NHS SPINE Project

Generating CSR and Installing Certificates

Issue 1 Draft A

08 May 2006Copyright

Confidentiality

Distribution

BT Project Office	BT Guidion House, Harvest Crescent, Ancells Business Park, Fleet, Hampshire, GU51 2QP
Other Parties	

Document Control

Title	CSR-Install-Certificates
Author	Prasad Avadhanula
Doc Ref	CSR-Install-Certificatesv1.doc

Owner (Responsible for Approval of Issued Versions)				
Name	Role	Signature	Date	Issue
Prasad Avadhanula				

Review Panel			
Name	Role	Name	Role

Change History			
Issue	Date	Author/ Editor	Details of Change
Issue 1 Draft A	08 May 2006	Prasad Avadhanula	Draft for Internal review

Table of Contents

1 INTRODUCTION 5

2 GENERATING CSR 6

2.1 Overview CSR 6

2.2 To generate keys and a CSR on Microsoft® IIS 4.x 6

2.3 To generate keys and a CSR on Microsoft® IIS 5.x/6.x 8

2.4 To generate keys and a CSR on Sun™ ONE 9

2.5 To generate keys and a CSR on Red Hat Stronghold 10

2.6 To generate keys and a CSR on IBM® HTTP Server 12

2.7 To generate keys and a CSR Apache mod_ssl 13

3 SUBMITTING THE CERTIFICATE REQUEST 16

3.1 To Install the Web server certificate on Microsoft® IIS 4.x 17

3.2 To Install the Web server certificate on Microsoft® IIS 5.x/6.x 17

3.3 To install the Web server certificate on Sun™ ONE 18

3.4 To install the Web server certificate on Red Hat® Stronghold 18

3.5 To install the Web server certificate on IBM® HTTP Server 19

3.6 To install the Web server certificate on Apache mod_ssl 19

4 IMPORTING CA CERTIFICATES INTO WEB SERVER.....21

4.1 To import the CA certificate using Internet Explorer on IIS 21

4.2 To import the CA certificate on Sun ONE™ 21

4.3 To import the CA certificate on Red Hat® Stronghold 22

4.4 To import the CA certificate on IBM® HTTP Server 23

5 IMPORTING THE CA CERTIFICATE INTO A WEB BROWSER 24

5.1 Importing the CA certificate using Internet Explorer 24

1 Introduction

This document provides instructions on how to generate a Web server certificate Request, submit it to NHS Certificate Enrollment Service and Install certificates on Web servers.

Topics in this section:

- Generating a certificate request (CSR)
- Submitting the certificate request to NHS Certificate Enrollment Service
- Installing certificates on Webserver
- Importing CA certificates into web server

2 Generating CSR

2.1 Overview CSR

A certificate signing request (CSR) is a message sent from an Entity (applicant or server) to a certificate authority in order to apply for a digital identity certificate.

The Certificate Signing Request is required by NHS Certificate Enrollment service to generate your SSL/TLS certificate, and must be submitted to NHS Certificate Enrollment service during the enrollment process.

CSR contains the following:

Before generating a CSR, the Entity generates a key pair, keeping the private key secret. The CSR contains information about Entity (such as a domain name, common name), and the public key chosen by the applicant.

The Web Server Technical Guide should help you to generate a CSR. However you may use the information provided in this Guide to generate CSR.

Once you generate CSR you need to submit the request to NHS Certificate Enrollment service. After you submitting the CSR on NHS Certificate Enrollment service you can obtain a signed certificate from NHS CA.

NHS Certificate Enrollment service accepts two different types of certificate requests:

- PKCS #10
- SPKAC

Once NHS Certificate Enrollment server accepts the certificate request, it actually uses proto-PKIX (pre-finalized version of PKIX) to sent it to CA. SPKAC is not a standard, but Netscape publishes the format and at least one other vendor (Opera) uses it. Note: PKCS #10 is the Default standard for all certificate requests.

Follow the instructions that apply to your Web server to generate a certificate request:

2.2 To generate keys and a CSR on Microsoft® IIS 4.x

1) Run the Management Console.

2) Expand the (IIS) Internet Information Server.

3) Expand the computer name you are securing.

3) Right-click on the website you want to apply certificate, and select Properties.

4) Open Directory Security tab.

5) Under Secure Communications, Select Create New Key.

6) The Create New Key Wizard is launched.

6) Select 'Put the request in a file...', and select a filename or accept the default.

