NHS SPINE Project

1096 Guidelines for using the Spine ESW interface for self-serv

Issue 2 Draft B

28th July 2006

Copyright

Confidentiality

All information in this document is provided in confidence for the sole purpose of adjudication of the document and shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without BT's prior permission in writing and shall be held in safe custody. These obligations shall not apply to information which is published or becomes known legitimately from some source other than BT.

Many of the product, service and company names referred to in this document are trademarks or registered trademarks.

They are all hereby acknowledged.

Distribution

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

Document Control

Title	1096 Guidelines for using the Spine ESW interface for self-serv
Author	David Ginn
Doc Ref	Guidelines for use of the NCRS Spine ESW interface.doc

Owner (Responsible for Approval of Issued Versions)				
Name	**Role**	**Signature**	**Date**	**Issue**
Mat Morrell				

Review Panel			
Name	**Role**	**Name**	**Role**
Stephen Eyre			
Julie Barber			
David Ginn	IDM Development Specialist		

Change History			
Issue	**Date**	**Author/ Editor**	**Details of Change**
Issue 1 Draft A	30th June 2005	Mat Raynor	Draft for Internal review
Issue 1	7th July 2005	Mat Raynor	Issue 1 for publication
Issue 2 Draft A	14th February 2006	Mat Morrell	Embedded link for NIS1 in section 2.3 amended
Issue 2 Draft B	28th July 2006	David Ginn	Updated to include new screen shots of ESW with modified LHK

Table of Contents

1 About This Document

Scope and Objectives

This document provides guidance to Endpoint Administrators who wish to use the Spine Entrust Enrollment Services for Web (ESW) interface to request and receive an endpoint TLS certificate to install on their approved Spine accredited system instance.

This use of ESW to request and receive an endpoint TLS certificate is a sub-task of the Endpoint Registration Process.

Background

This document is created as part of a communication pack that will be sent to all endpoint requestors to help them undertake the new endpoint registration process that will come into place on 11th July 2005.

1.1 Assumptions and Constraints

The endpoint administrator or user of ESW is familiar with X.509 and PKI technologies and understands the technical standards, naming conventions and tasks required to request, receive and install X.509 TLS certificates.

The endpoint administrator is familiar with and agrees to comply with all relevant NPfIT Security, Key Management and X.509 Certificate policies.

Document Hierarchy

This document is part of the ‘Communication Pack’ that will be delivered as part of the Interim Endpoint Registration Process acceptance into service programme.

2 ESW Guidance notes

What is Entrust Enrollment Services for Web (ESW)

It's primary purpose is to allow anybody who has the necessary registration and activation code for an endpoint that is undergoing registration or re-issuance to request and receive their TLS Certificate.

Who uses ESW?

Typically the endpoint administrator will be the person who accesses and uses ESW. The endpoint administrator is the person who is installing the accredited system instance on the physical endpoint.

In some circumstances the endpoint administrator may forward a PKCS#10 to another party who will access ESW on the administrator's behalf. E.g. where the endpoint does not yet have NHSNet/N3 access and thus cannot access ESW directly the endpoint administrator may allow a trusted representative of their system supplier to retrieve their certificate. In this instance the endpoint administrator must ensure the registration number and activation code are communicated securely.

How do I get to ESW

You will need an NHSNet/N3 connected PC with a web browser. If you use a browser other than Internet Explorer some of the options may not be available to you. This is due to the way access to the Microsoft CAPI store is controlled by Windows.

To access ESW browse to the following URLS.

