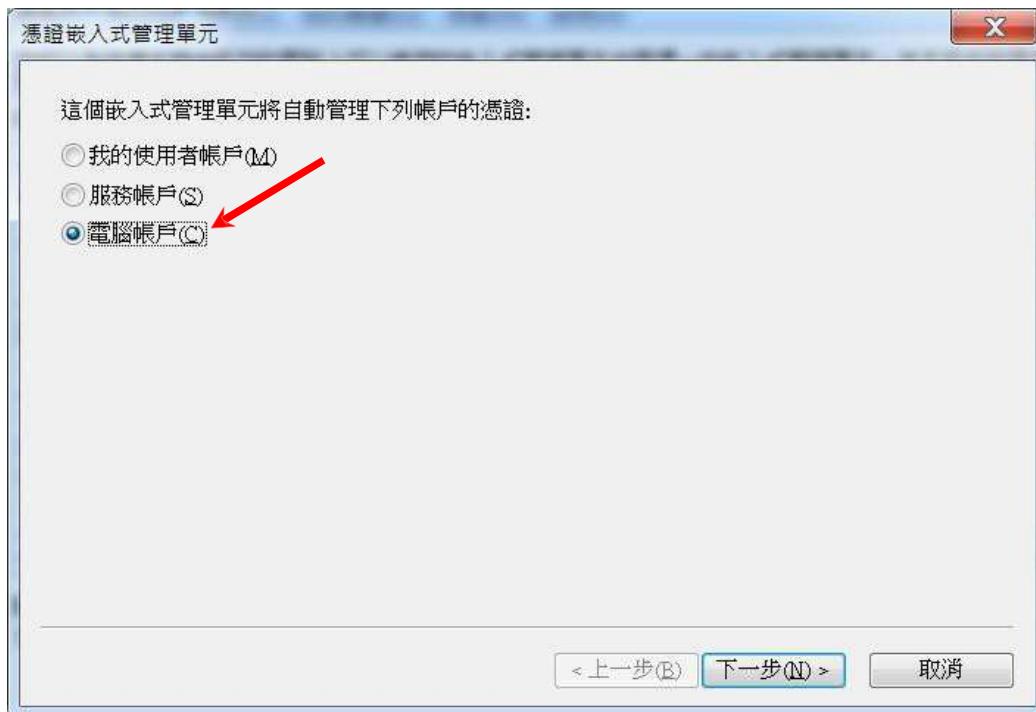
- 按[開始]>[執行]，然後輸入“mmc”及按[確定]來啟動 Microsoft Management Console (MMC)，然後從[檔案]選單中選取[新增/移除嵌入式管理單元]。