7) Fill in the required information as below:

Name	Description	Example
Friendly name	Name of the request	mynewcsr
Password	Password to protect your private key and select next	mypassword
Select a bit length value for your new Private Key	It is recommended that you choose a 1024-bit key if that option is available.	512
Select Next.	Select Next.	Select Next.
Organization Name	Supply the name of your company or organization.	BT Syntegra
Organizational Unit Name	Department/Division Name	IT
Common Name	**Enter the reference number you obtained from the Administrator.**	904720177E
Select Next.	Select Next.	Select Next.
Country Name	Enter the corresponding ISO3166 country code for the country.	GB
State or Province Name	Enter the corresponding state or province, without abbreviations.	YorkShire
Locality Name	Supply the city or locality name	Leeds
Your Name	Your Name	Administrator
Email address	Email address	sysadmin@bt.com
Phone number	Phone number	93287947632

Select finish

8) Before closing the Key Manager: Select Computer from the toolbar menu. Select Commit Changes Now to save your information and Select Yes when prompted with the dialogue alert.

9) Now open the CSR file using a text editor such as notepad, and copy and paste the text (including the BEGIN and END tags) into the NHS Certificate Enrollment Service order form.(Refer : Submitting the certificate request to NHS Certificate Enrollment Service)

2.3 To generate keys and a CSR on Microsoft® IIS 5.x/6.x

1) From the Administrative Tools, run the Internet Services Manager

2) Right-click on the website you are securing

3) Select Properties. Click on the Directory Security tab

4) Click the Server Certificate button.

5) Click next. Choose 'Create a new certificate' and click next.

6) Choose 'Prepare the request now, but send it later' and click next.

Name	Description	Example
Name of the new Certificate	Enter a name for the certificate that you can identify on your server	My New Certificate
Bit-length	Choose a bit-length of 1024. Leave the other boxed un-checked.	1024
Click Next	Click Next	Click Next
Organization Name	Enter the full legal name of your company.	BT Syntegra
Organizational Unit Name	Enter a department such as 'IT Development' in the organizational unit.	IT Development
Click Next	Click Next	Click Next
Common Name	Enter the reference number you obtained from the	904720177E

	Administrator.	
Click Next	Click Next	Click Next
Country Name	Enter the corresponding ISO3166 country code for the country.	GB
State or Province Name	Enter the corresponding state or province, without abbreviations.	YorkShire
Locality Name	Supply the city or locality name	Leeds
Click Next	Click Next	Click Next
File name CSR	Choose a file name and a location to save your Certificate Signing Request (CSR). The file should be saved as a text file (.txt)	csr.txt
Click next to generate the file	Click next to generate the file	Click next to generate the file
Name of the new Certificate	Enter a name for the certificate that you can identify on your server	My New Certificate
Click Next	Click Next	Click Next

7) Now open the CSR file using a text editor such as notepad, and copy and paste the text (including the BEGIN and END tags) into the NHS Certificate Enrollment Service order form.(Refer : Submitting the certificate request to NHS Certificate Enrollment Service)

2.4 To generate keys and a CSR on Sun™ ONE

1) Log into App Server as Admin

2) Server<instance>: Security -> Manage Database

3) Create a new trust database password

4) Server<instance>: Security -> Certificate Management tab, fill in the Request a Certificate fields as follows:

Name	Description	Example
CA Email Address	E-mail Address of requestor	myname@mycompany.com
Key pair password	Password that used above	mypassword
Requester name	Requester name	System Admin
Telephone number	Telephone number.	36432625234
Common name	Enter the reference number you obtained from the Administrator.	904720177E
Organization Name	Enter the full legal name of your company.	BT Syntegra
Organizational Unit Name	Enter a department such as 'IT Development' in the organizational unit.	IT Development
Country Name	Enter the corresponding ISO3166 country code for the country.	GB

5) Click OK; and copy and paste the text (including the BEGIN and END tags) into the NHS Certificate Enrollment Service order form. (Refer: Submitting the certificate request to NHS Certificate Enrollment Service)

2.5 To generate keys and a CSR on Red Hat Stronghold

1) Run the genkey utility, specifying the name of the host or virtual host:

bin/genkey <hostname>

genkey prints the filenames and locations of the key file and certificate file it is about to generate.

The key is stored in:

<ServerRoot>/ssl/private/<hostname>.key

The certificate is stored in:

<ServerRoot>/ssl/certs/<hostname>.cert

2) Press the Enter key.

genkey reminds you not to overwrite an existing key pair and certificate.

3) Press the Enter key.

genkey prompts you to specify the size of the key.

4) Enter a key size between 512 or 1024 bits.

Note: If you choose a key length less than 768, your certificate lasts for 12 months, by default. If you choose a key between 768 and 1024 bits, your certificate lasts for 24 months, by default. If you customize the lifetime of the certificate in Security Manager, you cannot exceed these default values. genkey generates random data with which to create a unique key pair. It then prompts you for random keystrokes.

5) Type random keystrokes on your keyboard. Stop when the counter reads “0” and genkey beeps and displays this message:

0 * -Enough, thank you

genkey generates the key pair and saves it in the following location:

ServerRoot/ssl/private/hostname.key

genkey asks if you want to use the genreq utility to send a CSR.

