电子证书（伺服器）用户指南

Microsoft Exchange Server 2010 适用

修订日期：2026年1月

目录

A. 电子证书（伺服器）申请人指引

香港邮政核证机关在收到及批核电子证书（伺服器）申请后，会向获授权代表发出主旨为 “Submission of Certificate Signing Request (CSR)” 的电邮，要求获授权代表到香港邮政核证机关的网站提交CSR。

本用户指南旨在提供参考给电子证书（伺服器）申请人如何在 Windows 2008 上的 Exchange Sever 2010产生配对密码匙和证书签署要求(CSR)的详细步骤。包含公匙的 CSR 将会提交到香港邮政核证机关以作证书签署。

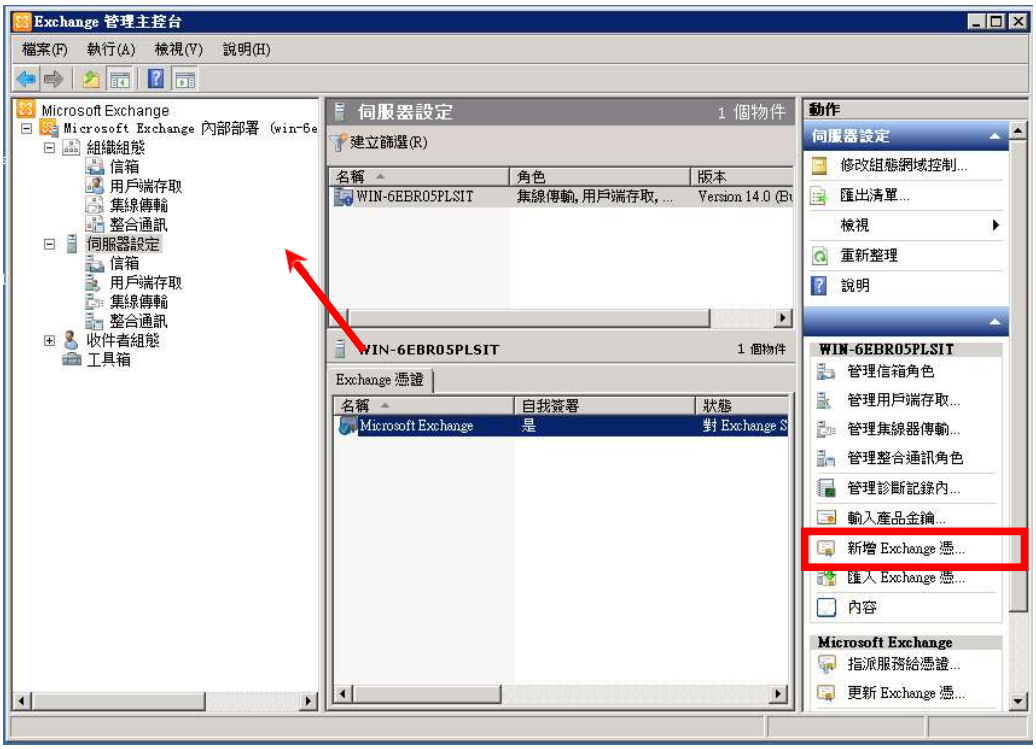
如阁下在证书签发后遗失密码匙，您将不能安装或使用该证书。因此强烈建议阁下于**提交证书签署要求(CSR)前**及**完成安装伺服器证书后**均为密码匙进行备份。有关备份及还原密码匙的方法，请参阅以下部分的详细步骤：

新申请及续期申请

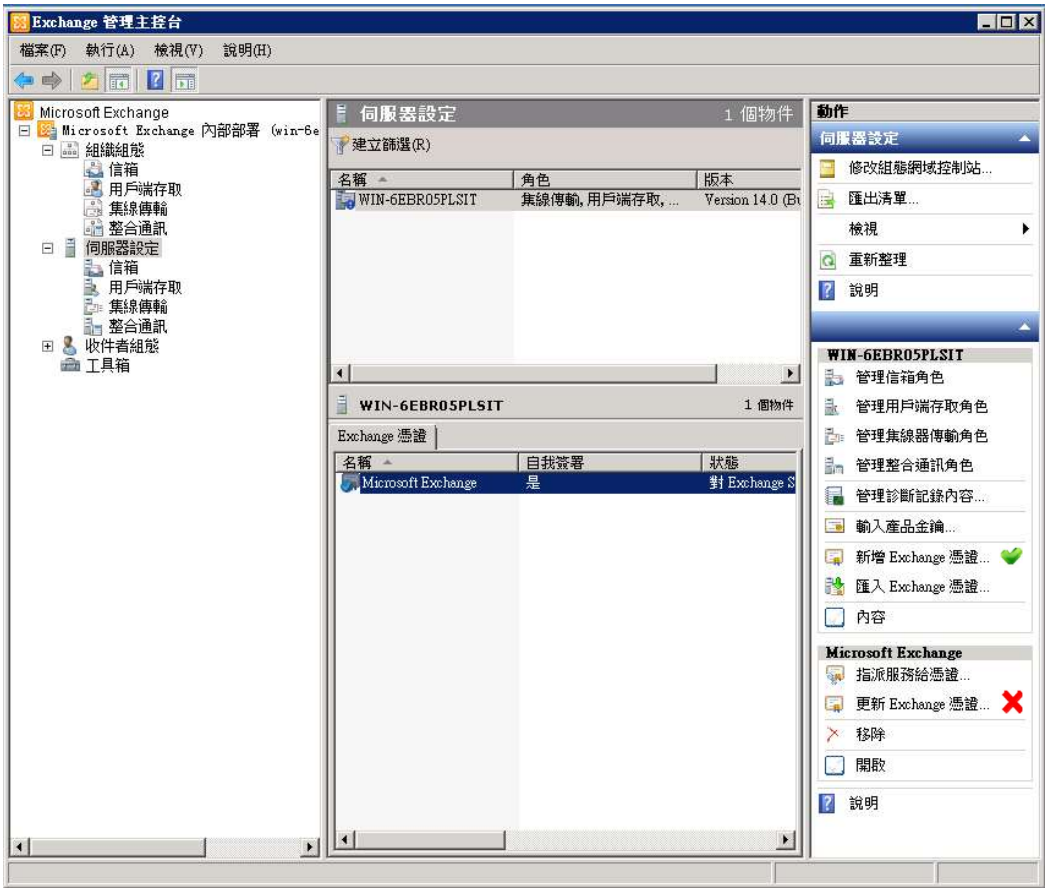
首次及续期申请电子证书（伺服器），请参阅以下部分的详细步骤：

B. 产生证书签署要求(CSR)

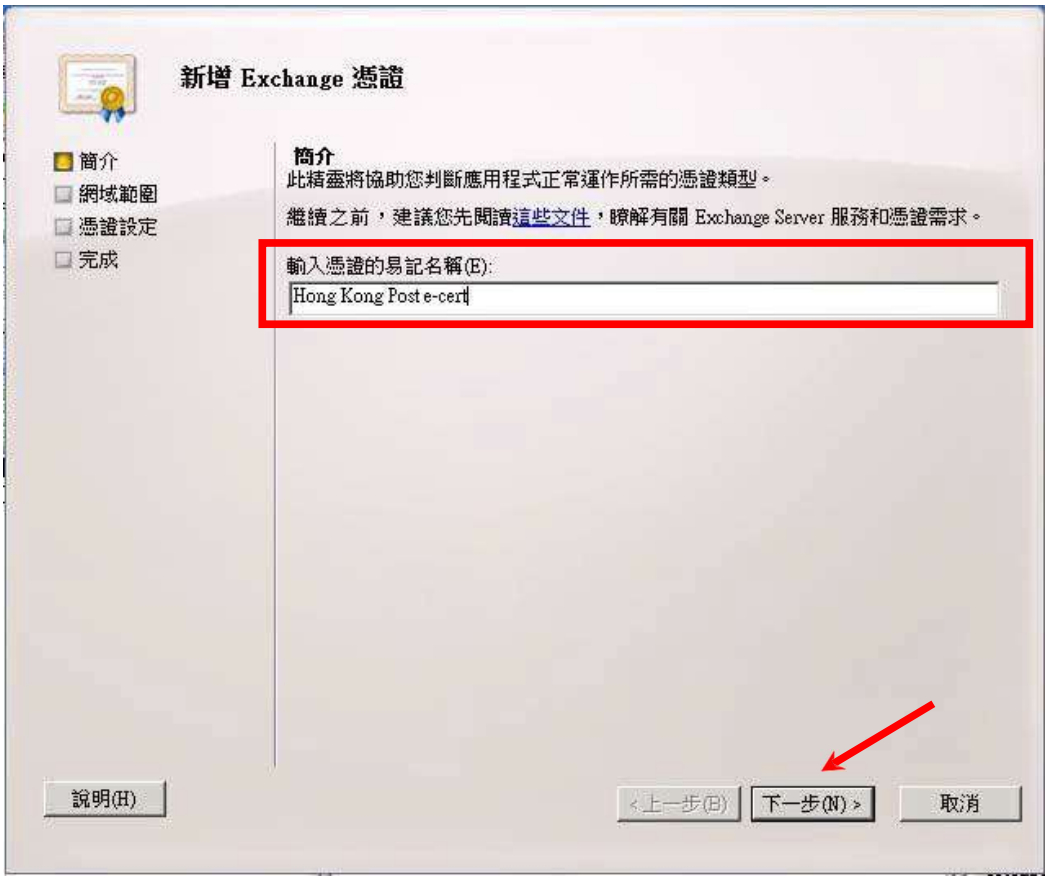
1. 按[开始]>[所有程式]>[Exchange Sever 2010]>[Exchange 管理主控台]来启动 Exchange 管理工具。
2. 在 [Exchange 管理主控台] 视窗内，展开[Microsoft Exchange 内部部署]。
3. 选择[伺服器设定]，在右手边[动作]一栏内，按[新增 Exchange 凭证]。



