

e-Cert (Server) User Guide

For Microsoft IIS 5.0 / 6.0 For SHA-1 e-Cert(Server) Only

Revision Date: Dec 2014

Table of Content

| A. | Guidelines for e-Cert (Server) Applicant | 2 |
|----|---|----|
| | New Application | |
| | Renewal Application | 4 |
| B. | Generating Certificate Signing Request (CSR) | 5 |
| | Creating a New Server Certificate | 7 |
| | Renewing your Current Server Certificate | 13 |
| C. | Submitting Certificate Signing Request (CSR) | 16 |
| D. | Installing Hongkong Post Root CA Certificate | 20 |
| | Installing the "Hongkong Post e-Cert CA 1 - 10" Certificate | 23 |
| | Installing the "Hongkong Post Root CA 1" Certificate | 26 |
| E. | Installing Server Certificate | 29 |
| F. | Backing up the Private Key | 35 |
| | Backing up the Private Key for IIS 5.0 | 35 |
| | Backing up the Private Key for IIS 6.0 | 42 |
| G. | Restoring the Private Key | 47 |
| | Restoring the Private Key for IIS 5.0 | 47 |
| | Restoring the Private Key for IIS 6.0 | 53 |

A. Guidelines for e-Cert (Server) Applicant

After receipt and approval of an e-Cert (Server) application, Hongkong Post Certification Authority will send an e-mail with subject "Submission of Certificate Signing Request (CSR)" to request the applicant (i.e. the Authorized Representative) to submit the CSR at the Hongkong Post CA web site.

This user guide is for reference by applicants of e-Cert (Server) in generating their key pair and Certificate Signing Request (CSR) using Microsoft IIS 5.0 / 6.0 on Windows 2000 / 2003. The CSR containing the public key will then be submitted to Hongkong Post Certification Authority for certificate signing.

If you lose the private key after the certificate is issued, you will be unable to install or use the certificate. Therefore, it is strongly recommended that you should backup the private key **before the submission of the Certificate Signing Request (CSR)** and **after the installation of the server certificate**. To learn the backup and restore procedures of the private key, please follow the instructions as described in the following sections:

| F. | Backing up the Private Key | .35 |
|----|----------------------------|-----|
| G. | Restoring the Private Key | .47 |

New Application

If this is the first time you apply for e-Cert (Server), please follow the instructions as described in the following sections:

| B. | Generating Certificate Signing Request (CSR) | 5 |
|----|---|----|
| | Creating a New Server Certificate | 7 |
| C. | Submitting Certificate Signing Request (CSR) | 16 |
| D. | Installing Hongkong Post Root CA Certificate | 20 |
| | Installing the "Hongkong Post e-Cert CA 1 - 10" Certificate | 23 |
| | Installing the "Hongkong Post Root CA 1" Certificate | 26 |
| E. | Installing Server Certificate | 29 |

Renewal Application

If you are renewing your current e-Cert (Server) on your server, please follow the instructions as described in the following sections:

| B. | Generating Certificate Signing Request (CSR) | 5 |
|----|--|-----|
| | Renewing your Current Server Certificate | .13 |
| C. | Submitting Certificate Signing Request (CSR) | |
| E. | Installing Server Certificate | 29 |

B. Generating Certificate Signing Request (CSR)

- Start Internet Information Services (IIS) Manager by clicking "Start" > "All Programs" / "Program" > "Administrative Tools" > "Internet Information Services (IIS) Manager".
- 2. In the "Internet Information Services (IIS) Manager" pane, expand "Web Sites" and select your web site, right-click and then click "Properties".

| 🐚 Internet Information Servi | ces (IIS) Manager | | |
|---|---|------|--------------|
| ዃ Eile <u>A</u> ction <u>V</u> iew <u>W</u> indo | w <u>H</u> elp | | _ B × |
| ← → 🗈 💽 🗙 😭 💈 | 🗈 😫 🖬 💂 🕨 🗉 | I II | |
| Internet Information Services → → → Application Pools → → → Web Sites → → → Default Web Site → → → Web Service Extensic | Name iisstart.htm pagerror.gif Explore Open Permissions Browse Start Stop Pause New All Tasks View New Window from Here Delete Rename Refresh Export List | Path | Statı |
| Opens the properties dialog box fc | Help | | |

3. In the "Directory Security" tab, click "Server Certificate".

| Default Web Site | Properties | | <u>? ×</u> |
|--|--------------------------------|-------------------------------|--|
| Web Site Documents | Performance Directory Security | ISAPI Filters HTTP Headers | Home Directory |
| Authentication and access control Enable anonymous access and edit the authentication methods for this resource. | | | <u>E</u> dit |
| IP address and domain name restrictions Grant or deny access to this resource using IP addresses or Internet domain names. Edįt | | | |
| Secure communications Require secure communications and enable client certificates when this resource is accessed. | | ns and S | erver Certificate View Certificate E <u>d</u> it |
| | ОК | Cancel | Apply Help |

Creating a New Server Certificate

Note: Please skip to Step14 if you are renewing your current server certificate.

4. In the "Web Server Certificate Wizard", click "Next" to continue.

| Welcome to the Web Server Certificate Wizard. | | |
|---|--|--|
| | Welcome to the Web Server Certificate Wizard | |
| | This wizard helps you create and administer server certificates used in secure Web communications between your server and a client. | |
| | Status of your Web Server: | |
| | Your Web Server doesn't have a certificate installed and you don't have any pending requests. Certificate Wizard will help you to create a new certificate for this Web Server or attach to an existing certificate. | |
| | To continue, click Next. | |
| | < Back (Next> Cancel | |

5. Select "Create a new certificate", and then click "Next".

| IIS Certificate Wizard |
|---|
| Server Certificate These are the methods for assigning a certificate to a Web site. |
| Select the method you want to use for this web site: |
| Import a certificate from a .pfx file Copy or Move a certificate from a remote server site to this site. |
| < <u>B</u> ack <u>N</u> ext > Cancel |

6. Select "Prepare the request now, but send it later", and then click "Next".

| IIS Certificate Wizard X | | | | |
|---|--|--|--|--|
| Delayed or Immediate Request You can prepare a request to be sent later, or you can send one immediately. | | | | |
| Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority? | | | | |
| Prepare the request now, but send it later | | | | |
| Send the request immediately to an online certification authority | | | | |
| < <u>B</u> ack Cancel | | | | |

7. Type a name (or accept the default) for the new certificate and choose 2048 for the "Bit length", and then click "Next".

Note: Bit length smaller than 2048 may not be strong enough, while greater than 2048 may be incompatible with certain web browsers. It is recommended the bit length of the encryption key to be 2048 in order to support better security strength.

| IIS Certificate Wizard | | |
|---|--|--|
| Name and Security Settings Your new certificate must have a name and a specific bit length. | | |
| Type a name for the new certificate. The name should be easy for you to refer to and remember. Name: | | |
| Default Web Site The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance. | | |
| Bit lengt <u>h</u> : 2048 Select cryptographic service provider (CSP) for this certificate | | |
| < <u>B</u> ack <u>N</u> ext > Cancel | | |

8. Type your organization's name and your organizational unit, and then click "Next".

| IIS Certificate Wizard |
|---|
| Organization Information Your certificate must include information about your organization that distinguishes it from other organizations. |
| Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department. For further information, consult certification authority's Web site. |
| |
| My Urganization |
| Organizational unit: |
| My Organizational Unit |
| |
| |
| |
| |
| < <u>B</u> ack <u>N</u> ext > Cancel |

9. Type the common name (i.e. server name) for your site, and then click "Next".

Note: For application of e-Cert (Server) with "Multi-domain" feature, please input the "Common Name" field with "Server name used as Subject Name in the Certificate" being filled in the application form. It is not necessary to specify any "Additional Server Name(s)" in the Subject Alternative Name of the CSR to be generated. It will be assigned by the Hongkong Post CA system automatically based on the information applied in the application form when the certificate is issued.