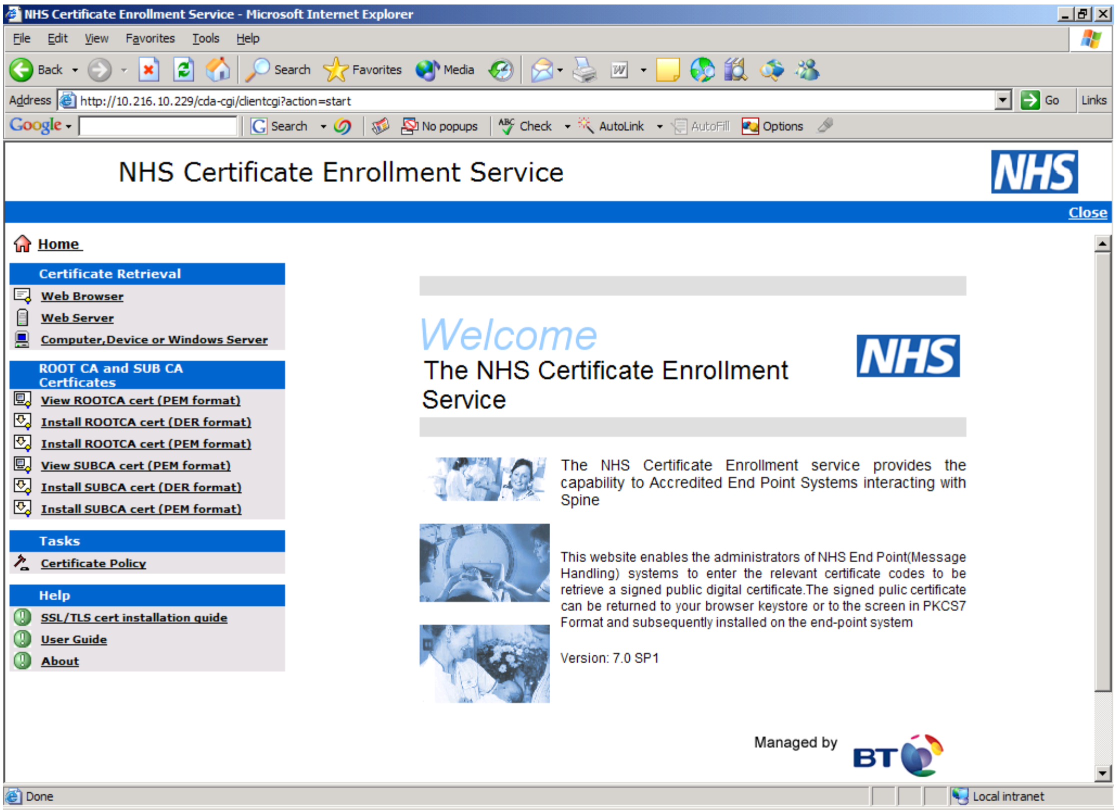
- The URL to access the Live ESW interface is https://esw.national.ncrs.nhs.uk/cda-cgi/clientcgi?action=start.
- The URL to access the Sandpit ESW interface is https://esw.nis1.national.ncrs.nhs.uk/cda-cgi/clientcgi?action=start.

How do I use ESW?

ESW provides the ability for an administrator to submit a 'certificate signing request' typically in the PKCS#10 format (although other more automatic methods are available) after they have created their public/private cryptographic key pair on which the certificate signing request is based.

This part of the endpoint registration can only take place after the endpoint administrator has received the registration number and activation codes associated with their endpoint registration (see document “Device and Service Endpoint Registration Ver2.0” for a full description of the endpoint registration process).

After deciding which environment the endpoint is registering for access the relevant ESW URL with your web browser (the Live environment has been used for this document). You are presented with the following screen:



NHS Certificate Enrollment Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.216.10.229/cda-cgi/clientcgi?action=start
Go Links
Google Search No popups Check AutoLink AutoFill Options
NHS Certificate Enrollment Service
NHS
Close
Home
Certificate Retrieval
Web Browser
Web Server
Computer,Device or Windows Server
ROOT CA and SUB CA Certficates
View ROOTCA cert (PEM format)
Install ROOTCA cert (DER format)
Install ROOTCA cert (PEM format)
View SUBCA cert (PEM format)
Install SUBCA cert (DER format)
Install SUBCA cert (PEM format)
Tasks
Certificate Policy
Help
SSL/TLS cert installation guide
User Guide
About
Welcome
Managed by BT
Done
Local intranet

The NHS Certificate Enrollment Service

The NHS Certificate Enrollment service provides the capability to Accredited End Point Systems interacting with Spine

This website enables the administrators of NHS End Point(Message Handling) systems to enter the relevant certificate codes to be retrieve a signed public digital certificate.The signed pulic certificate can be returned to your browser keystore or to the screen in PKCS7 Format and subsequently installed on the end-point system

Version: 7.0 SP1

There are three main options available to submit a request to ESW.