6) Type Y to send a CSR.

The genreq utility is launched automatically. genreq displays a lettered list of CAs and asks which one you want to use.

7) Type the letter that corresponds to your preferred CA.

8) Type the two-letter code for your country. For example, type US for the United States, DE for Germany or JP for Japan.

9) Type the following information when prompted:

. The full name of your province or state

• Your city, town, or other locality

• Your organization

• Your unit within the organization

• The reference number you obtained from Administrator This information goes in the Common Name field.

genreq generates the CSR, which looks something like this:

-----BEGIN NEW CERTIFICATE REQUEST-----

MIIBEzCBzgIBADB7MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5p

YTEQMA4GA1UEBxMHT2FrbGFuZDEbMBkGA1UEChMSQzJOZXQgU29mdHdhcmUg

SW5jMRAwDgYDVQQLEwdUZXN0aW5nMRYwFAYDVQQDEw1nYWJiZXIuYzIubmV0

MEwwDQYJKoZIhvcNAQEBBQADOwAwOAIxAJukoQhq4LanG2k+LnRTGJAcgv9L

JPsdfCsjqRs8ygoyaw4ucOEdx+WdnM0x36NcQIDAQABMA0GCSqGSIb3DQEBB

AUAAzEABRLR6IkG70oNG1MnvuMDeWou4kIvc98ysjssCNKsDKsHAXBSEbfsI

Qs5JRNagVBW

-----END NEW CERTIFICATE REQUEST-----

10) You have generated a certificate request. Copy CSR into the clipboard and Proceed to “Web Server" link under Certificate Retrieval on the NHS Certificate Enrollment Service website

2.6 To generate keys and a CSR on IBM® HTTP Server

1) Start the iKeyMan utility. For instructions on starting this utility, refer to the iKeyMan User Guide.

2) Select Key Database File, and then click New.

3) In the Password Prompt dialog box, enter a new password and click OK. Ensure you select the “Stash the Password to file” option to create the key.sth file.

4) Save this file into the default key.kdb file or create your own file name.

5) Click OK.

6) Select Create from the main User Interface, and then click New Certificate Request.

7) The New Key and Certificate Request dialog box opens.

Name	Description	Example
Key Label	Enter descriptive comments that will identify the key and certificate in the database.	Key Label
Keysize	Enter a size for the key	Keysize

	between 512 and 1024 bits.	
Common Name	Enter the reference number you obtained from the Administrator.	Common Name
Organization Name	Supply the name of your company or organization.	Organization Name
Organizational Unit Name	Department/Division Name	Organizational Unit Name
Country Name	Enter the corresponding ISO3166 country code for the country.	Country Name
State or Province Name	Enter the corresponding state or province, without abbreviations.	State or Province Name
Filename	Certificate request filename Enter a new name for the certificate request file, or use the default file name.	Filename

10) You have generated a certificate request. Copy and paste the text (including the BEGIN and END tags) into the NHS Certificate Enrollment Service order form. (Refer: Submitting the certificate request to NHS Certificate Enrollment Service)

2.7 To generate keys and a CSR Apache mod_ssl

1) Logon to the server and type the following command

openssl req -new -nodes -keyout <server-name>.key -out <server-name>.csr Where <server-name> is your server name.

Note: This generates two files: the Private-Key file for the decryption of your SSL Certificate, and a certificate signing request (CSR) file. CSR is used to apply for your SSL/TLS Certificate on NHS Certificate Enrollment Service.

Note: Be sure to backup the private key, as there is no means to recover it should it be lost. The private key wil be needed later when installing the certificate issued to you in response to submitting your Certificate Signing Request (CSR).

2) You will then be prompted for following information

Name	Description	Example
Country Name	Enter the corresponding ISO3166 country code for the country.	GB
State or Province Name	Enter the corresponding state or province, without abbreviations.	YorkShire
Locality Name	Supply the city or locality name	Leeds
Organization Name	Supply the name of your company or organization.	BT Syntegra
Organizational Unit Name	Department/Division Name	IT Development
Common Name	Enter the reference number you obtained from the Administrator.	904720177E
Email Address	DO NOT USE.	Leave Blank
A challenge password []:	DO NOT USE.	Leave Blank
An optional company name	DO NOT USE.	Leave Blank

3 Submitting the certificate request

After generating a Web server certificate request (CSR) for the Web server, submit the certificate request to NHS Certificate Enrollment Service.

To submit the request

1) Access NHS Certificate Enrollment Service by typing http://<esw-host>/cda-cgi/clientcgi?action=start

2) In the Certificate Retrieval menu on the left, click Web server.

The Web server Certificate Request page opens.

3) Enter the reference number and authorization code for the Web server that you obtained.