For application of e-Cert (Server) with "Wildcard" feature, please input the "Common Name" field with "Server Name with Wildcard" (including the wildcard component, i.e. the asterisk '*', in the left-most component of the server name), e.g. *.myserver.com, being filled in the application form.

| IIS Certificate Wizard | × | | |
|--|---|--|--|
| Your Site's Common Name | | | |
| Your Web site's common name is its fully qualified domain name. | 2 | | |
| Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name. | | | |
| If the common name changes, you will need to obtain a new certificate. | | | |
| Common name: | | | |
| www.myserver.com | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| < <u>B</u> ack <u>N</u> ext > Cancel | | | |
| | | | |

10. Select "HK (Hong Kong S.A.R.)" for the "Country/Region". Type "Hong Kong" for both "State/province" and "City/locality", and then click "Next".

| ieographical Information The certification authority req | quires the following geographical information. |
|---|--|
| <u>C</u> ountry/Region: HK (Hong Kong S.A.F ▼ | |
| <u>S</u> tate/province: | |
| Hong Kong | |
| City/Jocality: | |
| Hong Kong | |
| | ality must be complete, official names and may not contain |
| State/province and City/loca abbreviations. | |

11. Enter a file name for the certificate request, and then click "Next".

| IIS Certificate Wizard | × |
|--|-----------------|
| Certificate Request File Name Your certificate request is saved as a text file with the file name you specify. | |
| Enter a file name for the certificate request. File name: | |
| c:\certreq.txt | B <u>r</u> owse |
| | |
| | |
| | |
| | |
| | |
| | |
| < <u>B</u> ack <u>N</u> ext> | Cancel |

12. Click "Next".

Note: Please make sure that the correct domain name (i.e. server name) is shown in the "Issued To" field and "HK" in the "Country/Region" field.

| IIS Certificate Wizard | | × |
|---|---|--------|
| Request File Summary You have chosen to generate | a request file. | |
| To generate the following requ | iest, click Next. | |
| File name:c:\certreq.txt | | |
| Your request contains the follo | wing information: | |
| Issued To Friendly Name Country/Region State / Province City Organization Organizational Unit | www.myserver.com Default Web Site HK Hong Kong Hong Kong My Organization My Organizational Unit | |
| | < <u>B</u> ack (<u>Next</u> >) | Cancel |

13. Click "Finish" to close the wizard.



Renewing your Current Server Certificate

14. In the "Web Server Certificate Wizard", click "Next" to continue.



15. Select "Renew the current certificate", and then click "Next".

| IIS Certificate Wizard 🔀 |
|---|
| Modify the Current Certificate Assignment A certificate is currently installed on this Web site. |
| What do you want to do with the currently installed certificate? |
| Renew the current certificate |
| © <u>R</u> emove the current certificate |
| C Replace the current certificate |
| C Export the current certificate to a .pfx file |
| C Copy or Move the current certificate to a remote server site |
| |
| |
| |
| |
| < <u>B</u> ack <u>N</u> ext> Cancel |

16. Select "Prepare the request now, but send it later", and then click "Next".

| IIS Certificate Wizard |
|---|
| Delayed or Immediate Request You can prepare a request to be sent later, or you can send one immediately. |
| Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority? |
| Prepare the request now, but send it later |
| C <u>S</u> end the request immediately to an online certification authority |
| < <u>B</u> ack <u>N</u> ext > Cancel |

17. Enter a file name for the certificate request, and then click "Next".

| IIS Certificate Wizard | X |
|--|-----------------|
| Certificate Request File Name Your certificate request is saved as a text file with the file name you | (Est |
| specity. | |
| Enter a file name for the certificate request. | |
| <u>File name:</u> | |
| c:\certreq.txt | B <u>r</u> owse |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| Z Rank Mouth | Cancel |
| | |

18. Click "Next".

Note: Please make sure that the correct domain name (i.e. server name) is shown in the "Issued To" field and "HK" in the "Country/Region" field.

| IIS Certificate Wizard | | × |
|---|---|--------|
| Request File Summary You have chosen to generate a | a request file. | |
| To generate the following reque | est, click Next. | |
| File name: c:\certreq.txt | | |
| Your request contains the follow | ving information: | |
| Issued To Friendly Name Country/Region Organization Organizational Unit | www.myserver.com Default Web Site HK Hongkong Post e-Cert (Server) 0000812105 | |
| | < Back | Cancel |

19. Click "Finish" to close the wizard.

| IIS Certificate Wizard | × |
|------------------------|--|
| | Completing the Web Server Certificate Wizard |
| | You have successfully completed the Web Server Certificate wizard. A certificate request was created and saved to the file: |
| | c:\certreq.txt |
| | Send or e-mail this file to your certification authority, which will send you a response file containing your new certificate. |
| | To close this wizard, click Finish. |
| | < <u>B</u> ack Finish Cancel |

C. Submitting Certificate Signing Request (CSR)

1. Click on the hyperlink in the e-mail with subject "Submission of Certificate Signing Request (CSR)" sent from Hongkong Post Certification Authority to access the Hongkong Post CA web site.

| Submission of Certificate Signing Request (CSR) - Unicode (UTF-8) | |
|--|--------|
| Ble Edit Yew Iools Message Beb | |
| Sev Sev <th></th> | |
| rom: enquiry@hongkongpost.gov.hk Nate: Friday, July 29, 2011 3:04 PM ac ar@myserver.com Subject: Submission of Certificate Signing Request (CSR) | |
| Dear AR One. | |
| | |
| Submission of Certificate Signing Request (CSR) | |
| | |
| We are pleased to inform you that your application / renewal application for Hongkong Post e-Cert (Server) certificate | e has |
| been approved. The PIN Envelope will be sent to you separately by registered mail. You may then use the PIN Envelo | ope to |
| ne og ger Creape og Sillend Kredneg (CSK) te in te paper berevend og | |
| https://www1.honokonopost.gov.hk/hkpost/app/certreguest/web/home?lang=endich&channel=WFR&certCategory= | 5 |
| mprovide and a subscription of the subscription of the subscription and the subscription of | 2 |
| Please note that the new CA certificate (Hongkong Post e-Cert CA 1 - 10) is in effect from 26 February 2010 for isst | ing e- |
| Cert (Server). If you have not installed this new CA certificate in your server, please install it now from the following lin | ık |
| before the installation of your new e-Cert (Server). | |
| F. March March 1990 (and 1 and 1990 (and 19 | |
| http://www1.hongkongpost.gov.hk/root/ecert_ca_1-10_pem.crt | |
| | |
| Know how any analysis along a statut wat 2021 (C22 as he amality any in the status his | |
| If you have any enquiries, please contact us at 2921 6633 or by email to enquiry@hongkongpost.gov.hk. | |
| If you have any enquiries, please contact us at 2921 6633 or by email to <u>enquiry@hongkongpost.gov.hk</u> . Yours sincerely, | |

2. Type the "Server Name", the "Reference Number" (9-digit) as shown on the cover of the PIN Envelope and the "e-Cert PIN" (16-digit) as shown inside the PIN Envelope, and then click "Submit".