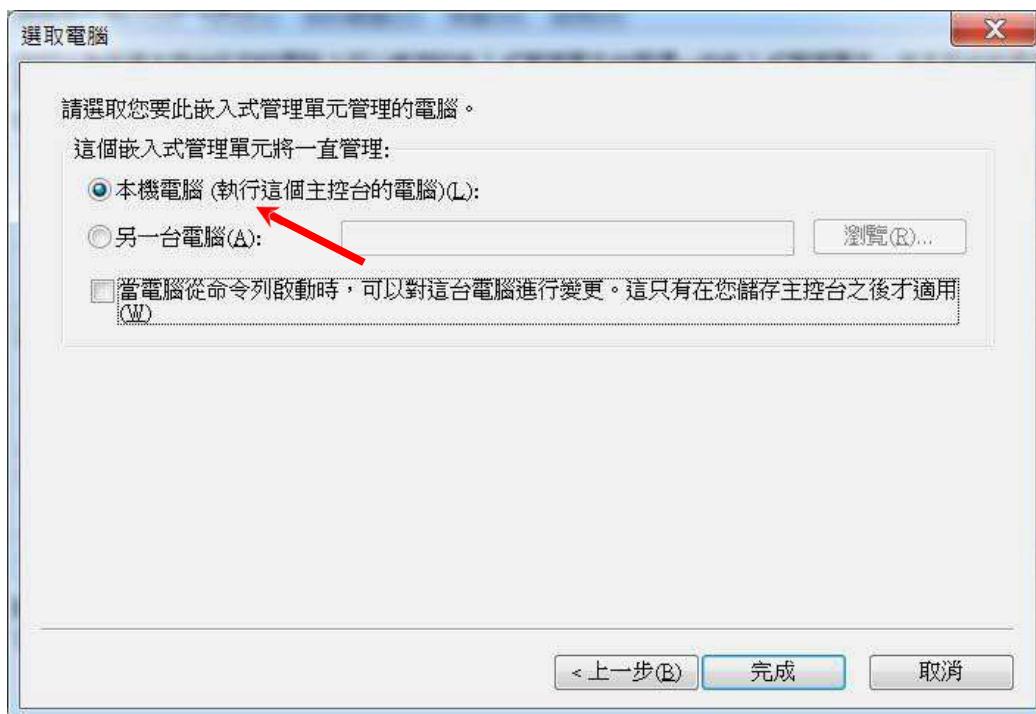
- 選擇[憑證]，然後按[新增]。



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]。

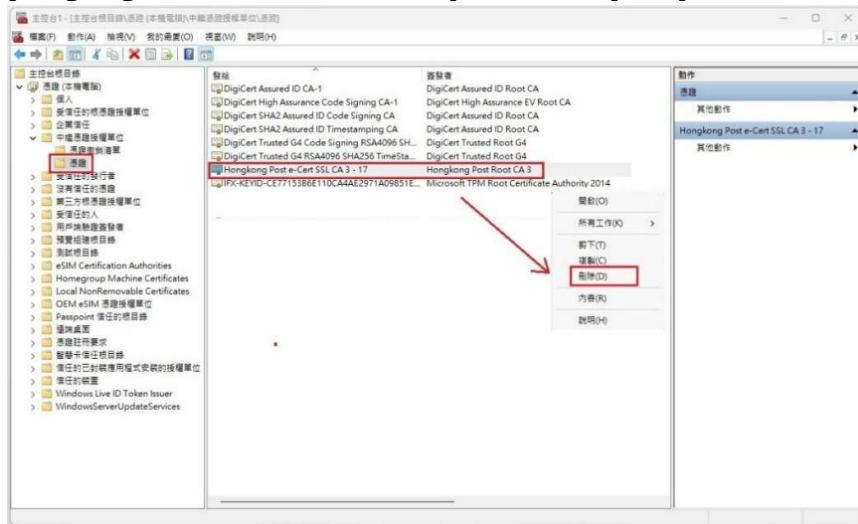


以下內容以 “**Hongkong Post e-Cert SSL CA 3 - 17**” 中繼證書為例子。

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]。



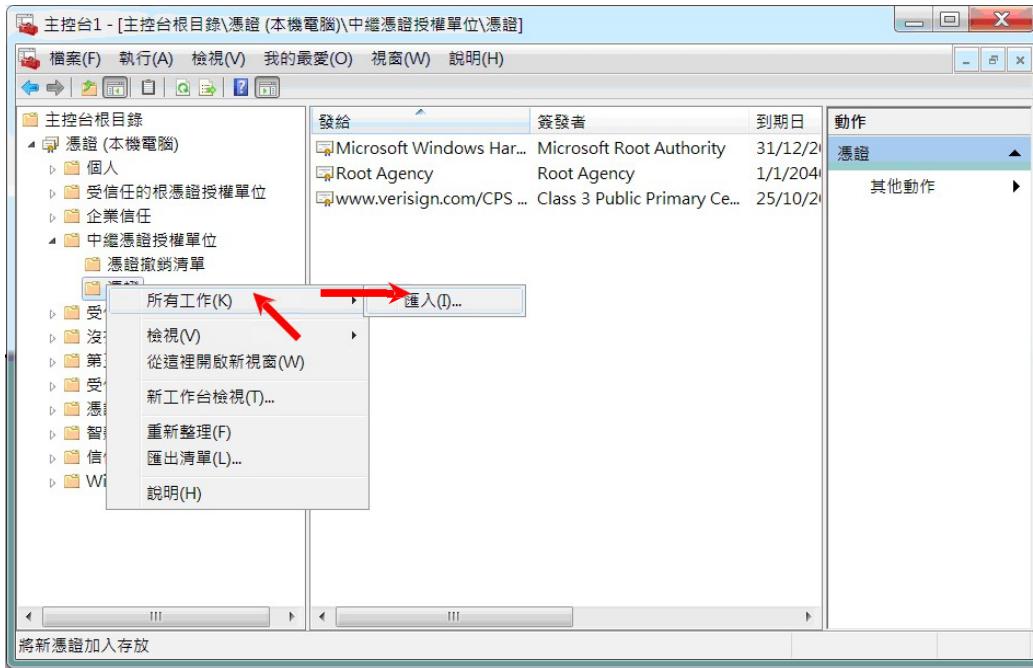
選擇[是]確定刪除。



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

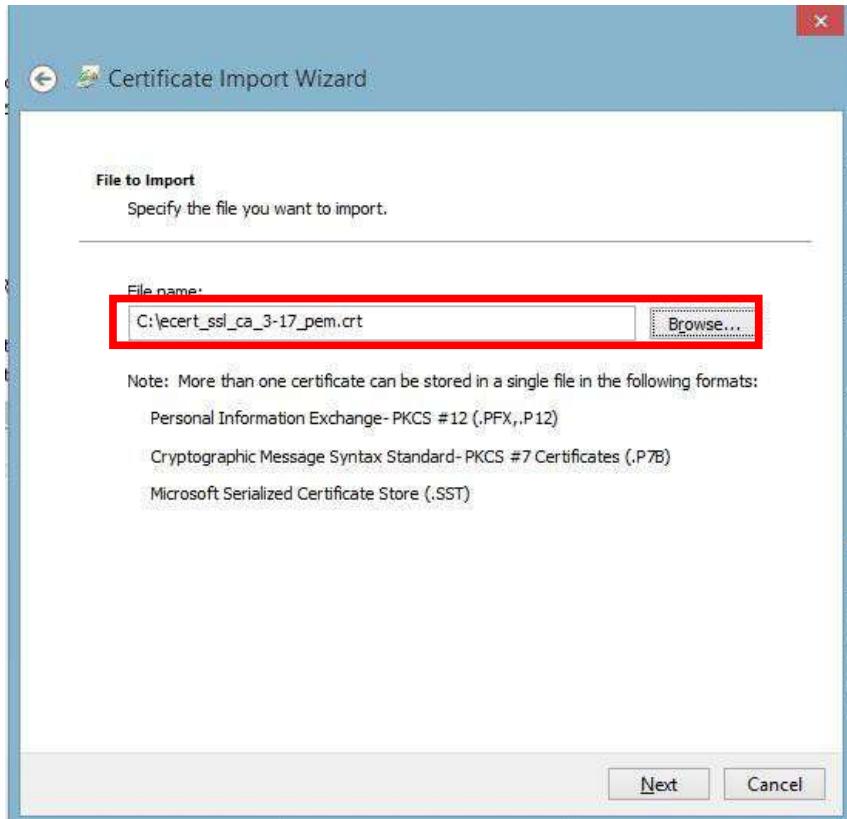
5. 展開[中繼憑證授權單位]及以滑鼠右鍵按一下[憑證]，然後選擇[所有工作]>[匯入]。