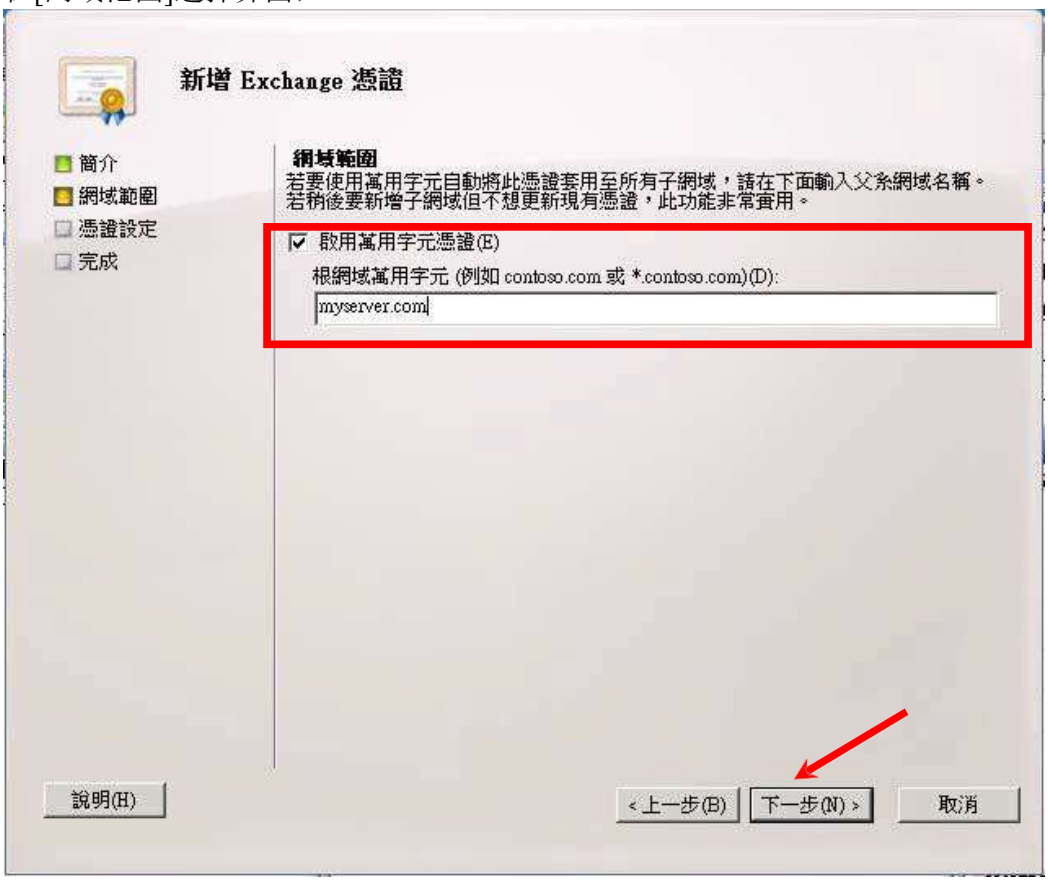
注意：新申请及续期申请电子证书（伺服器）的步骤相同，即使是续期电子证书，请不要使用[更新Exchange凭证]，要选择[新增Exchange凭证]。



4. 输入凭证的易记名称（如:Hong Kong Post e-cert），并按[下一步]来继续。



5. 在[网域范围]选择界面，



- 如您为电子证书（伺服器）“通用版”的用户，请钩选“启用万用字元凭证”并与[根网域万用字元]填入您的伺服器名称，按[下一步]， 并直接进入步骤 6。

注意：请确定[根网域万用字元]中所填项目与申请表格中‘有通配符的电子证书伺服器名称’相同，可包括有通配符「＊」的部份。

- 如果您为电子证书（伺服器）或电子证书（伺服器）“多域版”的用户，请直接按“下一步”，并完成步骤 5.1 与 5.2 。

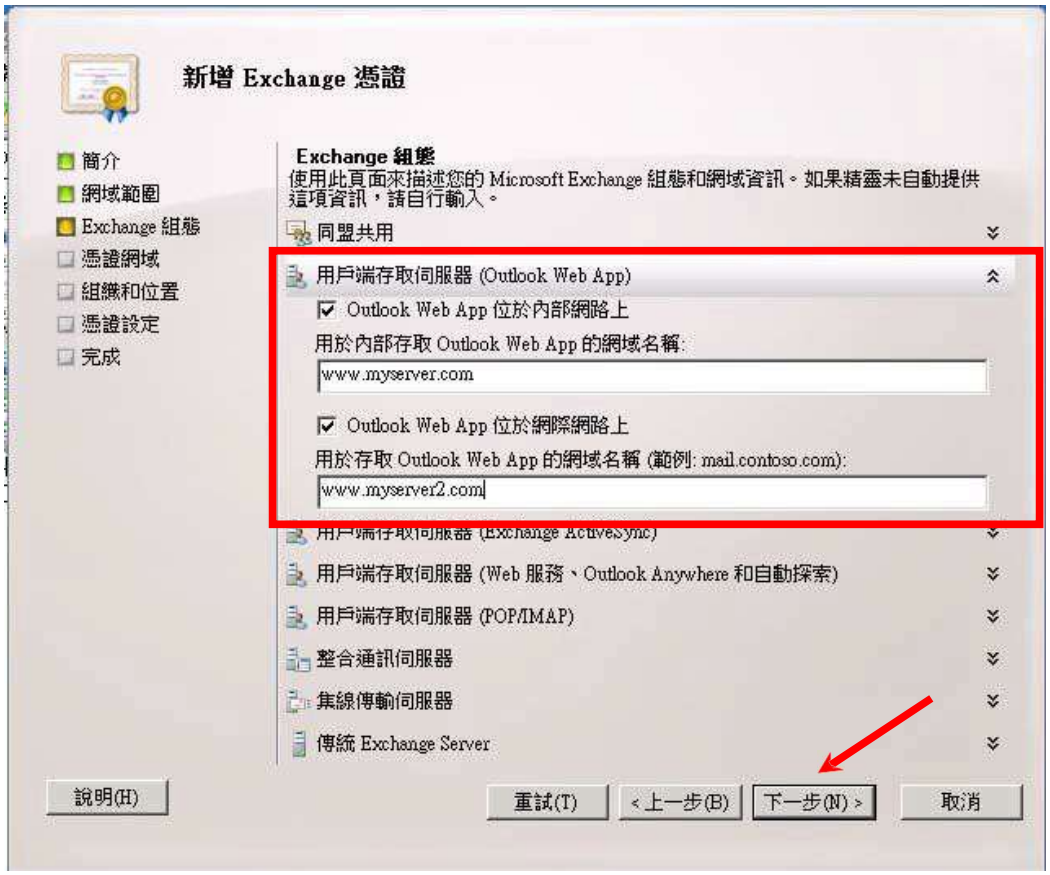
5. 1 在 Exchange 组态界面，钩选您所需要的服务，并按[下一步]来继续。