| こと Hongkong Post e-Cert 香港郵政電子核證 | The solution for e-Security | |
|--|---|---|
| | Welcome to generate e-Cert | ^ |
| | e-Cert (Server) | |
| | The personal data provided by Subscriber in this form will be used by Hongkong Post for processing the application. The Subscriber has the right of access and correction with respect to personal data as provided for in the Personal Data (Privacy) Ordinance. The right of access includes the right to obtain a copy of the Subscriber's personal data provided in this form. For other details, please read the Hongkong Post's Privacy Policy Statement and Personal Information Collection Statement | |
| िरितपुरुपाल Post मिनिय propa belanding kalanca स ∂ मा आत म | Server Particulars Server Name : www.myserver.com e-Cert PIN Envelope information: Reference Number: 000214360 (Shown on the cover of the PIN Envelope, 9-digit) e-Cert PIN: (No need to input the space within the 16-digit PIN) Submit Reset | |
| | 2007 © Important Notices Privacy Policy | |

3. Click "Submit" to confirm the application information. (If the information is incorrect, please contact Hongkong Post Certification Authority.)

| | Welcom e | e to generate e-Cert -Cert (Server) |
|------------------|---|--|
| | Subscriber Details | |
| | Server Name: | www.myserver.com |
| | Additional Server Name(s): | www.myserver2.com |
| | Number of Additional Server Name(s): | 1 |
| | Type of Certificate: | e-Cert (Server) with "Multi-domain" Feature |
| Svering business | Organization Name: | |
| | Branch Name: | |
| | Business Registraction No.: | 1234567890123456 |
| | Certificate of Incorporation / Certificate of Registration: | 12345678 |
| | Others: | |
| | Information of the certificate to be g | enerated |
| | Validity Period (in Month): | 12 |
| | This page is to confirm the applicati correct, please click "Confirm" to pro- | on data. If the above information is occeed |
| | Submit | Reject Back |

4. Open the previously generated Certificate Signing Request (CSR) with a text editor (e.g. Notepad) and copy the entire content including the "-----BEGIN NEW CERTIFICATE REQUEST-----" and "-----END NEW CERTIFICATE REQUEST-----". (You may refer to Part B Step 11 or Step 17 for the location of certificate request file.)

| 🗗 certreg - Notepad | | × |
|---|---|---|
| File Edit Format View Help | | |
| BEGIN NEW CERTIFICATE REQUEST MIIDZ2CCATACAQAwgYsxC2AJBGNVBAYTAKhLMRIWEAYDVQQIEw]Ib25nIEtvbmcx EjAQBgNvBACTCUhvbmcgS29uZ2EYMBYGALUEChMPTxkgT3JnYw5pemF0aw9uMR8w HQYDVQQLEXZNesBPcmdhbml6YxRpb25hbCBvbm]OMRkwFwyDVQQDExB3d3cubx1z ZXJ2ZXIuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCheR3SKJmgZxvB Qxse2lItQ37jNxQAEkPa2kxVJvBRM3VJOAZIpDvWfIk1md87n+ashNIKtxETm7j6 Vm6bu/JeQ/9X6Mgj4v9NU0I+P3Ixwf+R2D6nX361zBii6kSDnTV+beU/aQUrc1u 2IPktD5M7vhvZsjjWvIfb6NEiZRfnQIDAQABOIIBmTAaBgorBgEEAYI3DQIDMQwW CjuUmi4zNzkwLjIwewYKKWYBBAGCNWIBDjFtMGswDgYDVR0PAQH/BAQDAgTwMEQG CSqGSIb3DQEJDwQ3MDUwDgYIKoZIhvCNAWICAgCAMA4GCCqGSIb3DQMEAgIAgDAH BgUrDgMCBZAKBggqhkiG9w0DBZATBgNVHSUEDDAKBggrBgEFBQCDATCB/QYKKWYB BAGCNW0CAjGB7jCB6wIBAR5aAE0AaQBjAHIAbwBZAG8AZgB0ACAAUgBTAEEAIABT AEMAAABhAG4AbgBlAGwAIABDAHIAeQBwAHQAbwBnAHIAYQBwAGAAaQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA | | |
| | | ~ |
| <u><</u> | > | : |

5. Paste the content to the text box, and then click "Submit".



6. Click "Accept" to confirm acceptance of the certificate.

| ingkong/bute-Cert 香港都設電子机證 | The solution for e-security | | |
|---|--|--|--|
| | AAA | Welcome to generate e-Cert e-Cert (Server) | |
| | The following is the information of this | certificate | |
| ERTIZEN | Subscriber Details | | |
| | Server Name : | www.mvserver.com | |
| 2 M 1 | Additional Server Name(s) | www.myserver2.com | |
| 10000 | Organization Name : | My Organization | |
| | Branch Name : | and the second second | |
| Children and an inclusion of the second | Business Registraction No. : | 1234567890123456 | |
| | Certificate of Incorporation / Certificate of Registration | 12345678 | |
| | Others : | | |
| | The following is the system generated infor | mation | |
| | Subscriber Reference Number : | 0000821069 | |
| | e-Cert Type : | Hongkong Post e-Cert (Server) | |
| | Issued by : | Hongkong Post e-Cert CA 1 - 1 | 10 |
| | e-Cert Serial No. : | 2E4594 | |
| | e-Cert Validity Period : | 27/04/2013 to 27/04/2014 | |
| | Please click "Accept" to confirm accept rejecting the certificate. | ance of this certificate. Otherwise, please click "Rej | ect" and state the reasons for |
| | (Note :- Your personal data collected by of access and correction with respect to | Hongkong Post will be used for processing your e.c personal data as provided for in the Personal Data | ert application. You have the right (Privacy) Ordinance.) |
| | Accept | Reject | Cancel |
| | | | |

- 7. Click to download the following certificates:
 - Hongkong Post e-Cert (Server)
 - Hongkong Post e-Cert CA 1 10
 - Hongkong Post Root CA 1

Note: You can also download your e-Cert (Server) from the Search and Download Certificate web page. http://www.hongkongpost.gov.hk/en/sc

Note: If the "Hongkong Post e-Cert CA 1 - 10" certificate and the "Hongkong Post Root CA 1" certificate have been installed on your server before, you only need to download the "Hongkong Post e-Cert (Server)" certificate.



D. Installing Hongkong Post Root CA Certificate

 Start Microsoft Management Console (MMC) by clicking "Start" > "Run", type "mmc" and click OK, and then select "Add/Remove Snap-in" from the "File" / "Console" menu.

| 🚡 Console1 | | | |
|---------------------------------|-----------------------|--|--|
| File <u>A</u> ction <u>V</u> ie | ew Fav <u>o</u> rites | Vindow Help | |
| New | Ctrl+N | | |
| Open | Ctrl+O | | |
| Save | Ctrl+S | | |
| заve <u>н</u> s | | | |
| Add/Re <u>m</u> ove Sn | ap-in Ctrl+M | There are no items to show in this view. | |
| Options | | | |
| Recent File | | | |
| Exit | | | |
| h | | · | |
| | | | |
| | | | |
| Enables you to add | snap-ins to or rem | ove them from th | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

2. Click "Add".

| Add/Remove Snap-in |
|--|
| Standalone Extensions |
| Use this page to add or remove a stand-alone snap-in from the console. |
| Snap-ins added to: |
| |
| |
| |
| |
| Description |
| |
| Add <u>R</u> emove About |
| OK Cancel |

3. Select "Certificates", and then click "Add".

| 4 | dd Standalone Snap-in | | ? × | |
|--|---------------------------------------|---------------------------|-----|--|
| | Available standalone snap-ins: | | | |
| | Snap-in | Vendor | | |
| | NET Framework 1.1 Configuration | Microsoft Corporation | | |
| | Characteria and Trusts | Microsoft Corporation | | |
| | 🔛 Active Directory Sites and Services | Microsoft Corporation | | |
| | Active Directory Users and Compu | Microsoft Corporation | | |
| | al ActiveX Control | Microsoft Corporation | | |
| | 🛺 Authorization Manager | Microsoft Corporation | | |
| | 🗱 Certificate Templates | Microsoft Corporation | | |
| | 🖾 Certificates | Microsoft Corporation | | |
| | E Certification Authoncy | Microsoft Corporation | | |
| | Component Services | Microsoft Corporation | - | |
| Description The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer. | | | | |
| | [| <u>A</u> dd <u>C</u> lose | | |