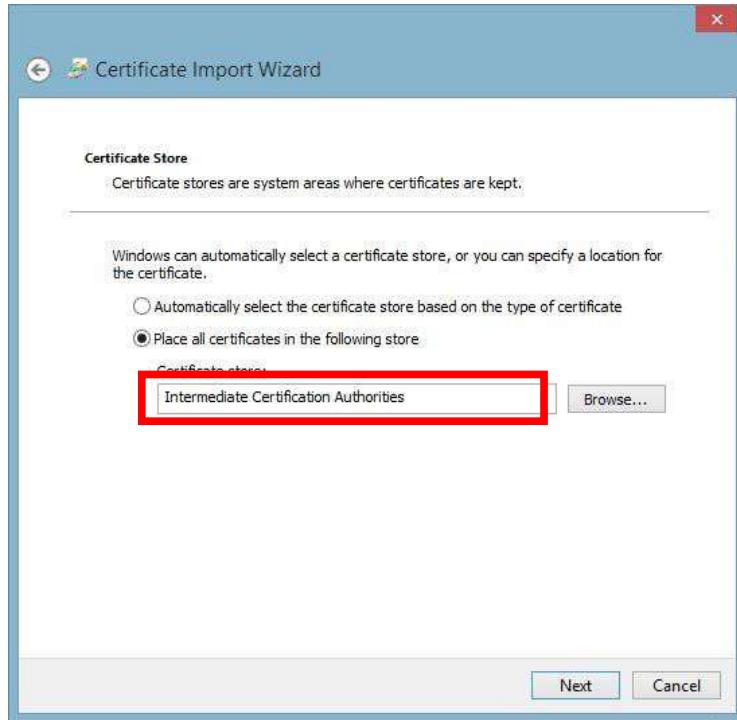
6. 在[憑證匯入精靈]內，按[下一步]繼續。



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]。



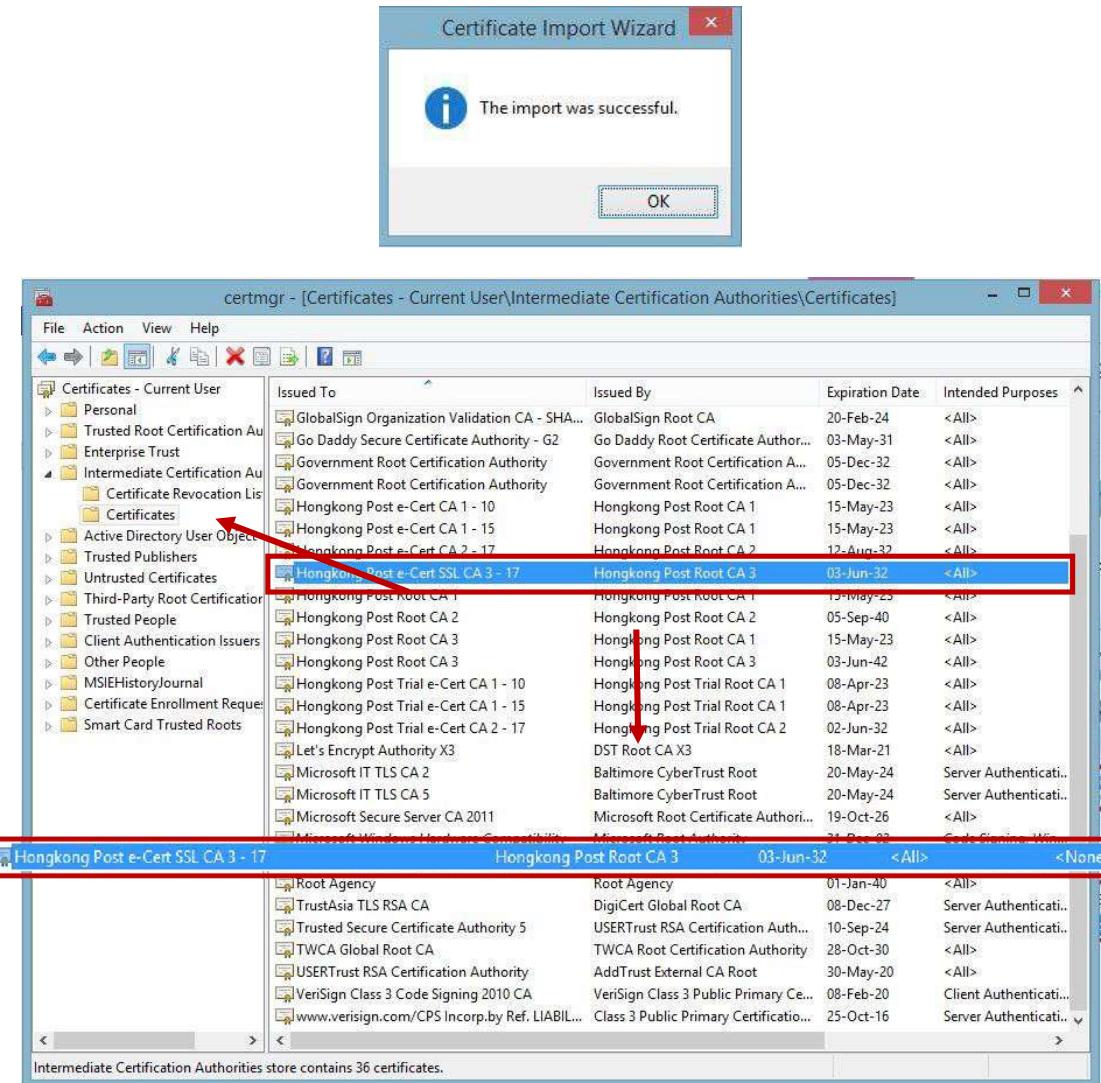
8. 選擇[將所有憑證放入以下的存放區]，然後按[下一步]。



9. 按[完成]來關閉精靈。



10. 按[確定]來完成。

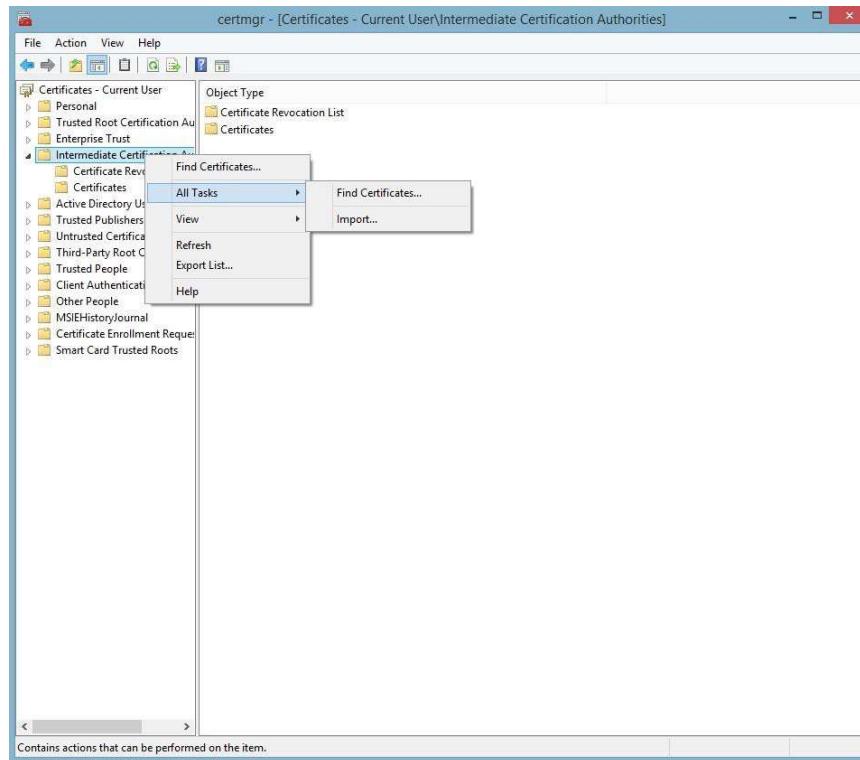


圖表 1：“Hongkong Post e-Cert SSL CA 3 - 17” 中繼證書已成功安裝

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)

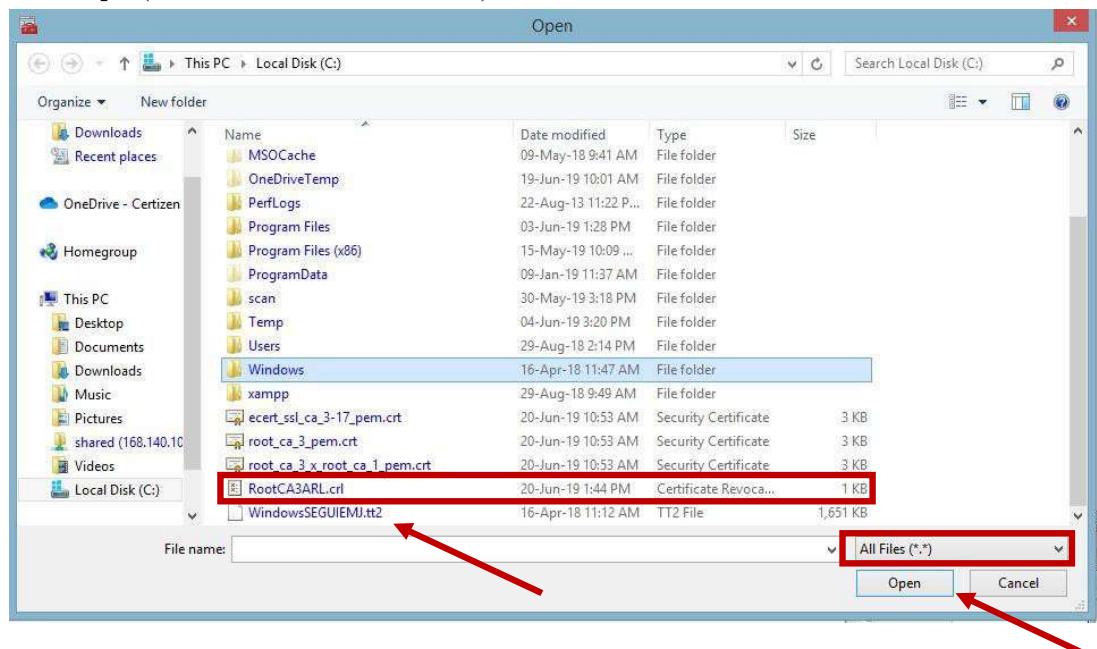
11. 下載授權撤銷清單(ARL)：<http://crl1.eCert.gov.hk/crl/RootCA3ARL.crl>
12. 展開[中繼憑證授權]及以滑鼠右鍵按一下，然後選擇[所有工作]>[匯入]。