注意：您应将依据您的伺服器的服务类别进行相应的配置，以下所示范例为电子证书（伺服器）“多域版”。

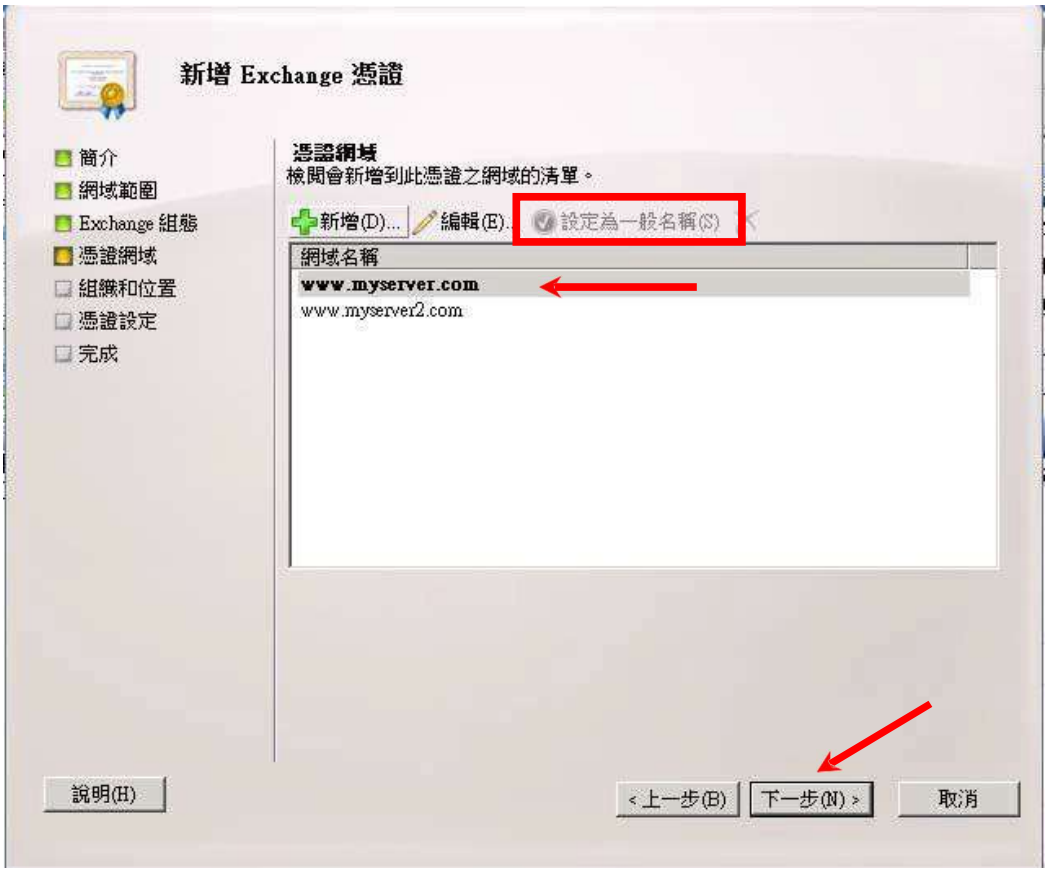
注意：若申请中文伺服器名称的电子证书（伺服器）

选项 1：请在网域名称一欄中，输入与申请表格中所填写的「用作电子证书主体名称的伺服器名称」相同的登记伺服器名称。

选项 2: 请使用国际网域名称转换工具把中文网域名称转换成 ASCII 字元，并可以在网域名称一欄中输入转换后的名称。



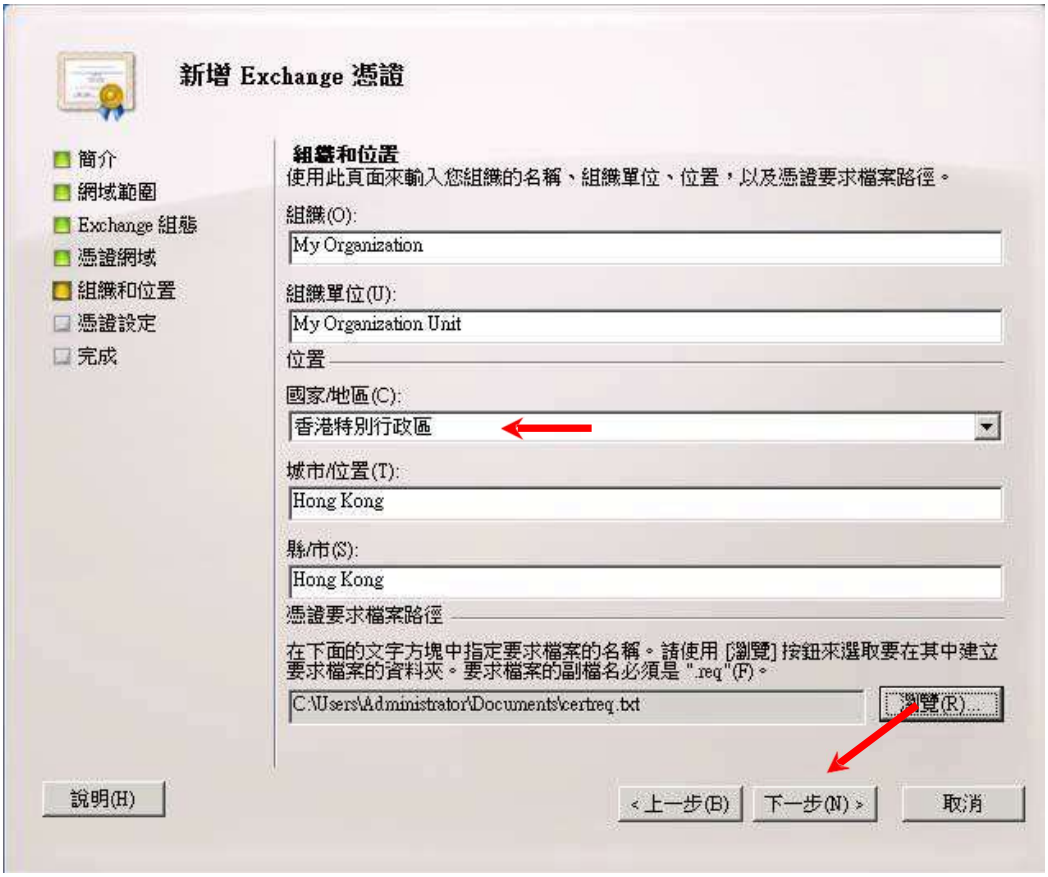
5.2 选择「一般名称」设定为一般名称，并按[下一步]来继续。



注意：若申请电子证书（伺服器）“多域版”或延伸认证电子证书（伺服器）“多域版”，请在「一般名称」一欄中，输入与申请表格中所填写的「用作电子证书主体名称的伺服器名称」相同的登记伺服器名称。

6. 输入您的组织及组织单位, 及选择 “香港特别行政区” 作为[国家/地区]，输入“Hong Kong” 作为[城市/位置] 及[县/市]，选择您的 CSR 存放路径， 然后按[下一步]来继续。

注意: 请确保「国家/地区」一栏输入「香港特别行政区」。

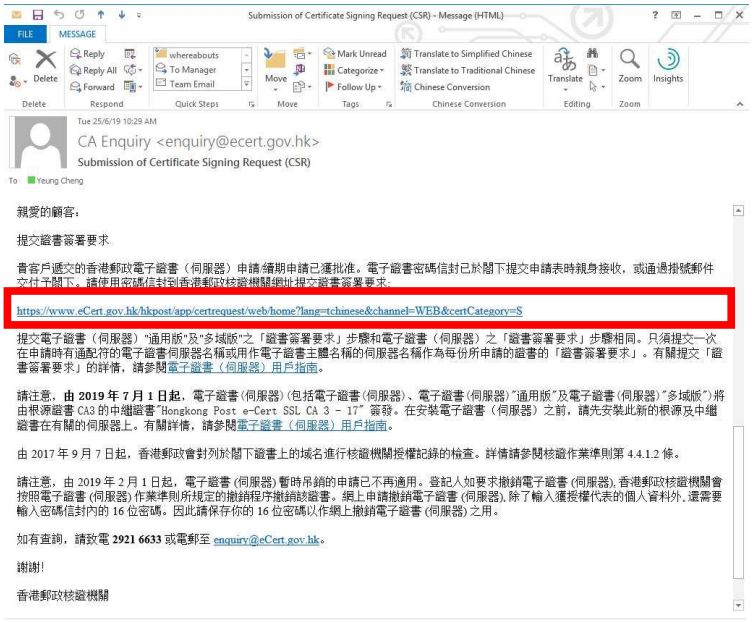


7. 检查凭证设定并按[新增]。

8. 按[完成]来设定。

C. 提交证书签署要求(CSR)

1. 在香港邮政核证机关发出主旨为 “Submission of Certificate Signing Request (CSR)” 的电邮内按一下超连结以连线至香港邮政核证机关的网站。



2. 输入[伺服器名称]、印于密码信封面的[参考编号](九位数字)及印于密码信封内的[电子证书密码](十六位数字)，然后按[**提交**]。

3. 按 [**提交**] 确认申请资料。(如发现资料不正确，请电邮至 enquiry@eCert.gov.hk 联络香港邮政核证机关。)

注意：若电子证书申请表格上提供了机构中文名称和/或分部中文名称，如要发出一张主体名称为机构中文名称的电子证书(伺服器)，请按[确认使用中文]键。

4. （**自 2026 年 3 月 15 日起生效，且仅适用于非政府登记人**）请从适用于您的电子证书（伺服器）的网域控制验证 (DCV) 方法清单中选择您所需的方法，并按照萤幕上的指示进行操作。确认后，系统将自动验证并确认您对电子证书（伺服器）所包含域名的控制权。如果 DCV 验证成功，您将可以提交 CSR。
（请注意，系统只会显示适用于您的电子证书（伺服器）类型的验证方法供您选择。）

A. 如选择「网站变更」网域控制验证 (DCV) 方法，请下载验证档案“fileauth.txt”，并将其上传到您电子证书（伺服器）所包含的每个域名对应的网站上的指定位置。上传档案并确认档案可公开存取后，按「确认」继续。请注意，此方法不适用于电子证书（伺服器）"通用版"。

B. 如选择「网域名称系统变更」网域控制验证 (DCV) 方法，请为您的电子证书（伺服器）所包含的每个域名新增包含验证码的 DNS TXT 记录。新增 DNS 记录并确保可公开解析后，按「确认」继续。

C. 如选择「构建电邮」网域控制验证 (DCV) 方法，请选择指定的电子邮件地址，然后按「发送验证码」。收到电子邮件后，在网页中输入验证码，然后按「确认」继续。请注意，此方法不适用于电子证书（伺服器）″多域版″。

5. 用文字编辑器(例如：记事本)开启早前产生的证书签署要求(CSR)及复制全部内容包括 “-----BEGIN NEW CERTIFICATE REQUEST-----” 及 “-----END NEW CERTIFICATE REQUEST-----”。在方格内贴上内容，然后按[**提交**]。

6. 按 [**接受**] 确认接受此证书。

7. 下载 Hongkong Post e-Cert (Server)证书。

注意：

1. *您也可以从搜寻及下载证书网页下载您的电子证书（伺服器）。*
   https://www.ecert.gov.hk/tc/sc/index_sc.html
2. *安装由根源证书 Root CA3 签发的中继证书"Hongkong Post e-Cert SSL CA 3 - 17"。下载地址如下：*

