



电子证书（伺服器）用户指南

Microsoft IIS 5.0 / 6.0 适用
仅适用于 SHA-1 电子证书（伺服器）

目錄

A.	电子证书（伺服器）申请人指引	2
	新申请.....	3
	续期申请.....	4
B.	产生证书签署要求(CSR).....	5
	建立新伺服器证书.....	7
	更新目前的伺服器证书.....	13
C.	提交证书签署要求(CSR)	16
D.	安装香港邮政根源证书	20
	安装“Hongkong Post e-Cert CA 1 - 10”根源证书	23
	安装“Hongkong Post Root CA 1”根源证书	26
E.	安装伺服器证书	29
F.	备份密码匙	35
	在 IIS 5.0 上备份密码匙	35
	在 IIS 6.0 上备份密码匙	40
G.	还原密码匙	45
	在 IIS 5.0 上还原密码匙	45
	在 IIS 6.0 上还原密码匙	51

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，会向申请人（即获授权代表）发出主旨为“Submission of Certificate Signing Request (CSR)”的电子邮件，要求申请人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 2000 / 2003 上的 Microsoft IIS 5.0 / 6.0 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：

F. 备份密码匙	35
G. 还原密码匙	45

新申请

如阁下是首次申请电子证书（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).....	5
	建立新伺服器证书.....	7
C.	提交证书签署要求(CSR)	16
D.	安装香港邮政根源证书	20
	安装“Hongkong Post e-Cert CA 1 - 10”根源证书	23
	安装“Hongkong Post Root CA 1”根源证书	26
E.	安装伺服器证书	29

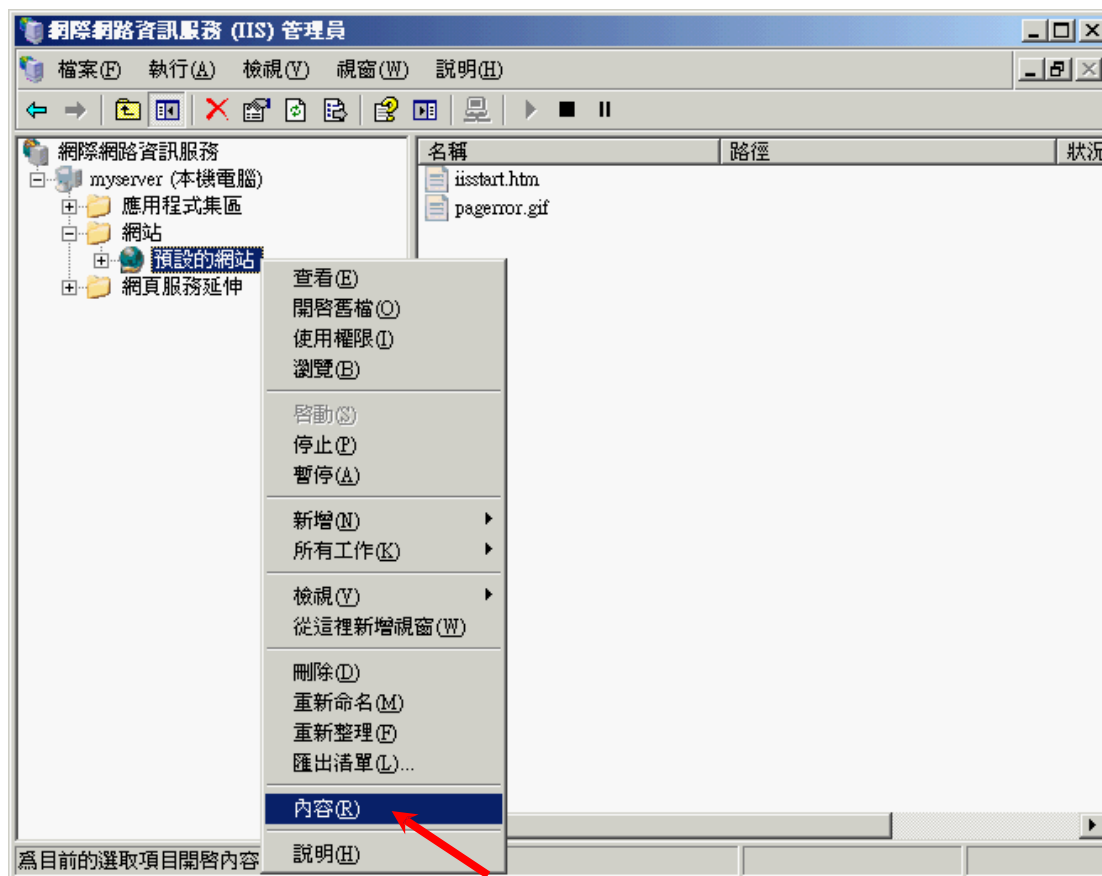
续期申请

如阁下正更新目前伺服器上的电子证书（伺服器），请参阅以下部分的详细步骤：

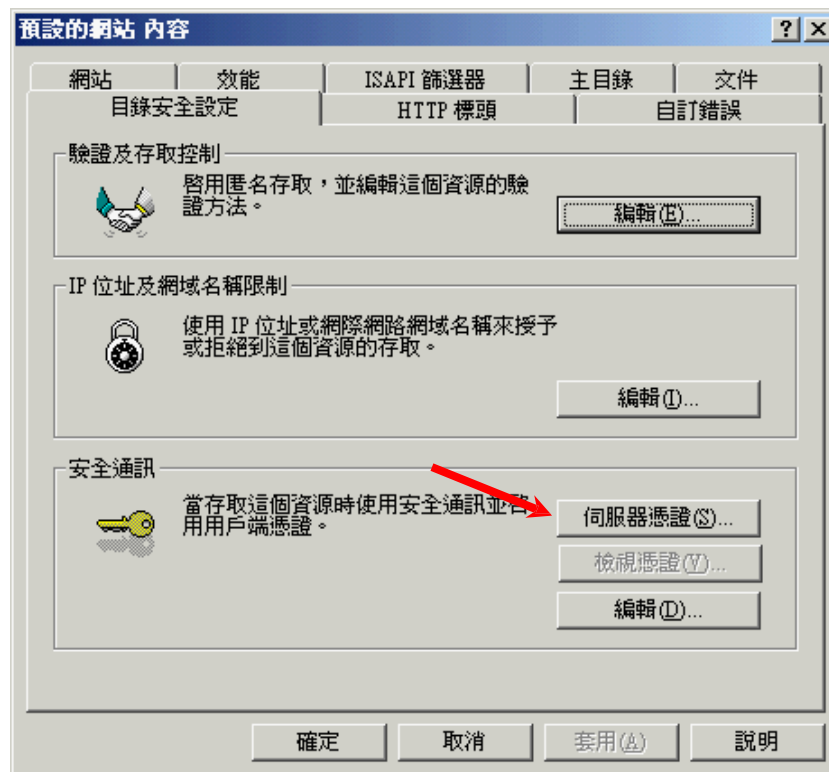
B. 产生证书签署要求(CSR).....	5
更新目前的伺服器证书.....	13
C. 提交证书签署要求(CSR).....	16
E. 安装伺服器证书	28

B. 产生证书签署要求(CSR)

1. 按 [开始] > [所有程式] / [程式集] > [系统管理工具] > [网际网路资讯服务 (IIS) 管理员] / [Internet 服务管理员]來启动网际网路资讯服务 (IIS) 管理员。
2. 在 [网际网路资讯服务 (IIS) 管理员] / [Internet Information Services]视窗内, 展开[网站]及选择您的网站, 以滑鼠右键按一下, 然后按[内容]。



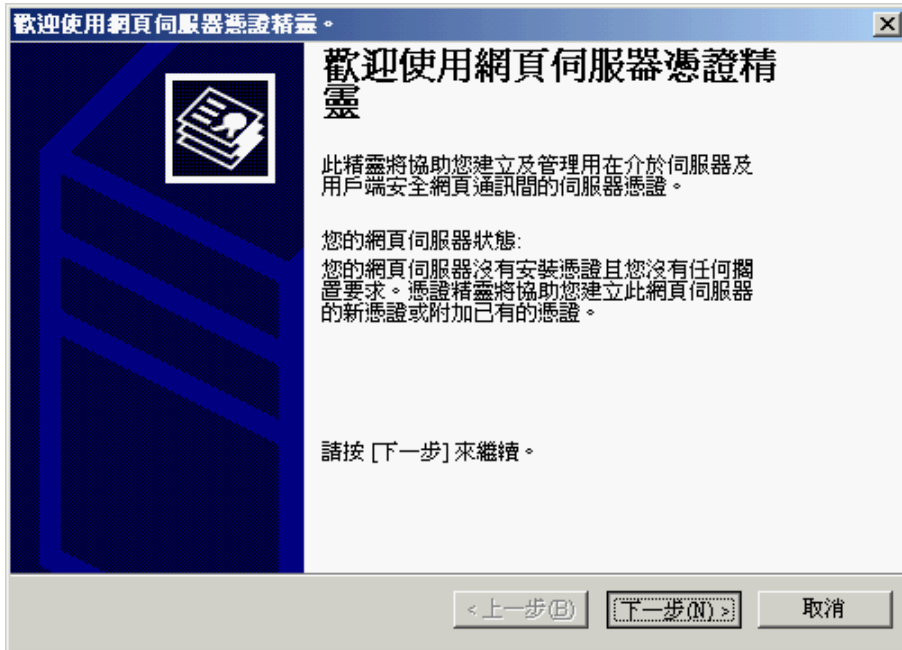
3. 在[目錄安全設定]索引標籤內，按一下[伺服器憑證]。



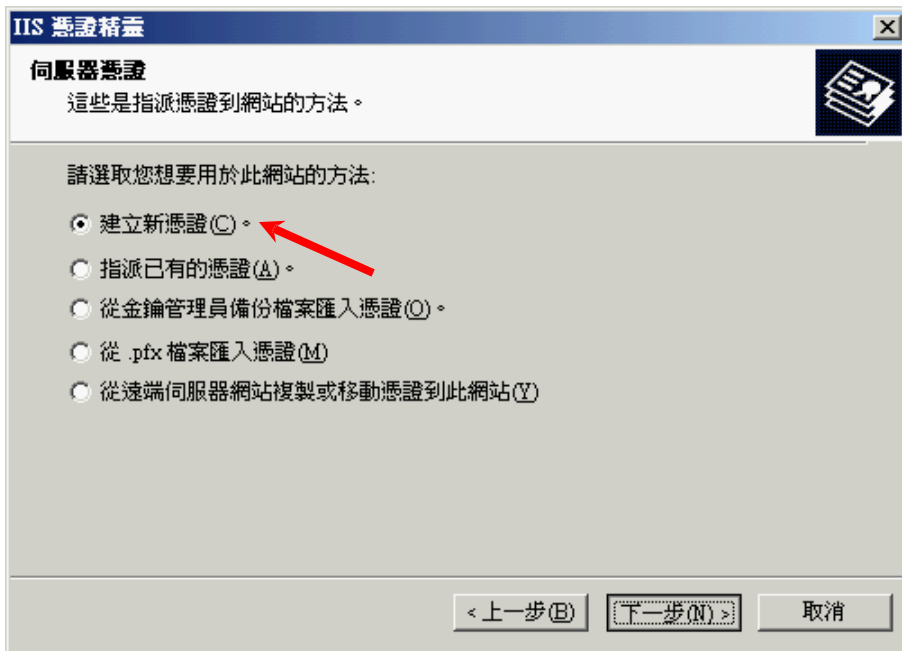
建立新伺服器证书

注意：如阁下正更新目前的伺服器证书，请跳到步骤 14。

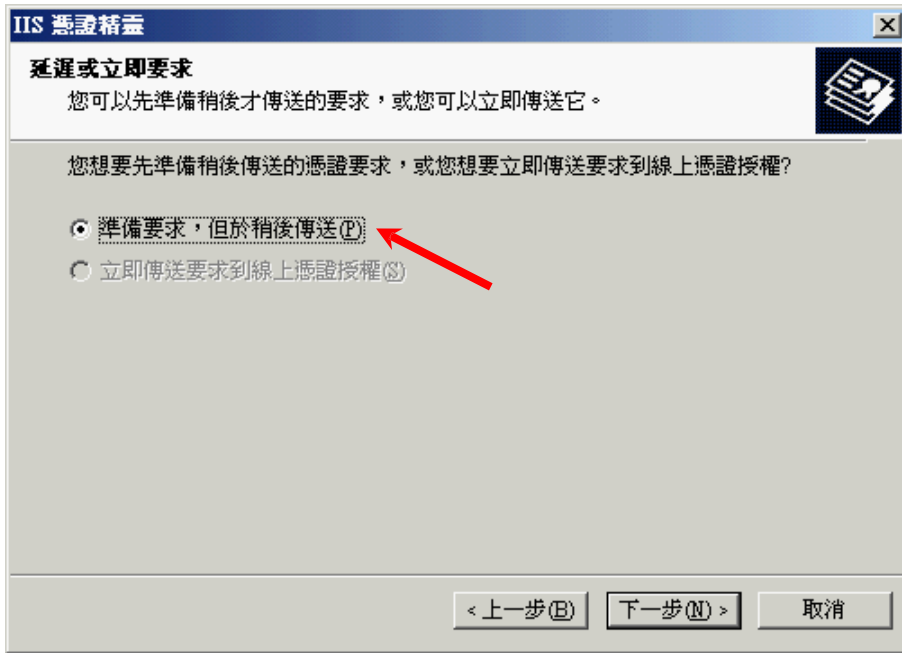
- 在[网页伺服器凭证精灵]内，按[下一步]继续。



- 选择[建立新凭证]，然后按[下一步]。

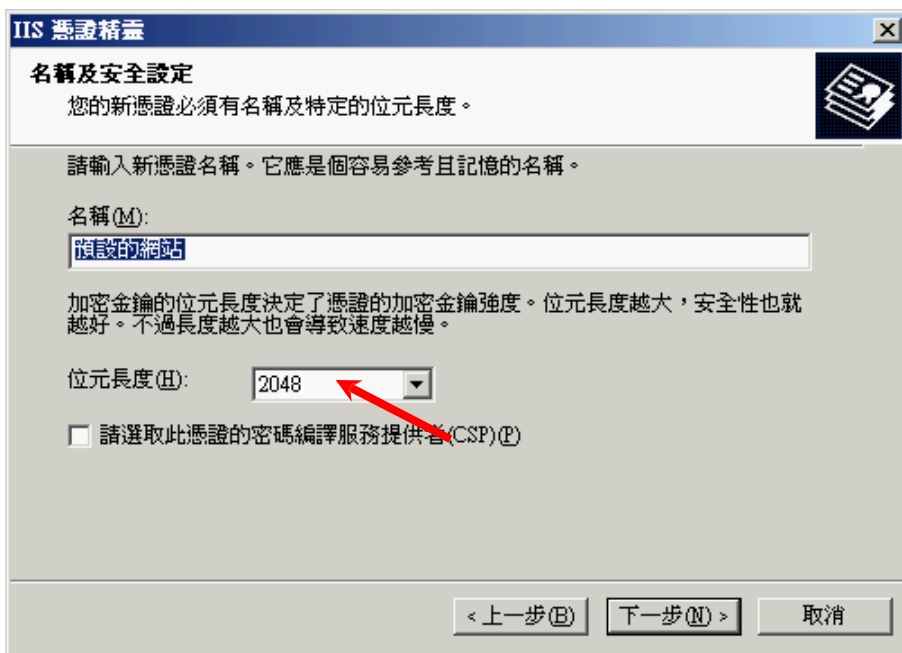


6. 选择[准备要求，但于稍后传送]，然后按[下一步]。

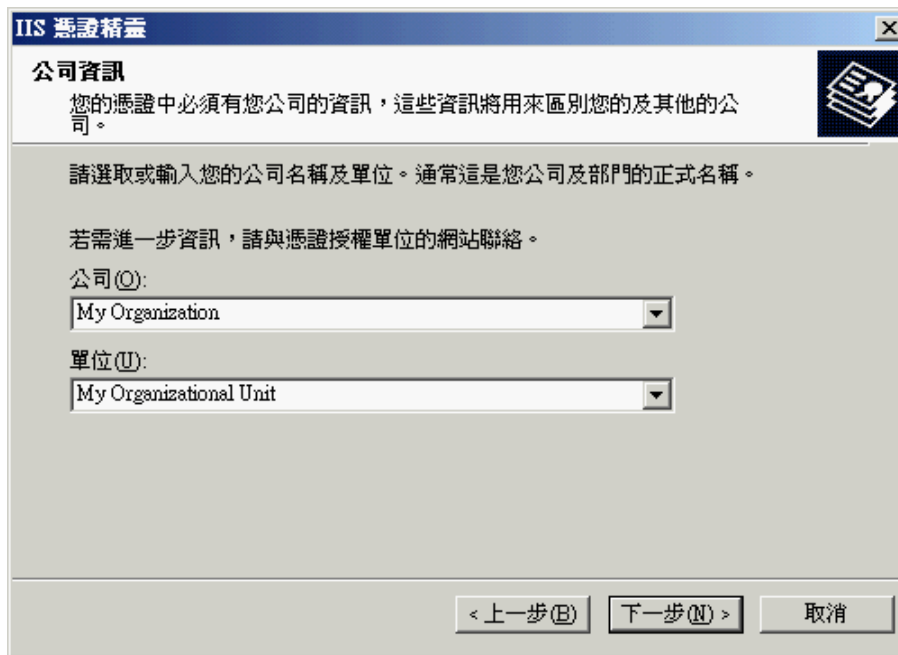


7. 输入新凭证名称（或接受预设）及选择 2048 作为密码匙的[位元长度]，然后按[下一步]。

注意：小于 2048 位元的密码匙或未能提供足够保密程度，相反大于 2048 位元有可能与某些浏览器不兼容。建议选择长度为 2048 位元的密码匙，从而提供较佳的保密程度。



8. 输入您的公司名称及单位，然后按[下一步]。



The screenshot shows a Windows dialog box titled "IIS 憑證精靈" (IIS Certificate Wizard). The current step is "公司資訊" (Company Information). The text inside the dialog reads: "您的憑證中必須有您公司的資訊，這些資訊將用來區別您的及其他的公司。" (Your certificate must contain information about your company, which will be used to distinguish your company from others.) Below this, it says: "請選取或輸入您的公司名稱及單位。通常這是您公司及部門的正式名稱。" (Please select or enter your company name and unit. This is usually the formal name of your company and department.) It then asks: "若需進一步資訊，請與憑證授權單位的網站聯絡。" (If you need more information, please contact the website of the certificate authority.) There are two dropdown menus: "公司(O):" (Company) with "My Organization" selected, and "單位(U):" (Unit) with "My Organizational Unit" selected. At the bottom, there are three buttons: "< 上一步(B)" (Previous), "下一步(N) >" (Next), and "取消" (Cancel).