1. Submit a PKCS#10 certificate signing request. This could have been created on the machine being used to browse ESW or any other host. E.g where a new system instance is being built the physical machine may not be connected to a network. This option allows the PKCS#10 to be taken from that machine and submitted from any NHSNet connected host. This is the "Web Server" option under Certificate Retrieval option.

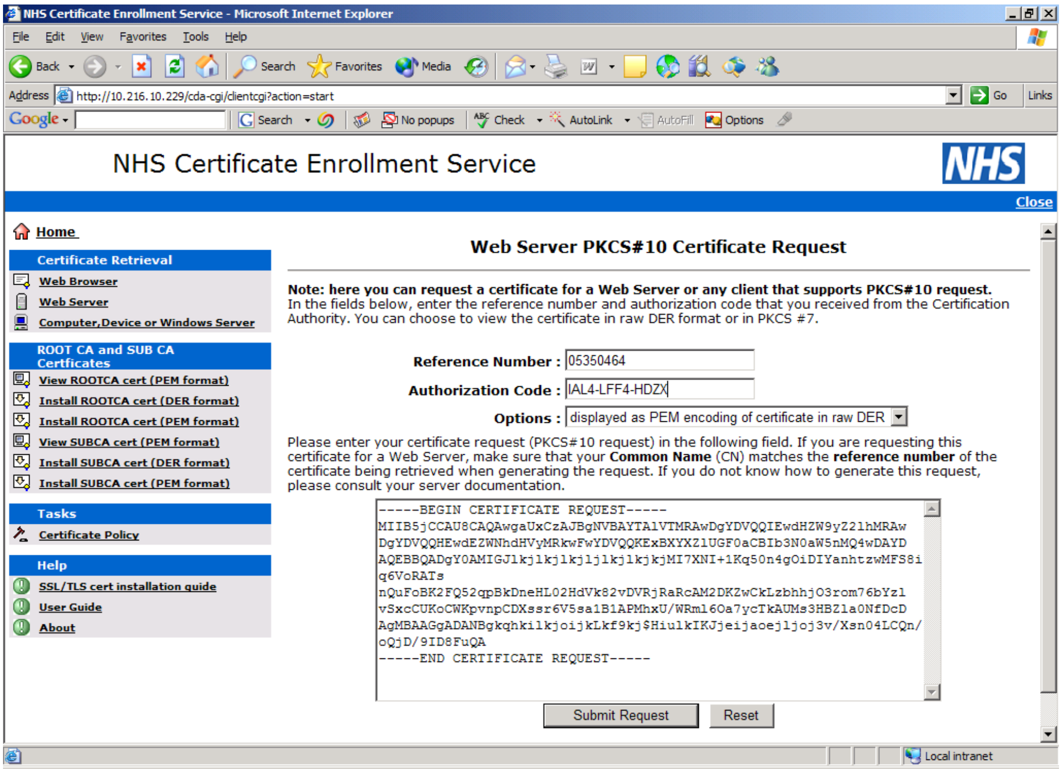
2. Automatically create a key pair and request a certificate for the Internet Browser certificate store on a connecting machine. This is the "Web Browser" option under Certificate Retrieval.

3. Automatically create a key pair and request a certificate for the Local Machine CAPI store on a connecting Microsoft Windows machine. This is the "Computer,Device or Windows Server" option under Certificate Retrieval. NB this option is only available if you use MS Internet Explorer to access ESW.

In the majority of cases the first option will be used as the third option is limited to Microsoft technologies and the machine where the certificate is to be used must have the necessary NHSNet/N3 access for both options (I.e. only option one allows for 'indirect' certificate requests).

Option one – Create Web Server request

Select the "Web Server" option under Certificate Retrieval. You will be presented with the following screen.