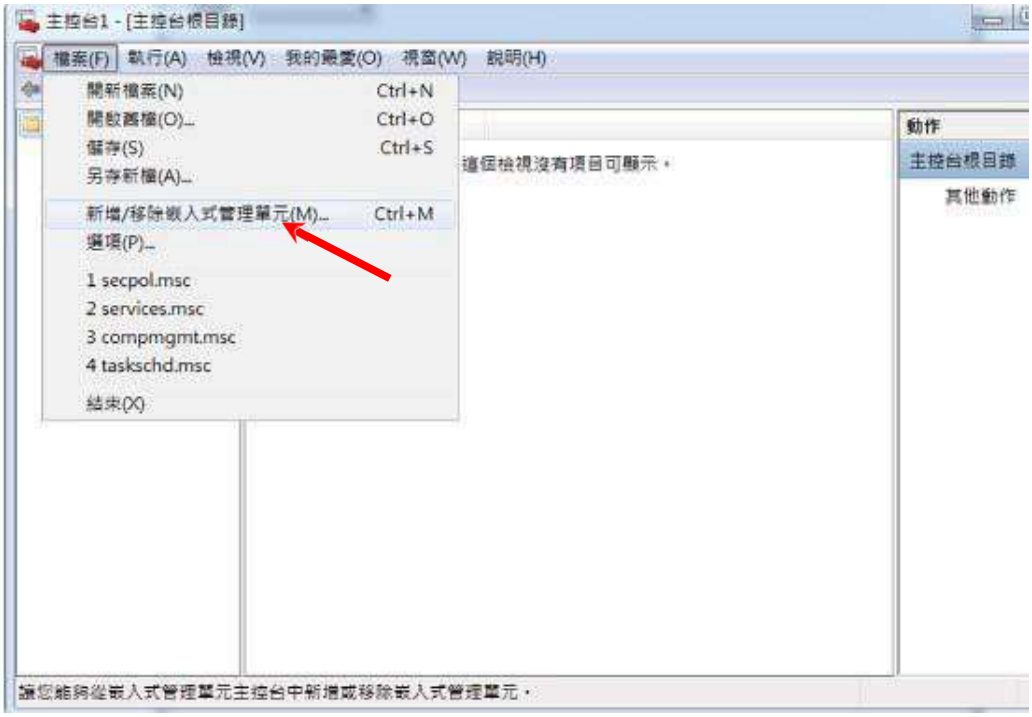
   http://www1.ecert.gov.hk/root/ecert_ssl_ca_3-17_pem.crt

   安装由根源证书 GlobalSign Root CA - R3 签发的交叉证书"Hongkong Post Root CA 3"。
   下载地址如下：
   http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt
3. *安装由根源证书 Root CA3 签发的中继证书"Hongkong Post e-Cert EV SSL CA 3 - 17"。下载地址如下：*

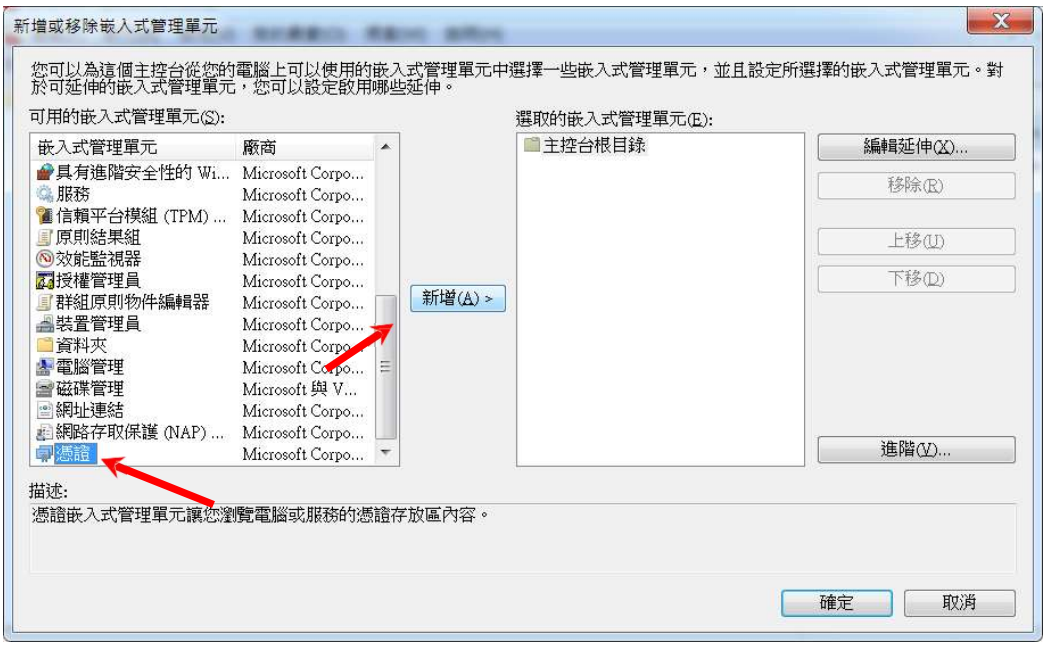
   http://www1.ecert.gov.hk/root/ecert_ev_ssl_ca_3-17_pem.crt
   安装由根源证书 GlobalSign Root CA - R3 签发的交叉证书"Hongkong Post Root CA 3"。
   下载地址如下：
   http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt

D. 安装中继 / 交叉证书

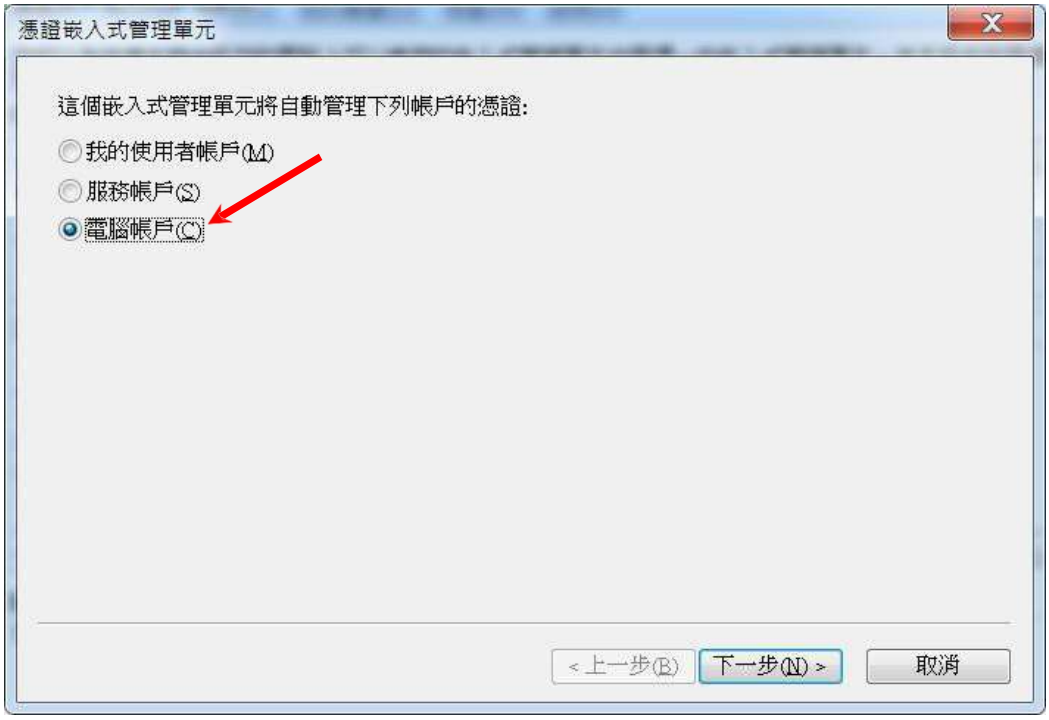
1. 按[开始]>[执行]，然后输入 “mmc” 及按[确定]来启动 MicrosoftManagement Console (MMC)，然后从[档案]选单中选取[新增/移除嵌入式管理单元]。