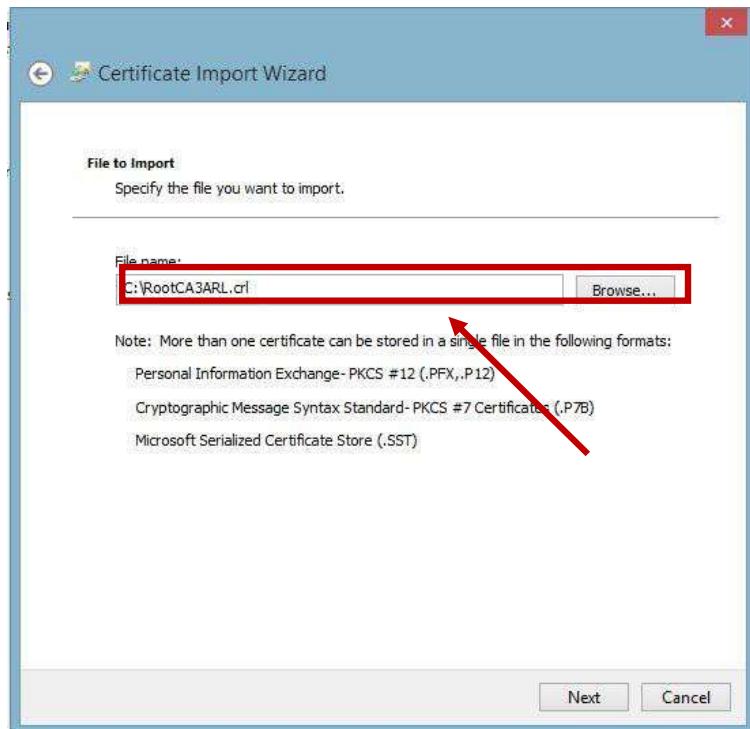


13. 在[憑證匯入精靈]內，按[下一步]繼續。

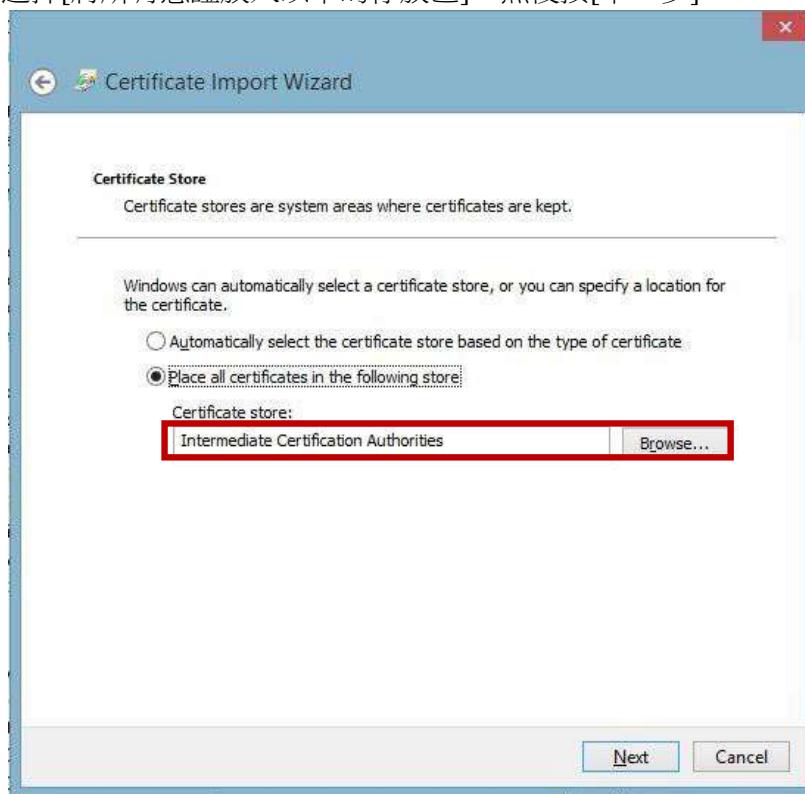


14. 按[瀏覽]選擇早前於步驟 11 下載的“Hongkong Post Authority Revocation List (ARL)”授權撤銷清單 (RootCA3ARL.crl)，然後按[下一步]。(提示：選擇“所有檔案”)