9. 输入您网站的一般名称(即伺服器名称)，然后按[下一步]。

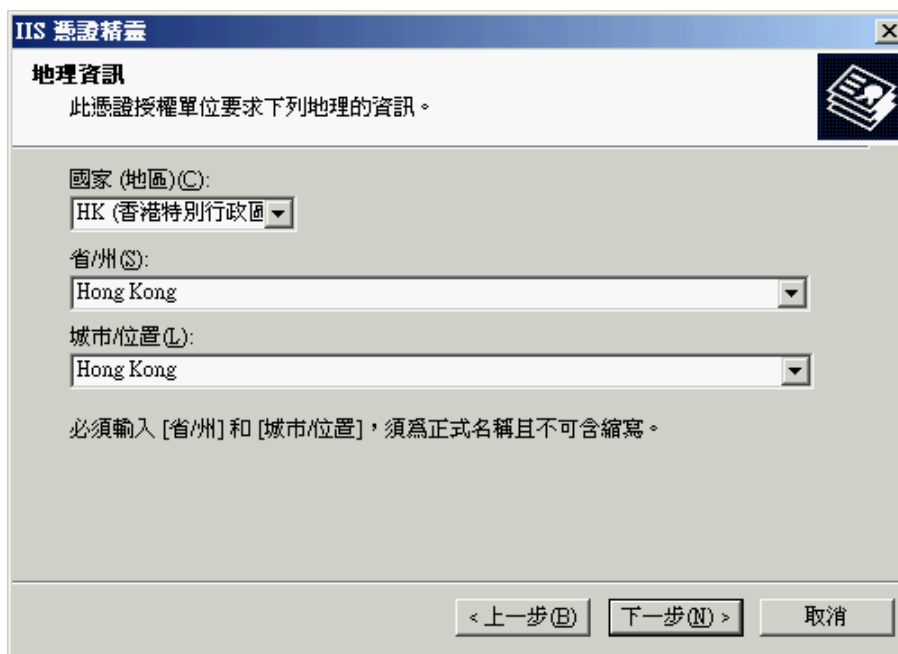
注意：若申请电子证书（伺服器）“多域版”，请在「一般名称」一欄中，输入与申请表格中所填写的「用作电子证书主体名称的伺服器名称」相同的登记伺服器名称。而「电子证书主体别名内的额外伺服器名称」，则无需在产生证书签署要求(CSR)过程中输入，香港邮政核证机关系统在签发证书时，会根据申请表格所申请的资料自动填写。

若申请电子证书（伺服器）“通用版”，请在「一般名称」一欄中，输入与申请表格中所填写的「有通配符的电子证书伺服器名称」相同的登记伺服器名称(伺服器名称的最左部份需包括有通配符「*」的部份)。例如 *.myserver.com。



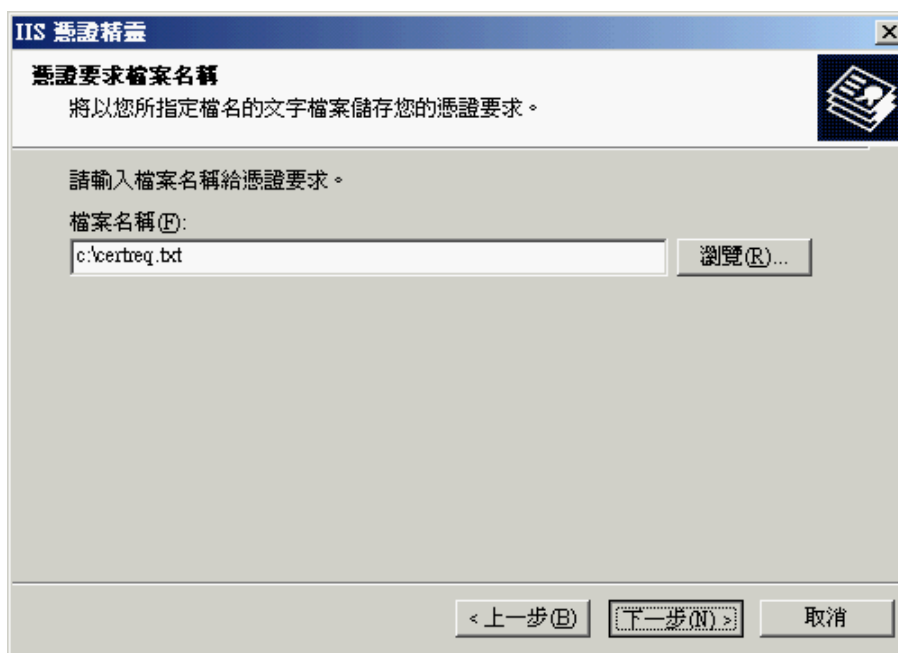
The screenshot shows a Windows dialog box titled "IIS 憑證精靈" (IIS Certificate Wizard). The current step is "您網站的一般名稱" (General Name of Your Site). The text inside the dialog reads: "您的網站的一般名稱是一個完全符合規定的網域名稱。" (The general name of your site is a domain name that fully complies with the specifications.) Below this, it provides instructions: "請為您的網站輸入一般名稱。若伺服器在網際網路上，請用有效的 DNS 名稱。若伺服器在近端內部網路上，您也許想用電腦的 NetBIOS 名稱。" (Please enter a general name for your site. If the server is on the Internet, use a valid DNS name. If the server is on a local intranet, you may want to use the computer's NetBIOS name.) A note states: "如果變更一般名稱，您將需要取得新的憑證。" (If you change the general name, you will need to obtain a new certificate.) There is a text input field labeled "一般名稱(C):" (General name(C):) containing the text "www.myserver.com". At the bottom, there are three buttons: "< 上一步(B)" (Previous Step), "下一步(N) >" (Next Step), and "取消" (Cancel).

10. 选择“HK (香港特别行政区)”作为[国家(地区)], 输入“Hong Kong”作为[省/州]/[州/省] 及[城市/位置], 然后按[下一步]。



The screenshot shows the 'IIS 憑證精靈' (IIS Certificate Wizard) window at the '地理資訊' (Geographic Information) step. The title bar reads 'IIS 憑證精靈'. The main heading is '地理資訊' with a sub-heading '此憑證授權單位要求下列地理的資訊。' (This certificate authority requires the following geographic information). There are three dropdown menus: '國家(地區)(C):' (Country/Region) set to 'HK (香港特別行政區)', '省/州(S):' (State) set to 'Hong Kong', and '城市/位置(L):' (City/Location) set to 'Hong Kong'. A note below the dropdowns states: '必須輸入 [省/州] 和 [城市/位置], 須為正式名稱且不可含縮寫。' (You must enter [State] and [City/Location], must be the full name and cannot contain abbreviations). At the bottom, there are three buttons: '< 上一步(B)' (Previous), '下一步(N) >' (Next), and '取消' (Cancel).

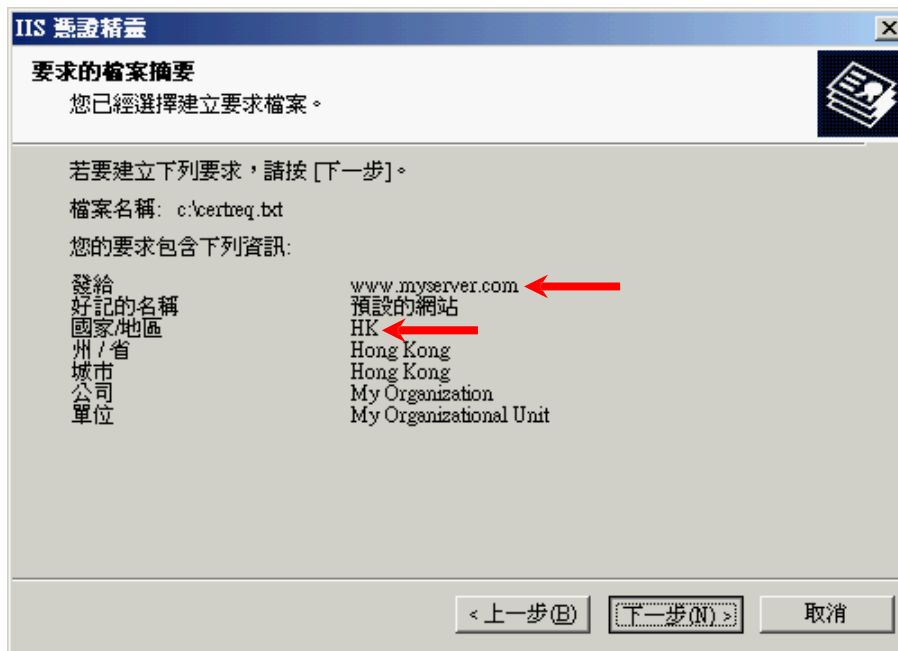
11. 输入凭证要求的档案名称, 然后按[下一步]。



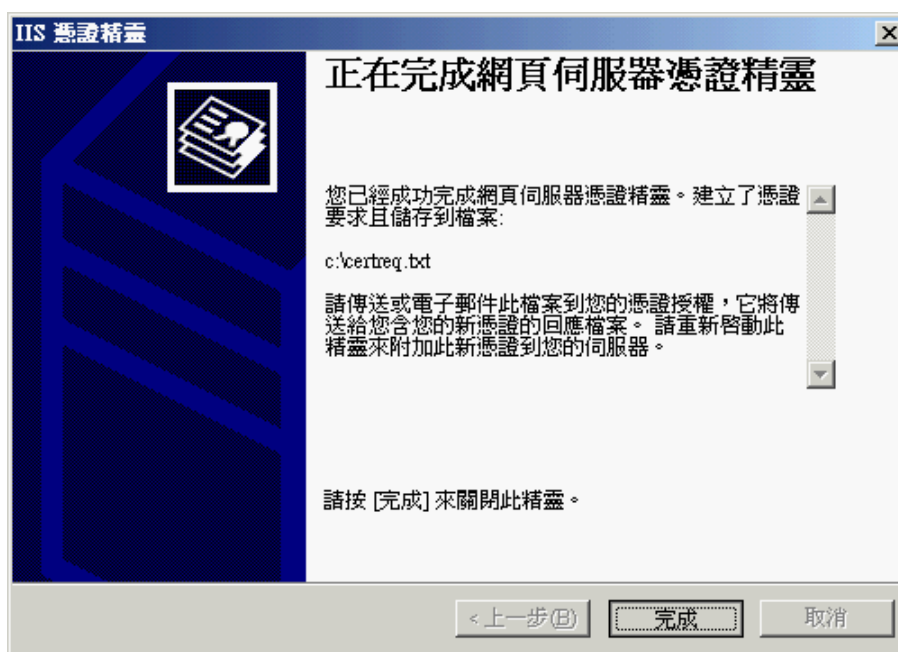
The screenshot shows the 'IIS 憑證精靈' (IIS Certificate Wizard) window at the '憑證要求檔案名稱' (Certificate Request File Name) step. The title bar reads 'IIS 憑證精靈'. The main heading is '憑證要求檔案名稱' with a sub-heading '將以您所指定檔名的文字檔案儲存您的憑證要求。' (Your certificate request will be stored in a text file with the name you specify). The instruction says '請輸入檔案名稱給憑證要求。' (Please enter the file name for the certificate request). There is a text input field labeled '檔案名稱(F):' (File Name) containing 'c:\certreq.txt' and a '瀏覽(R)...' (Browse...) button. At the bottom, there are three buttons: '< 上一步(B)' (Previous), '下一步(N) >' (Next), and '取消' (Cancel).