4) In the Options field, choose the format for the Web server certificate. The choices are:

• Raw Distinguished Encoding Rules (DER) format

DER format displays the certificate in raw text format.

• Public-Key Cryptographic Standard #7 (PKCS7).

PKCS7 displays the certificate with mark-up tags.

To determine which option to choose, find out how your Web server processes certificates. For more information, consult your Web server documentation.

5) Paste the certificate request (CSR) into the large text box.

6) Click Submit Request.

CA generates a Web server certificate and sends it to browser.

7) Click Download on the page displaying your certificate.

8) In the File Download dialog box, click OK to save this file to disk.

9) In the Save As dialog box, choose a name and path of a text file in which to save the certificate.

10) Click Save. The certificate is saved in the text file you specified. Proceed to “Install Web server certificates”.

3.1 To Install the Web server certificate on Microsoft® IIS 4.x

1) Launch the Microsoft Management Console (MMC) and Go to Key Manager.

2) Select the web site you want to secure and select the Key Manager.

3) Right-click the key that was created when you generated the Certificate Signing Request (CSR) and select Install Key Certificate.

4) The Open dialog box appears.

5) Select the file that contains your SSL Certificate and click Open. The Password dialog box appears.

6) Supply the password you chose when you created the key pair and click the OK button.

7) The Server Bindings dialog appears and click the OK button unless you want to use this certificate with specific IP addresses and port numbers and Select OK.

8) Select Computers/ Commit Changes Now, to save your changes and Select OK.

9) Restart the server.

You have installed the Web server certificate into your Web server.

Now check you can navigate to the sever by using https:/ /<server-host> you should see the browser padlock turn on.

3.2 To Install the Web server certificate on Microsoft® IIS 5.x/6.x

1) Go to your Administrative Tools, and Open the Internet Services Manager.

2) Right-Click on the Default Website and select Properties.

3) Go to the Directory Security panel.

4) Click on Server Certificate

5) You will be prompted to either process the Pending Certificate Request or delete it.

6) Select process the Pending Certificate Request and Click Next.

7) Supply the Path and file name of the file that contains your Entrust SSL Certificate and Select Next.

8) Review the Certificate Summary and Select Next

9) Select Finish completing the certificate installation.

10) Restart the Server.

Now check you can navigate to the sever by using https:/ /<server-host> you should see the browser padlock turn on.

3.3 To install the Web server certificate on Sun™ ONE

1) Open the Sun ONE Administer Web Server page.

2) Click Admin Server server1: Security General, click the Install hyperlink

3) Enter the Key Pair File Password

4) Click Message Text (with Headers)

5) Paste the PKCS#7 certificate content that you retrieved from NHS Certificate Enrollment Service

6) Click OK

7) Navigate to HTTP Listeners

8) Click the New tab

Name: <hostname>-sec

Port: 443

9) Return Server Name: <hostname>-sec

10) Check SSL/TLS Enabled, SSL3 Enabled, TLS Enabled

11) Save

12) Navigate to top level Server1, Apply changes and restart the server. You will need to enter the Key Pair File Password again.

Now check you can navigate to the sever by using https:/ /<server-host> you should see the browser padlock turn on.

3.4 To install the Web server certificate on Red Hat® Stronghold

1) Copy the PKCS#7 certificate that you retrieved from NHS Certificate Enrollment Service into a text editor and save as servercert.txt

2) Save the file.

3) Run Stronghold's getca utility, specifying the name of the host that owns this certificate and providing the certificate file as input:

getca <hostname> <path_of_file_that_contains_certificate>

For example:

getca webserverA.YourCompany.com c:/certificate/servercert.txt

This command saves the certificate in the file hostname.cert.

4 Restart Stronghold to implement the new certificate by entering the following command:

reload-server

You have installed the Web server certificate into your Web server.

Now check you can navigate to the sever by using https:/ /<server-host> you should see the browser padlock turn on and receive no errors.

3.5 To install the Web server certificate on IBM® HTTP Server

1) Start the iKeyMan utility. For instructions on starting this utility, refer to the iKeyMan User Guide.

2) Select Key Database File and click Open.

3) In the Open dialog box, enter the key database name. You created this name while generating CSR.

4) Click OK.

5) In the Password Prompt dialog box, enter the password.

6) Click OK.

7) Select Personal Certificates in the Key Database menu and click Receive.

8) In the Receive Certificate from a File dialog box, enter the name of a valid Base64-encoded file in the Certificate filename text field.

If the CA who issues your certificate is not a trusted CA in the key database you might be unable to import the certificate. To store the CA certificate and designate the CA as trusted, please import the CA Certificate into Webserver.

9) Click OK.

3.6 To install the Web server certificate on Apache mod_ssl

1) Copy the PKCS#7 certificate that you retrieved from NHS Certificate Enrollment Service into a text editor

2) Save the file as server.crt.