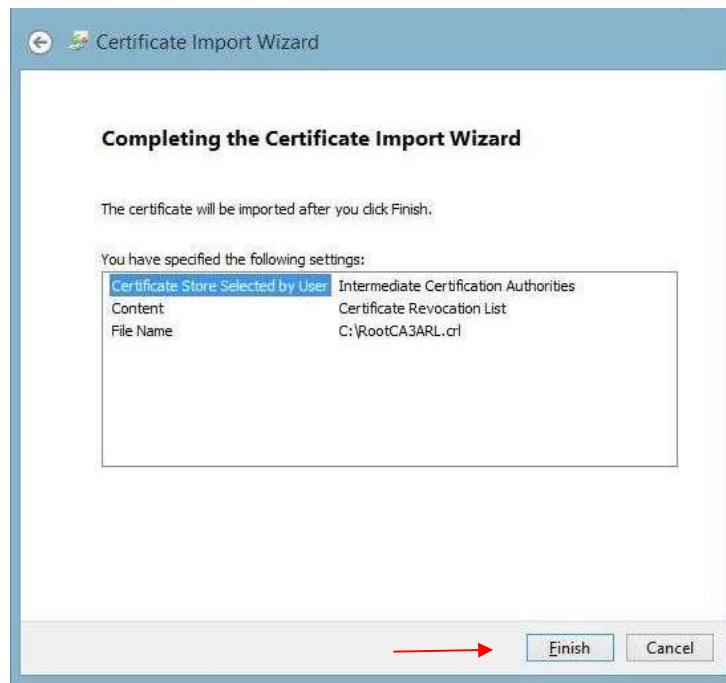




15. 選擇[將所有憑證放入以下的存放區]，然後按[下一步]。



16. 按[完成]來關閉精靈。



17. 按[確定]來完成。

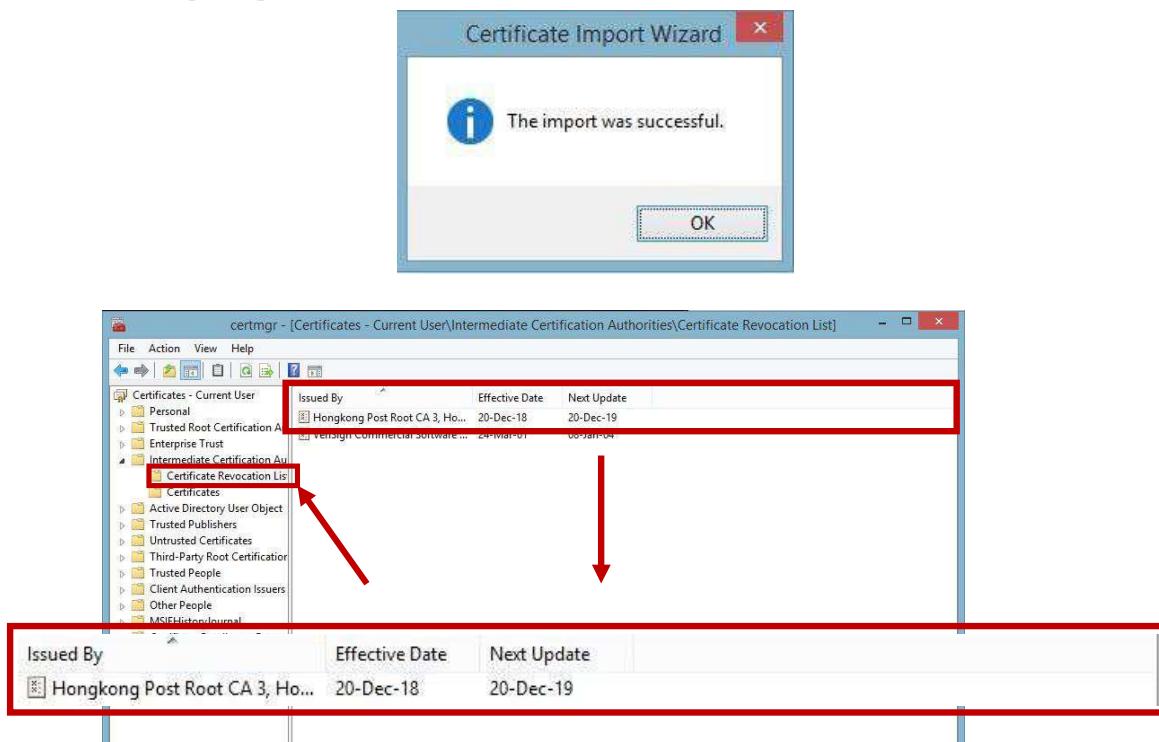
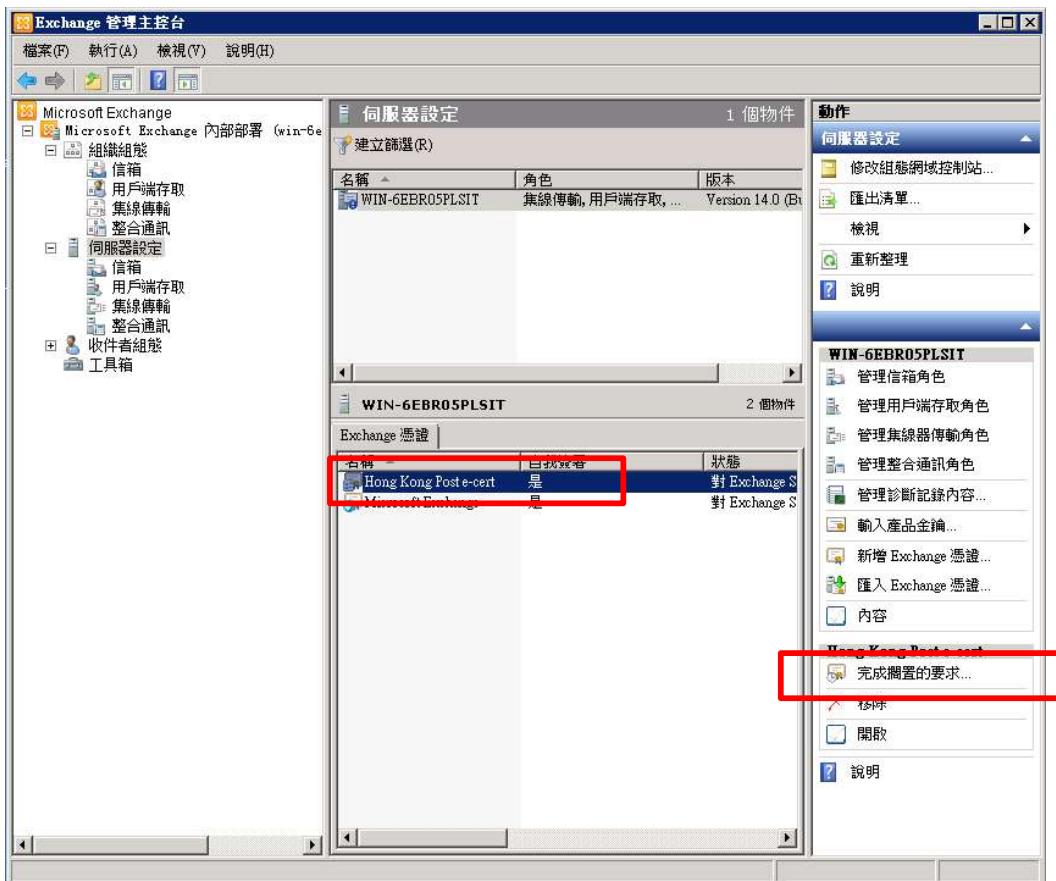


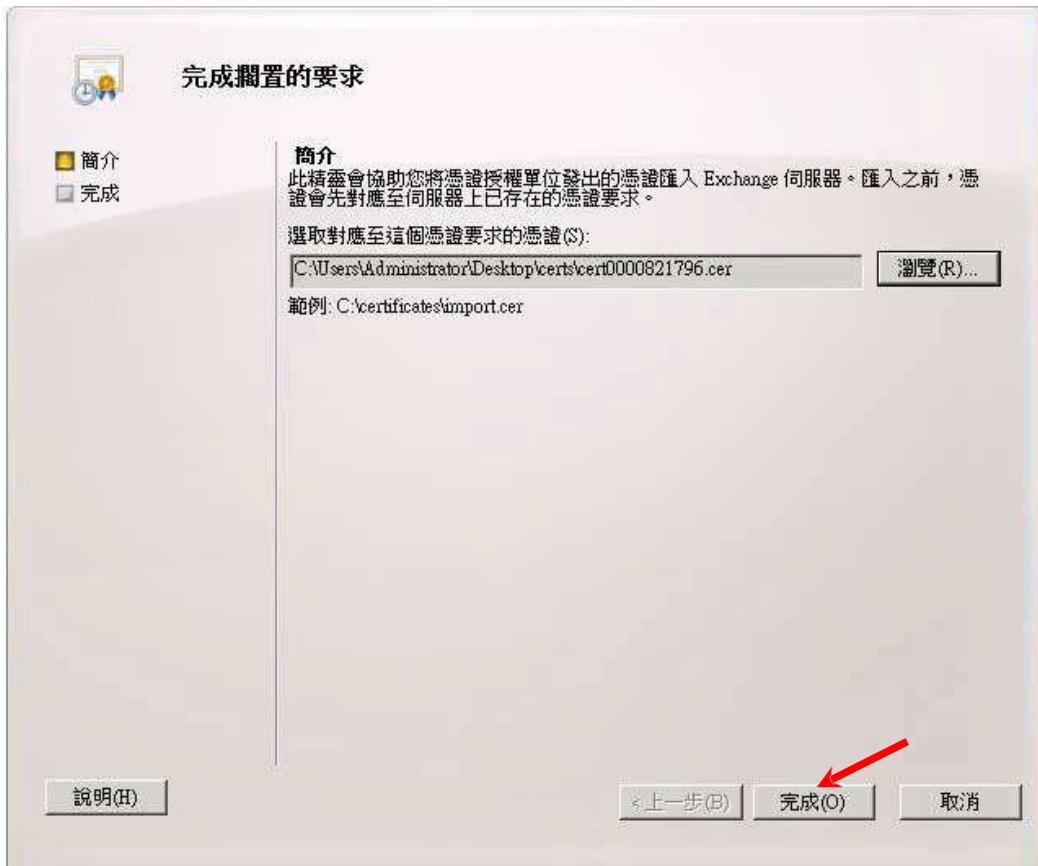
圖 3：“Hongkong Post Authority Revocation List (ARL)” 授權撤銷清單已成功安裝