12. 按[下一步]。

注意：请确定于「发给」一欄显示正确的登记域名(即伺服器名称)及「国家(地区)」一欄显示「HK」。

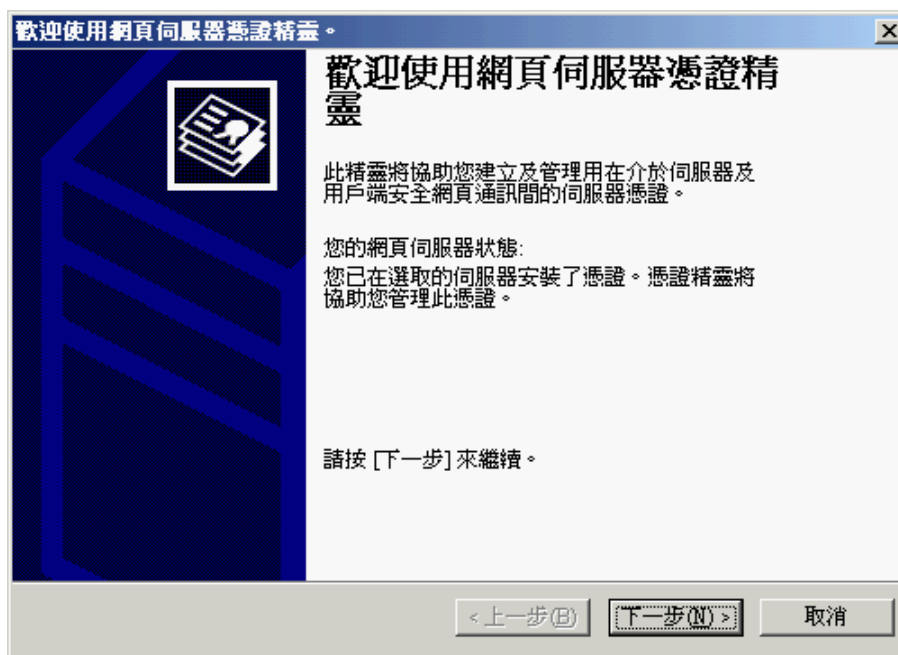


13. 按[完成]來关闭精靈。

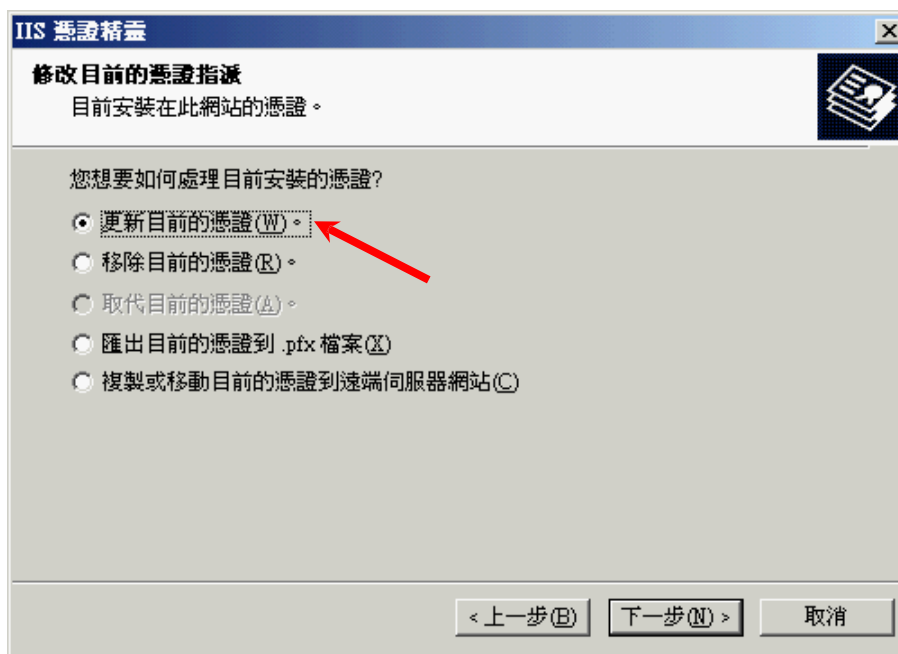


更新目前的伺服器证书

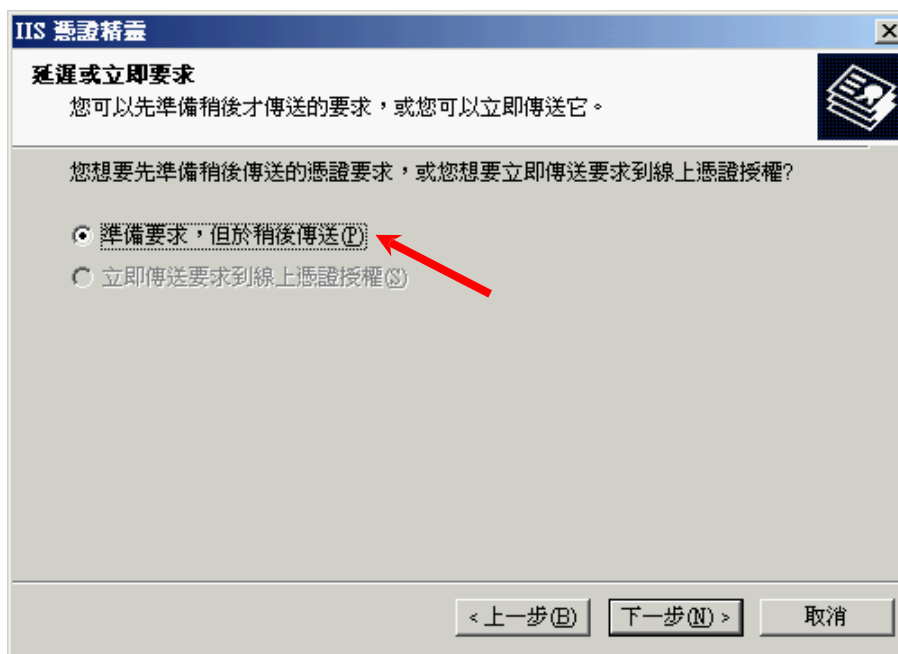
14. 在[网页伺服器凭证精灵]内，按[下一步]继续。



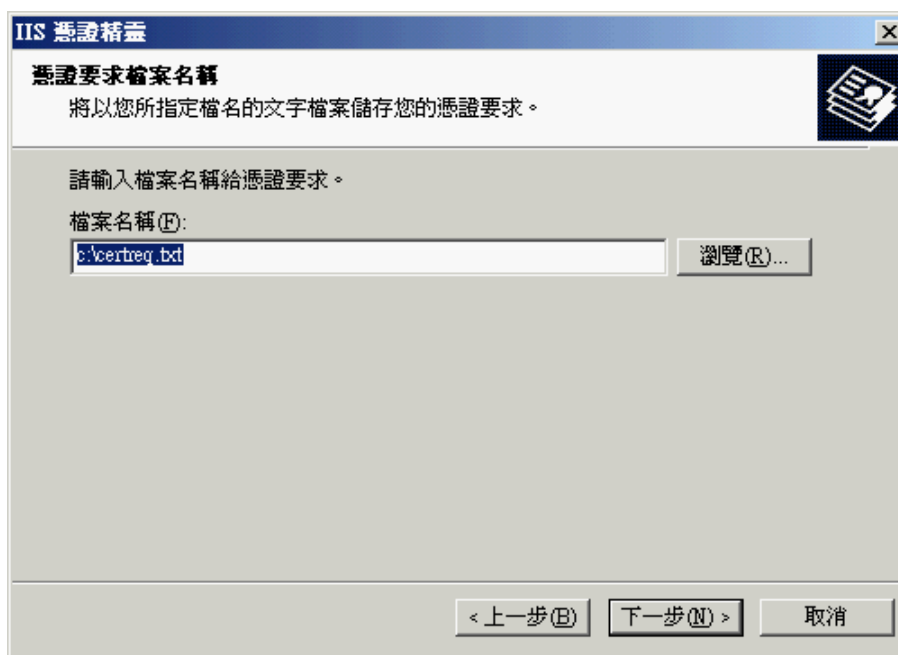
15. 选择[更新目前的凭证]，然后按[下一步]。



16. 选择[准备要求，但于稍后传送] / [准备要求，但稍后再传送]，然后按[下一步]。

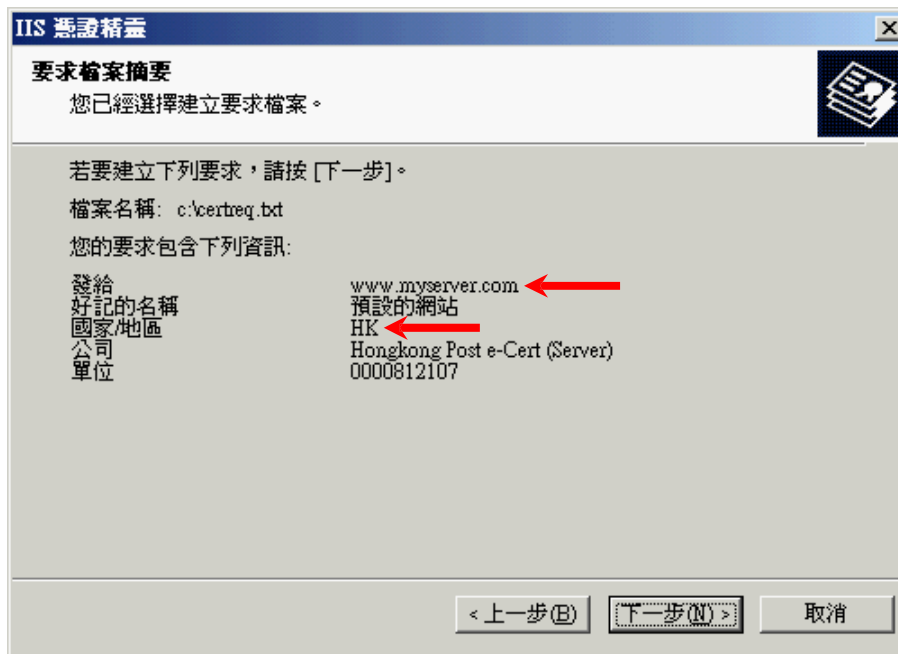


17. 输入凭证要求的档案名称，然后按[下一步]。

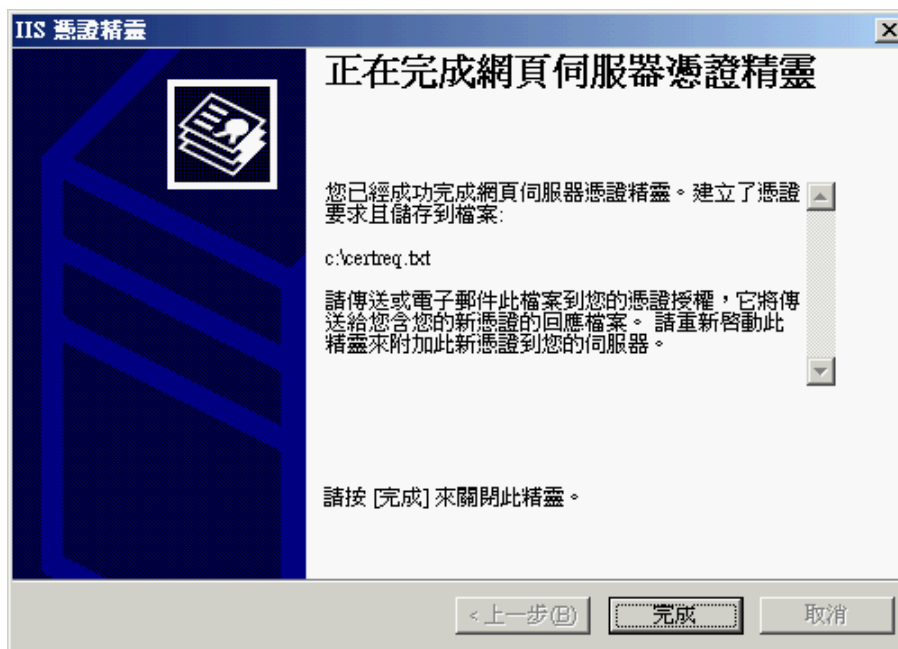


18. 按[下一步]。

注意：请确定于「发给」一欄显示正确的登记域名(即伺服器名称)及「国家(地区)」一欄显示「HK」。

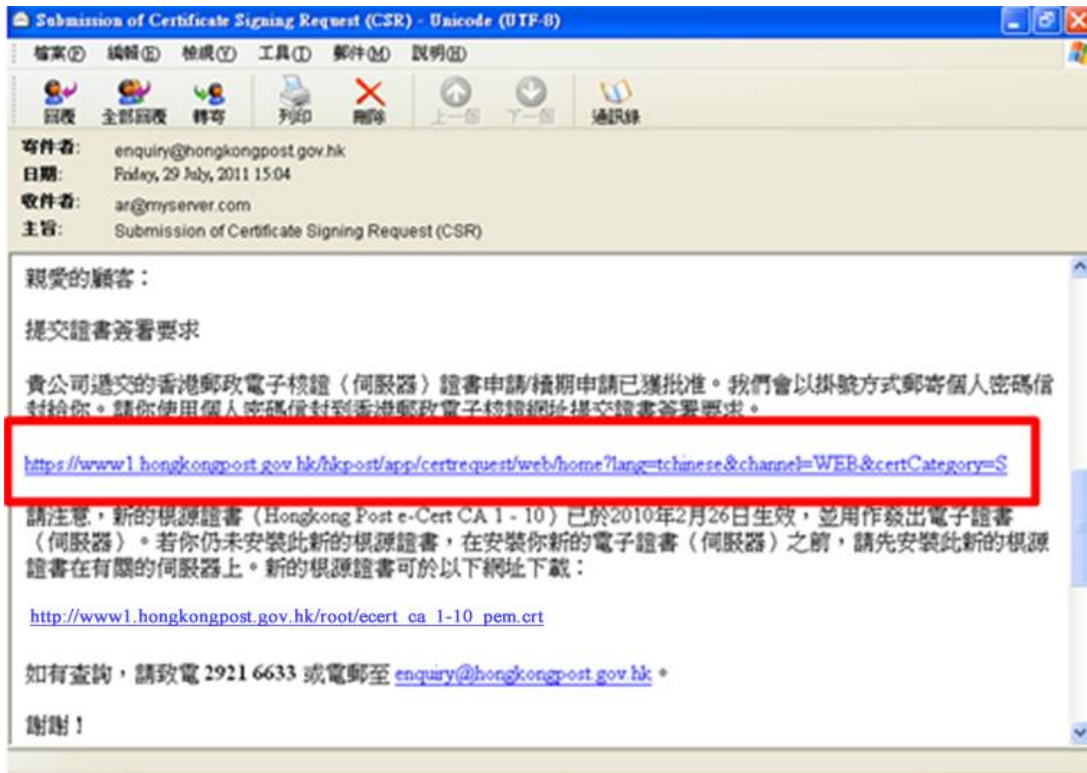


19. 按[完成]來关闭精靈。



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)”的电邮内按一下超連結以連線至香港邮政核证机关的网站。



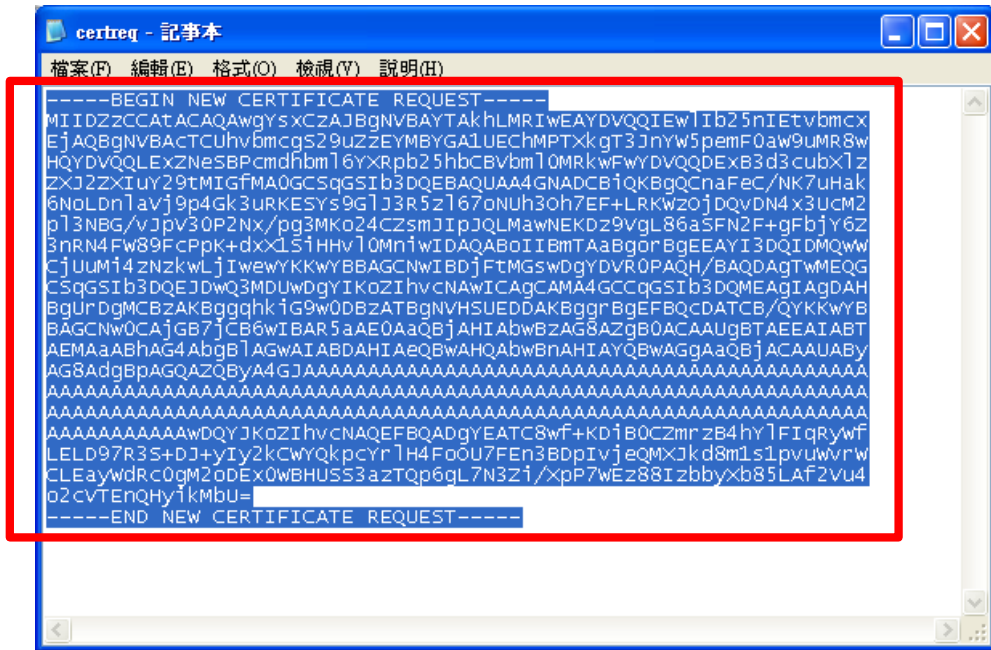
2. 輸入[伺服器名称]、印于密碼信封封面的[參考編號](九位數字)及印于密碼信封內的[電子證書密碼](十六位數字)，然後按[提交]。



- 按[提交]确认申请资料。(如发现资料不正确，请联络香港邮政核证机关。)



- 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----- ”。(您可参考 B 部的步骤 11 或步骤 17 的凭证要求档案的位置。)



5. 在方格内贴上内容，然后按[提交]。



6. 按[接受证书]确认接受此证书。



7. 分别下载以下证书：

- Hongkong Post e-Cert (Server)
- Hongkong Post e-Cert CA 1 - 10
- Hongkong Post Root CA 1

注意：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）。

<http://www.hongkongpost.gov.hk/sc>

注意：如“*Hongkong Post e-Cert CA 1 - 10*”根源证书及“*Hongkong Post Root CA 1*”根源证书已安装于伺服器上，您只需下载“*Hongkong Post e-Cert (Server)*”证书。



The screenshot shows the Hongkong Post e-Cert website interface. At the top, it says "The solution for e-Security" and "歡迎自製電子證書" (Welcome to self-made electronic certificates). Below that, it says "電子證書 (伺服器)" (Electronic certificates (server)). A red box highlights the section "你現可以:" (You can now:), which lists three items:

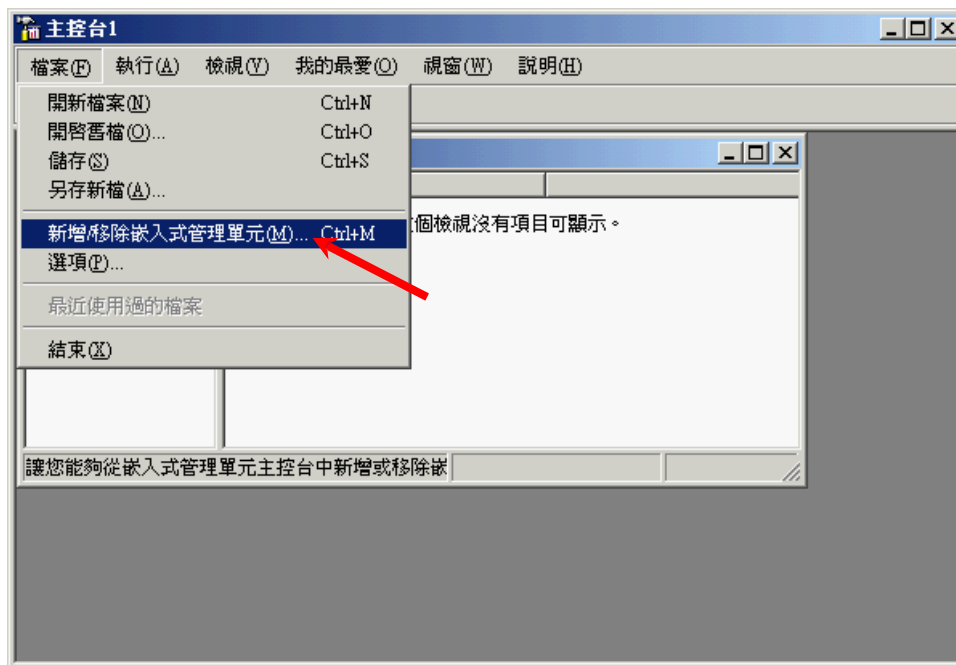
- 下載 "Hongkong Post e-Cert (Server)" 證書
- 下載 "Hongkong Post e-Cert CA 1 - 10" 根源證書
- 下載 "Hongkong Post Root CA 1" 根源證書

Below the list, there is a note in red text: "請注意，新的根源證書 (Hongkong Post e-Cert CA 1 - 10) 已於2010年2月26日生效，並用作發出電子證書 (伺服器)。若你仍未安裝此新的根源證書，在安裝你新的電子證書 (伺服器) 之前，請先安裝此新的根源證書在有關的伺服器上。"

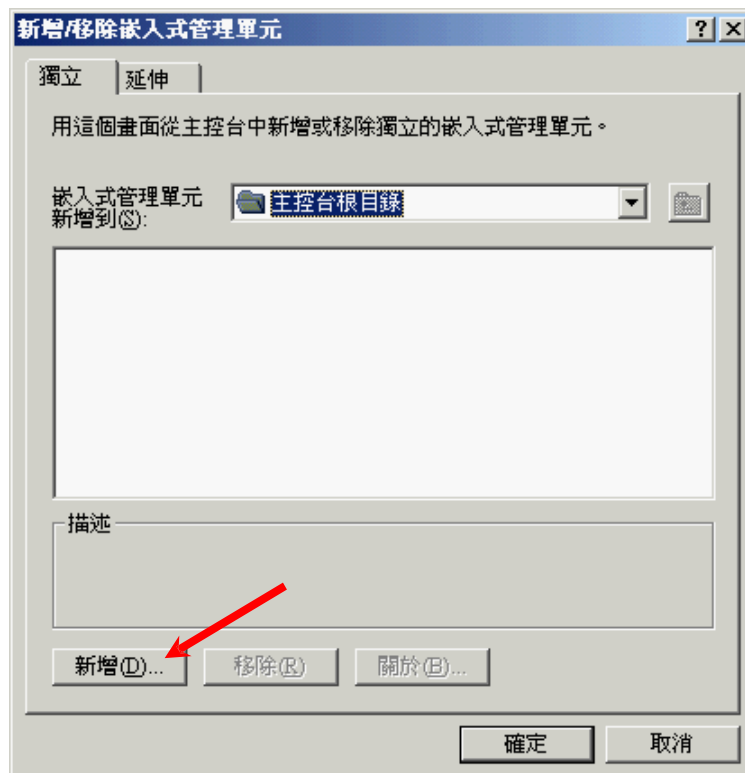
At the bottom of the page, it says "2007 © | 重要告示 | 私隱政策"

D. 安装香港邮政根源证书

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



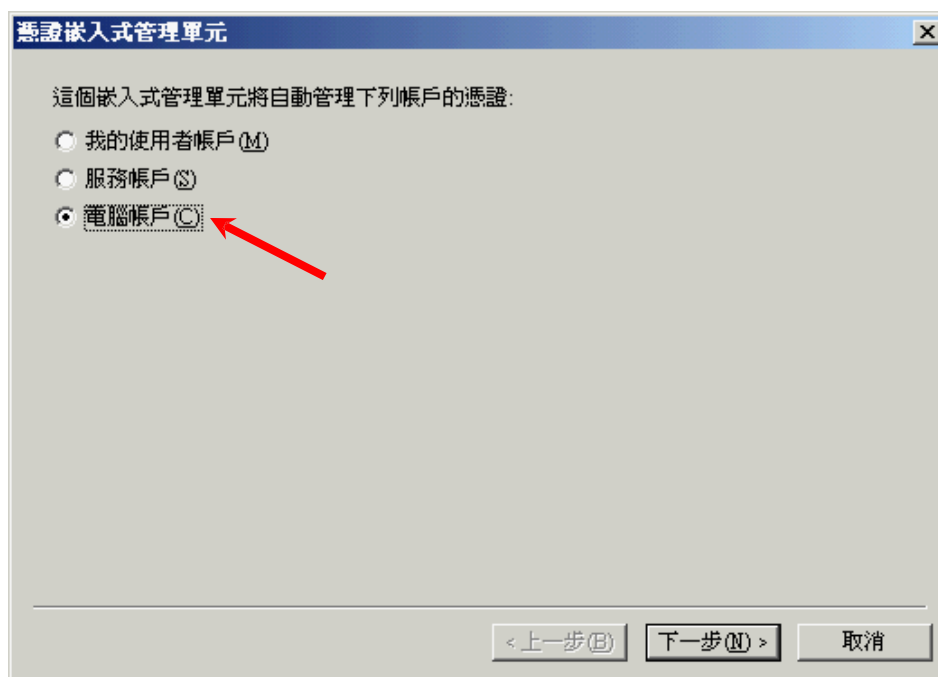
2. 按[新增]。



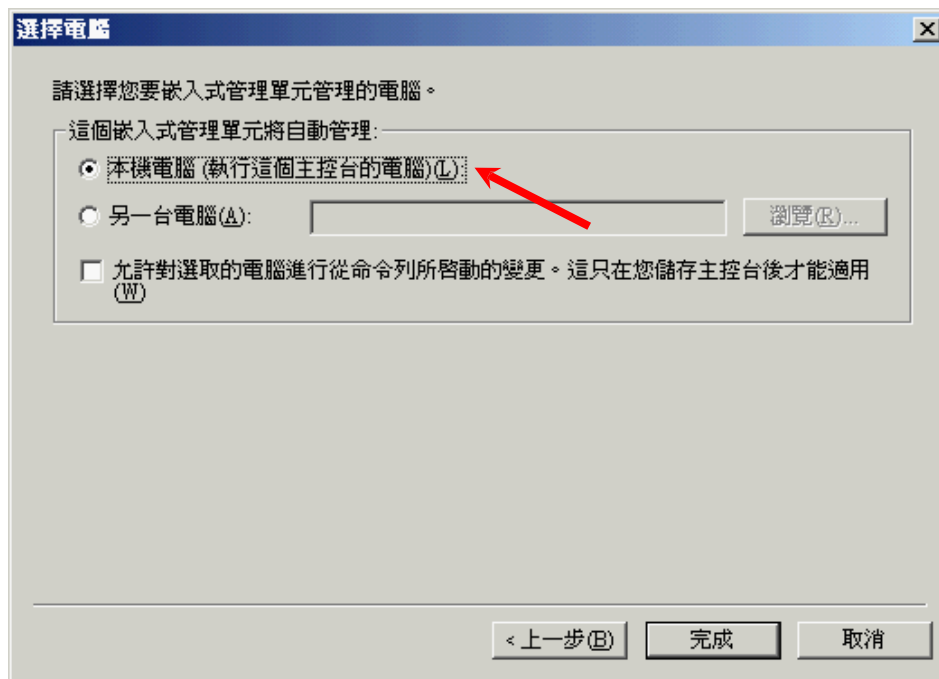
3. 选择[凭证], 然后按[新增]。



4. 选择[电脑帐户], 然后按[下一步]。



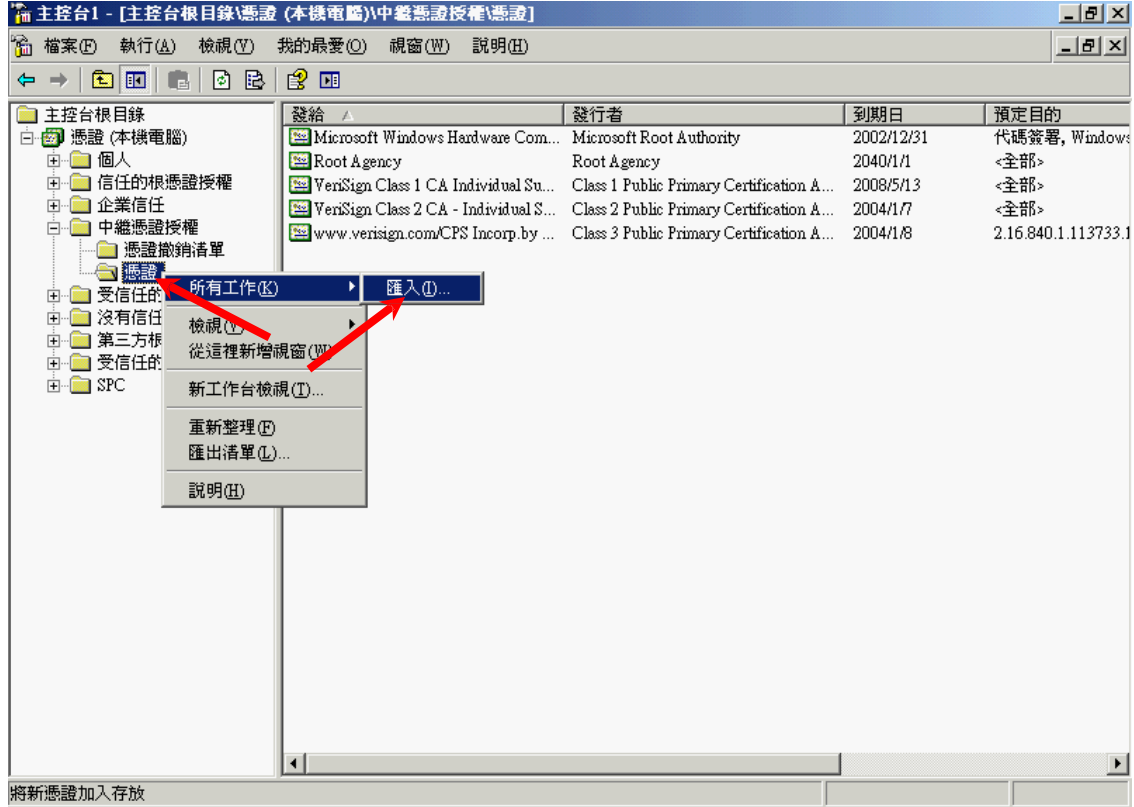
5. 选择[本机电脑]，然后按[完成]。



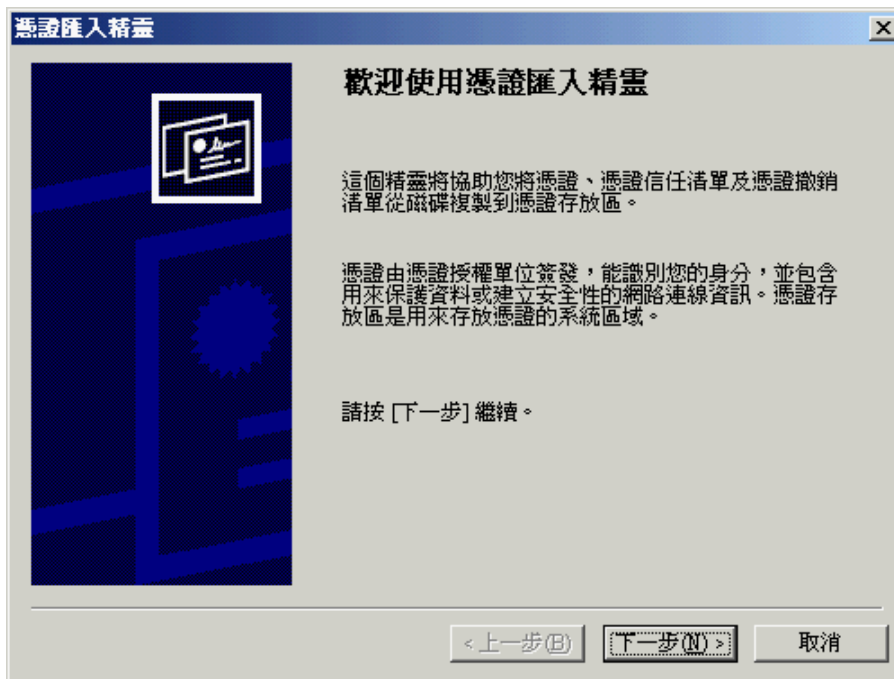
6. 关闭[新增独立嵌入式管理单元]对话框，然后按[确定]关闭[新增/移除嵌入式管理单元]对话框。