3) Now you have two files: server.key and server.crt. These now can be used as following inside your Apache's httpd.conf file:

```
SSLCertificateFile     /path/to/this/server.crt
SSLCertificateKeyFile /path/to/this/server.key
```

4 Importing CA certificates into web server

4.1 To import the CA certificate using Internet Explorer on IIS

1) Access NHS Certificate Enrollment Service.

2) In the menu “ROOT CA and SUB CA Certficates”, click “Install ROOTCA cert (DER format)

3) The File Download dialog box appears.

The Save As dialog box appears.

4) Click OK to download the file.

5) Enter a path and name for the text file in which to save the certificate.

6) Click Save.

7) Right-click the certificate you just retrieved and click install Certificate from the pop-up menu.

8) Click Next.

9) Select Place all certificates into the following store.

10) Click Browse....

The Certificate Store dialog box appears.

11) Select Show Physical Stores.

12) Expand the Trusted Root Certification Authorities folder.

13) Click the Local Computer folder and click OK.

14) Click Next and then click Finish.

The message “The import was successful” appears.

15) Click OK.

4.2 To import the CA certificate on Sun ONE™

1) Access NHS Certificate Enrollment Service

2) In the "ROOT CA and SUB CA Certficates" menu on the left, View ROOTCA cert .

3) The CA Certificate window opens with the CA certificate included.

4) Copy the entire certificate into the clipboard.

5) Open the Sun ONE Administer Web Server page.

6) Choose the Web server which will manage Enrollment Server for Web and click Manage.

7) Click the Securities tab.

8) Click Install Certificate.

9) In the Certificate For frame, select the Trusted Certificate Authority (CA) option.

10) Enter your Key Pair File Password.

11) Select the Message Text (with headers) option.

12) In the Message Text (with headers) field, paste the certificate that you copied to the clipboard.

9 Click OK.

The Add Server Certificate Web page appears.

10 Click Add Server Certificate.

You have imported the Web server certificate into the Trust database on your Web server. Now the Sun ONE Web Server can verify signatures on all browser certificates signed by that NHS CA.

4.3 To import the CA certificate on Red Hat® Stronghold

1) Access NHS Certificate Enrollment Service

2) In the "ROOT CA and SUB CA Certficates" menu on the left, View ROOTCA cert (PEM format).

3) The CA Certificate window opens with the CA certificate included.

4) Copy the entire certificate into the clipboard.

5) Ensure that the CA certificate is in PEM format.

6) Open a text editor and paste the CA certificate you copied to the clipboard.

7) Save the file with a .pem extension.

8) Go to the directory that contains the text file containing CA certificate.

9) Enter the following command to append the CA certificate to the existing

Certificate file you downloaded:

cat newcert.pem >> <CA_certificate_filename>.pem

10) You have imported the CA certificate into your Web server. Now the Stronghold Web Server can verify signatures on all browser certificates signed by that CA.

4.4 To import the CA certificate on IBM® HTTP Server

1) Access NHS Certificate Enrollment Service

2) In the "ROOT CA and SUB CA Certficates" menu on the left, View ROOTCA cert (PEM format).

3) The CA Certificate window opens with the CA certificate included.

4) Copy the entire certificate into the clipboard.

5) Start the iKeyMan utility. For instructions on starting this utility, refer to the iKeyMan User Guide.

6) Select Key Database File and click Open.

7) In the Open dialog box, enter the key database name.

8) Click OK.

9) In the Password Prompt dialog box, enter the password.

10) Copy and paste the entire certificate, including the BEGIN and END lines, into a file with an .arm extension.

13) Select Signer Certificates in the Key Database window, then click Add.

14) In the Add CA's Certificate from a File dialog box, select the certificate file name, or browse to the file.

15) Click OK.

16) In the Label dialog box, enter a label name and click OK.

17) You have imported the CA certificate into your Web server. Now the IBM HTTP Server can verify signatures on all browser certificates signed by that CA.