NHS Certificate Enrollment Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.216.10.229/cda-cgi/clientcgi?action=start
Go Links
Google Search No popups Check AutoLink AutoFill Options
NHS Certificate Enrollment Service
NHS
Close
Home
Certificate Retrieval
Web Browser
Web Server
Computer,Device or Windows Server
ROOT CA and SUB CA Certficates
View ROOTCA cert (PEM format)
Install ROOTCA cert (DER format)
Install ROOTCA cert (PEM format)
View SUBCA cert (PEM format)
Install SUBCA cert (DER format)
Install SUBCA cert (PEM format)
Tasks
Certificate Policy
Help
SSL/TLS cert installation guide
User Guide
About
Submit Request
Reset
Local intranet

Web Server PKCS#10 Certificate Request

Note: here you can request a certificate for a Web Server or any client that supports PKCS#10 request. In the fields below, enter the reference number and authorization code that you received from the Certification Authority. You can choose to view the certificate in raw DER format or in PKCS #7.

Reference Number : 05350464

Authorization Code : IAL4-LFF4-HDZX

Options : displayed as PEM encoding of certificate in raw DER

Please enter your certificate request (PKCS#10 request) in the following field. If you are requesting this certificate for a Web Server, make sure that your **Common Name** (CN) matches the **reference number** of the certificate being retrieved when generating the request. If you do not know how to generate this request, please consult your server documentation.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB5jCCAU8CAQAwgaUxCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdHZW9yZ21hMRAw
DgYDVQQHEwdEZWNhdHVyMRkwFwYDVQQKExBXYXZlUGF0aCBIb3N0aW5nMQ4wDAYD
AQEBBQADgY0AMIGJlkjlkjlkjljlkjlkjkjMI7XNI+1Kq50n4gOiDIYanhtzwMFS8i
q6VoRATs
nQuFoBK2FQ52qpBkDneHL02HdVk82vDVRjRaRcAM2DKZwCkLzbhhjO3rom76bYzl
vSxcCUKoCWKpvnpCDXssr6V5sa1B1APMhxU/WRml6Oa7ycTkAUMs3HBZla0NfDcD
AgMBAAGgADANBgkqhkilkjoijkLkf9kj$HiulkIKJjeijaoejljoj3v/Xsn04LCQn/