安装“Hongkong Post e-Cert CA 1 - 10” 根源证书

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



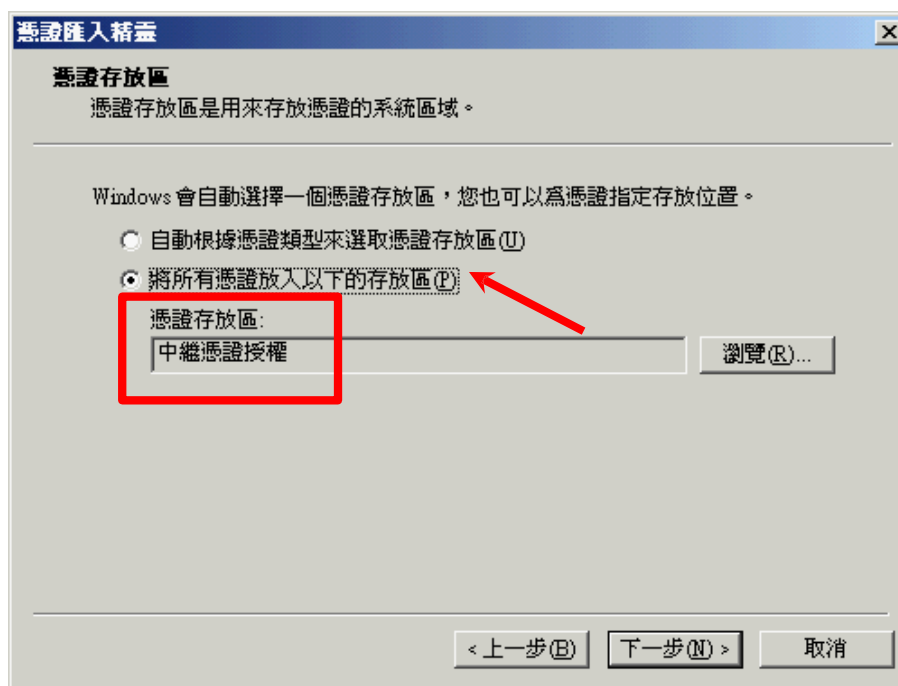
8. 在[凭证汇入精靈]内，按[下一步]继续。



- 按[浏览]指定早前于 C 部的步骤 7 下载的“Hongkong Post e-Cert CA 1 - 10”根源证书 (ecert_ca_1-10_pem.crt)，然后按[下一步]。



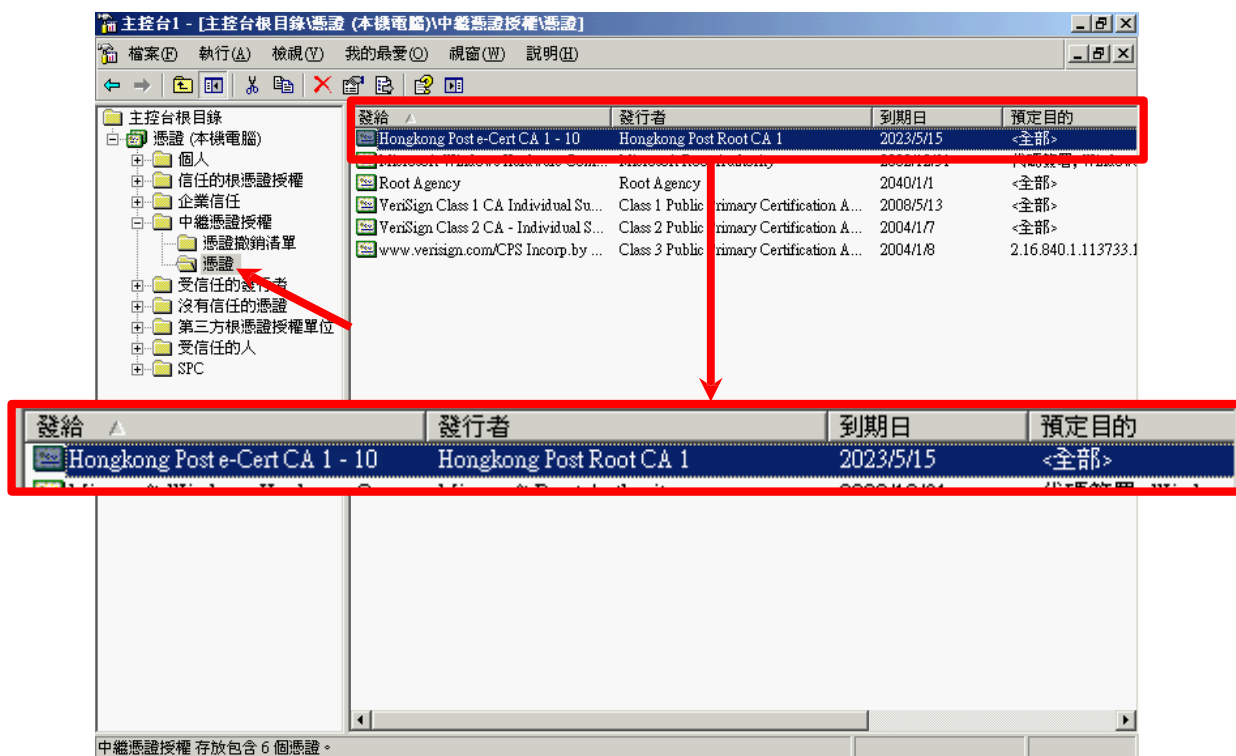
- 选择[将所有凭证放入以下的存放区]，然后按[下一步]。



11. 按[完成]來关闭精靈。



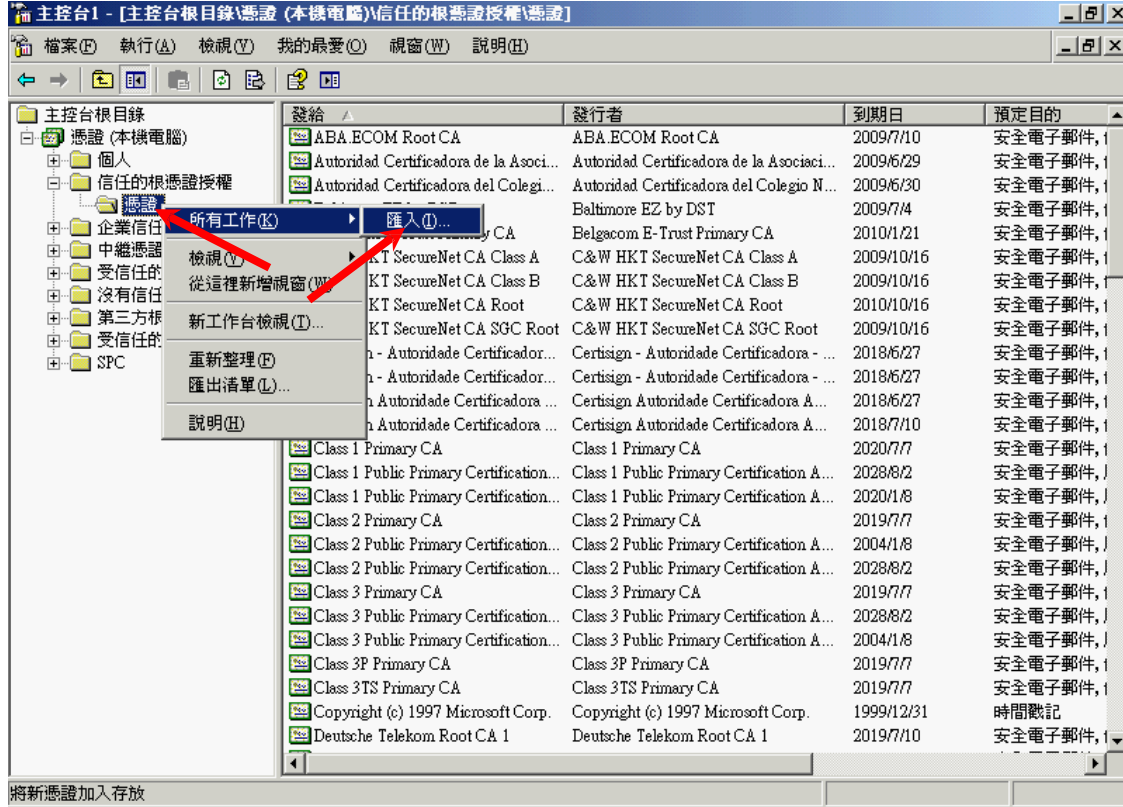
12. 按[确定]來完成。



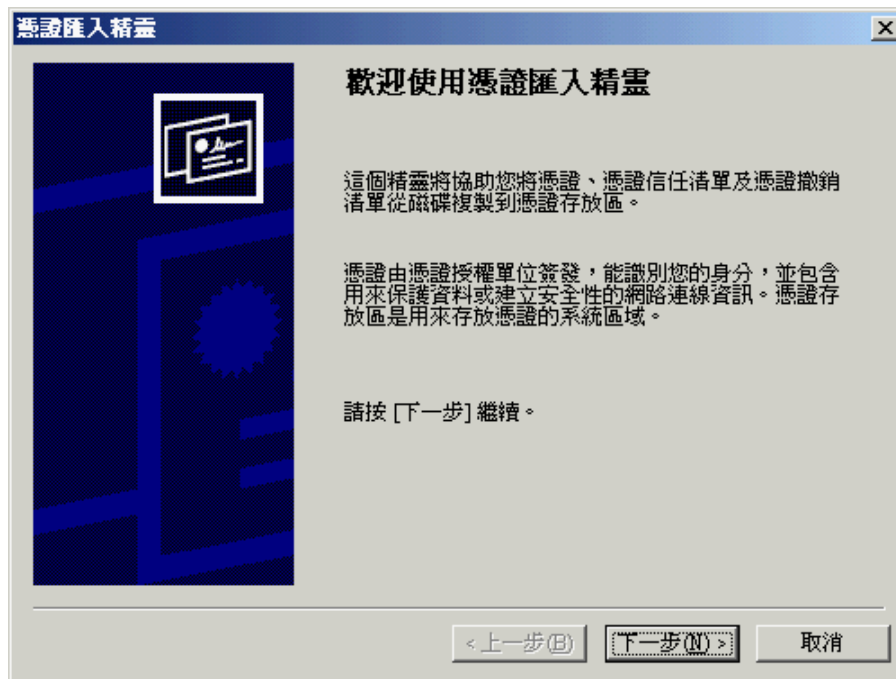
图表 1: “Hongkong Post e-Cert CA 1 - 10” 根源证书已成功安装

安装“Hongkong Post Root CA 1”根源证书

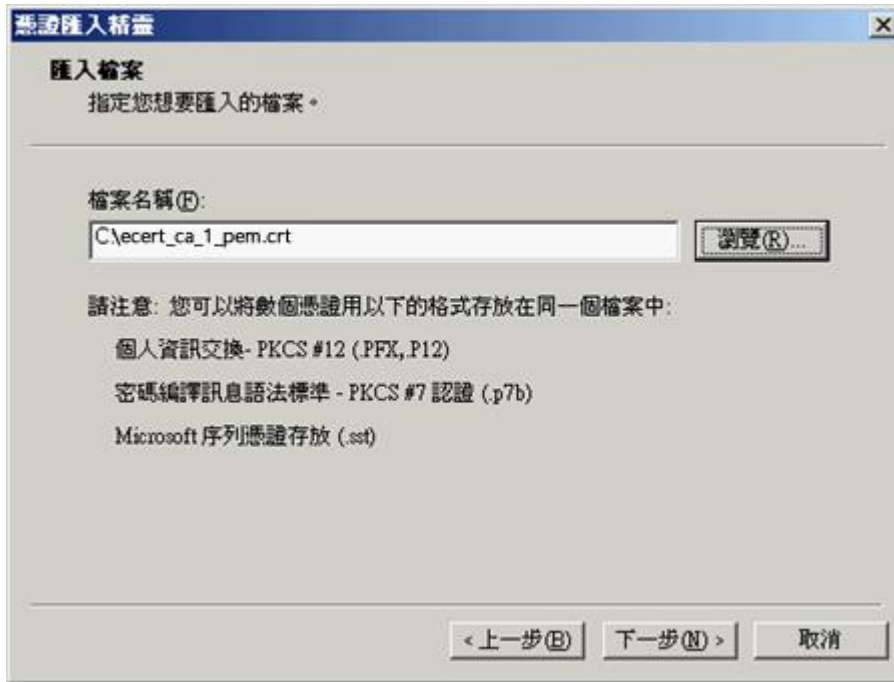
13. 展开[信任的根凭证授权]及以滑鼠右键按一下[凭证]，然后选择[所有工作] > [汇入]。



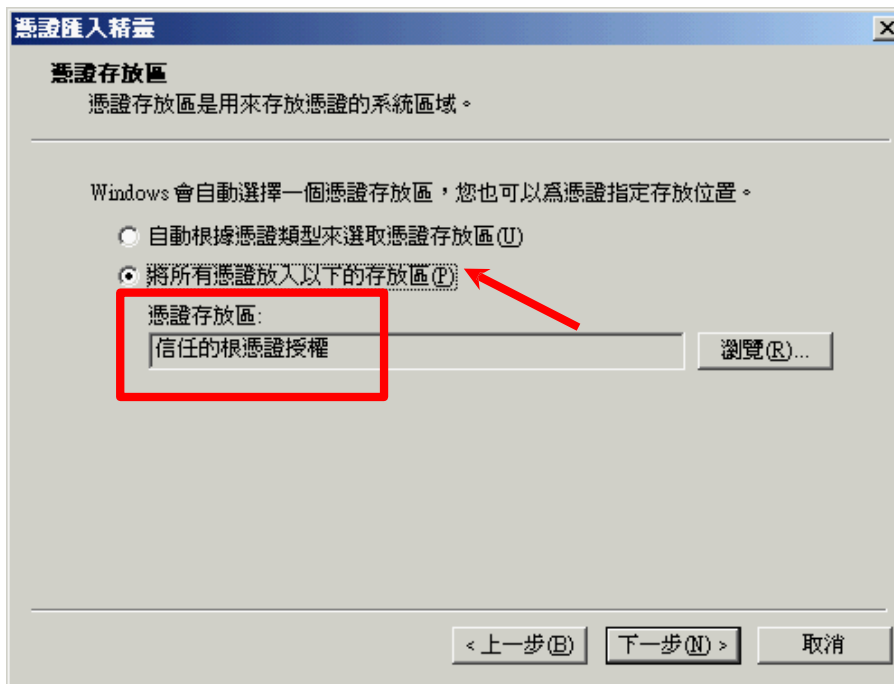
14. 在[凭证汇入精灵]内，按[下一步]继续。



- 按[浏览]指定早前于 C 部的步骤 7 下载的“Hongkong Post Root CA 1”根源证书 (ecert_ca_1_pem.crt)，然后按[下一步]。



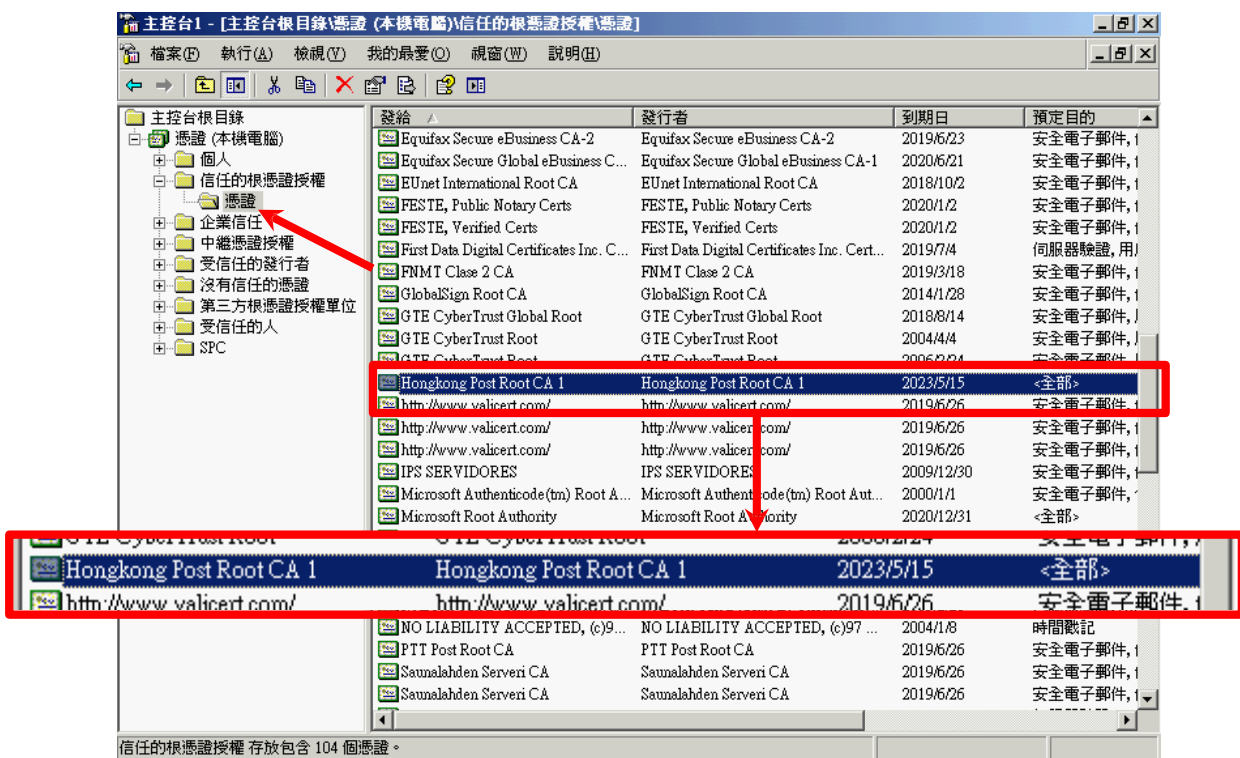
- 选择[将所有凭证放入以下的存放区]，然后按[下一步]。



17. 按[完成]來关闭精靈。



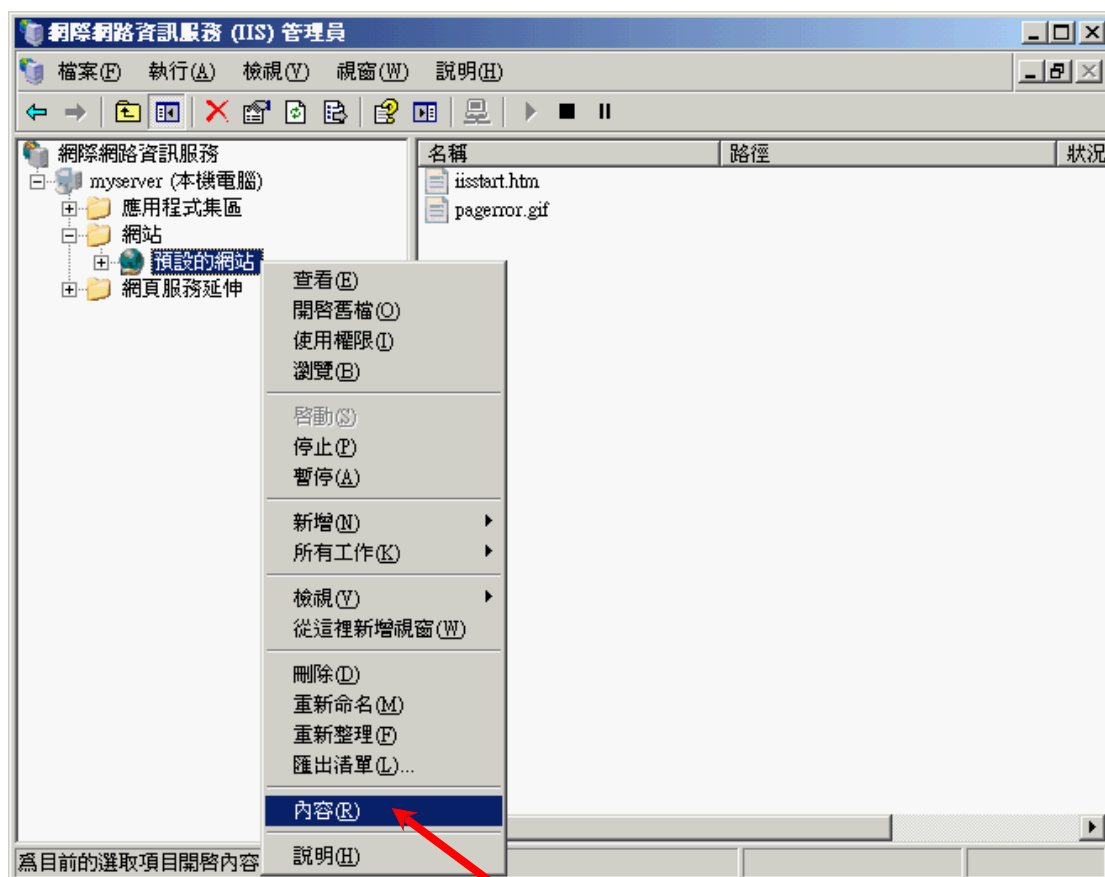
18. 按[确定]來完成。



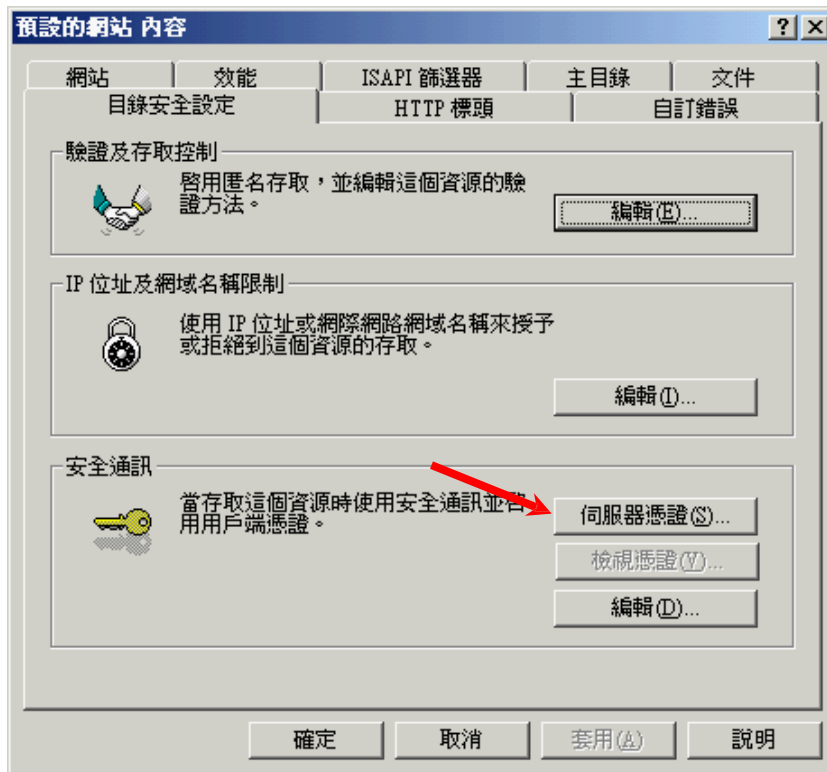
图表 2: “Hongkong Post Root CA 1” 根源证书已成功安装