E. 安裝伺服器證書

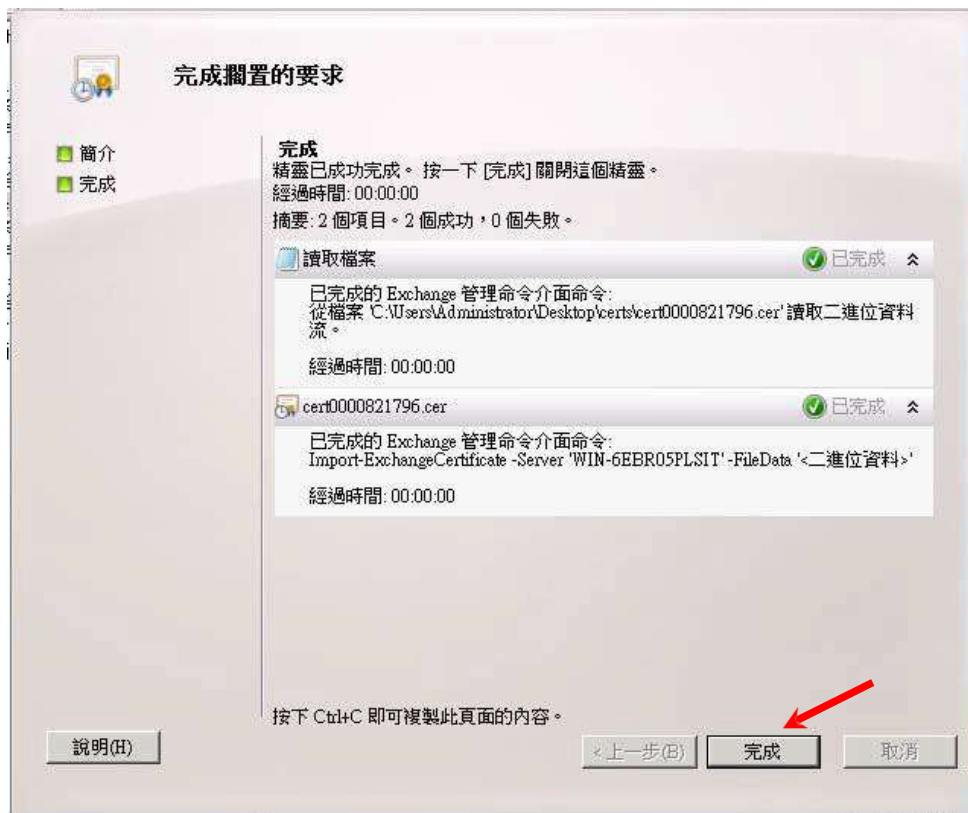
- 在 [Exchange 管理主控台] 視窗內，選擇[伺服器設定]，然後選擇您於步驟 B 中所申請的 Exchange 憑證。在右手邊動作一欄內，按[完成擱置的要求]。



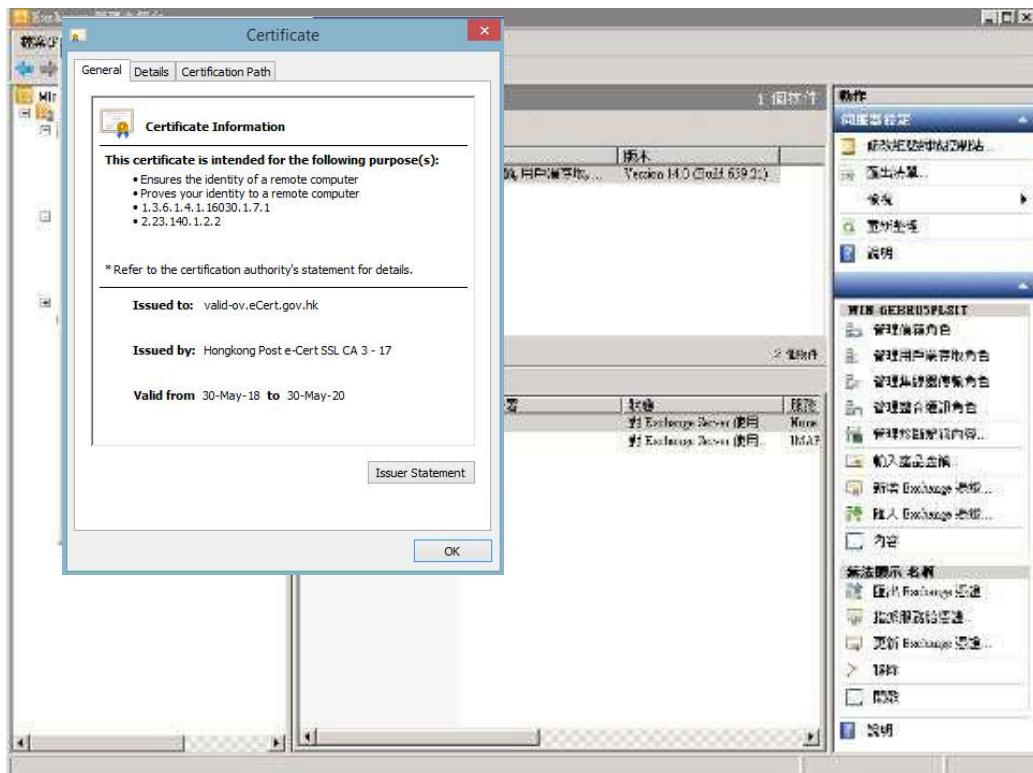
2. 按[瀏覽] 選擇早前於 C 部的步驟 7 下載的“Hongkong Post e-Cert (Server)” 證書，然後按[完成]。