4. Select "Computer account", and then click "Next".

| Certificates snap-in | × |
|---|---|
| | |
| This snap-in will always manage certificates for: | |
| ○ <u>My</u> user account | |
| O <u>S</u> ervice account | |
| Computer account | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| < <u>B</u> ack <u>N</u> ext > Cancel | |

5. Select "Local computer", and then click "Finish".

| Select Computer | × |
|---|---|
| Select the computer you want this snap-in to manage. This snap-in will always manage: | |
| < <u>B</u> ack Finish Cancel | |

6. Close the "Add Standalone Snap-in" dialog box, and then click "OK" to close the "Add/Remove Snap-in" dialog box.

Installing the "Hongkong Post e-Cert CA 1 - 10" Certificate

7. Expand "Intermediate Certification Authorities" and right-click "Certificates", and then select "All Tasks" > "Import".

| 🚡 Console1 - [Console Root\Certificates (Local Computer)\Intermediate Certification Authorities\Certificates] | | | | | |
|--|---|--|---|--|--|
| 📸 Eile Action View Favorites Window He | эlp | | _ & × | | |
| | | | | | |
| Console Root Cortificates (Local Computer) Orever Personal Orever Personal | Issued To A Microsoft Windows Hardware Com Root Agency VeriSign Class 1 CA Individual Sub | Issued By Microsoft Root Authority Root Agency Class 1 Public Primary Certification A | Expiration Date Inte 12/31/2002 Code 1/1/2040 <all< td=""> 5/13/2008 <all< td=""></all<></all<> | | |
| Enterprise Trust Enterprise Trust Enterprise Trust Intermediate Certification Authorities Certificates Certificates All Tasks Untrusted Publish Trusted People Trusted People SPC New <u>Uindow from Her</u> New <u>Uindow from Her</u> New <u>Iaskpad View</u> Refresh Export List Help | Verbign Class 1 CA Individual Sub Verbign Class 2 CA - Individual Sub Www.verisign.com/CPS Incorp.by Import | Class 1 Public Primary Certification A Class 2 Public Primary Certification A Class 3 Public Primary Certification A | 5/13/2008 <aii 1/7/2004 <aii 1/8/2004 2.16</aii </aii | | |
| | < | | Þ | | |
| Add a certificate to a store | | | | | |

8. In the "Certificate Import Wizard", click "Next" to continue.



9. Click "Browse" to locate the "Hongkong Post e-Cert CA 1 - 10" certificate that you downloaded in Part C Step 7 (ecert_ca_1-10_pem.crt), and then click "Next".

| Specify the file you want to import | rt. |
|---|--|
| | |
| Eile name: | |
| C:\ecert_ca_1-10_pem.crt | Browse |
| Note: More than one certificate | can be stored in a single file in the following formats: |
| | |
| Personal Information Exchang | <pre>pe- PKCS #12 (.PFX,.P12)</pre> |
| Personal Information Exchang Cryptographic Message Synta | ge- PKCS #12 (.PFX,.P12) ax Standard- PKCS #7 Certificates (.P7B) |
| Personal Information Exchang Cryptographic Message Synta Microsoft Serialized Certificate | ge- PKCS #12 (.PFX,.P12) ax Standard- PKCS #7 Certificates (.P7B) e Store (.SST) |
| Personal Information Exchang Cryptographic Message Synta Microsoft Serialized Certificate | ge- PKCS #12 (.PFX,.P12) ax Standard- PKCS #7 Certificates (.P7B) e Store (.SST) |
| Personal Information Exchang Cryptographic Message Synta Microsoft Serialized Certificate | ge- PKCS #12 (.PFX,.P12) ax Standard- PKCS #7 Certificates (.P7B) e Store (.SST) |
| Personal Information Exchang Cryptographic Message Synta Microsoft Serialized Certificate | ge- PKCS #12 (.PFX,.P12) ax Standard- PKCS #7 Certificates (.P7B) e Store (.SST) |
| Personal Information Exchang Cryptographic Message Synta Microsoft Serialized Certificate | ge- PKCS #12 (.PFX,.P12) ax Standard- PKCS #7 Certificates (.P7B) e Store (.SST) |

10. Select "Place all certificates in the following store", and then click "Next".

| Certificate Import Wizard | × |
|---|---|
| Certificate Store Certificate stores are system areas where certificates are kept. | |
| Windows can automatically select a certificate store, or you can specify a location for Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Intermediate Certification Authorities Browse | |
| < <u>B</u> ack <u>N</u> ext > Cancel | _ |

11. Click "Finish" to close the wizard.

| ertificate Import Wizard | Completing the Certif Wizard You have successfully completed the wizard. | ficate Import |
|--------------------------|---|--|
| | Certificate Store Selected by User Content File Name | Intermediate Certifica Certificate C:\ecert_ca_1-10_P ⁴ |
| | • | > |
| | < Back | inish Cancel |

12. Click "OK" to complete.

| Certificat | e Import Wizard 📃 🗙 | 1 |
|------------|----------------------------|---|
| (į) | The import was successful. | |
| | OK | |



Figure 1: "Hongkong Post e-Cert CA 1 - 10" certificate has been successfully installed

Installing the "Hongkong Post Root CA 1" Certificate

13. Expand "Trusted Root Certification Authorities" and right-click "Certificates", and then select "All Tasks" > "Import".