E. 安装伺服器证书

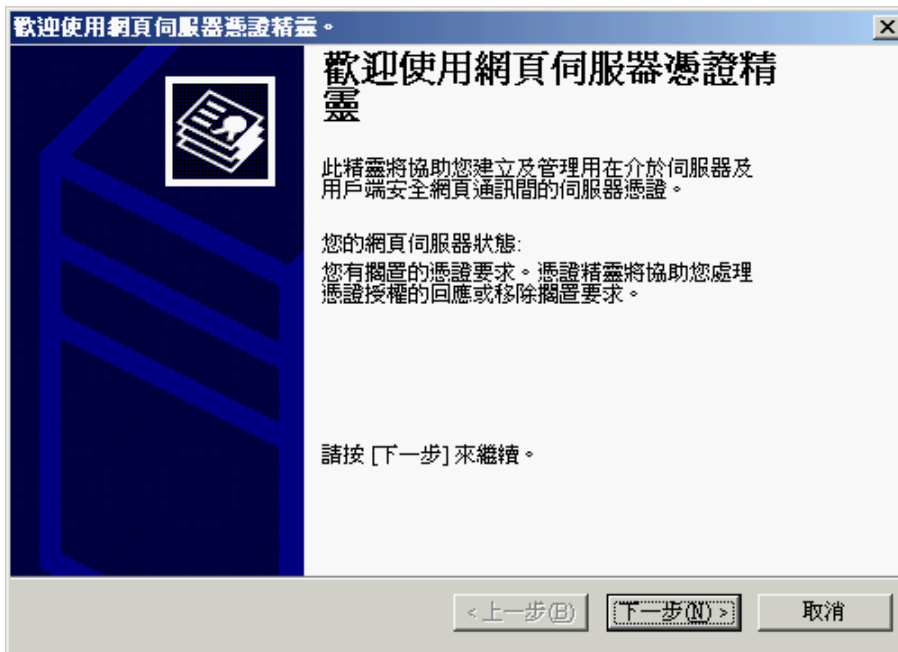
1. 按 [开始] > [所有程式] > [系统管理工具] > [网际网路资讯服务 (IIS) 管理员] / [Internet 服务管理员] 来启动网际网路资讯服务 (IIS) 管理员。
2. 在 [网际网路资讯服务 (IIS) 管理员] / [Internet Information Services] 视窗内, 展开[网站]及选择您的网站, 以滑鼠右键按一下, 然后按[内容]。



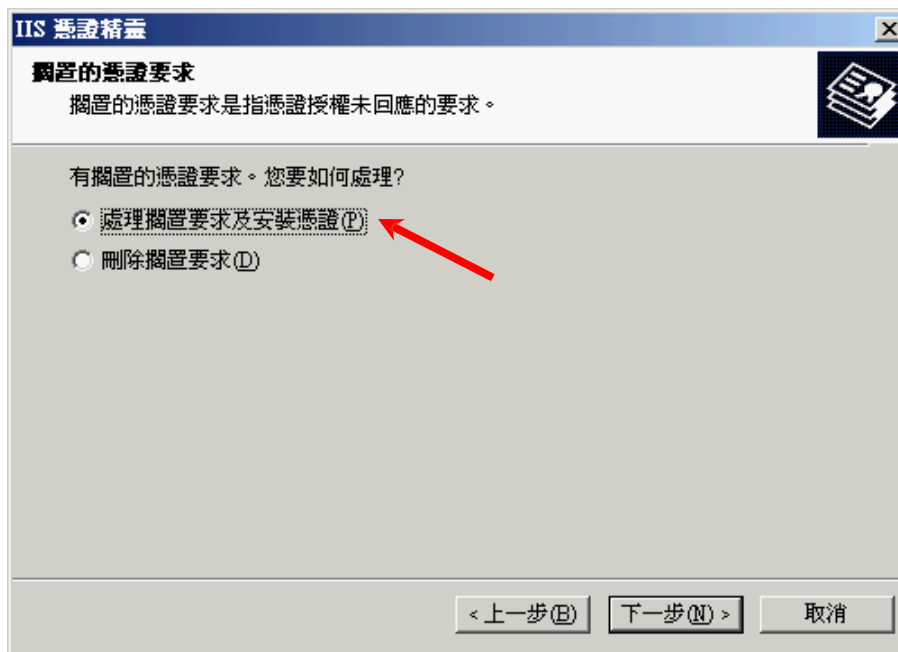
3. 在[目錄安全設定]索引標籤內，按一下[伺服器憑證]。



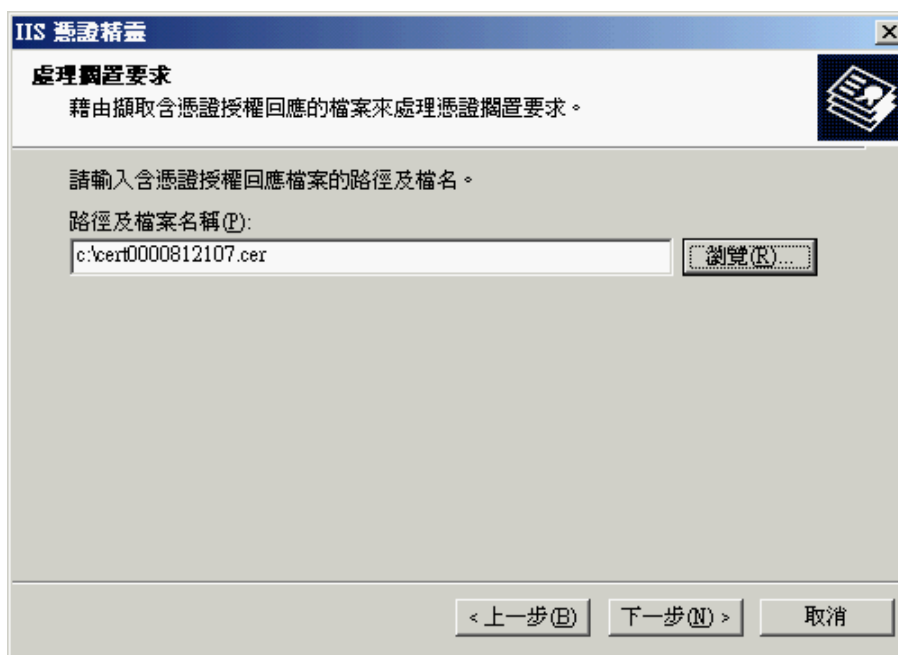
4. 在[網頁伺服器憑證精靈] / [Web 伺服器憑證精靈]內，按[下一步]繼續。



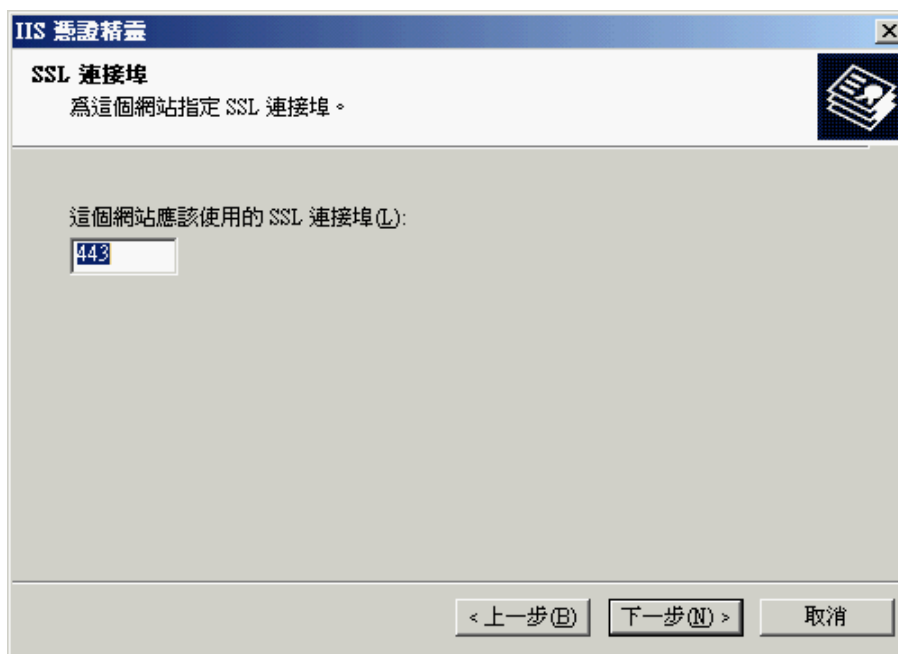
5. 选择[处理搁置要求及安装凭证]，然后按[下一步]。



6. 按[浏览]指定早前于 C 部的步骤 7 下载的“Hongkong Post e-Cert (Server)”证书，然后按[下一步]。



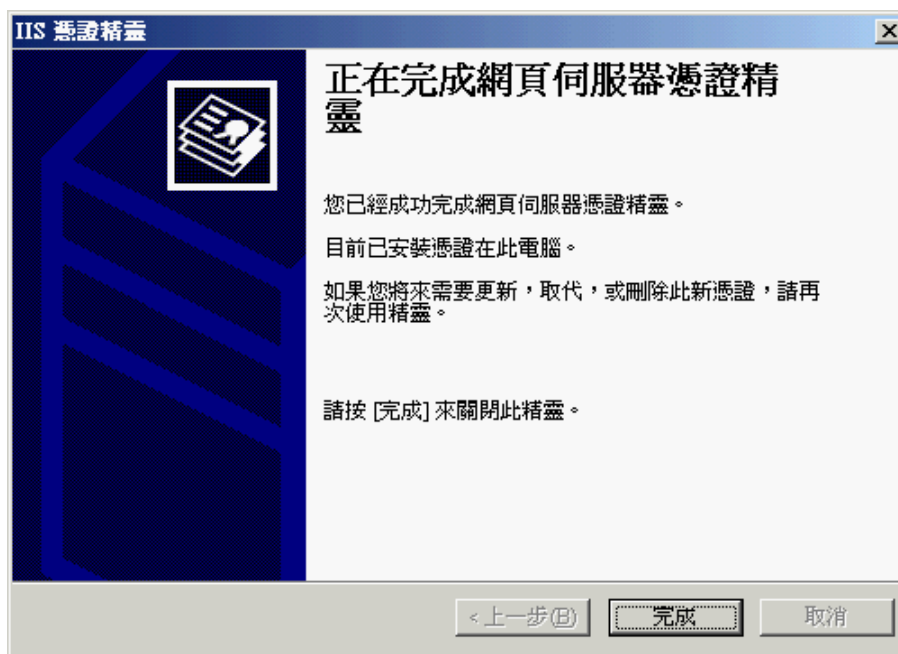
7. 在[这个网站应该使用的 SSL 连接埠]输入 443，然后按[下一步]。
(若使用 IIS 5.0，请跳到步骤 8)



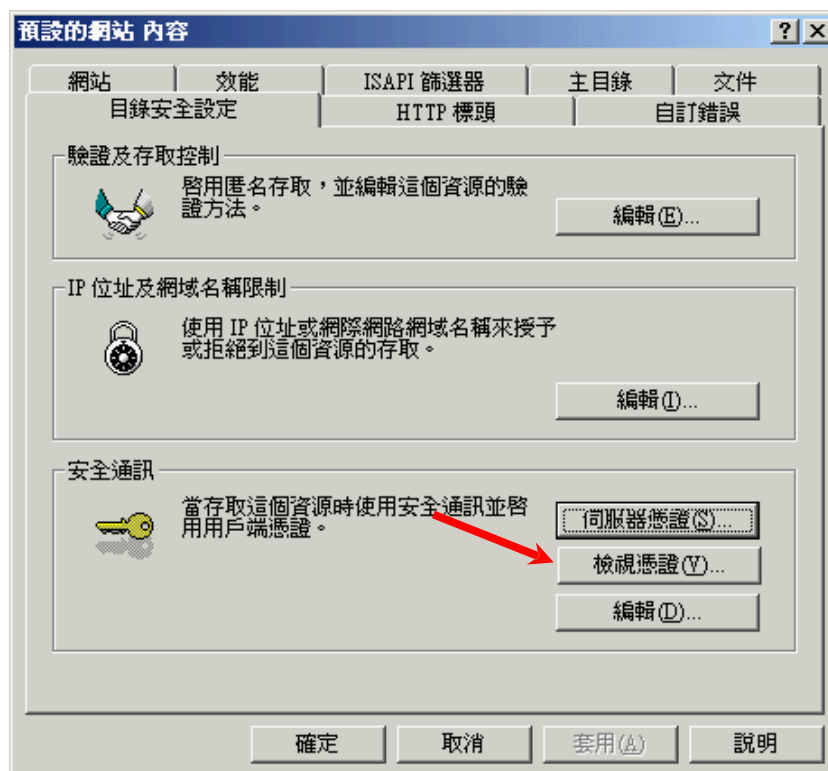
8. 按[下一步]。



- 按[完成]來关闭精靈。



10. 按[检视凭证]來检视伺服器证书。

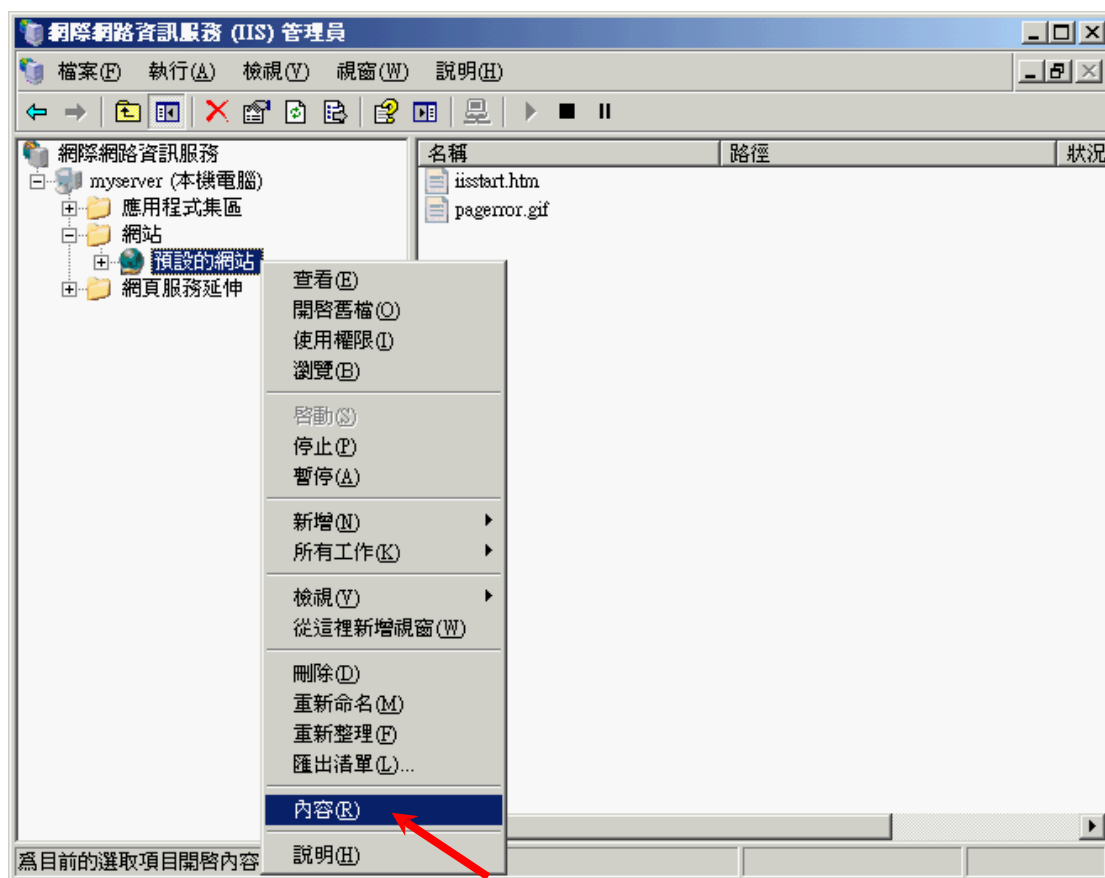


图表 3: “Hongkong Post e-Cert (Server)” 证书已成功安装

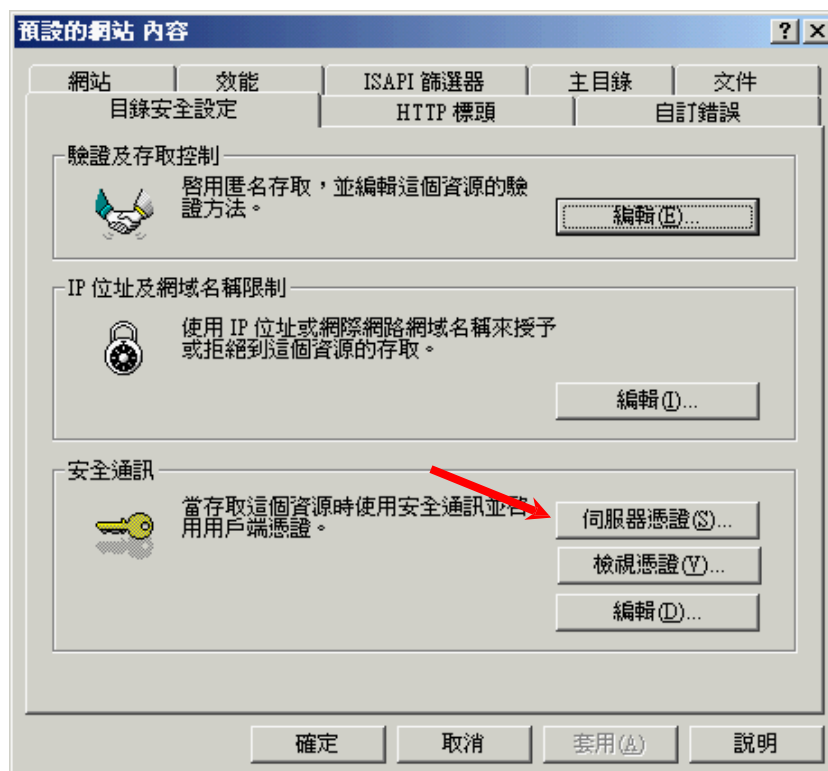
F. 备份密码匙

在 IIS 5.0 上备份密码匙

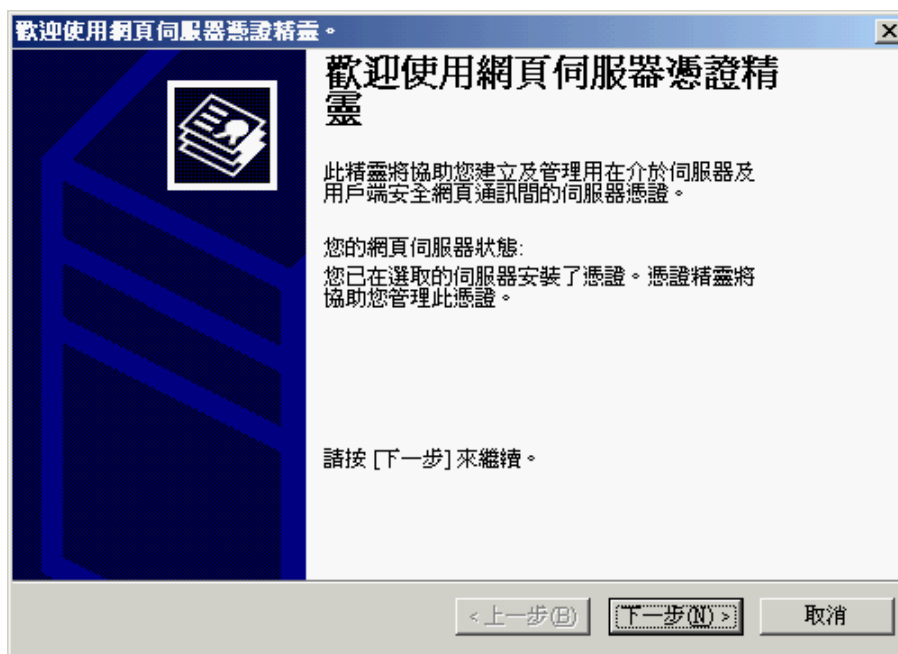
1. 按 [开始] > [所有程式] > [系统管理工具] > [网际网路资讯服务 (IIS) 管理员] 来启动网际网路资讯服务 (IIS) 管理员。
2. 在 [网际网路资讯服务 (IIS) 管理员] 视窗内，展开[网站]及选择您的网站，以滑鼠右键按一下，然后按[内容]。