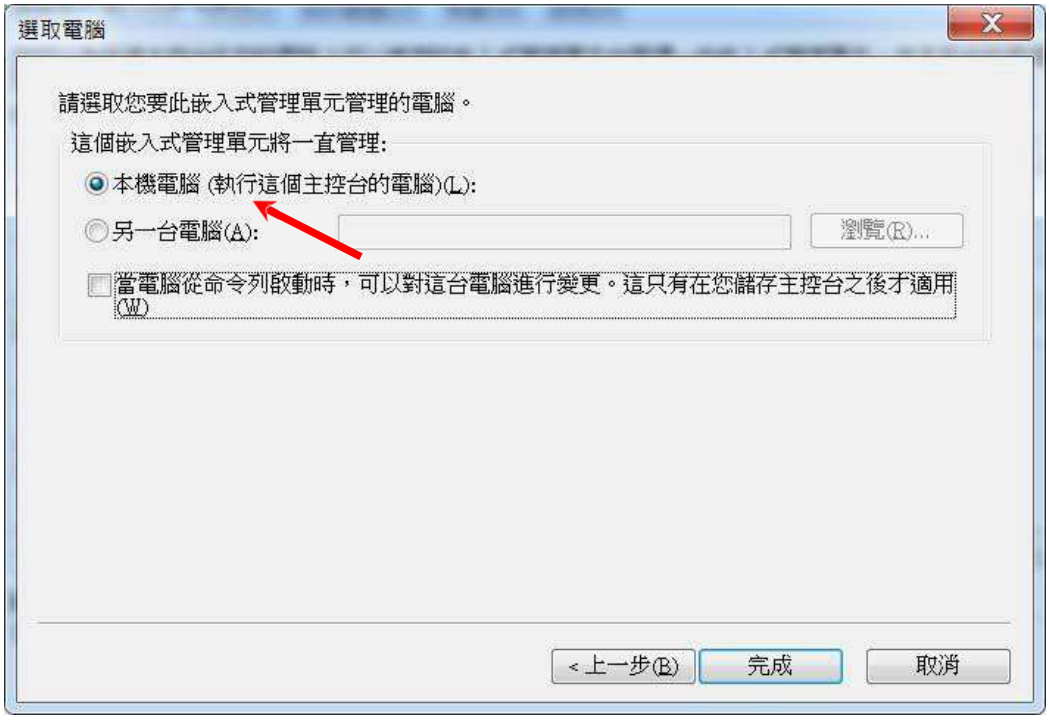
2. 选择[凭证]，然后按[新增]。



3. 选择[电脑帐户]，然后按[下一步]。



4. 选择[本机电脑]，然后按[完成]。

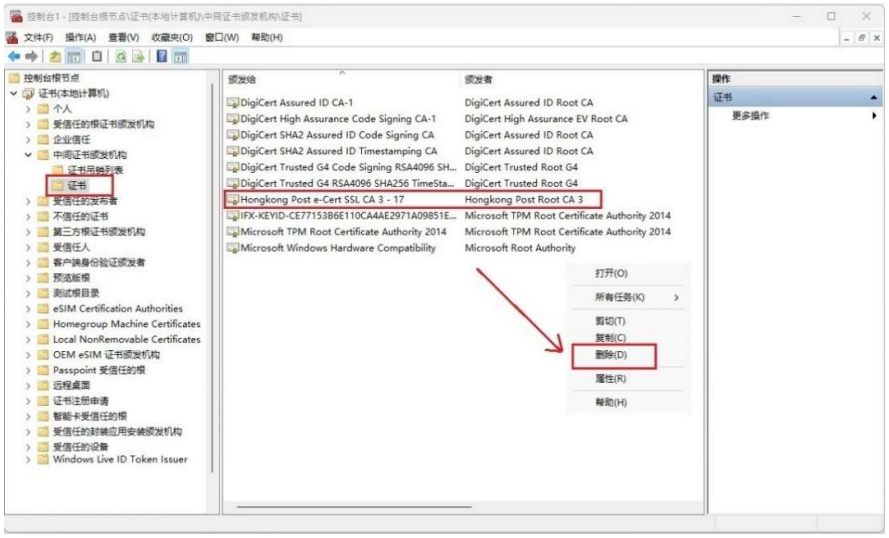


以下内容以 “Hongkong Post e-Cert SSL CA 3 - 17” 中继证书为例子。

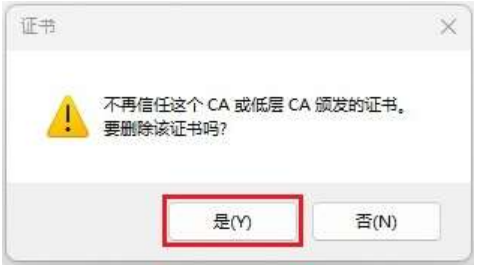
*注意：由2025年5月1日起，电子证书（服务器）会以新中继证书签发。在安装 2025年5月1日或之后发出的电子证书（伺服器）时，**请先移除旧有中继证书（如适用），然后在相关伺服器上安装新的中继证书**。*

移除旧有中继证书（如适用）

展开[中继证书颁发机构]，选择[证书]，及以滑鼠右键按一下旧有中继证书[Hongkong Post e-Cert SSL CA 3 - 17]，然后选择[删除]。