| 🚡 Console 1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates] | | | | | | |
|--|------------------------------|--------------------------------------|--|------------|------------|--|
| 🚡 Eile Action View Favorites Window Help | | | | | BX | |
| | | | | | | |
| Console Root Issued To A Issued By Expiration Date | | | | | | |
| 🖹 🗑 🐻 Certificates (Local Compu | uter) | ABA.ECOM Root CA | ABA.ECOM Root CA | 7/10/2009 | 2 | |
| 🕀 💼 Personal | | 🖼 Autoridad Certificadora de la Asoc | Autoridad Certificadora de la Asocia | 6/29/2009 | 2 | |
| 📄 📄 Trusted Root Certific | ation Authorities | 🖼 Autoridad Certificadora del Colegi | Autoridad Certificadora del Colegio | 6/30/2009 | 2 | |
| Certificates | All Tacks | N Import | Baltimore EZ by DST | 7/4/2009 | 2 | |
| Enterprise Trost | | Primary CA | Belgacom E-Trust Primary CA | 1/21/2010 | 2 | |
| Intermediate Ce Trucked Dublishe | <u>V</u> iew | KW HKT SecureNet CA Class A | C&W HKT SecureNet CA Class A | 10/16/2009 | 2 | |
| | New <u>W</u> indow from Here | 2&W HKT SecureNet CA Class B | C&W HKT SecureNet CA Class B | 10/16/2009 | | |
| Third-Party Poo | New Teckned View | 2&W HKT SecureNet CA Root | C&W HKT SecureNet CA Root | 10/16/2010 | 2 | |
| | New Taythan New | 2&W HKT SecureNet CA SGC Root | C&W HKT SecureNet CA SGC Root | 10/16/2009 | 5 | |
| F SPC | Refresh | Certisign - Autoridade Certificador | Certisign - Autoridade Certificadora | 6/27/2018 | 2 | |
| | Export <u>L</u> ist | Certisign - Autoridade Certificador | Certisign - Autoridade Certificadora | 6/27/2018 | 2 | |
| | Help | Certisign Autoridade Certificadora | Certisign Autoridade Certificadora A | 6/27/2018 | 2 | |
| | | Lertisign Autoridade Certificadora | Certisign Autoridade Certificadora A | 7/10/2018 | 2 | |
| | | 🕮 Class 1 Primary CA | Class 1 Primary CA | 7/7/2020 | 2 | |
| | | Class 1 Public Primary Certification | Class 1 Public Primary Certification A | 8/2/2028 | 2 | |
| | | Class 1 Public Primary Certification | Class 1 Public Primary Certification A | 1/8/2020 | 2 | |
| | | 🕮 Class 2 Primary CA | Class 2 Primary CA | 7/7/2019 | 2 | |
| | | Class 2 Public Primary Certification | Class 2 Public Primary Certification A | 1/8/2004 | 2 | |
| | | Class 2 Public Primary Certification | Class 2 Public Primary Certification A | 8/2/2028 | 2 | |
| | | 🕮 Class 3 Primary CA | Class 3 Primary CA | 7/7/2019 | 2 | |
| | | Class 3 Public Primary Certification | Class 3 Public Primary Certification A | 8/2/2028 | 2 | |
| | | Class 3 Public Primary Certification | Class 3 Public Primary Certification A | 1/8/2004 | 2 | |
| | | 🕮 Class 3P Primary CA | Class 3P Primary CA | 7/7/2019 | 2 | |
| | | 🔤 Class 3TS Primary CA | Class 3TS Primary CA | 7/7/2019 | 2 | |
| | | Copyright (c) 1997 Microsoft Corp. | Copyright (c) 1997 Microsoft Corp. | 12/31/1999 | Т | |
| | | E Deutsche Telekom Root CA 1 | Deutsche Telekom Root CA 1 | 7/10/2019 | ⊆ ▼ | |
| | | 4 | | | ► I | |
| Add a certificate to a store | | | | | | |

14. In the "Certificate Import Wizard", click "Next" to continue.

| Certificate Import Wizard | | × |
|---------------------------|---|---|
| | Welcome to the Certificate Import WizardThis wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.To continue, click Next. | |
| | < Back Cancel | |

15. Click "Browse" to locate the "Hongkong Post Root CA 1" certificate that you downloaded in Part C Step 7 (ecert_ca_1_pem.crt), and then click "Next".

| | orc, |
|----------------------------------|--|
| Eile name: | |
| C:\ecert_ca_1_pem.crt | Browse |
| Note: More than one certificate | can be stored in a single file in the following formats: |
| Personal Information Exchange | ge- PKCS #12 (.PFX,.P12) |
| Cryptographic Message Synta | ax Standard- PKCS #7 Certificates (.P7B) |
| Microsoft Serialized Certificate | e Store (.SST) |
| | |
| | |
| | |

16. Select "Place all certificates in the following store", and then click "Next".

| Certificate Import Wizard | × |
|---|---|
| Certificate Store Certificate stores are system areas where certificates are kept. | |
| Windows can automatically select a certificate store, or you can specify a location for Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browse | |
| < <u>B</u> ack <u>N</u> ext > Cancel | _ |

17. Click "Finish" to close the wizard.

| Certificate Import Wizard | Concession of the local division of the loca | |
|---------------------------|--|--|
| | Completing the Certi Wizard You have successfully completed th wizard. You have specified the following set | ficate Import ne Certificate Import ttings: |
| | Certificate Store Selected by User Content File Name | Trusted Root Certific Certificate C\ecert_ca_1_pem.c |
| | (| ¥ |
| 2 <u></u> | < <u>B</u> ack | Finish Cancel |

18. Click "OK" to complete.

| Certificat | e Import Wizard | × |
|------------|-----------------------|-------|
| (į) | The import was succes | sful. |
| | ОК | |

| Console1 - [Console Root\Certificates (Loca | l Computer)\Trusted Root Certificati | on Authorities\Certificates] | _ | ₽× |
|--|---------------------------------------|---|-----------------|-------|
| Eile Action View Favorites Window He | əlp | | | B× |
| | | | | |
| Console Root | Issued To 🔺 | Issued By | Expiration Date | I 🔺 |
| 🖻 🚳 Certificates (Local Computer) | Equifax Secure eBusiness CA-2 | Equifax Secure eBusiness CA-2 | 6/23/2019 | 5 |
| 🕀 🖳 Personal | Equifax Secure Global eBusiness C | Equifax Secure Global eBusiness CA-1 | 6/21/2020 | 5 |
| Trusted Root Certification Authorities | EUnet International Root CA | EUnet International Root CA | 10/2/2018 | 2 |
| Certificates | 🖼 FESTE, Public Notary Certs | FESTE, Public Notary Certs | 1/2/2020 | 5 |
| | EFESTE, Verified Certs | FESTE, Verified Certs | 1/2/2020 | 5 |
| | 🔛 First Data Digital Certificates Inc | First Data Digital Certificates Inc. Ce | 7/4/2019 | 5 |
| | FNMT Clase 2 CA | FNMT Clase 2 CA | 3/18/2019 | 2 |
| Third-Party Root Certification Authorities | 🔛 GlobalSign Root CA | GlobalSign Root CA | 1/28/2014 | 2 |
| | 🔤 GTE CyberTrust Global Root | GTE CyberTrust Global Root | 8/14/2018 | 5 |
| | GTE CyberTrust Root | GTE CyberTrust Root | 4/4/2004 | 5 |
| | | ане суботнаяскоос | | |
| | Hongkong Post Root CA 1 | Hongkong Post Root CA 1 | 5/15/2023 | |
| | Bhttp://www.yalicert.com/ | http://www.valicert.com/ | 6/26/2019 | c |
| | http://www.valicert.com/ | http://www.valicert.com/ | 6/26/2019 | - |
| | IPS SERVIDORES | IPS SERVIDORES | 12/30/2009 | |
| | Microsoft Authenticode(tm) Root | Microsoft | 1/1/2000 | s |
| | Microsoft Root Authority | Microsoft oot Authority | 12/31/2020 | |
| 🚔 GTE Cyber Hust Koot | GTE Cyber must Root | 2/24/20 | 00 | - |
| 🔤 Hongkong Post Root CA 1 | Hongkong Post Root C | A 1 5/15/20 |)23 | |
| 🔤 bttp://www.yalicert.com/ | http://www.yalicert.co | oml 6/26/20 | 110 | c |
| | NO LIABILITY ACCEPTED, (c)97 V | NO LIABILITY ACCEPTED, (c)97 Veri | 1/8/2004 | Т |
| | EPTT Post Root CA | PTT Post Root CA | 6/26/2019 | 5 |
| | 🔤 Saunalahden Serveri CA | Saunalahden Serveri CA | 6/26/2019 | 2 |
| | 🔤 Saunalahden Serveri CA | Saunalahden Serveri CA | 6/26/2019 | S 🕶 🛛 |
| | <u>I</u> | | | |
| Trusted Root Certification Authorities store contains 10 | 4 certificates. | | | |

Figure 2: "Hongkong Post Root CA 1" certificate has been successfully installed

E. Installing Server Certificate

- Start Internet Information Services (IIS) Manager by clicking "Start" > "All Programs" / "Program" > "Administrative Tools" > "Internet Information Services (IIS) Manager".
- 2. In the "Internet Information Services (IIS) Manager" pane, expand "Web Sites" and select your web site, right-click and then click "Properties".