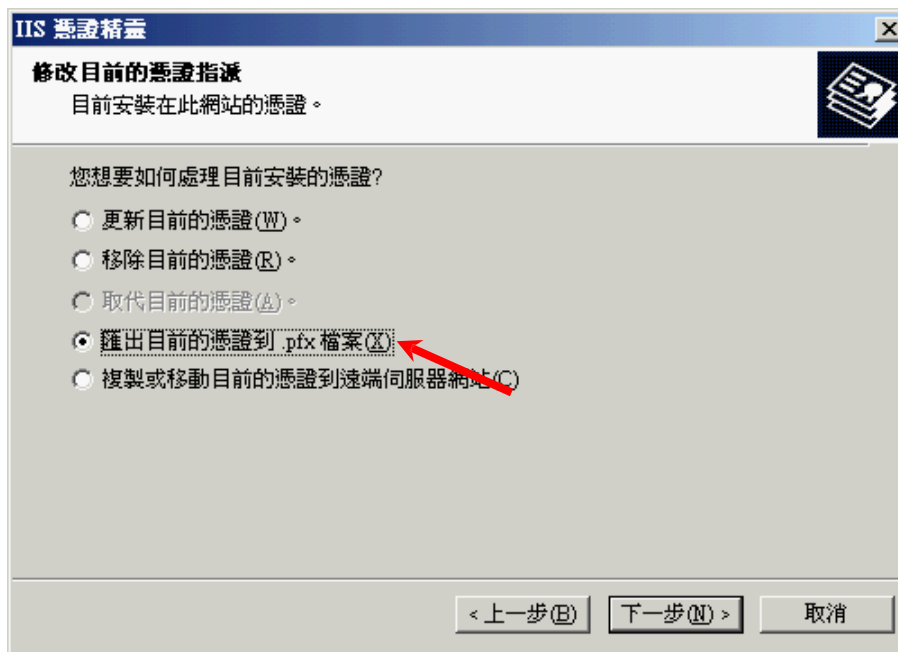
3. 在[目錄安全設定]索引標籤內，按一下[伺服器憑證]。



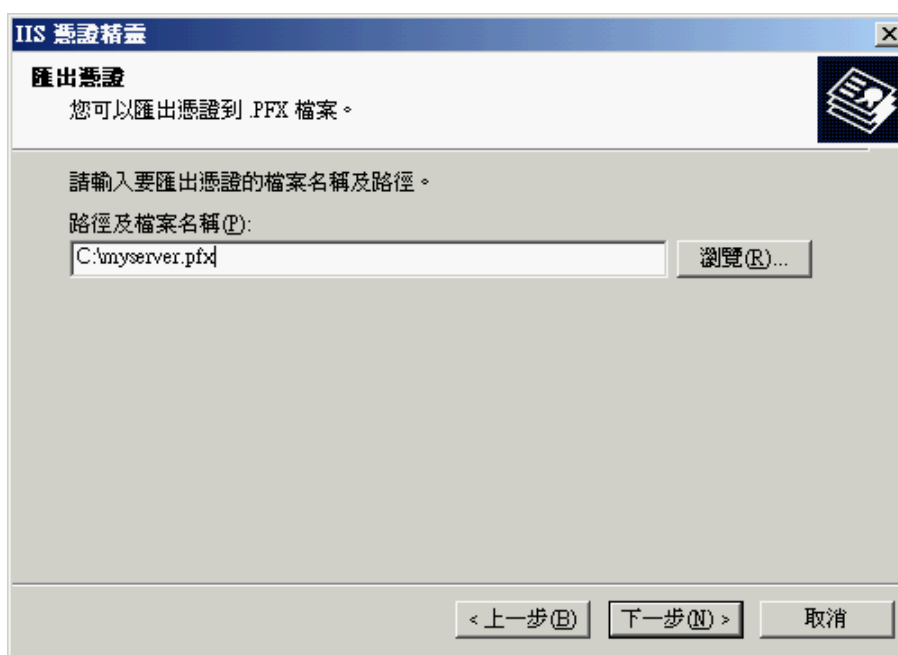
4. 在[网页伺服器凭证书精靈]內，按[下一步]继续。



5. 选择[汇出目前的凭证到.pfx 档案]，然后按[下一步]。

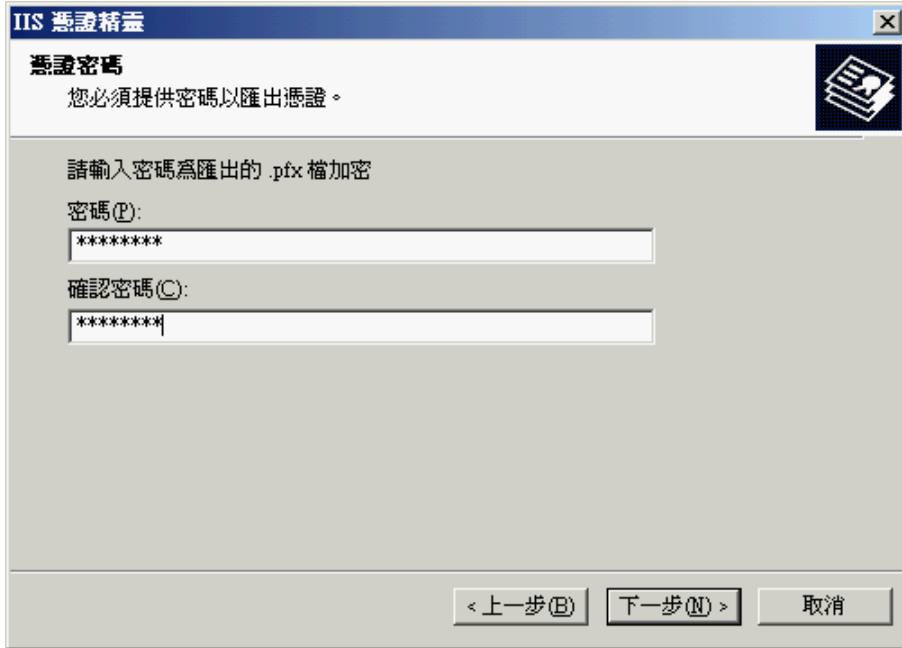


6. 输入要汇出凭证的档案名称及路径，然后按[下一步]。

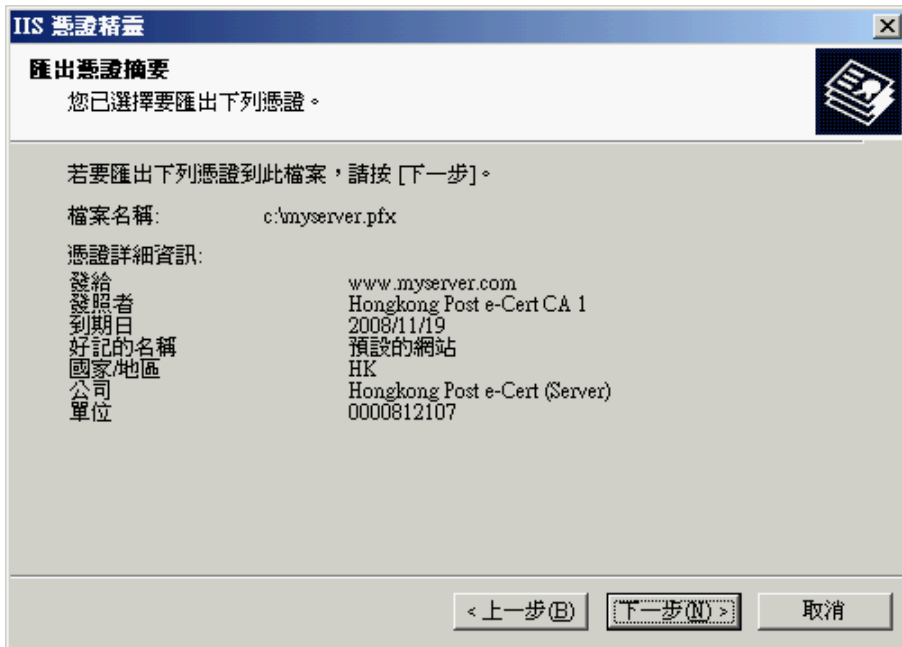


7. 输入并确认密码为汇出的.pfx 档加密。

注意：请牢记这个非常重要的密码。如果您忘记这密码，您将不能还原您的密码匙。



8. 按[下一步]。

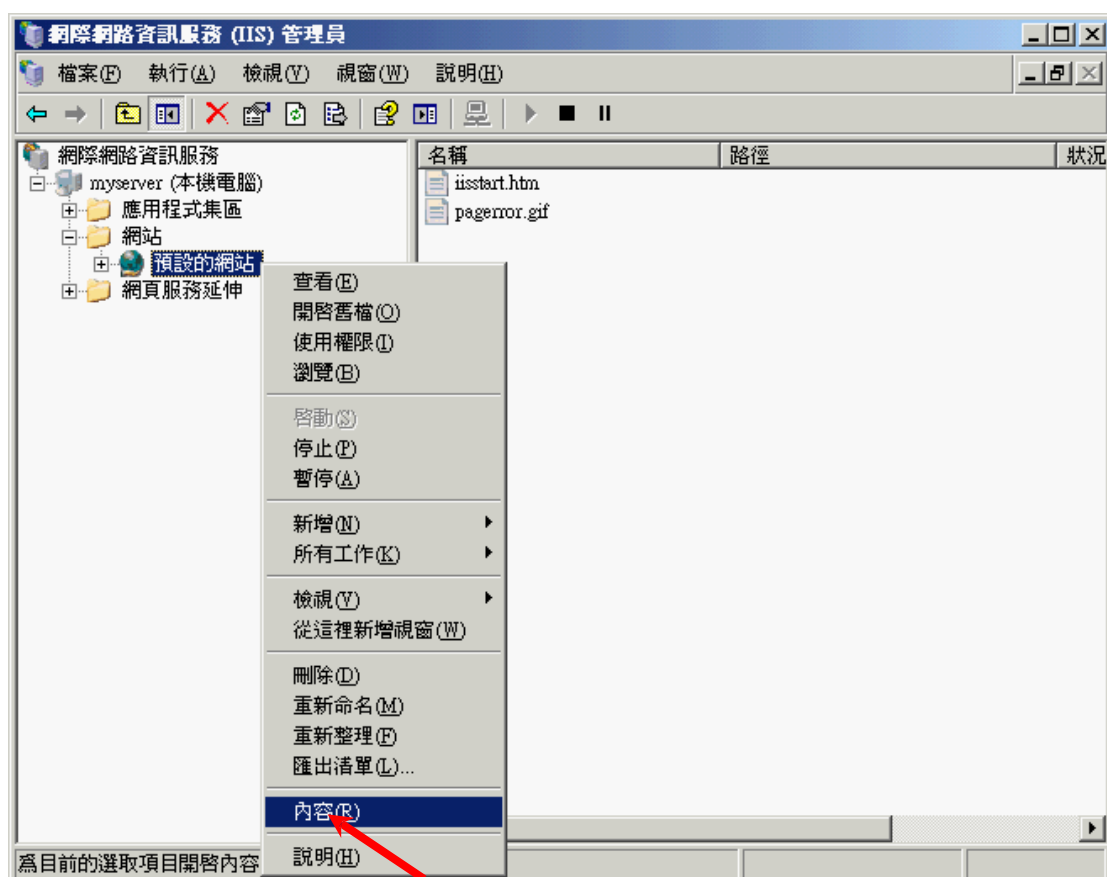


- 按[完成]來关闭精靈。

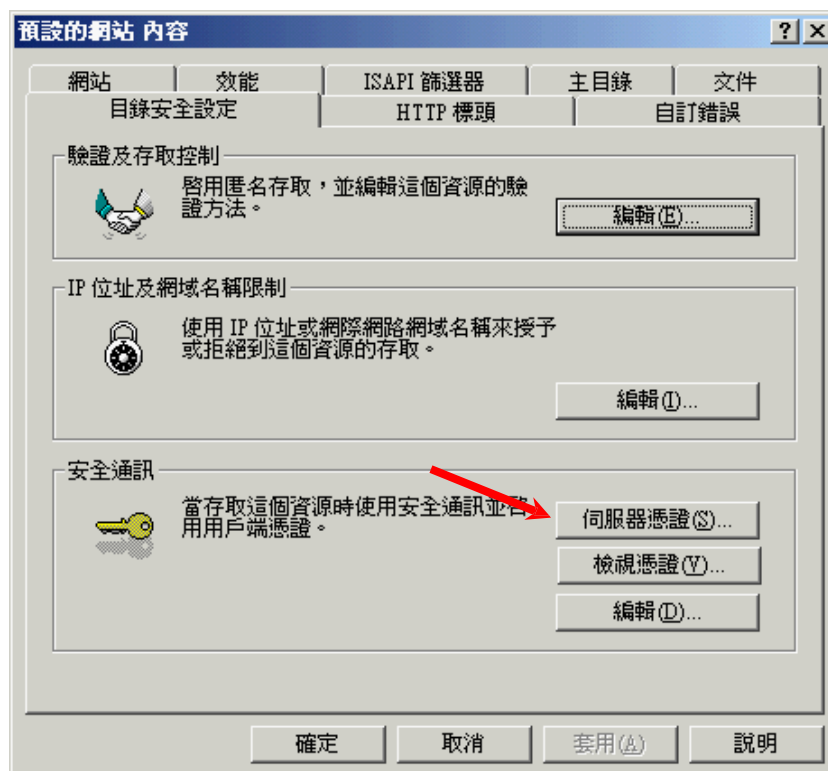


在 IIS 6.0 上备份密码匙

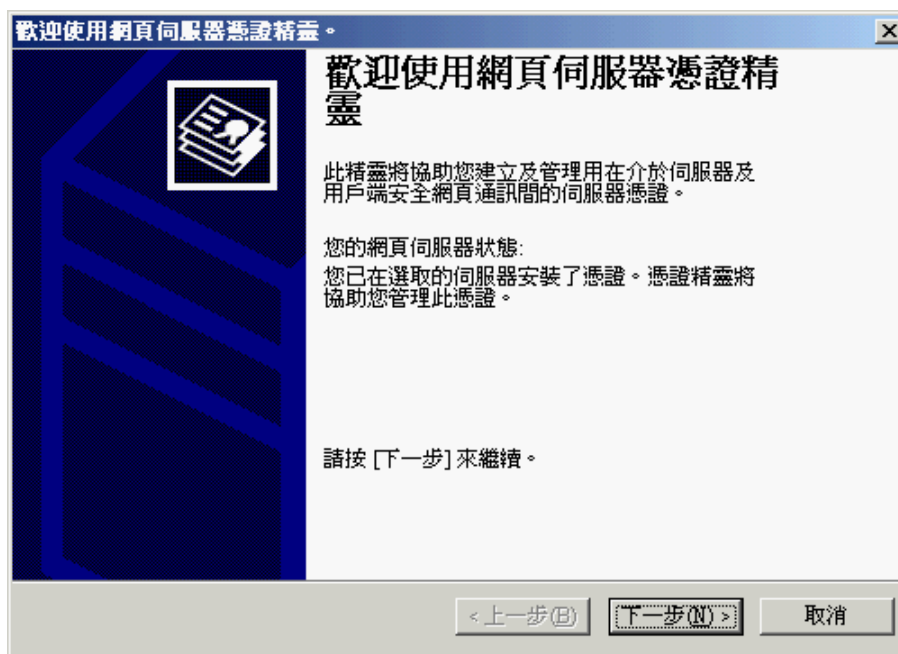
1. 按 [开始] > [所有程式] > [系统管理工具] > [网际网路资讯服务 (IIS) 管理员] 来启动网际网路资讯服务 (IIS) 管理员。
2. 在 [网际网路资讯服务 (IIS) 管理员] 视窗内，展开[网站]及选择您的网站，以滑鼠右键按一下，然后按[内容]。