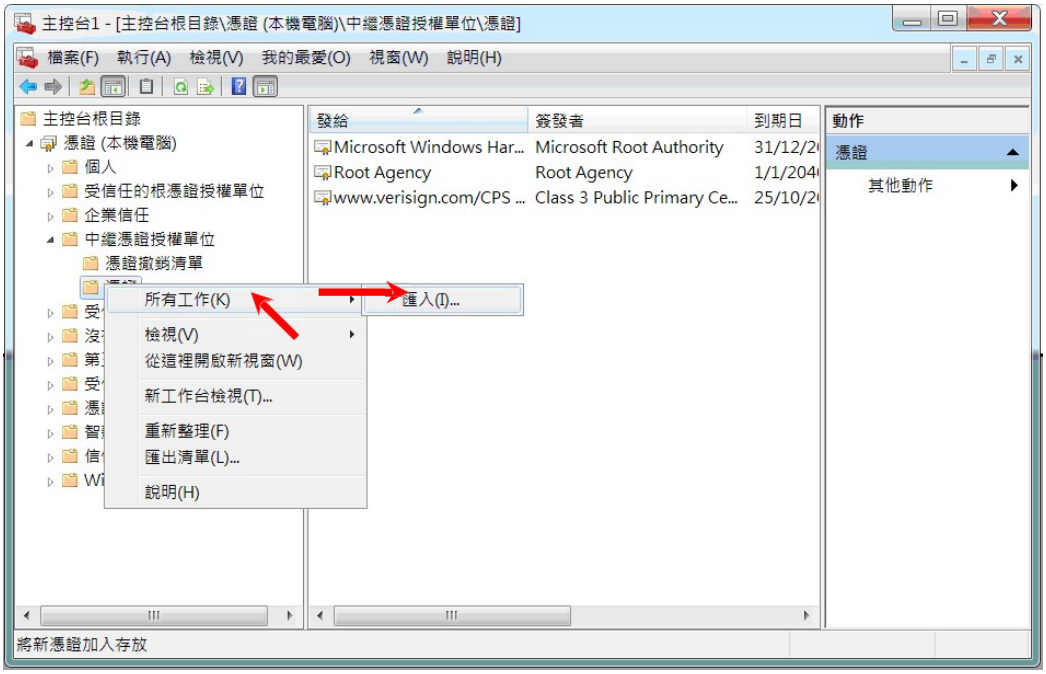
选择[是]确定删除。



以下内容以 “Hongkong Post e-Cert SSL CA 3 - 17” 中继证书为例子。

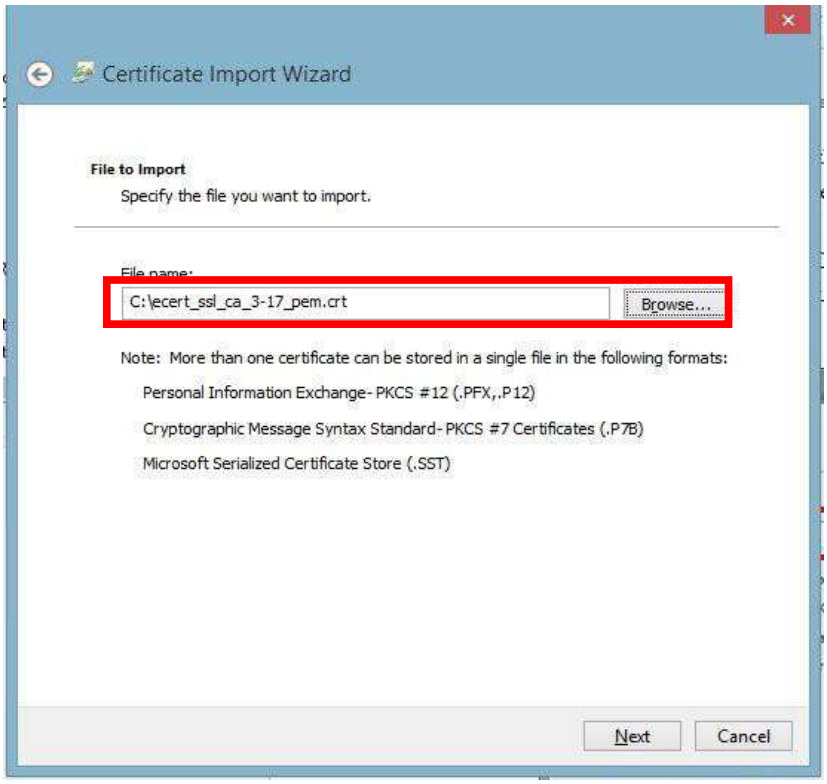
安装中继 / 交叉证书

5. 展开[中继凭证授权单位]及以滑鼠右键按一下[凭证]，然后选择[所有工作]>[汇入]。

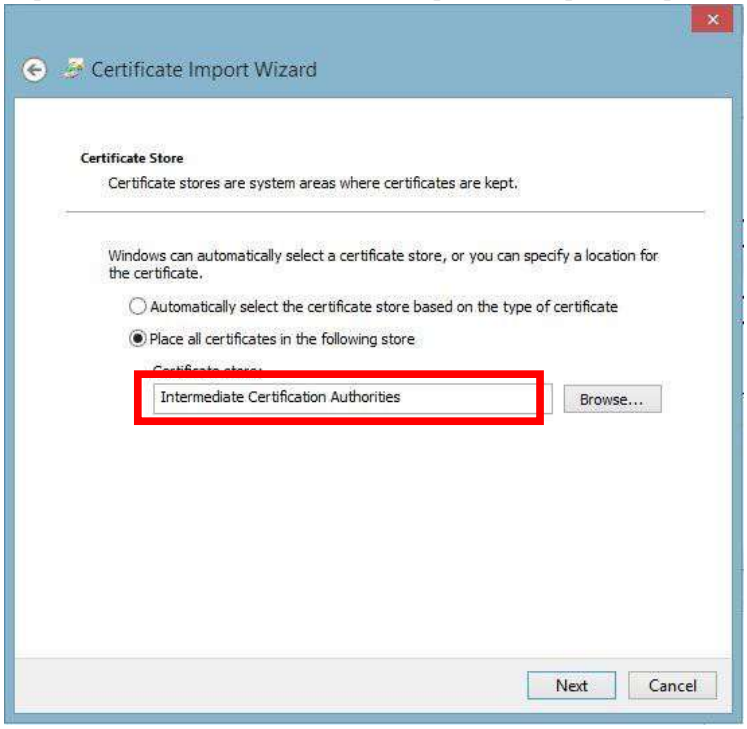


6. 在[凭证汇入精灵]内，按[下一步]继续。

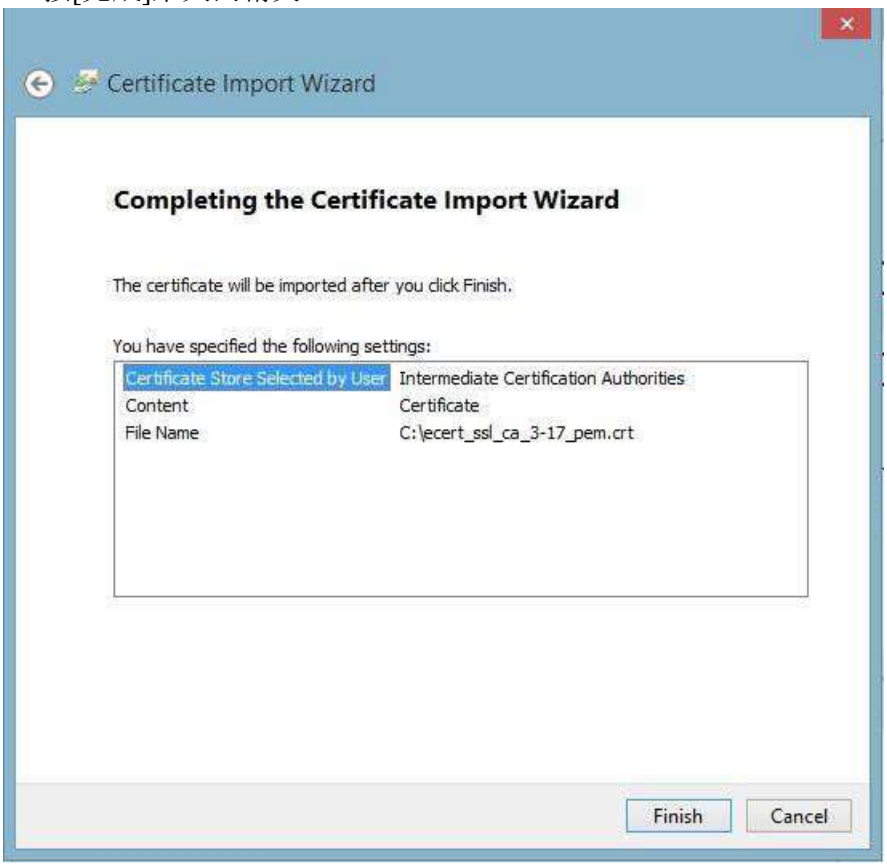
7. 按[浏览]指定早前于 C 部的步骤 7 下载的 **Hongkong Post e-Cert SSL CA 3 - 17** 中继证书 (ecert_ssl_ca_3-17_pem.crt)，然后按[下一步]。



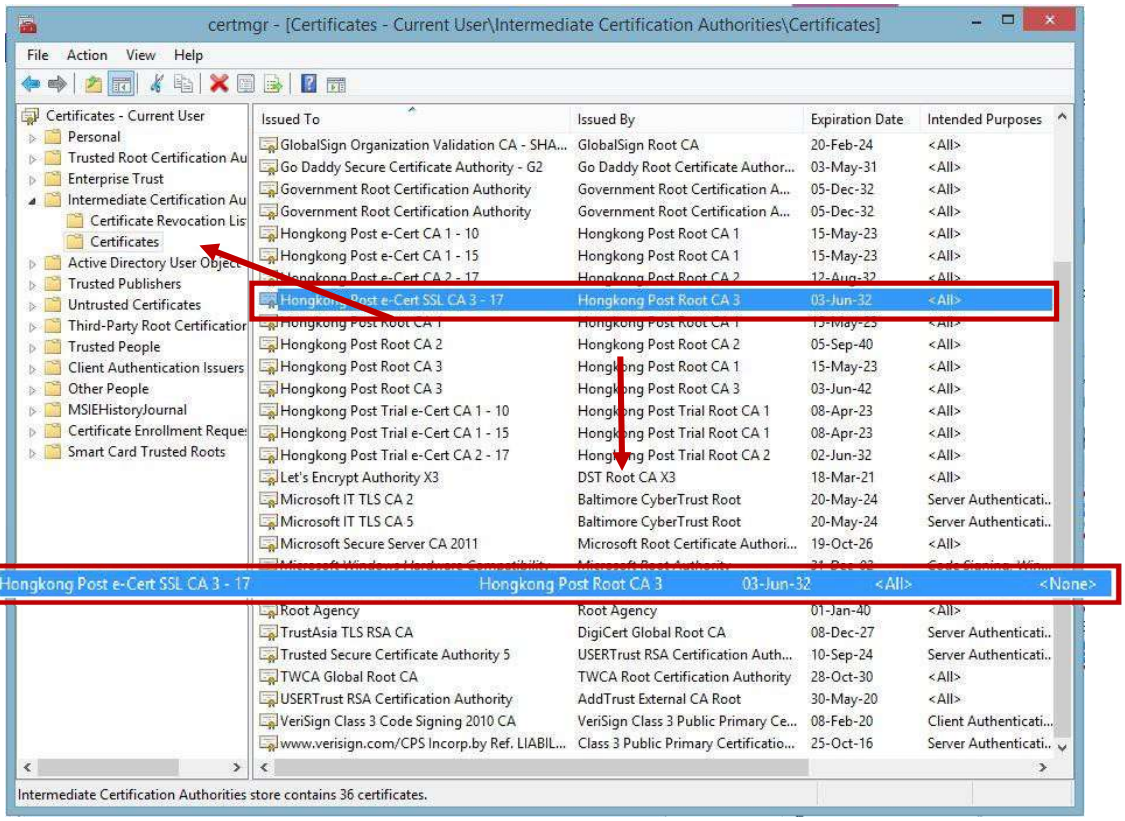
8. 选择[将所有凭证放入以下的存放区]，然后按[下一步]。



9. 按[完成]来关闭精灵。



10. 按[确定]来完成。

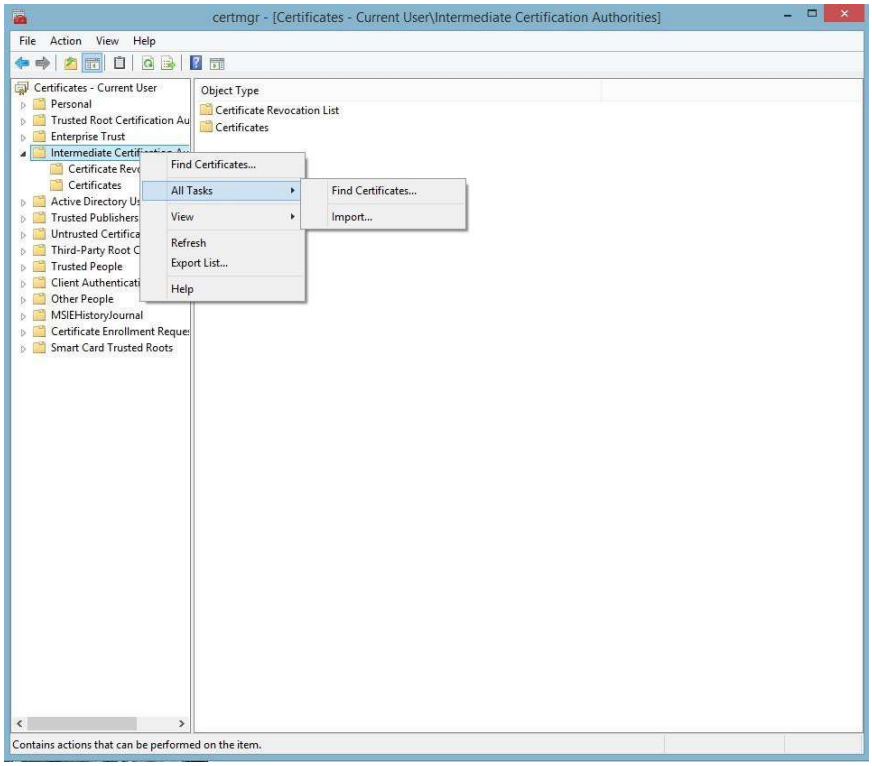


图表 1: “Hongkong Post e-Cert SSL CA 3 - 17” 中继证书已成功安装

重复步骤 5 到步骤 10 以安装通过 C 部分步骤 7 下载的交叉证书 (root_ca_3_x_gsca_r3_pem.crt)。

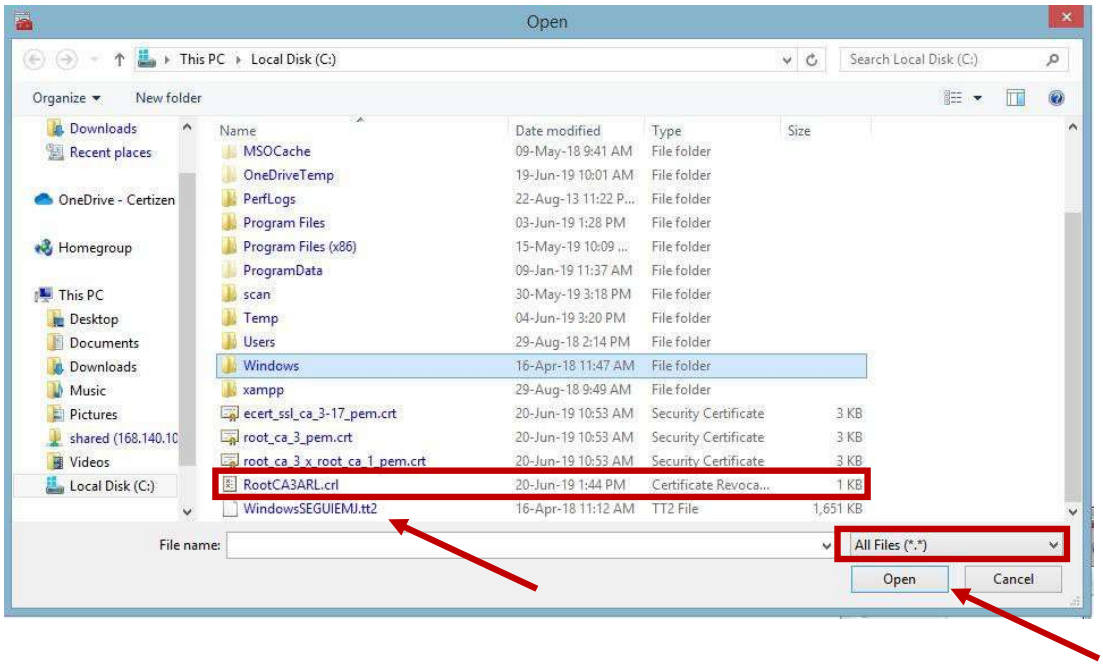
安装授权撤销清单(ARL)