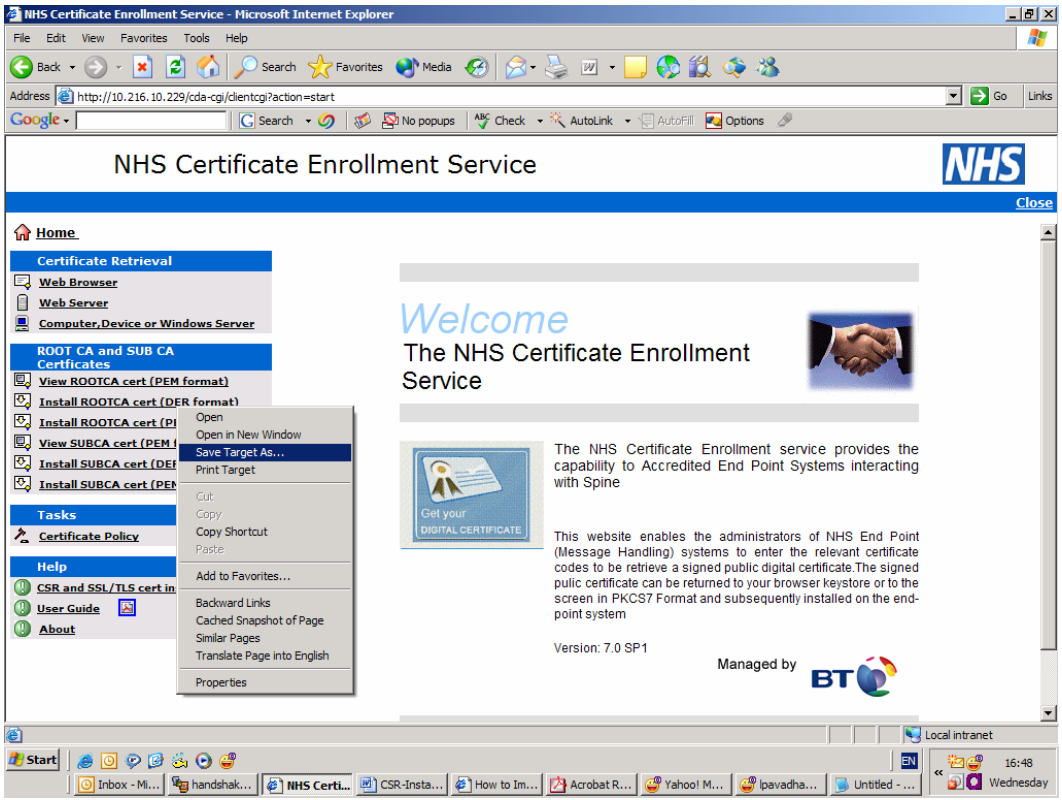
5 Importing the CA certificate into a Web browser

If NHS ROOT CA does not exist in browser root store, you can import it as follows:

5.1 Importing the CA certificate using Internet Explorer

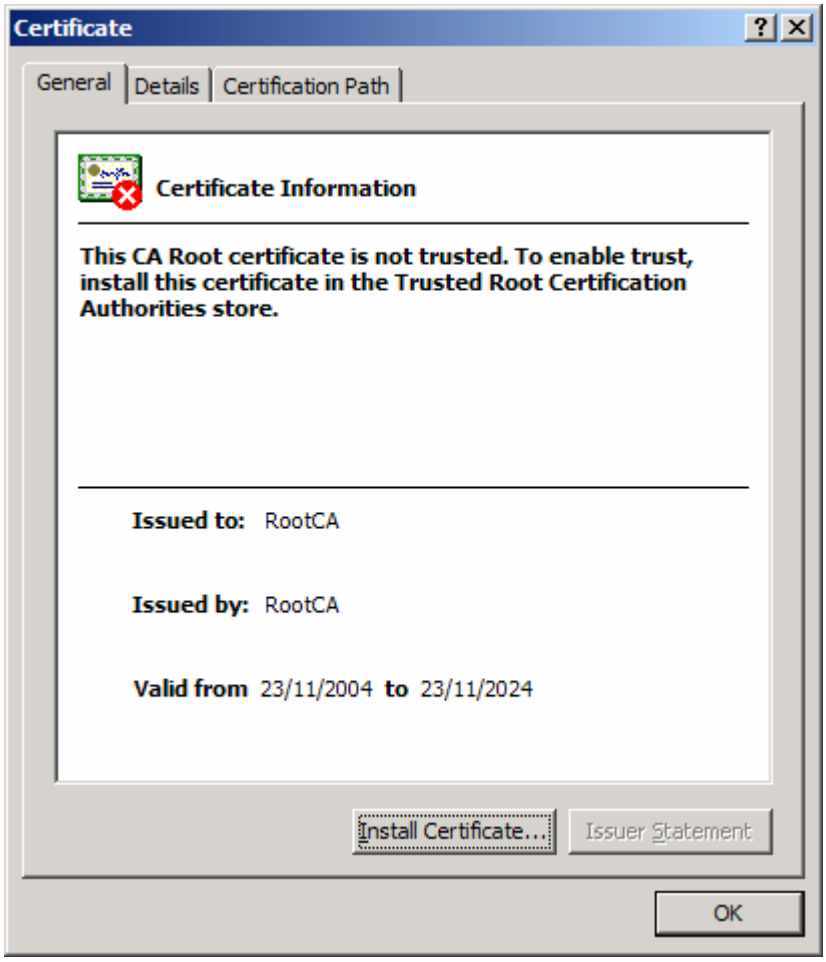
1) Visit the NHS Certificate Enrollment Service Website