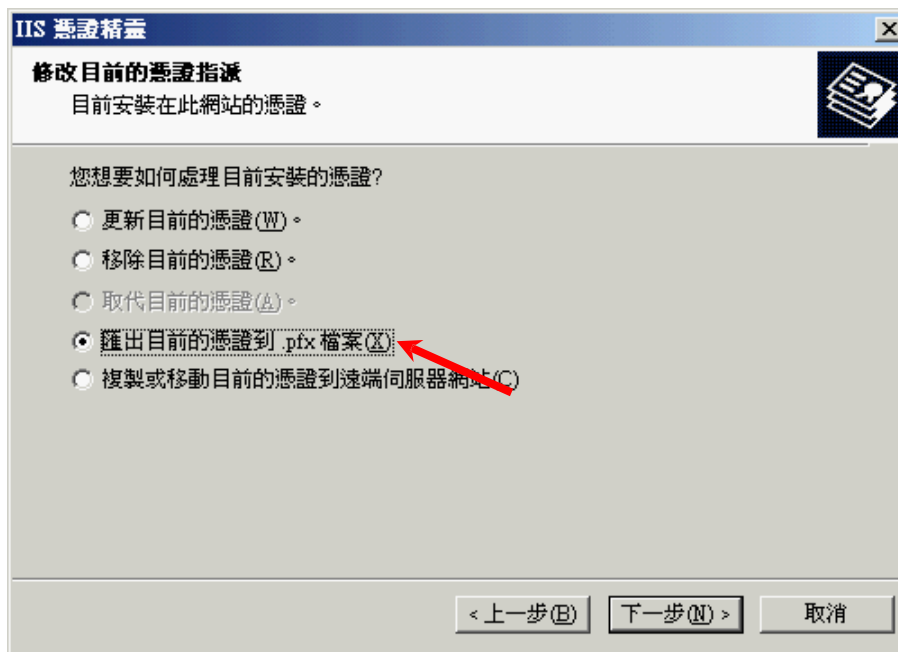
3. 在[目錄安全設定]索引標籤內，按一下[伺服器憑證]。



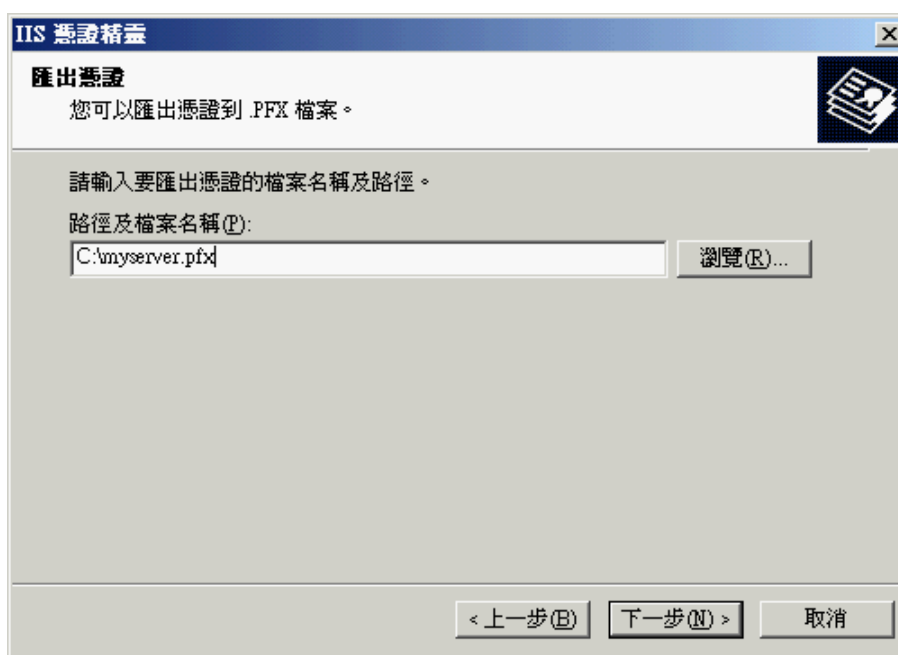
4. 在[网页伺服器凭证精灵]內，按[下一步]继续。



5. 选择[汇出目前的凭证到.pfx 档案]，然后按[下一步]。



6. 输入要汇出凭证的档案名称及路径，然后按[下一步]。

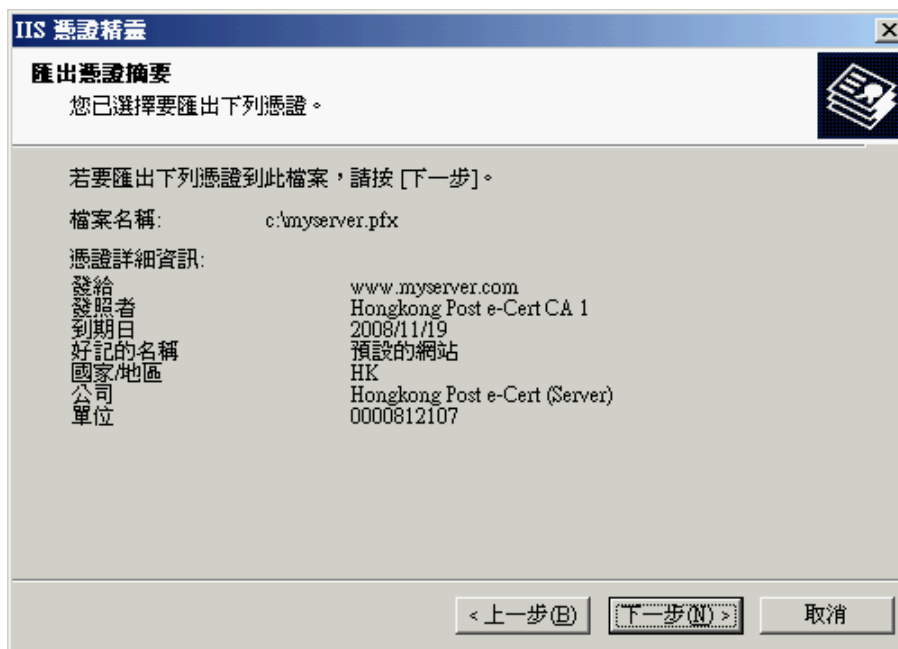


7. 输入并确认密码为汇出的.pfx 档加密。

注意：请牢记这个非常重要的密码。如果您忘记这密码，您将不能还原您的密码匙。



8. 按[下一步]。



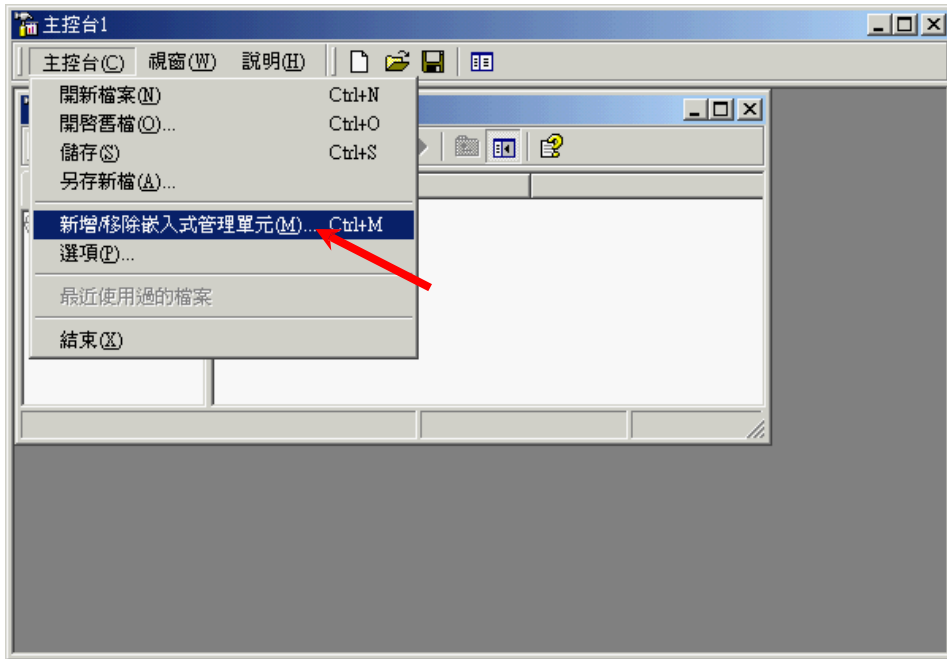
- 按[完成]來关闭精靈。



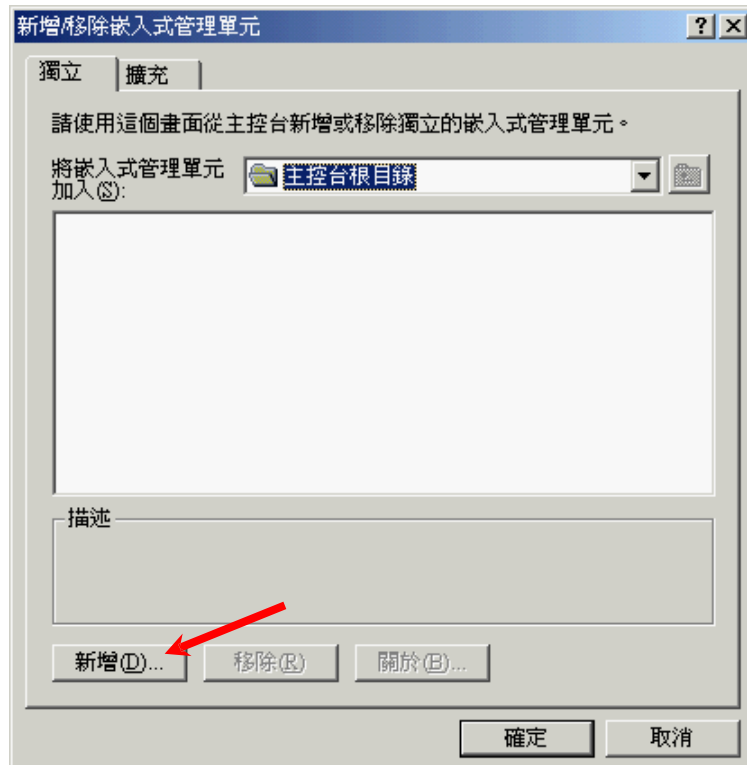
G. 还原密码匙

在 IIS 5.0 上还原密码匙

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



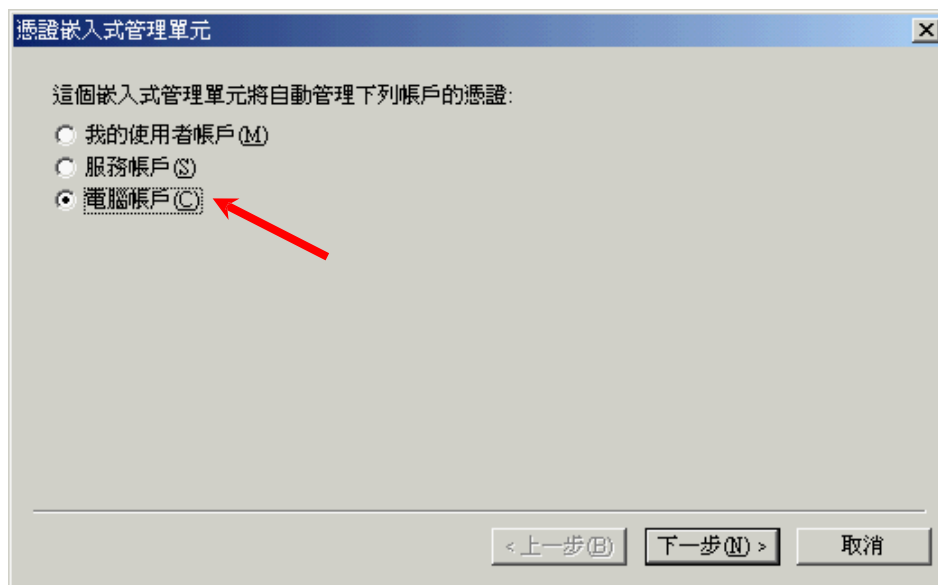
- 按 [新增]。



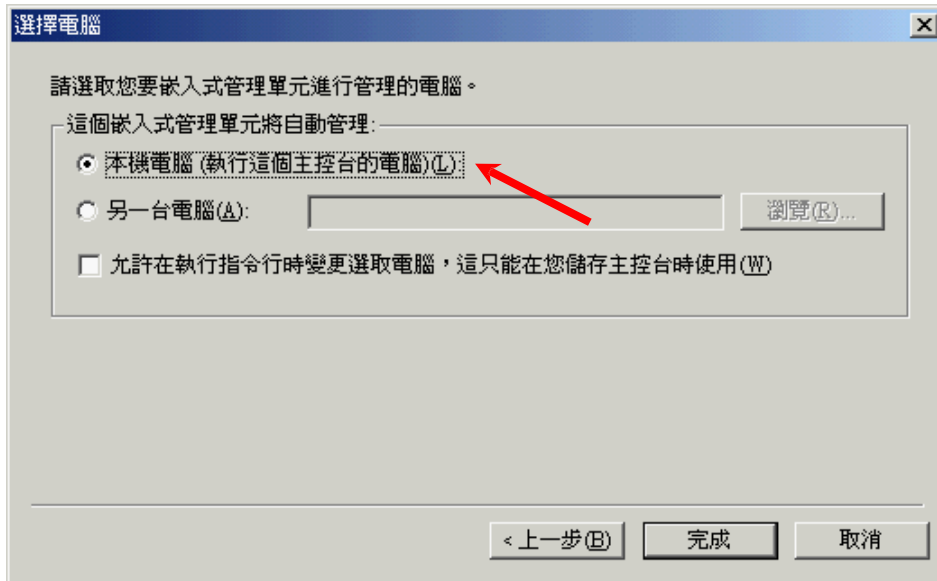
12. 选择[凭证]，然后按[新增]。



13. 选择[电脑帐户]，然后按[下一步]。

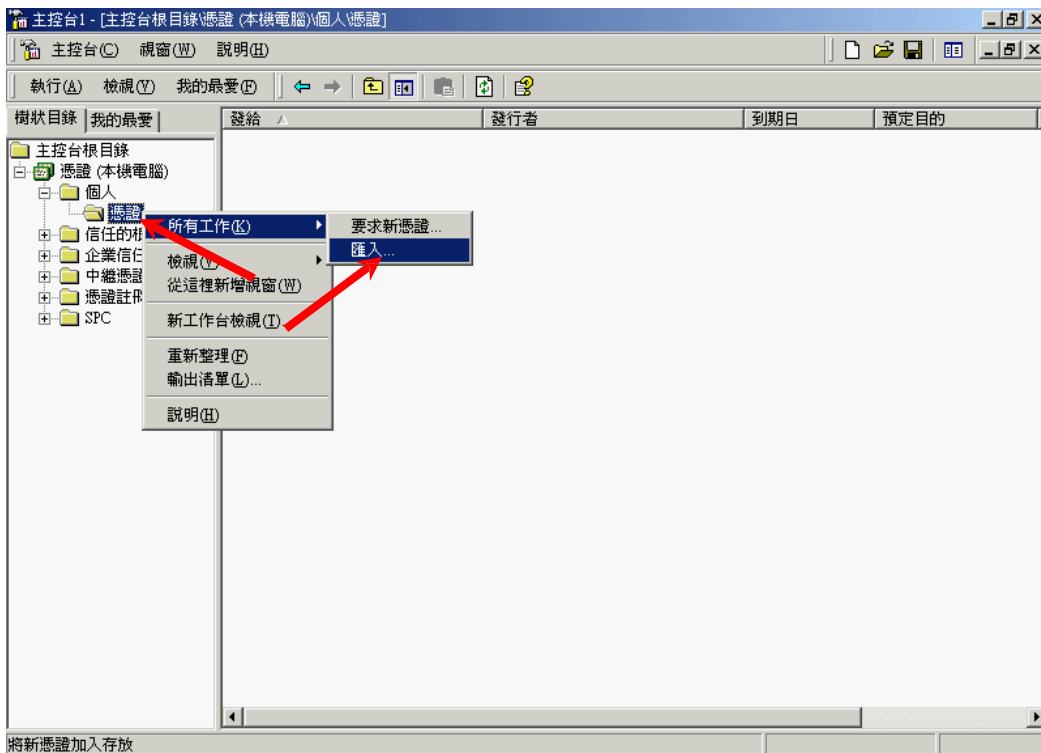


14. 选择[本机电脑]，然后按[完成]。

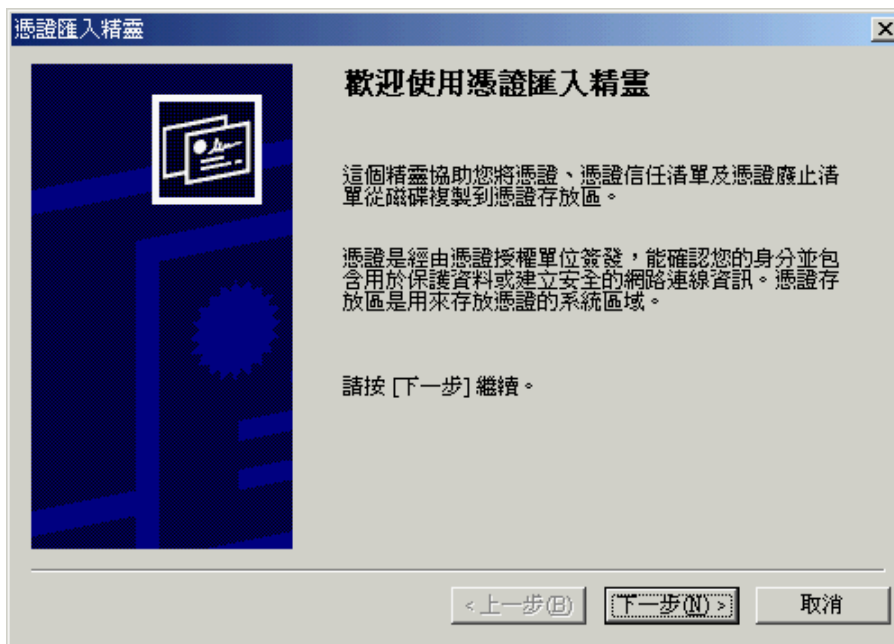


15. 关闭[新增独立嵌入式管理单元]对话框，然后按[确定]关闭[新增/移除嵌入式管理单元]对话框。

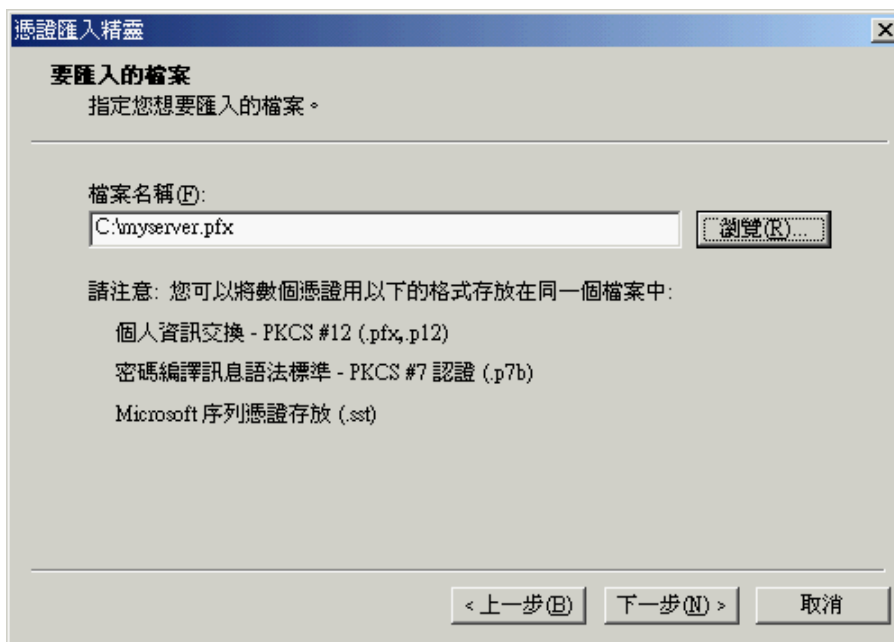
16. 展开[个人]及以滑鼠右键按一下[凭证]，然后选择[所有工作] > [汇入]。
(如要还原凭证要求的密码匙，请展开[凭证注册要求](或于某些系统称为[REQUESTS])。)