3. 按[完成]來結束憑證安裝。

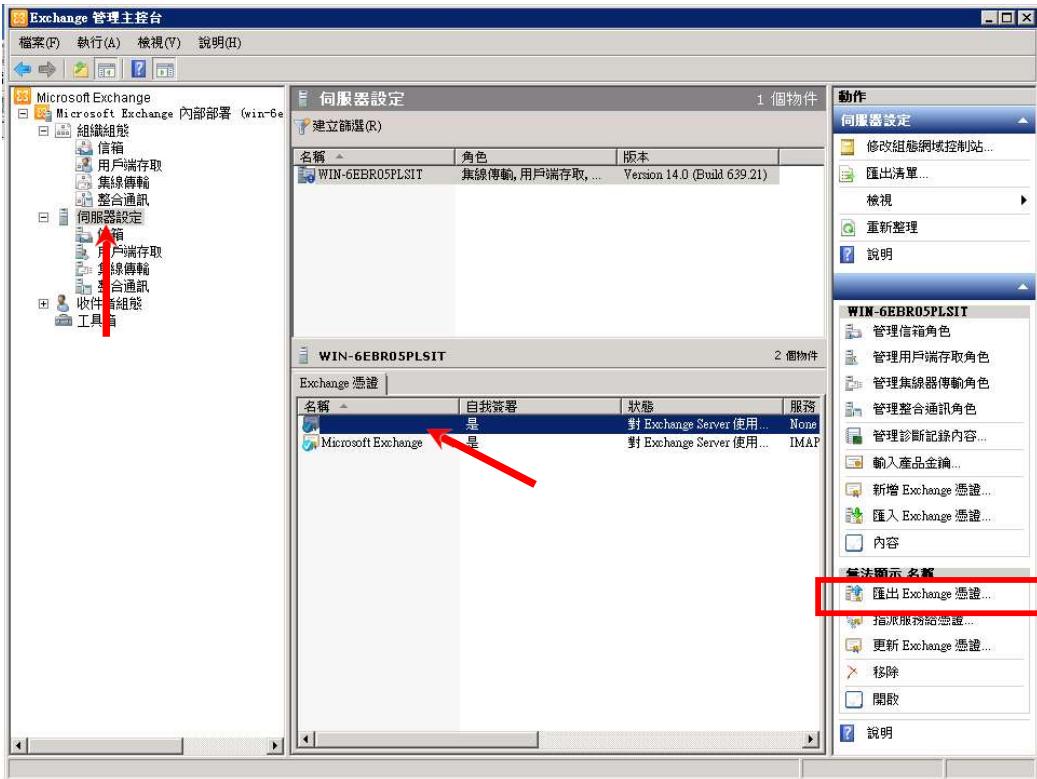


4. Hongkong Post 伺服器證書已經成功安裝，你可以雙擊證書以察看證書資訊。

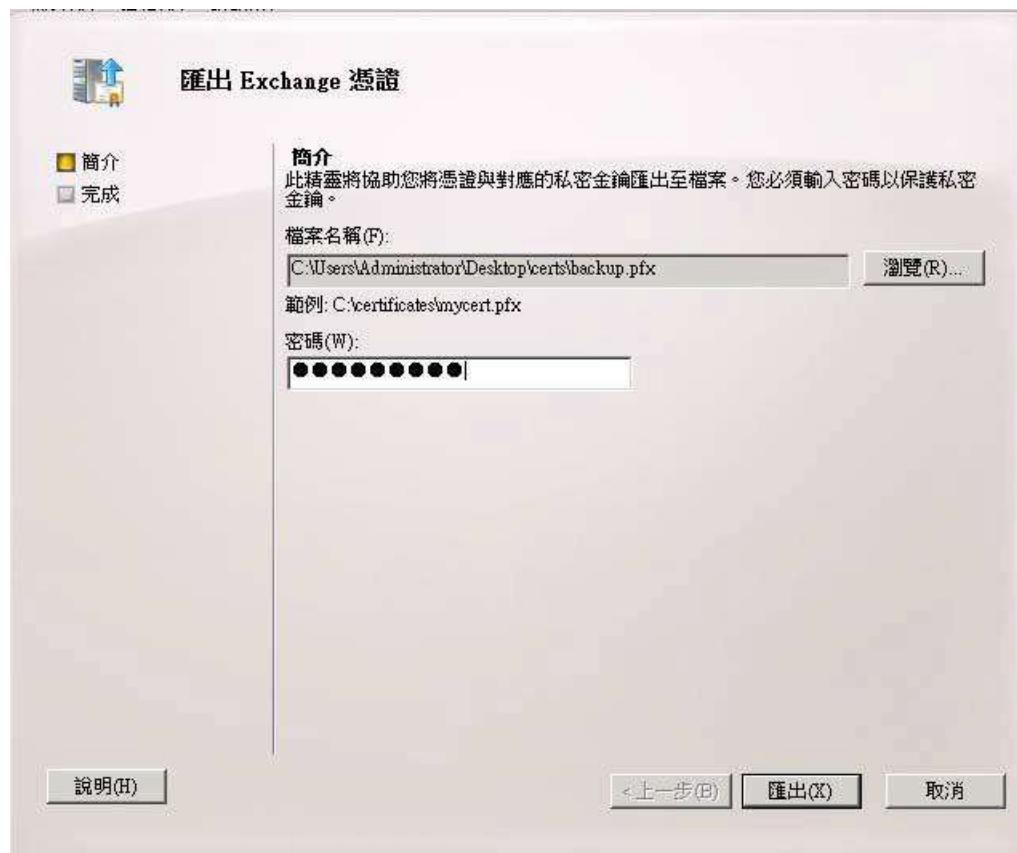


F. 備份密碼匙

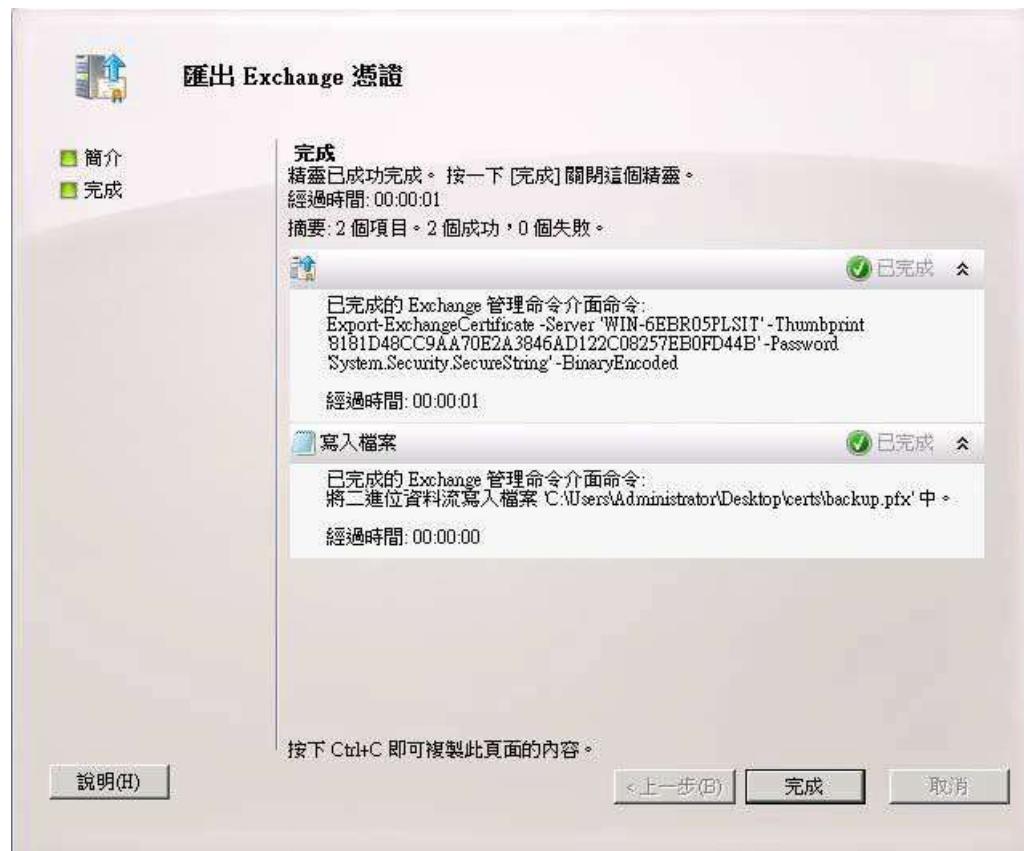
- 在“Exchange 管理主控台”界面，按“伺服器設定”，選擇您想要備份的密碼匙。於右手邊選項，選擇“匯出 Exchange 憑證”。