2) Right click and "Save As" the link "Install ROOTCA cert (DER format)" under ROOT CA and SUB CA Certificates

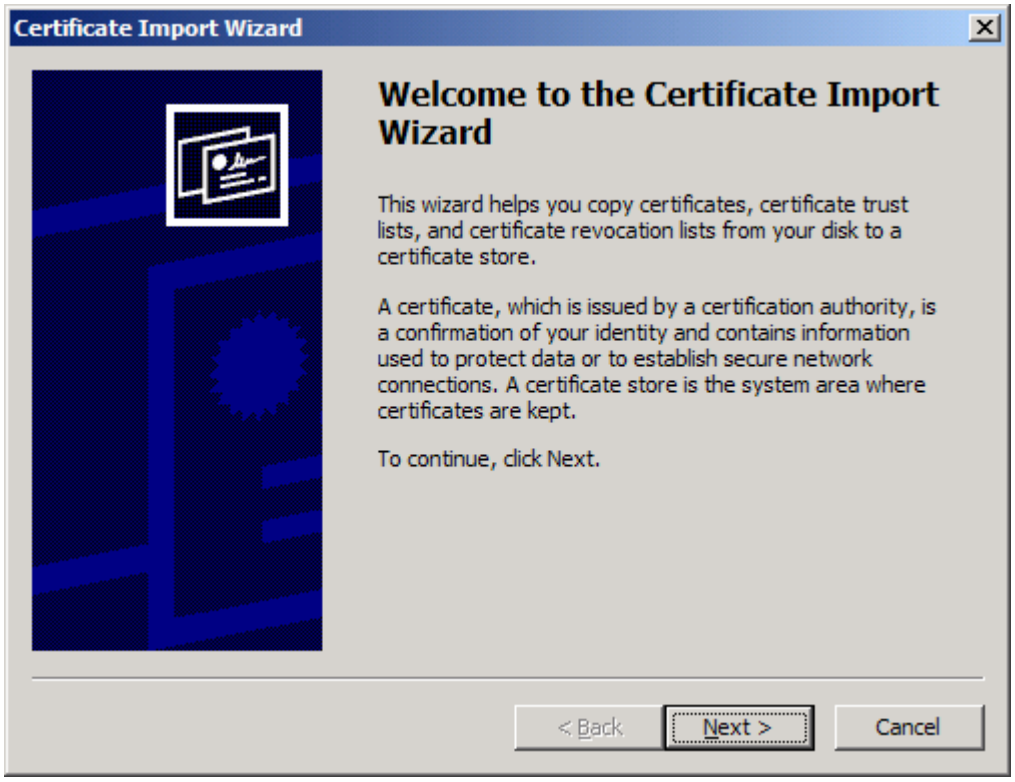


3) Save to a location where you can easily find this file.

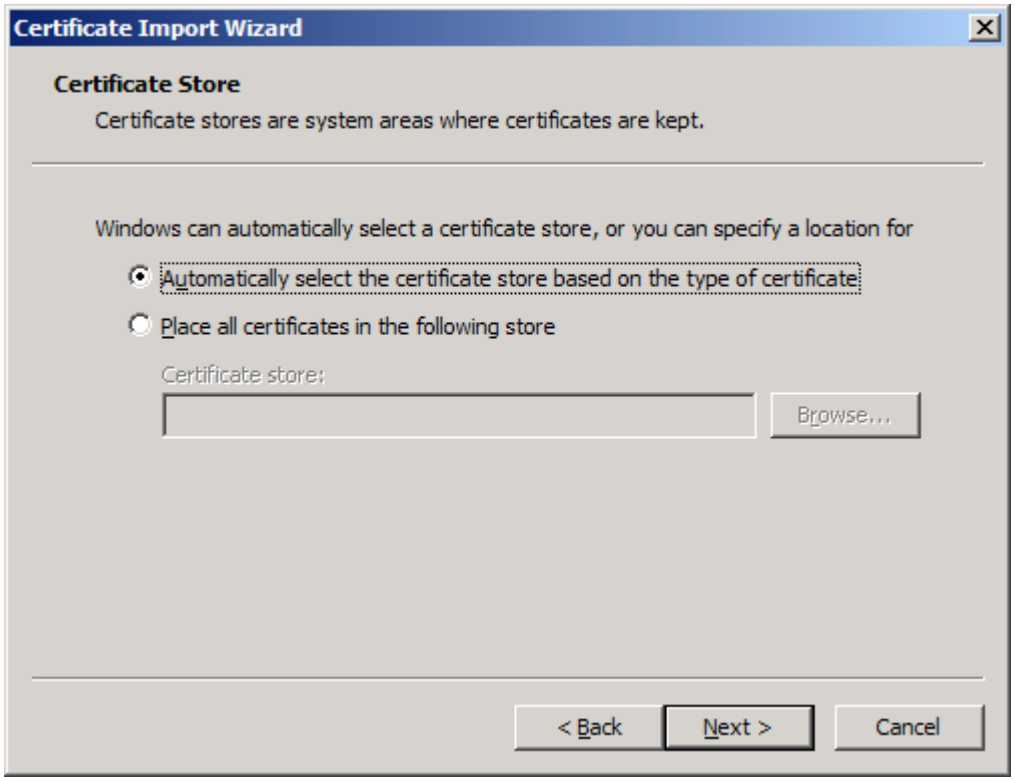
4) Locate and double click the file that you just downloaded. You will the certificate.