| 🐌 Internet Information Servi | ces (IIS) Manager | | |
|---|---|------|--------------|
| ዃ Eile <u>A</u> ction <u>V</u> iew <u>W</u> indo | w <u>H</u> elp | | _ 8 × |
| ← → 🗈 💽 🗙 😭 💈 |) 🗈 😫 🖬 💂 🕨 | ■ II | |
| Internet Information Services myserver (local computer) Application Pools Web Sites Web Sites Web Service Extensic | Name iisstart.htm pagerror.gif Qpen Permissions Browse Start Stop Pause New All Tasks View New Window from Here Delete Rename Refresh Export List | Path | Statu |
| Opens the properties dialog box fc | Help | | |

3. In the "Directory Security" tab, Click "Server Certificate".

| Default Web Site | Properties |
|-----------------------|--|
| Web Site Documents | Performance ISAPI Filters Home Directory Directory Security HTTP Headers Custom Errors |
| Authentication | n and access control Enable anonymous access and edit the authentication methods for this resource. |
| TP address an | d domain name restrictions Grant or deny access to this resource using (P addresses or Internet domain names. Edit |
| - Secure commu | unications Require secure communications and enable client certificates when this resource is accessed. <u>View Certificate</u> <u>Edit</u> |
| | OK Cancel Apply Help |

4. In the "Web Server Certificate Wizard", click "Next" to continue.



5. Select "Process the pending request and install the certificate", and then click "Next".

| IIS Certificate Wizard | × |
|--|--------|
| Pending Certificate Request A pending certificate request is a request to which the certification authority has not yet responded. | |
| A certificate request is pending. What would you like to do? Process the pending request and install the certificate Delete the pending request | |
| < <u>B</u> ack <u>N</u> ext > | Cancel |

6. Click "Browse" to locate the "Hongkong Post e-Cert (Server)" certificate that you downloaded in Part C Step 7, and then click "Next".

| IIS Certificate Wizard |
|--|
| Process a Pending Request Process a pending certificate request by retrieving the file that contains the certification authority's response. |
| Enter the path and file name of the file containing the certification authority's response. Path and file name: |
| c:\cert0000812105.cer |
| |
| |
| |
| |
| |
| < <u>B</u> ack <u>N</u> ext > Cancel |

 Specify 443 for the "SSL port this web site should use", and then click "Next". (For IIS 5.0, please skip this step and go to step 8)

| IIS Certificate Wizard | × |
|---|--------------------------------------|
| SSL Port Specify the SSL port for this web site. | |
| SSL port this web site should use: | |
| | < <u>B</u> ack <u>N</u> ext > Cancel |

8. Click "Next".

| IIS Certificate Wizard | | × |
|---|---|--------|
| Certificate Summary You have chosen to i | nstall a certificate from a response file. | |
| To install the following | g certificate, click Next. | |
| File name: | c:\cert0000812105.cer | |
| Certificate details: Issued To Issued By Expiration Date Friendly Name Country/Region Organization Organizational Unit | www.myserver.com Hongkong Post e-Cert CA 1 - 10 11/19/2008 Default Web Site HK Hongkong Post e-Cert (Server) 0000812105 | |
| | < <u>B</u> ack <u>Next</u> > | Cancel |

9. Click "Finish" to close the wizard.



10. Click "View Certificate" to view the server certificate.

| Default Web Site I | properties | | | ? × |
|--|---|-------------------------------|--|-----------|
| Web Site Documents | Performance Directory Security | ISAPI Filters HTTP Head | Home E lers Custo |)irectory |
| Authentication Er au | and access control able anonymous access an uthentication methods for th | id edit the his resource. | <u>E</u> dit | |
| IP address and | domain name restrictions – ant or deny access to this i addresses or Internet dom | resource using Nain names, | Edįt | |
| Secure communers of the secure | nications equire secure communicatio hable client certificates whe source is accessed. | ns and n this | [Server Certifica View Certificat Edit | ite |
| | ОК | Cancel | Apply | Help |

| Certificate | ? × | | | |
|--|-----|--|--|--|
| General Details Certification Path | 1 | | | |
| Certificate Information | | | | |
| This certificate is intended for the following purpose(s): • All application policies | | | | |
| * Refer to the certification authority's statement for details. Issued to: www.myserver.com | - | | | |
| Issued by: Hongkong Post e-Cert CA 1 - 10 | | | | |
| Valid from 11/19/2007 to 11/19/2008 | | | | |
| | nt | | | |
| 0 | < | | | |

Figure 3: "Hongkong Post e-Cert (Server)" certificate has been successfully installed

F. Backing up the Private Key

Backing up the Private Key for IIS 5.0

1. Start Microsoft Management Console (MMC) by clicking "Start" > "Run", type "mmc" and click OK, and then select "Add/Remove Snap-in" from the "Console" menu.

| 🚡 Console1 | | | - D × |
|--|----------------------------|--|-------|
| <u>C</u> onsole <u>W</u> indow | Help 🗍 🗋 🗃 | | |
| New Open Save Save As Add/Remove Sna Options Recent File Exit | Ctrl+N Ctrl+O Ctrl+S | | |
| | , | | |

2. Click "Add".

| Add/Remove Snap-in | ?× |
|---|-------|
| Standalone Extensions | |
| Use this page to add or remove a standalone Snap-in from the console. | |
| Snap-ins added to: 🔄 Console Root | |
| | _ |
| | |
| | |
| | |
| | |
| | |
| - Description | |
| Description | |
| | |
| | |
| Add Hemove About | |
| ОК Са | ancel |

3. Select "Certificates", and then click "Add".

| 40 | ld Standalone Snap-in | | ? × |
|---|---|-------------------------|-----|
| | Available Standalone Snap-ins: | | |
| | Snap-in | Vendor | |
| | Relative Directory Domains and Trusts | Microsoft Corporation | |
| | 🜃 Active Directory Sites and Services 👘 | Microsoft Corporation | |
| | Active Directory Users and Computers | Microsoft Corporation | |
| | ativeX Control | | |
| | 🕮 Certificates 🦟 | Microsoft Corporation | |
| | 🙆 Component Service | Microsoft Corporation | |
| | 📙 Computer Management | Microsoft Corporation | |
| | 🚚 Device Manager | Microsoft Corporation | |
| | 💕 Disk Defragmenter | Executive Software Inte | |
| | Disk Management | VERITAS Software Cor | - |
| ļ | - Description | | |
| The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer. | | | |
| | | Add Close | • |

4. Select "Computer account", and then click "Next".

| Certificates snap-in | × |
|---|----------------------|
| | |
| This snap-in will always manage certificates for: | |
| My user account | |
| C Service account | |
| 💿 Computer account 🚤 | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | < Back Next > Cancel |

5. Select "Local computer", and then click "Finish".

| Select Computer | × |
|--|---|
| Select the computer you want this Snap-in to manage. This snap-in will always manage: C Local computer: (the computer this console is running on) Another computer: Allow the selected computer to be changed when launching from the command line. This only applies if you save the console. | |
| < Back Finish Cancel | - |

- 6. Close the "Add Standalone Snap-in" dialog box, and then click "OK" to close the "Add/Remove Snap-in" dialog box.
- 7. Backup the private key.
 - To backup the private key of a pending request, expand "Certificate Enrollment Requests" (or named "REQUESTS" in some systems) and select "Certificates", select the pending request that you just created, right-click and then select "All Tasks" > "Export".



To backup the private key of an existing certificate, expand "Personal" and select "Certificates", select the certificate that you would like to make a backup, right-click and then select "All Tasks" > "Export".