oQjD/9ID8FuQA
-----END CERTIFICATE REQUEST-----
```

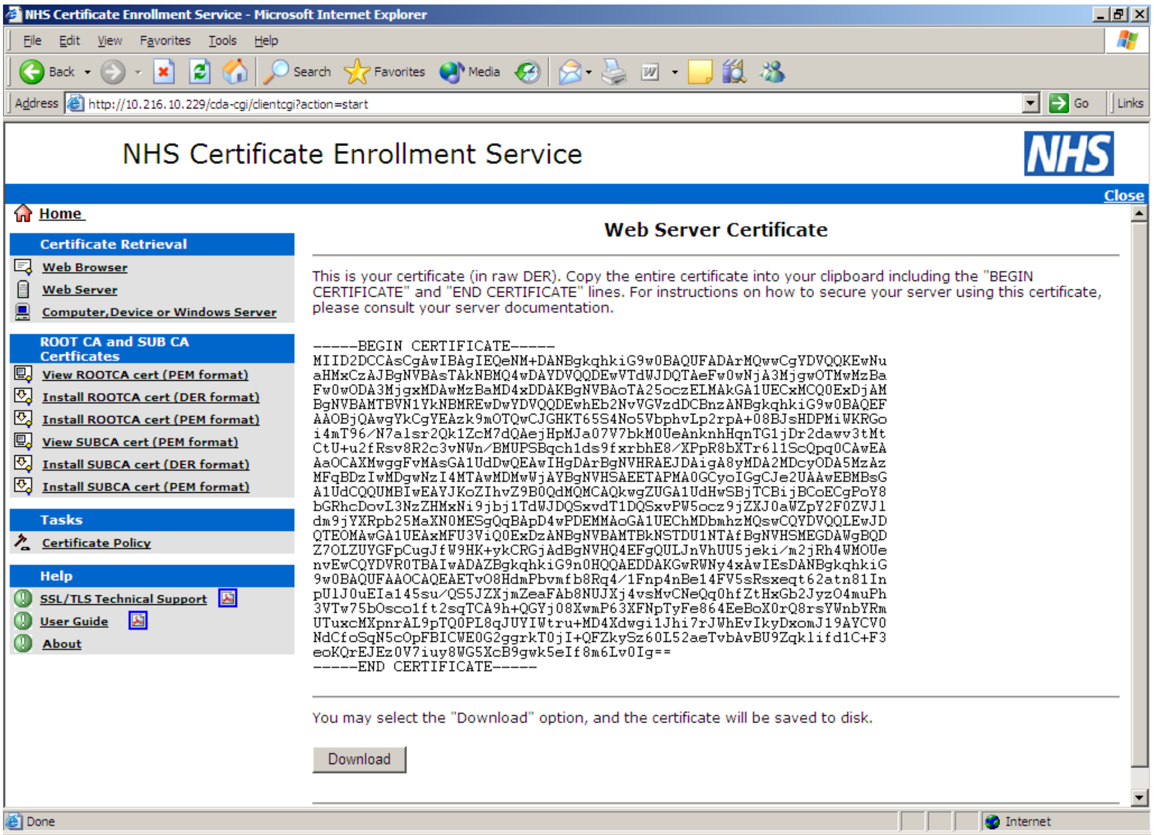
The screen shot shows the three fields that must be populated and the option drop down list where you can select the format that your certificate will be produced in.

The reference number is the number that was used as the CN when you created your PKCS#10 Certificate signing request. This is the first number communicated to the endpoint administrator (EA) by the endpoint registration team (EPR Team). The authorization code is the second number that is communicated to the EA by the EPR team.

The large freeform text field is where the PKCS#10 is pasted in.

The options drop down list is where the EA can choose the format of the certificate they need for their particular system.

Once the three fields have been populated and the certificate format chosen the EA presses the submit request button. ESW will then present the new certificate as a selectable text string as shown below:


NHS Certificate Enrollment Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.216.10.229/cda-cgi/clientcgi?action=start
Go Links
NHS
Close
Home
Certificate Retrieval
Web Browser
Web Server
Computer,Device or Windows Server
ROOT CA and SUB CA Certficates
View ROOTCA cert (PEM format)
Install ROOTCA cert (DER format)
Install ROOTCA cert (PEM format)
View SUBCA cert (PEM format)
Install SUBCA cert (DER format)
Install SUBCA cert (PEM format)
Tasks
Certificate Policy
Help
SSL/TLS Technical Support
User Guide
About
Download
Done
Internet

NHS Certificate Enrollment Service

Web Server Certificate

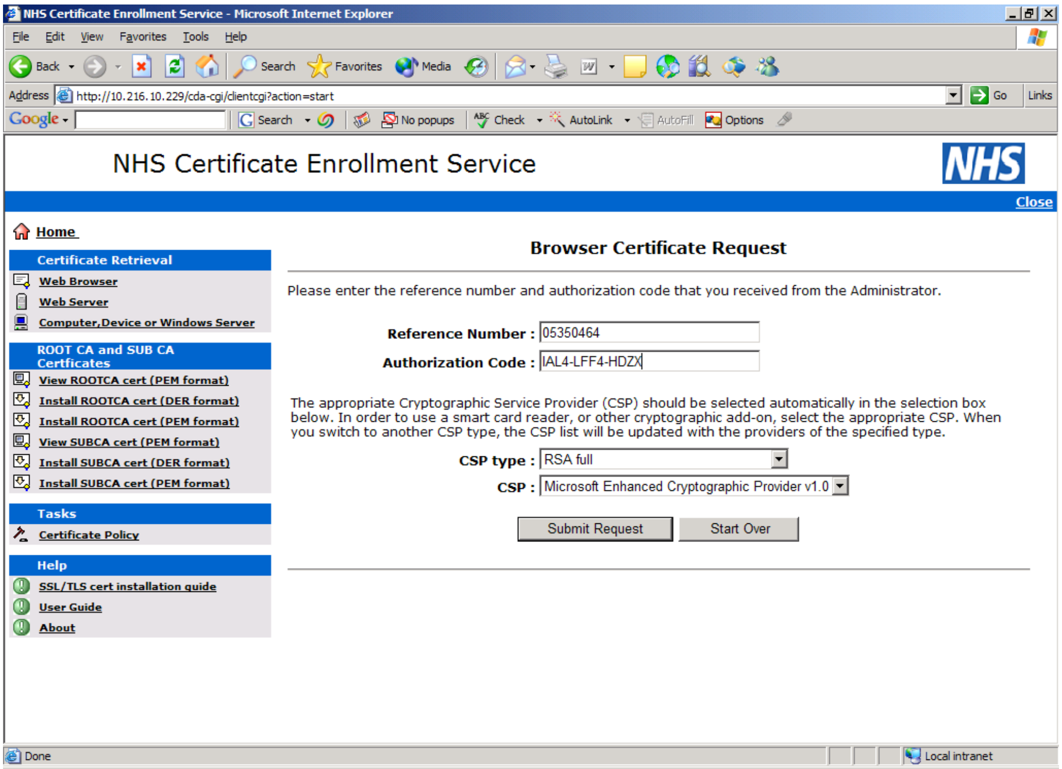
This is your certificate (in raw DER). Copy the entire certificate into your clipboard including the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. For instructions on how to secure your server using this certificate, please consult your server documentation.