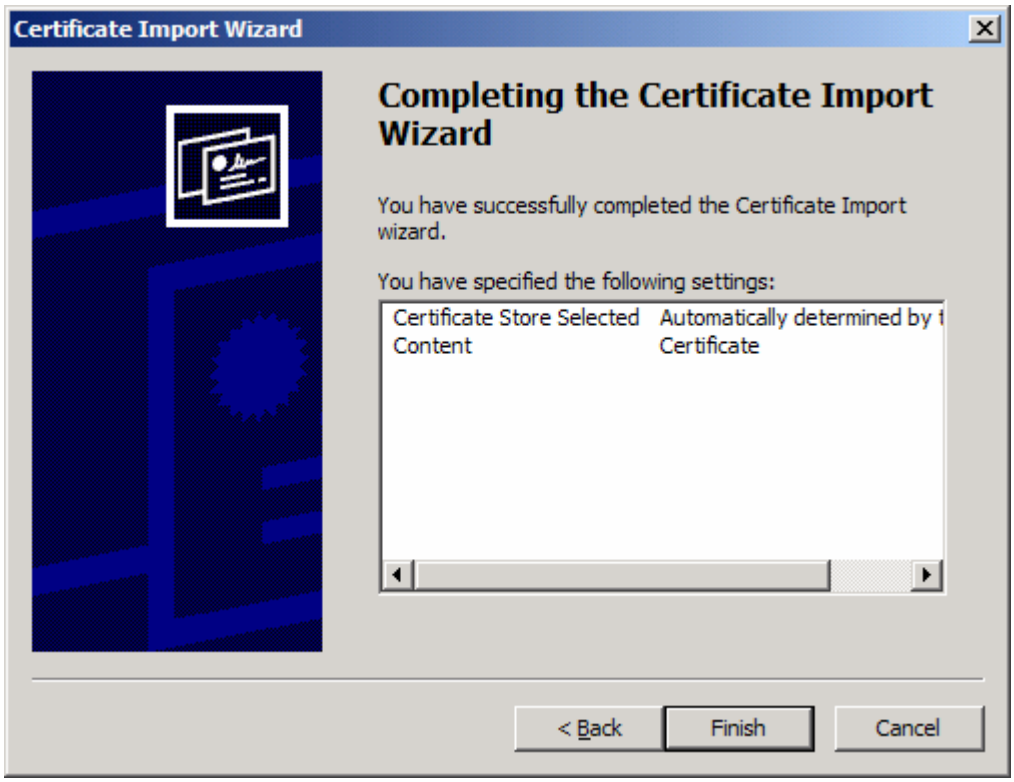
5) Click the Install Certificate button. You should then see the Certificate Import Wizard come up.



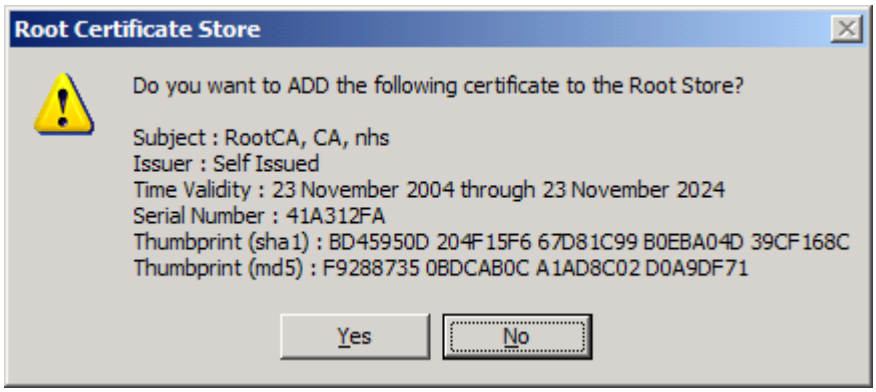
6) Click Next. You should then see the Certificate Store Screen pop up.



7) Choose Automatically select the certificate store based on the type of certificate and click Next. You should then see the Completing the Certificate Import Wizard screen come up.



8) IE Prompts a message before adding it to Root Store, Click Yes.



8) Click Finish and you should see the message The import was successful.