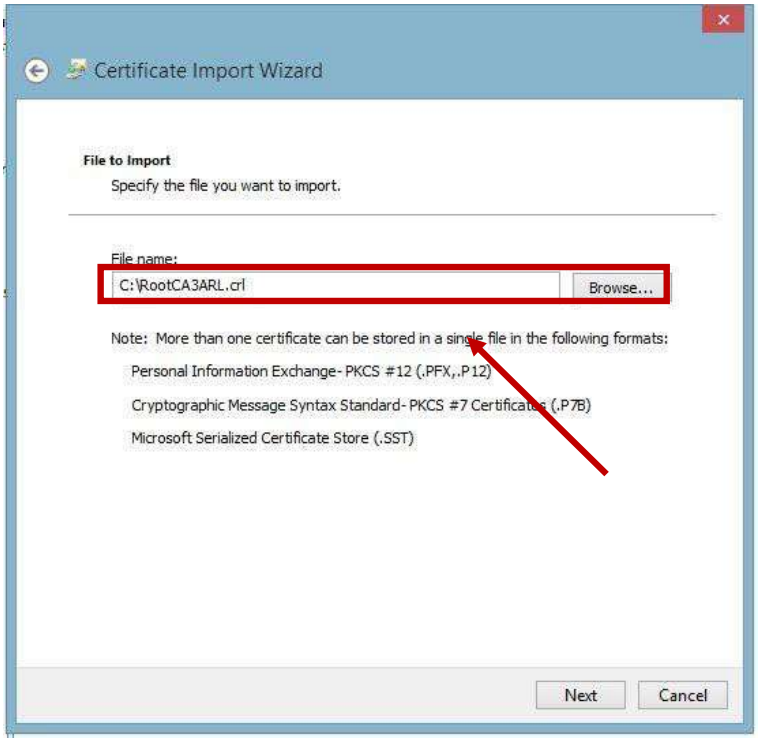
11. 下载**授权撤销清单(ARL)**：http://crl1.eCert.gov.hk/crl/RootCA3ARL.crl
12. 展开[中继凭证授权]及以滑鼠右键按一下，然后选择[所有工作]>[汇入]。



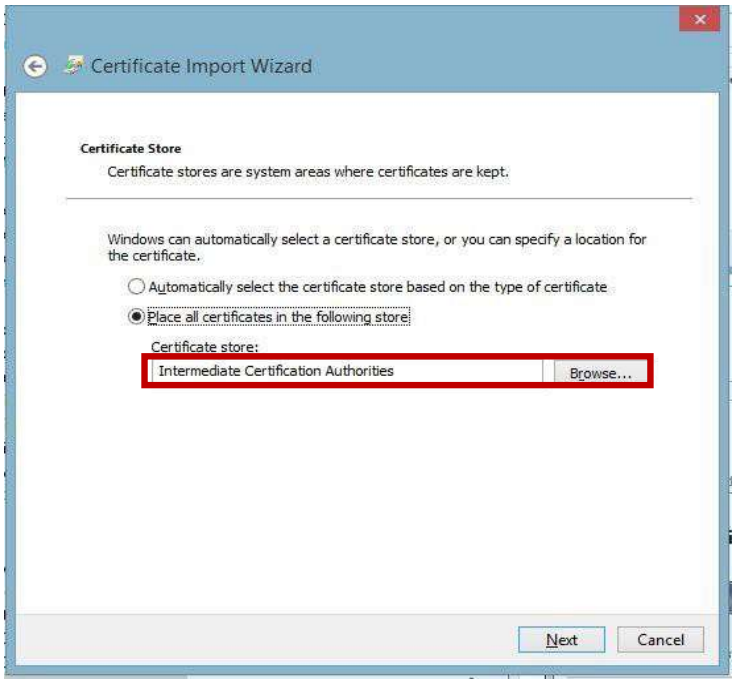
13. 在[凭证汇入精灵]内，按[下一步]继续。

14. 按[浏览]选择早前于步骤 11 下载的 “Hongkong Post Authority Revocation List (ARL)” 授权撤销清单 (RootCA3ARL.crl)，然后按[下一步]。(提示：选择 “所有档案”)

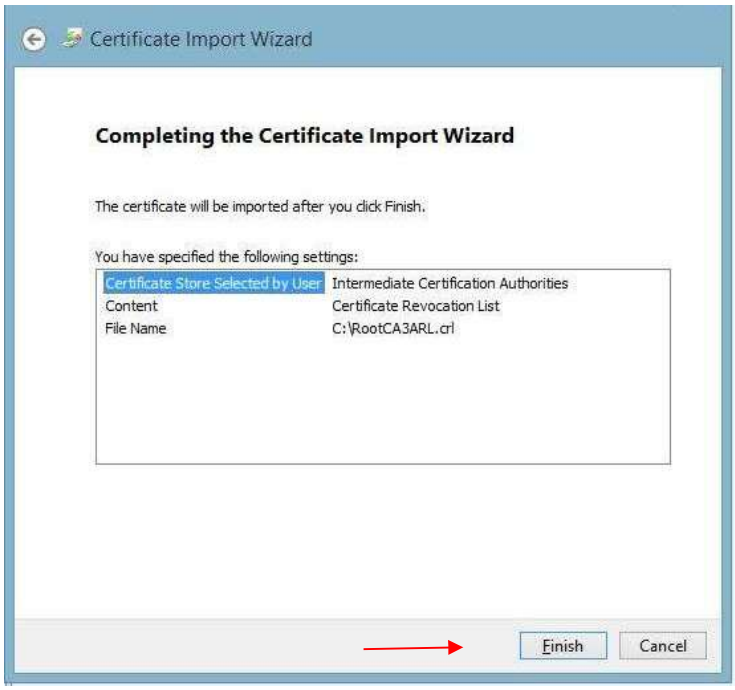




15. 选择[将所有凭证放入以下的存放区]，然后按[下一步]。



16. 按[完成]来关闭精灵。



17. 按[确定]来完成。

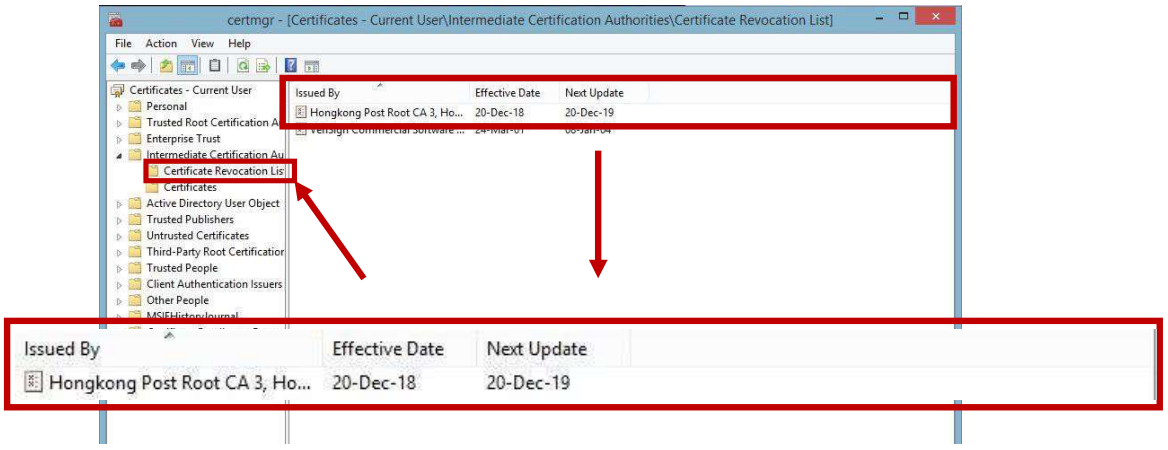
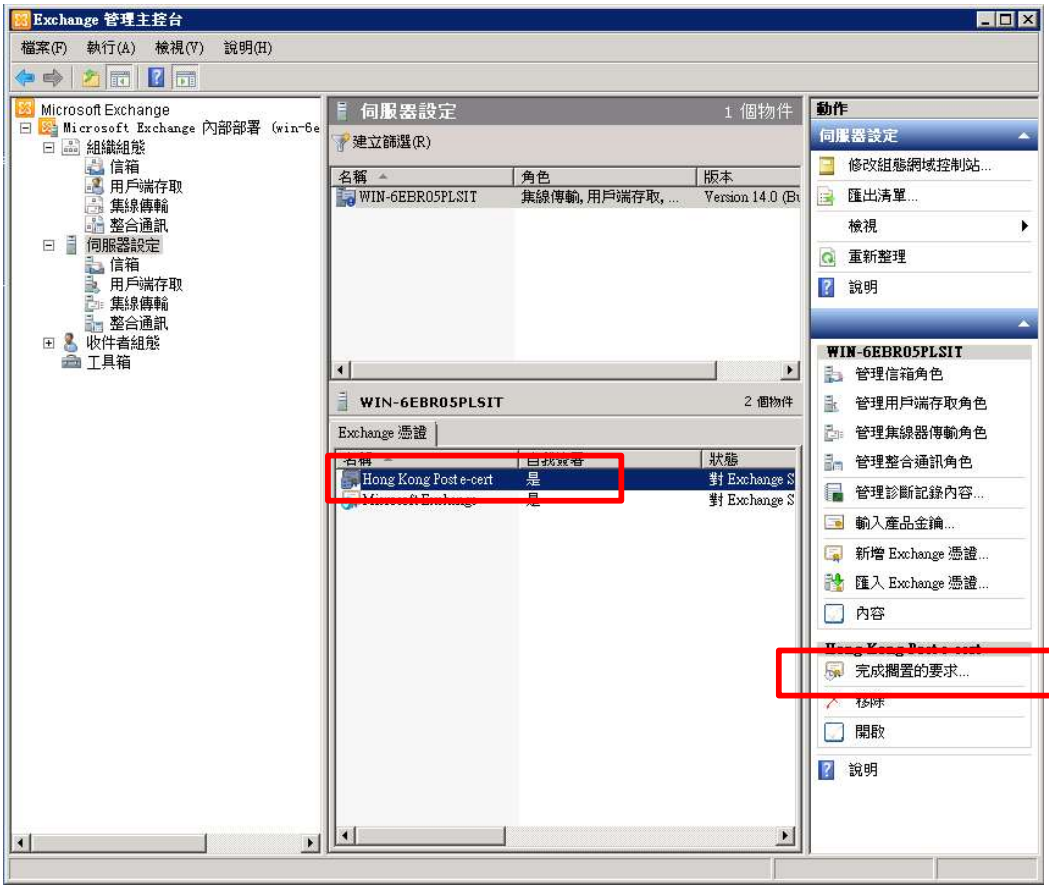