8. In the "Certificate Export Wizard", click "Next" to continue.



9. Select "Yes, export the private key", and then click "Next".

| Certificate Export Wizard | × | |
|--|---|--|
| Export Private Key You can choose to export the private key with the certificate. | | |
| Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page. | | |
| Do you want to export the private key with the certificate? | | |
| 💿 Yes, export the private key 🚤 | | |
| O No, do not export the private key | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | - | |
| < Back Next > Cancel | | |

10. Select "Personal Information Exchange - PKCS #12" and check the box "Enable strong protection", and then click "Next"

| Ce | ertificate Export Wizard | × | |
|--|--|---|--|
| _ | Export File Format Certificates can be exported in a variety of file formats. | | |
| | Select the format you want to use: | | |
| | C DER encoded binary X.509 (,CER) | | |
| C Base-64 encoded X.509 (,CER) | | | |
| | C Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B) | | |
| \square Include all certificates in the certification path if possible | | | |
| | Personal Information Exchange - PKCS #12 (.PFX) | | |
| \square Include all certificates in the certification path if possible | | | |
| | 🔽 Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above) | | |
| | Delete the private key if the export is successful | | |
| | | | |
| | < Back Next > Cancel | | |

11. Type and confirm a password for the private key, and then click "Next".

Note: It is very important that you remember this password. If you forget it, you will be unable to restore your private key.

| Certificate Export Wizard | × |
|---|-------|
| Password | |
| To maintain security, you must protect the private key by using a password. | |
| | |
| Type and confirm a password. | |
| Password: | |
| ***** | |
| Confirm password: | |
| **** | |
| , | |
| | |
| | |
| | |
| | |
| | |
| | |
| <back next=""> C</back> | ancel |

12. Specify the name of the file you want to export, and then click "Next". (By default, the file will be saved with a .PFX extension.)

| Certificate Export Wizard | | x |
|---|--|---|
| File to Export Specify the name of the file you want to ex | kport | |
| File name: | Prouto | |
| C: (myserver.prx | Browse | |
| | | |
| | | |
| | | |
| | | _ |
| | <pre> < Back Next > Cancel</pre> | |

13. Click "Finish" to close the wizard.

| Certificate Export Wizard | | × |
|---------------------------|--|-------------------------------|
| | Completing the Certificate E Wizard You have successfully completed the Certificate wizard. You have specified the following settings: | xport Export |
| | File Name Export Keys Include all certificates in the certification path File Format | C:\mys Yes No Person |
| | ✓ Sack Finish | Cancel |

14. Click "OK" to complete.

| Certificate Export Wizard | × |
|----------------------------|---|
| The export was successful. | |
| ОК | |

Backing up the Private Key for IIS 6.0

- Start Internet Information Services (IIS) Manager by clicking "Start" > "All Programs" > "Administrative Tools" > "Internet Information Services (IIS) Manager".
- 2. In the "Internet Information Services (IIS) Manager" pane, expand "Web Sites" and select your web site, right-click and then click "Properties".

| 🐌 Internet Information Servi | ces (IIS) Manager | | | |
|---|---|------|----|------------------|
| ዃ Eile <u>A</u> ction <u>V</u> iew <u>W</u> indo | w <u>H</u> elp | | | _ 8 × |
| ← → 🗈 💽 🗙 😭 |) 🗈 😫 🖬 💂 🕨 | ■ II | | |
| Internet Information Services Improve (local computer) Improve Application Pools Improve Sites Improve Default Web Site Improve Service Extensic Improve Service Extensic | Name iisstart.htm pagerror.g Explore Open Permissions Browse Stop Pause New All Tasks View New Window from Here Delete Rename Refresh Export List | Pat | th | Statı |
| Opens the properties dialog box fc | Help | | | |

3. In the "Directory Security" tab, click "Server Certificate".

|)efault Web Site | Properties ?> |
|---------------------------------|--|
| Web Site Documents | Performance ISAPI Filters Home Directory Directory Security HTTP Headers Custom Errors |
| Authentication | n and access control Enable anonymous access and edit the authentication methods for this resource. |
| □ IP address and C I I | d domain name restrictions Grant or deny access to this resource using IP addresses or Internet domain names. Edit |
| ⊂Secure commu e r | unications Require secure communications and enable client certificates when this resource is accessed. View Certificate Edit |
| | OK Cancel Apply Help |

4. In the "Web Server Certificate Wizard", click "Next" to continue.



5. Select "Export the current certificate to a .pfx file", and then click "Next".

| IIS Certificate Wizard | × |
|---|--------|
| Modify the Current Certificate Assignment A certificate is currently installed on this Web site. | |
| What do you want to do with the currently installed certificate? | |
| <u> Bemove the current certificate </u> | |
| Replace the current certificate Export the current certificate to a lofx file | |
| O Copy or Move the current certificate to a remote server site | |
| | |
| | |
| < <u>B</u> ack <u>N</u> ext > | Cancel |

6. Enter the path and file name of the file to export the certificate to, and then click "Next".

| IIS Certificate Wizard | × |
|--|-----------------|
| Export Certificate | |
| | |
| Enter the path and file name of the file to export the certificate to. | |
| Path and file name: | |
| c:\myserver.pfx | B <u>r</u> owse |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| < <u>B</u> ack <u>N</u> ext > | Cancel |

7. Type and confirm a password to encrypt the exported .pfx with, and then click "Next".

Note: It is very important that you remember this password. If you forget it, you will be unable to restore your private key.

| × |
|--------|
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| Cancel |
| |

8. Click "Next".

| IIS Certificate Wizard Export Certificate Summ You have chosen to exp | ary ort the following certificate. | × |
|---|--|--------|
| To export the following o | ertificate to this file, click Next. | |
| File name: c | :\myserver.pfx | |
| Certificate details: Issued To Issued By Expiration Date Friendly Name Country/Region Organization Organizational Unit | www.myserver.com Hongkong Post e-Cert CA 1 11/19/2008 Default Web Site HK Hongkong Post e-Cert (Server) 0000812105 | |
| | < <u>B</u> ack | Cancel |

9. Click "Finish" to close the wizard.



G. Restoring the Private Key

Restoring the Private Key for IIS 5.0

 Start Microsoft Management Console (MMC) by clicking "Start" > "Run", type "mmc" and click OK, and then select "Add/Remove Snap-in" from the "Console" menu.

| 🚡 Console1 | | | -OX |
|--|----------------------------|--|-----|
| <u>C</u> onsole <u>W</u> indow | Help 🛛 🗋 🚔 | | |
| New Open Save Save As Add/Remove Sna Options Recent File Exit | Ctrl+N Ctrl+O Ctrl+S | | |
| | | | |

2. Click "Add".

| Add/Remove Snap-in | ? × |
|---|----------|
| Standalone Extensions | |
| Use this page to add or remove a standalone Snap-in from the console. | |
| Snap-ins added to: 🔄 Console Root | |
| | <u> </u> |
| | |
| | |
| | |
| | |
| | |
| | |
| Description | _ |
| | |
| | |
| | |
| Add Hemove About | |
| OK Ca | ancel |

3. Select "Certificates", and then click "Add".

| 40 | ld Standalone Snap-in | | ? × |
|----|---|--|-----|
| | Available Standalone Snap-ins: | | |
| | Snap-in | Vendor | |
| | Relative Directory Domains and Trusts | Microsoft Corporation | |
| | 🜃 Active Directory Sites and Services 👘 | Microsoft Corporation | |
| | Active Directory Users and Computers | Microsoft Corporation | |
| | ativeX Control | | |
| | 🕮 Certificates | Microsoft Corporation | |
| | 🙆 Component Services | Microsoft Corporation | |
| | 📕 Computer Management 🎴 | Microsoft Corporation | |
| | 🚚 Device Manager | Microsoft Corporation | |
| | 💕 Disk Defragmenter | Executive Software Inte | |
| | Disk Management | VERITAS Software Cor | - |
| ļ | - Description | | |
| | The Certificates snap-in allows you to bro certificate stores for yourself, a service, o | wse the contents of the r a computer. | |
| | | Add Close | • |