- 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]。

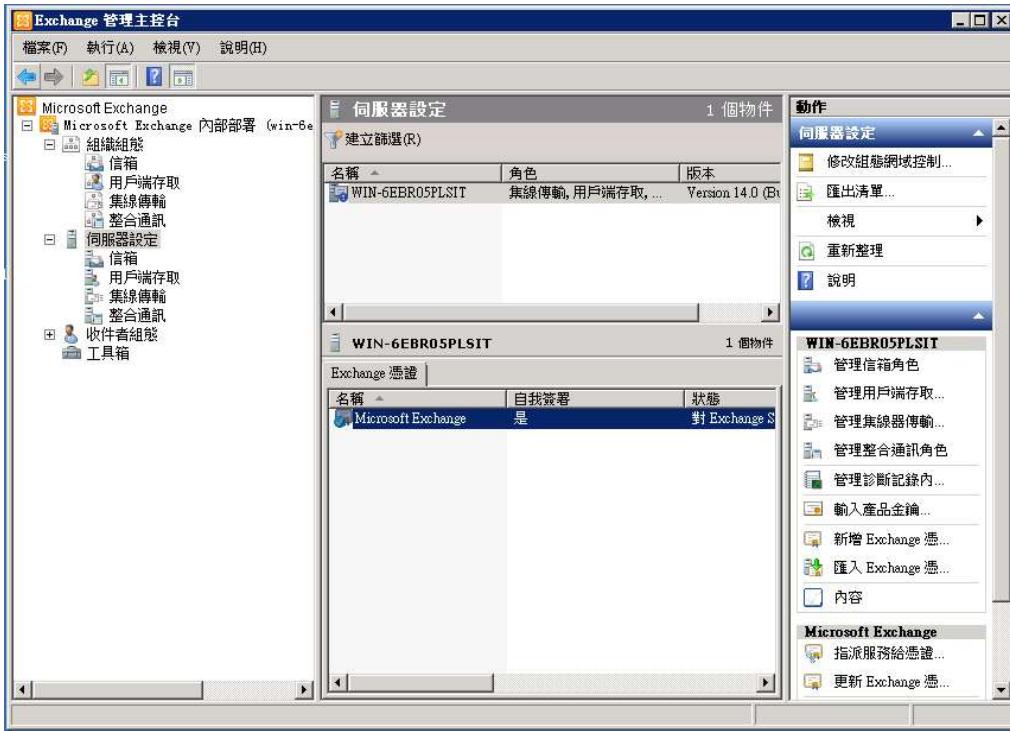


3. 按[完成]來結束匯出憑證，Hongkong Post e-cert 伺服器憑證已經成功匯出。



G. 還原密碼匙

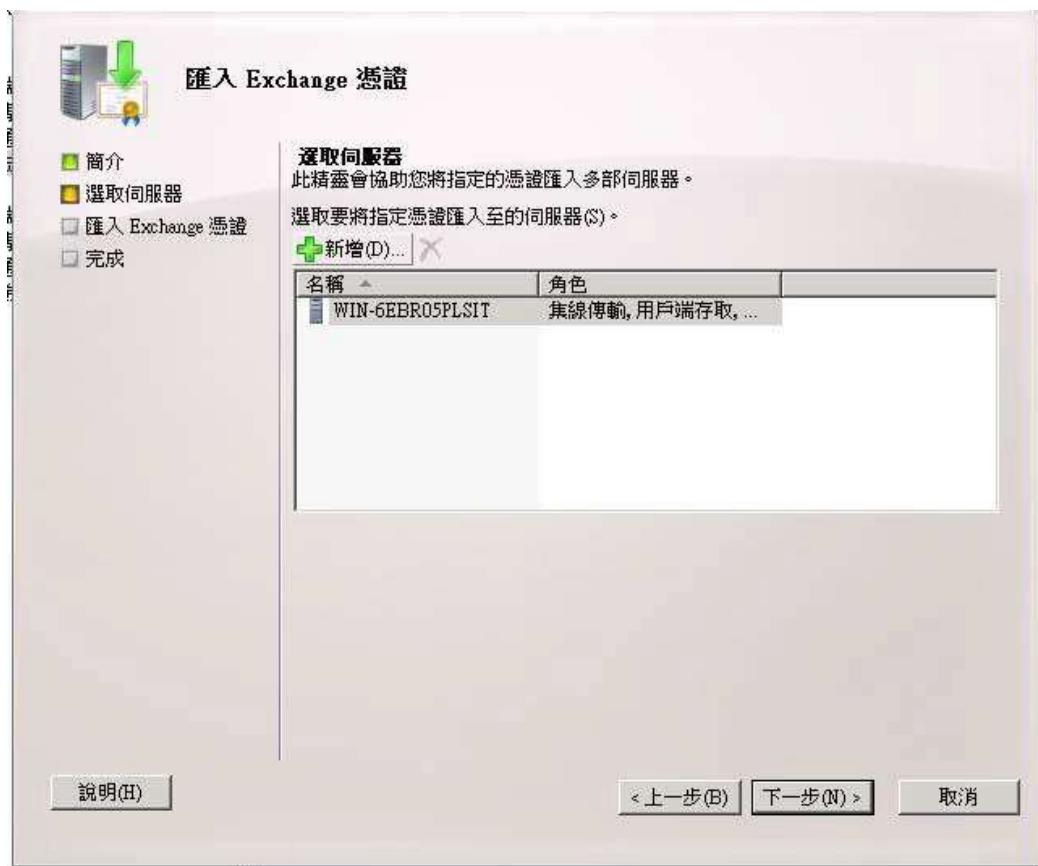
1. 在“Exchange 管理主控台”界面，按“伺服器設定”，於右手邊選項，選擇“匯入 Exchange 憑證”。



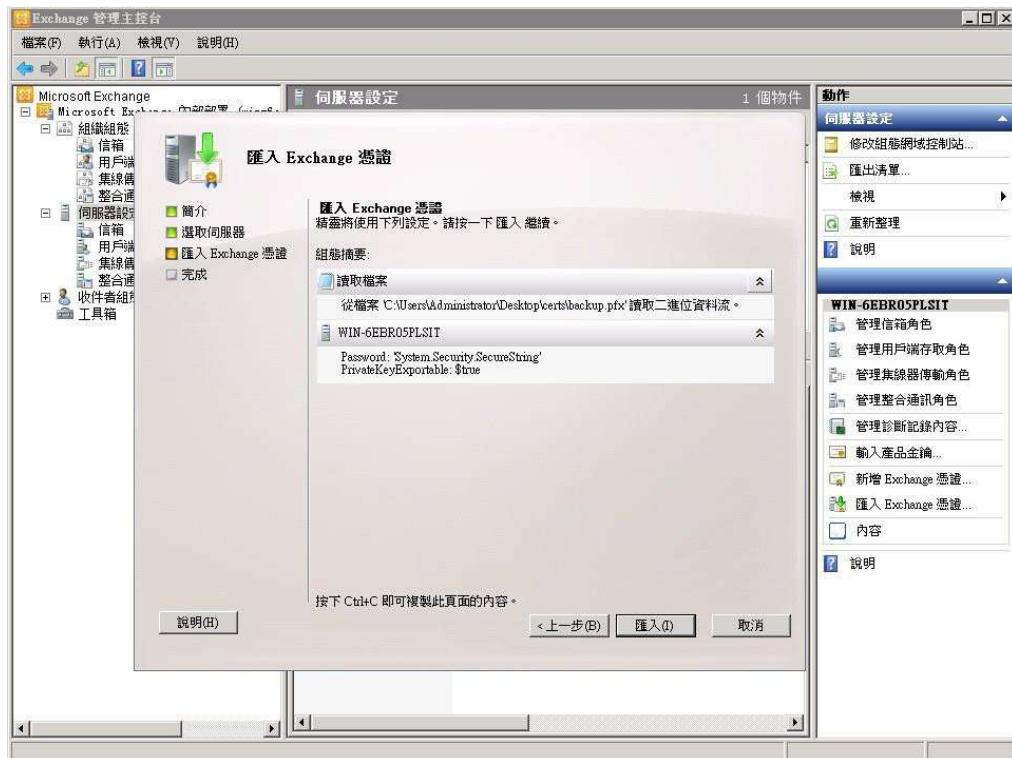
- 在“匯入 Exchange 憑證”界面中，選擇包含輸入包含憑證的檔案名稱及路徑及憑證的密碼，然後按[下一步]來繼續。



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]。



5. 按[完成]來結束匯入憑證，電子證書（伺服器）証書已成功匯入。