图 3:“Hongkong Post Authority Revocation List (ARL)” 授权撤销清单已成功安装

E. 安装伺服器证书

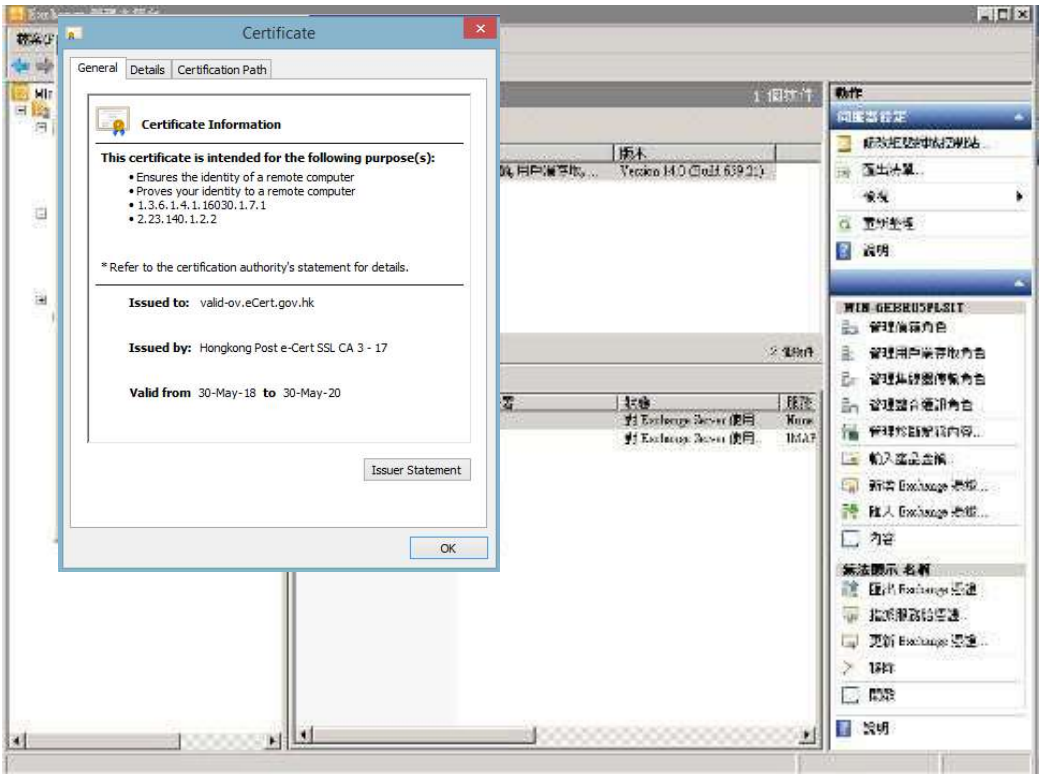
1. 在 [Exchange 管理主控台]视窗内，选择[伺服器设定]，然后选择您于步骤 B 中所申请的 Exchange 凭证。在右手边动作一栏内，按[完成搁置的要求]。



2. 按[浏览]选择早前于 C 部的步骤 7 下载的 “Hongkong Post e-Cert (Server)” 证书，然后按[完成]。

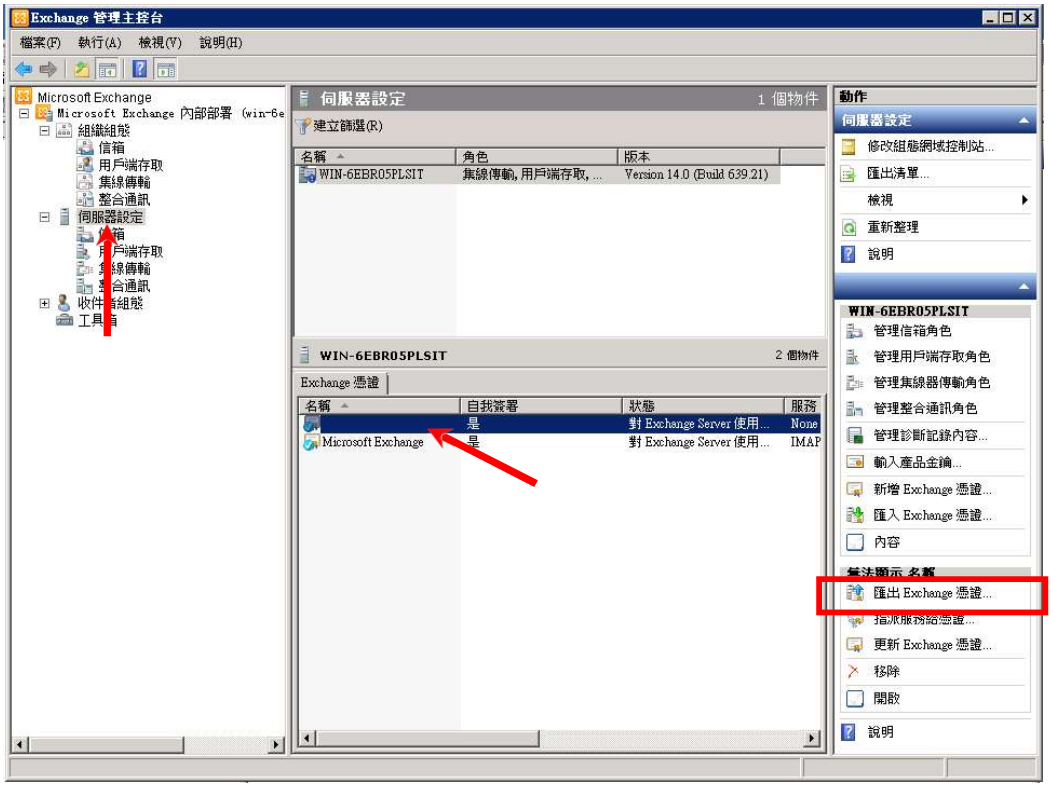
3. 按[完成]来结束凭证安装。

4. Hongkong Post 伺服器证书已经成功安装，你可以双击证书以察看证书资讯。



F. 备份密码匙

1. 在“Exchange 管理主控台”界面，按“伺服器设定”，选择您想要备份的密码匙。于右手边选项，选择“汇出 Exchange 凭证”。

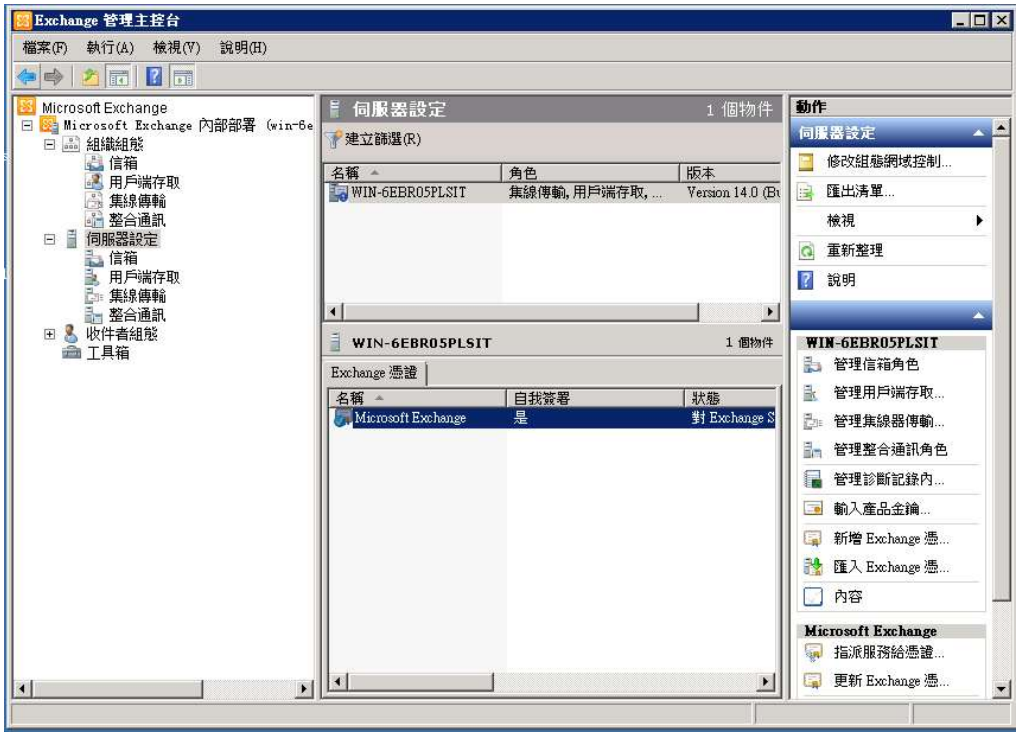


2. 选择存放名称及路径并输入密码（默认汇出文档格式为.PFX）。按[汇出]。

3. 按[完成]来结束汇出凭证，Hongkong Post e-cert 伺服器凭证已经成功汇出。

G. 还原密码匙

1. 在“Exchange 管理主控台”界面，按“伺服器设定”，于右手面选项， 选择“汇入 Exchange 凭证”。



2. 在“汇入 Exchange 凭证”界面中，选择包含输入包含凭证的档案名称 及路径及凭证的密码，然后按[下一步]来继续。

3. 选择相应的伺服器，并按[下一步]来继续。

4. 检查凭证相关资讯，并按[汇入]。

5. 按[完成]来结束汇入凭证，电子证书（伺服器）证书已成功汇入。