4. Select "Computer account", and then click "Next".

| Certificates snap-in | × |
|---|----------------------|
| | |
| This snap-in will always manage certificates for: | |
| O My user account | |
| C Service account | |
| 💿 Computer account 🚤 | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | < Back Next > Cancel |

5. Select "Local computer", and then click "Finish".

| Select Computer |
|---|
| Select the computer you want this Snap-in to manage. This snap-in will always manage: C Local computer: (the computer this console is running on) C Another computer: C Another computer: C Allow the selected computer to be changed when launching from the command line. This only applies if you save the console. |
| < Back Finish Cancel |

- 6. Close the "Add Standalone Snap-in" dialog box, and then click "OK" to close the "Add/Remove Snap-in" dialog box.
- Expand "Personal" and select "Certificates", right-click and then select "All Tasks" > "Import". (To restore the private key of a pending request, expand "Certificate Enrollment Requests" (or named "REQUESTS" in some



8. In the "Certificate Import Wizard", click "Next" to continue.

| Certificate Import Wizard | | × |
|---------------------------|---|---|
| | Welcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. To continue, click Next. | |
| | <back next=""> Cancel</back> | |

9. Click "Browse" to locate the backup file of your private key, and then click "Next".

| Certificate Import Wizard | | × |
|--|--|----|
| File to Import Specify the file you want to import. | | |
| File name: C:\myserver.pfx | Browse | |
| Note: More than one certificate can be Personal Information Exchange- PKC | stored in a single file in the following formats: S #12 (.PFX,.P12) | |
| Cryptographic Message Syntax Stan | dard- PKCS #7 Certificates (.P7B) | |
| Microsoft Serialized Certificate Store | (.SST) | |
| | | |
| | | |
| | | |
| | < Back Next > Cance | el |

10. Type the password for the private key and then click "Next".

Note: To allow you to back up or transport your private key at a later time, you may mark this private key as exportable.

| rtificate Import Wizard | | |
|--|-------------|-------|
| Password | | |
| To maintain security, the private key was protected with a | a password. | |
| Tupe the paceword for the private law | | |
| Password | | |
| ***** | | |
| 1 | | |
| Enable strong private key protection. You will be | | |
| application if you enable this option. | | |
| | | |
|) Mark the private key as exportable | | |
| | | |
| | | |
| < Back | Next > | ancel |
| | | |

11. Select "Place all certificates in the following store", and then click "Next".

| Certificate Import Wizard | × |
|---|---|
| Certificate Store Certificate stores are system areas where certificates are kept. | |
| Windows can automatically select a certificate store, or you can specify a location for C Automatically select the certificate store based on the type of certificate Place all certificates in the following store | |
| Certificate store: Personal Browse | |
| | |
| < Back Next > Cancel | |

12. Click "Finish" to close the wizard.

| Certificate Import Wizard | | × |
|---------------------------|---|---|
| | Completing the Certificate Import Wizard You have successfully completed the Certificate Import wizard. You have specified the following settings: Certificate Store Selected by User Personal Content PFX File Name C:\myserver.pfx | |
| | < Back Finish Cancel | |

13. Click "OK" to complete.

| Certificat | e Import Wizard 🛛 🗶 |
|------------|----------------------------|
| ٩ | The import was successful. |
| | ОК |

Restoring the Private Key for IIS 6.0

- Start Internet Information Services (IIS) Manager by clicking "Start" > "All Programs" > "Administrative Tools" > "Internet Information Services (IIS) Manager".
- 2. In the "Internet Information Services (IIS) Manager" pane, expand "Web Sites" and select your web site, right-click and then click "Properties".

| 🐌 Internet Information Servic | ces (IIS) Manager | |
|--|--|--------------|
| ዃ Eile Action <u>V</u> iew <u>W</u> indov | w <u>H</u> elp | _ 8 × |
| ← → 1 1 1 × 1 | 🗟 😫 💷 💂 ▶ ■ 💷 | 1 |
| Internet Information Services Myserver (local computer) Application Pools Web Sites Default Web Site Web Service Extensic | Name Path iisstart.htm pagerror.gif Explore Open Open Permissions Browse Stop Stop Pause New All Tasks View New Window from Here Delete Rename Refresh Export List Properties Listen and the state and the | Statı |
| Opens the properties dialog box fc | | |

3. In the "Directory Security" tab, click "Server Certificate".

|)efault Web Site | Properties ? X | |
|--|---|--|
| Web Site Documents | Performance ISAPI Filters Home Directory Directory Security HTTP Headers Custom Errors | |
| Authentication | n and access control Enable anonymous access and edit the authentication methods for this resource. | |
| IP address and domain name restrictions Grant or deny access to this resource using IP addresses or Internet domain names. Edįt | | |
| Secure communications Require secure communications and enable client certificates when this resource is accessed. | | |
| | OK Cancel Apply Help | |

4. In the "Web Server Certificate Wizard", click "Next" to continue.



5. Select "Import a certificate from a .pfx file", and then click "Next".

| IIS Certificate Wizard | × |
|--|--------|
| Server Certificate These are the methods for assigning a certificate to a Web site. | |
| Select the method you want to use for this web site: | |
| < <u>B</u> ack <u>N</u> ext > | Cancel |

6. Enter the path and file name of the file containing the certificate and then click "Next".

Note: To allow you to back up or transport your certificate at a later time, you may mark this certificate as exportable.

| IIS Certificate Wizard | | × |
|---|---|---|
| Import Certificate You can import a certificate from a .PFX file. | | |
| Enter the path and file name of the file containing the certificate. Path and file name: | | |
| c:\myserver.pfx Specify whether the imported certificate should be marked as exportable Marking a certificate as exportable is a higher security risk, however it a certificate to be exported to a file for backup. | B <u>r</u> owse e after import. llows the | |
| < <u>B</u> ack <u>N</u> ext > | Cance | 1 |

7. Type the password for the certificate you want to import, and then click "Next".

| IIS Certificate Wizard | X |
|---|--------|
| Import Certificate Password To import a certificate, you must supply a password. | |
| Type the password for the certificate you want to import. Password: | |
| ••••• | |
| | |
| | |
| | |
| < <u>B</u> ack <u>N</u> ext > | Cancel |

8. Specify 443 for the "SSL port this web site should use", and then click "Next".

| IIS Certificate Wizard | × |
|---|--------------------------------------|
| SSL Port Specify the SSL port for this web site. | |
| SSL port this web site should use: | |
| | < <u>B</u> ack <u>N</u> ext > Cancel |

9. Click "Next".

| IIS Certificate Wizard | | × |
|---|--|--------|
| Imported Certificate S You have chosen to in | ummary nstall the following certificate. | |
| To install the following | imported certificate, click Next. | |
| File name: | c:\myserver.pfx | |
| Certificate details: Issued To Issued By Expiration Date Friendly Name Country/Region Organization Organizational Unit | www.myserver.com Hongkong Post e-Cert CA 1 11/19/2008 Default Web Site HK Hongkong Post e-Cert (Server) 0000812105 | |
| | < <u>B</u> ack | Cancel |

10. Click "Finish" to close the wizard.

| IIS Certificate Wizard | | |
|-------------------------------|---|--|
| | Completing the Web Server Certificate Wizard | |
| | You have successfully completed the Web Server Certificate wizard. | |
| | A certificate is now installed on this server. | |
| | If you need to renew, replace, or delete the certificate in the future, you can use the wizard again. | |
| | To close this wizard, click Finish. | |
| < <u>Back</u> [Finish] Cancel | | |