17. 在[凭证汇入精靈]内，按[下一步]继续。

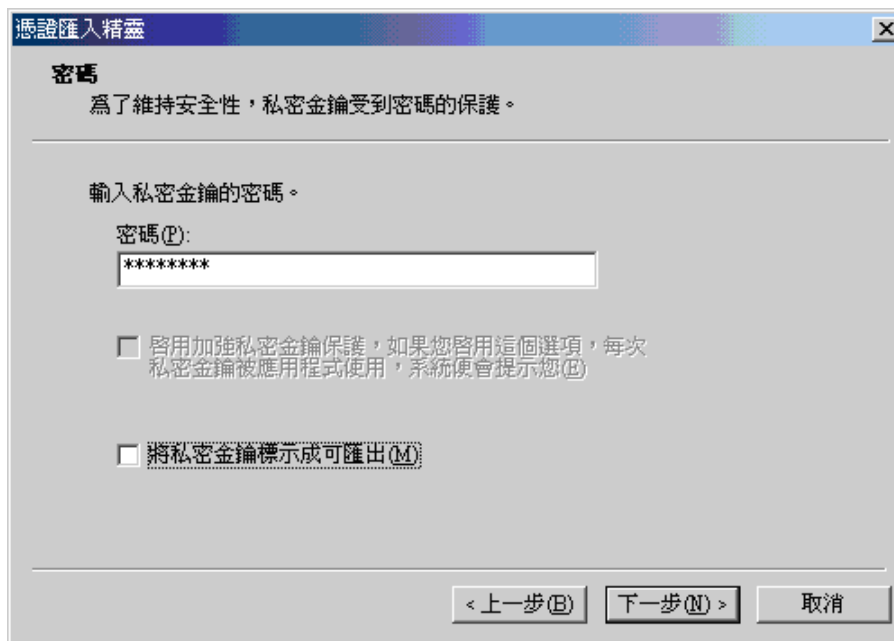


18. 按[浏览]指定密码匙的备份档案，然后按[下一步]。

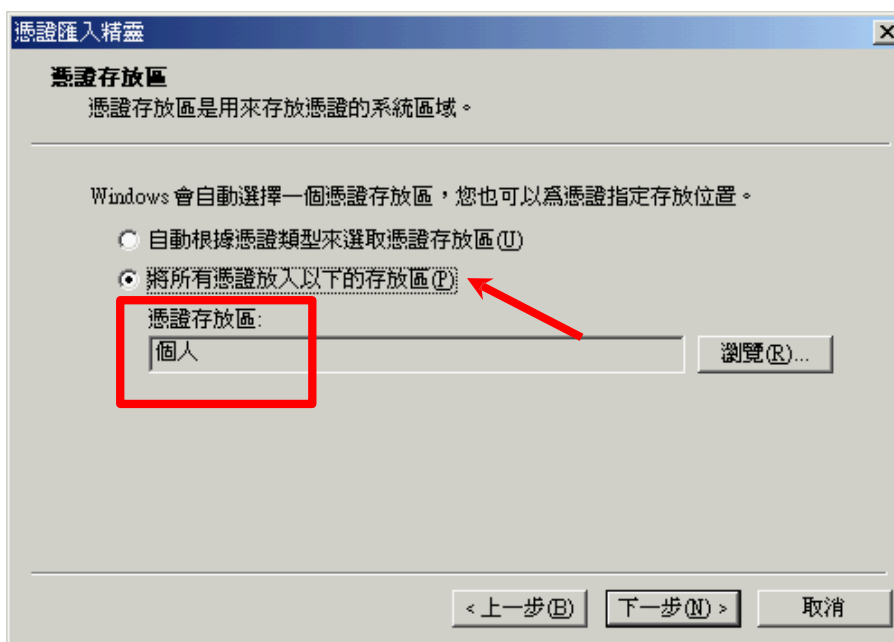


19. 输入密码匙的密码，然后按[下一步]。

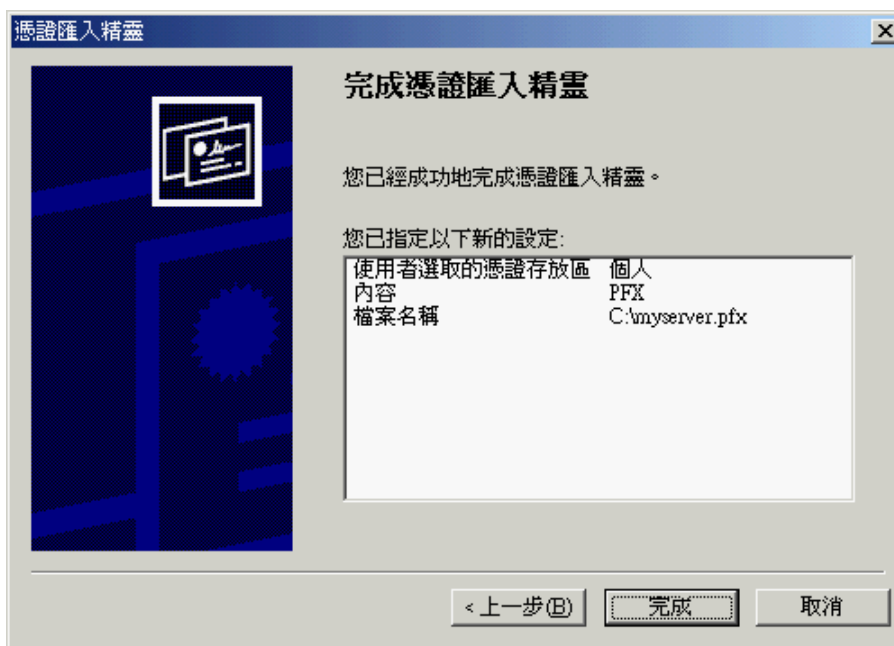
注意：为使您将来可以进行备份或传输您的密码匙，您可以将这个密码匙设成可汇出。



20. 选择[将所有凭证放入以下的存放区]，然后按[下一步]。



21. 按[完成]來关闭精靈。

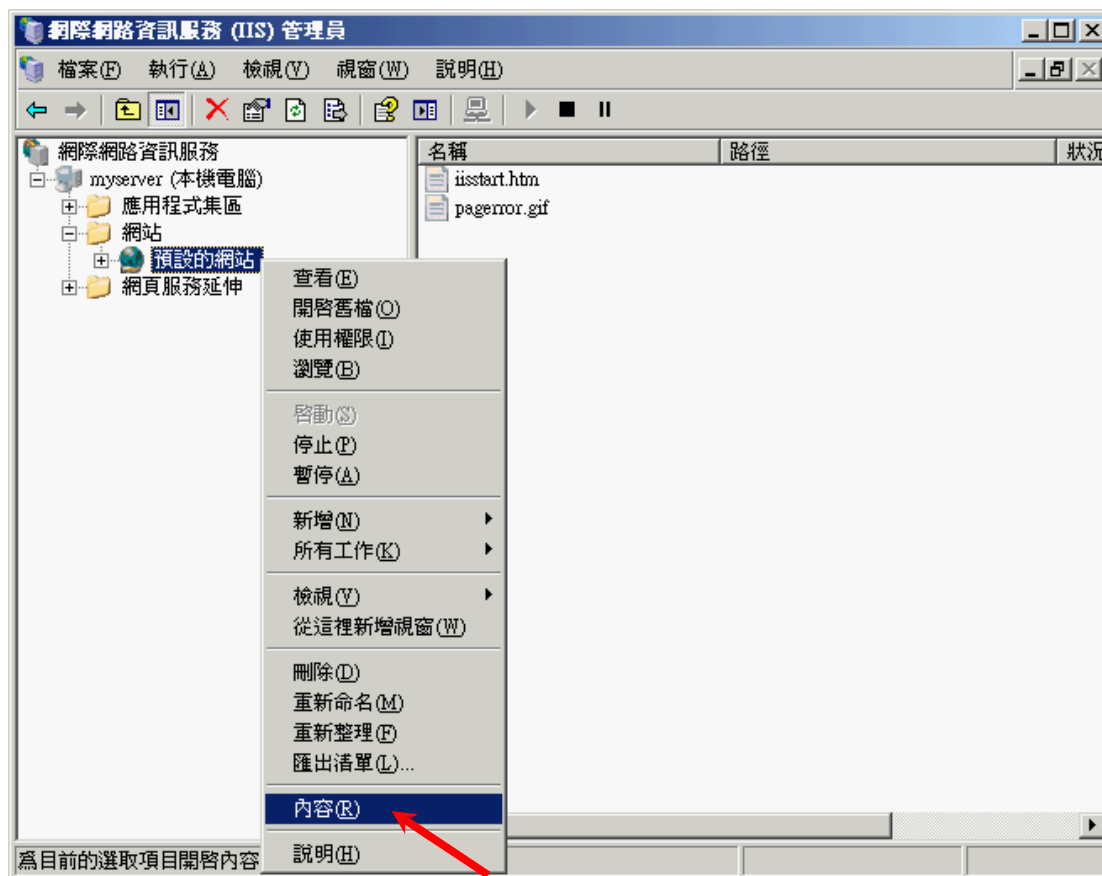


22. 按[确定]來完成。

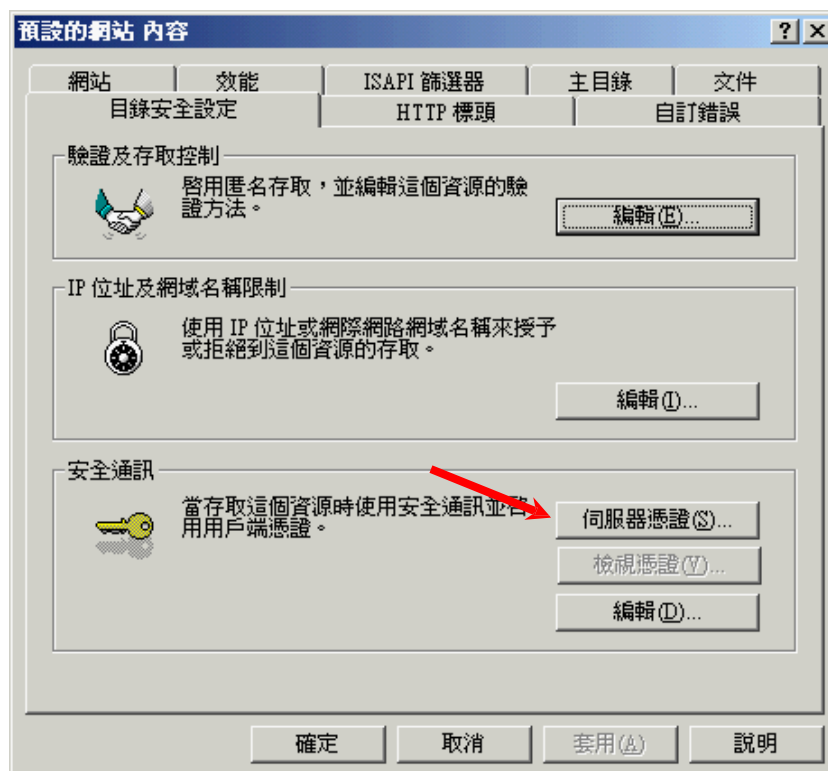


在 IIS 6.0 上还原密码匙

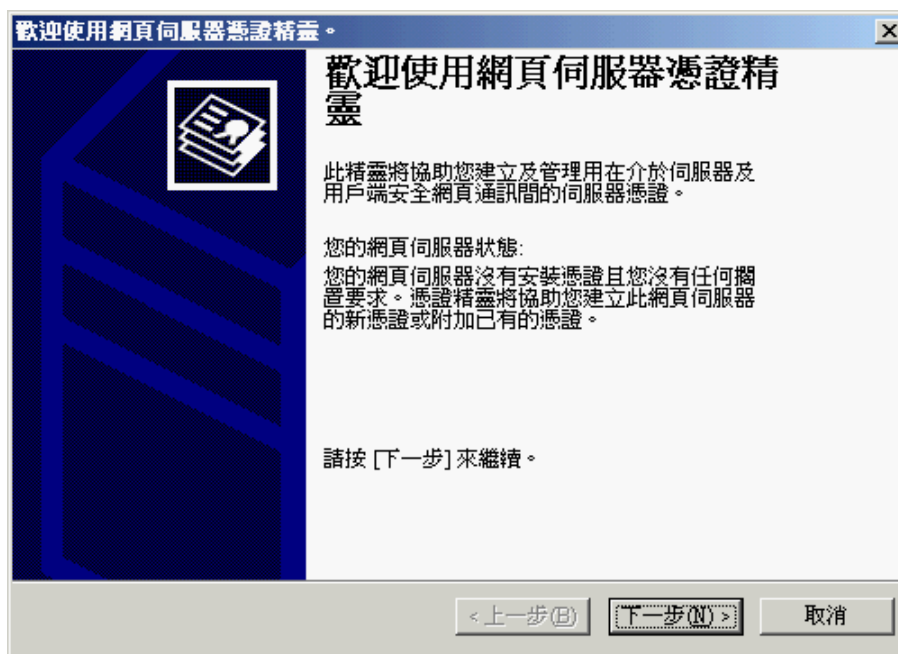
1. 按 [开始] > [所有程式] > [系统管理工具] > [网际网路资讯服务 (IIS) 管理员] 来启动网际网路资讯服务 (IIS) 管理员。
2. 在 [网际网路资讯服务 (IIS) 管理员] 视窗内，展开[网站]及选择您的网站，以滑鼠右键按一下，然后按[内容]。



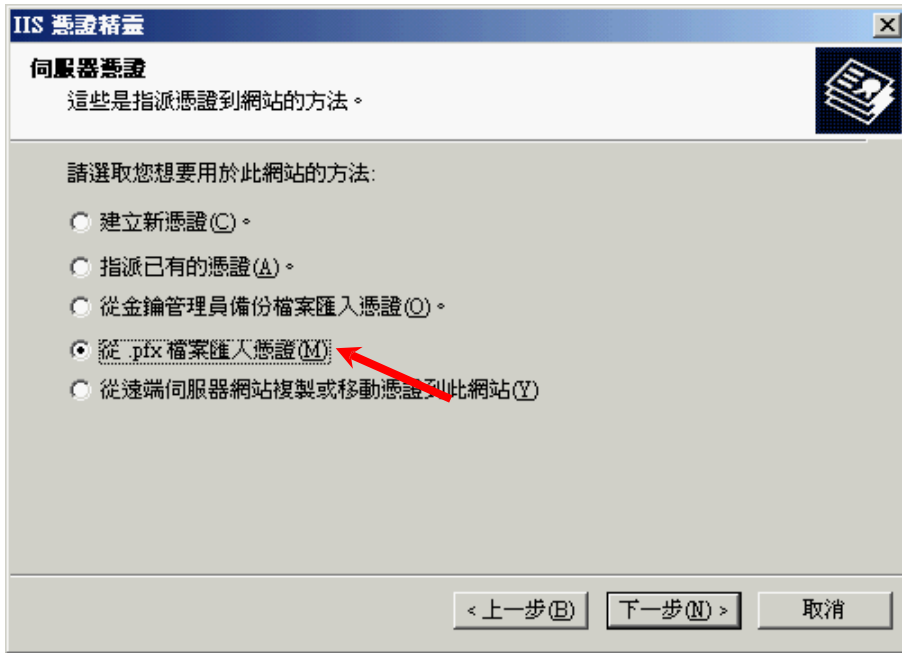
3. 在[目錄安全設定]索引標籤內，按一下[伺服器憑證]。



4. 在[网页伺服器凭证书精靈]內，按[下一步]继续。

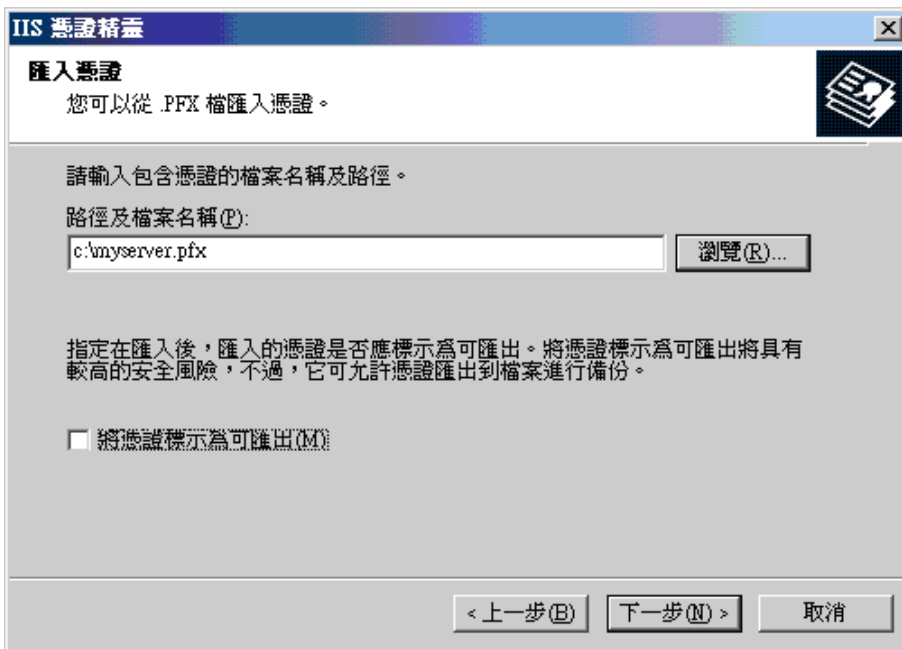


5. 选择[从.pfx 档案汇入凭证]，然后按[下一步]。

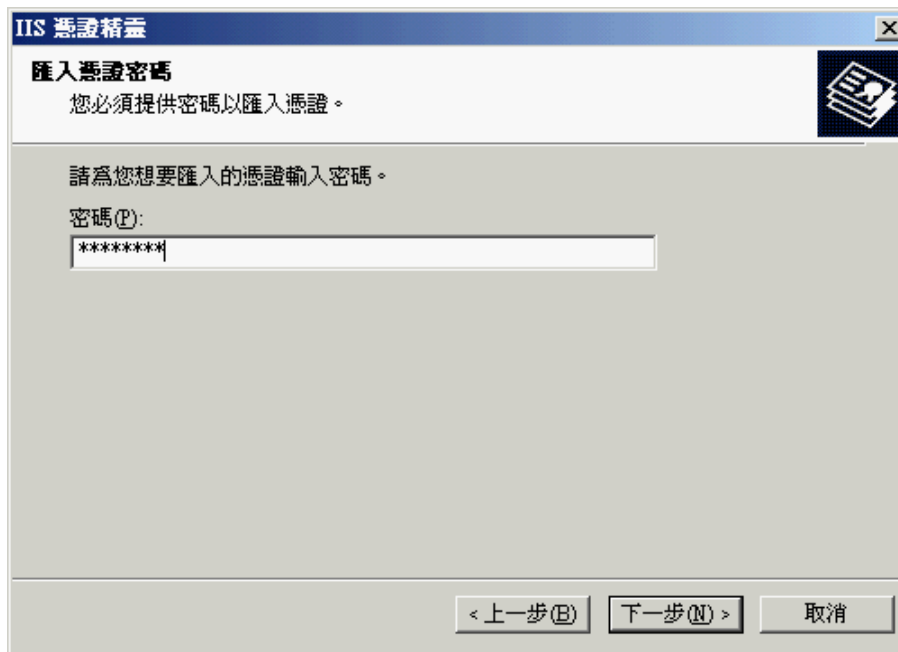


6. 输入包含凭证的档案名称及路径，然后按[下一步]。

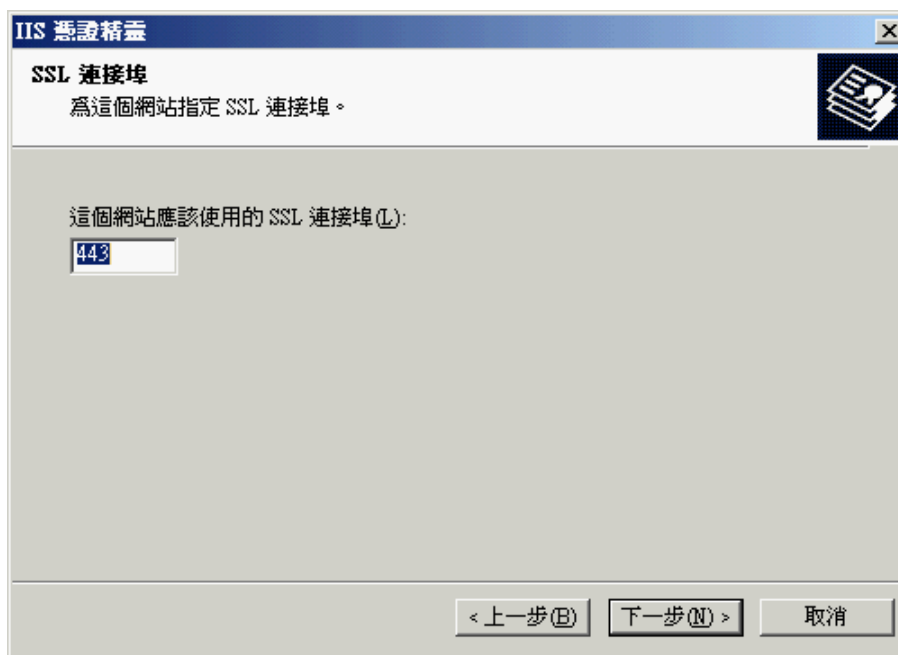
注意：为使您将来可以进行备份或传输您的凭证，您可以将这个凭证标示为可汇出。



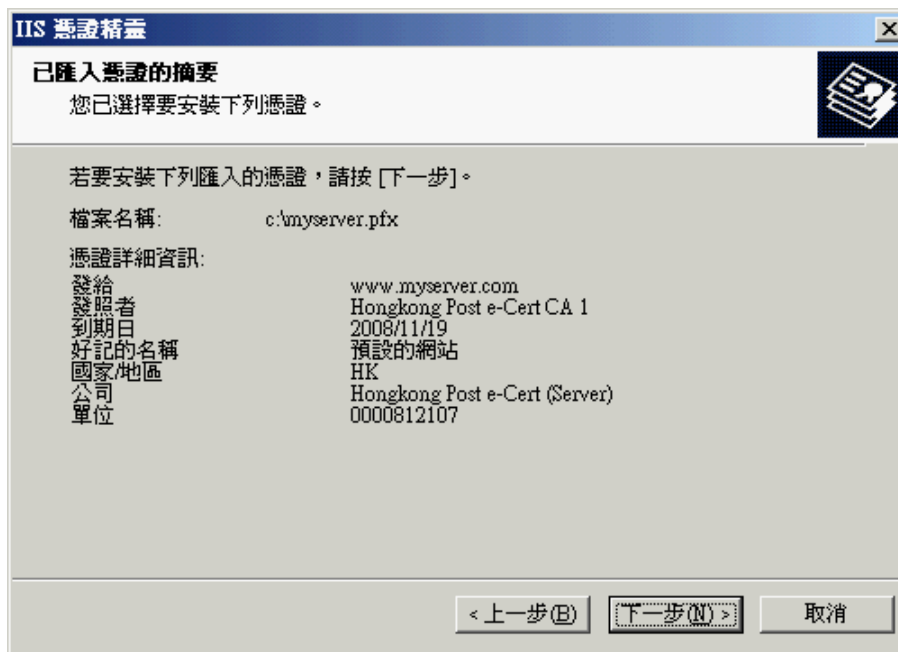
7. 输入凭证的密码，然后按[下一步]。



8. 在[这个网站应该使用的 SSL 连接埠]输入 443，然后按[下一步]。



9. 按[下一步]。



10. 按[完成]來关闭精靈。