```
-----BEGIN CERTIFICATE-----
MIID2DCCAsCgAwIBAgIEQeNM+DANBgkqhkiG9w0BAQUFADArMQwwCgYDVQQKEwNu
aHMxCzAJBgNVBAsTAkNBMQ4wDAYDVQQDEwVTdWJDQTAeFw0wNjA3MjgwOTMwMzBa
Fw0wODA3MjgxMDAwMzBaMD4xDDAKBgNVBAoTA25oczELMAkGA1UECxMCQ0ExDjAM
BgNVBAMTBVN1YkNBMREwDwYDVQQDEwhEb2NvVGVzdDCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEAzk9mOTQwCJGHKT65S4No5VbphvLp2rpA+08BJsHDPMiWKRGo
i4mT96/N7alsr2Qk1ZcM7dQAejHpMJa07V7bkM0UeAnknhHqnTG1jDr2dawv3tMt
CtU+u2fRsv8R2c3vNWn/BMUPSBqch1ds9fxrbhE8/XPpR8bXTr611ScQpq0CAwEA
AaOCAXMwggFvMAsGA1UdDwQEAwIHgDArBgNVHRAEJDAigA8yMDA2MDcyODA5MzAz
MFqBDzIwMDgwNzI4MTAwMDMwWjAYBgNVHSAEETAPMA0GCyoIGgCJe2UAAwEBMBsG
A1UdCQQUMBIwEAYJKoZIhvZ9B0QdMQMCAQkwgZUGA1UdHwSBjTCBijBCoECgPoY8
bGRhcDovL3NzZHMxNi9jbj1TdWJDQSxvdT1DQSxvPW5ocz9jZXJ0aWZpY2F0ZVJl
dm9jYXRpb25MaXN0MESgQqBApD4wPDEMMAoGA1UEChMDbmhzMQswCQYDVQQLEwJD
QTEOMAwGA1UEAxMFU3ViQ0ExDzANBgNVBAMTBkNSTDU1NTAfBgNVHSMEGDAWgBQD
Z7OLZUYGFpCugJfW9HK+ykCRGjAdBgNVHQ4EFgQULJnVhUU5jeki/m2jRh4WMOUe
nvEwCQYDVR0TBAIwADAZBgkqhkiG9n0HQQAEDDAKGwRWNy4xAwIEsDANBgkqhkiG
9w0BAQUFAAOCAQEAETvO8HdmPbvmfb8Rq4/1Fnp4nBe14FV5sRsxeqt62atn81In
pUlJ0uEIa145su/QS5JZXjmZeaFAb8NUJXj4vsMvCNeQq0hfZtHxGb2JyzO4muPh
3VTw75bOsco1ft2sqTCA9h+QGYj08XwmP63XFNpTyFe864EeBoX0rQ8rsYWnbYRm
UTuxcMXpnrAL9pTQ0PL8qJUYIWtru+MD4Xdwgi1Jhi7rJWhEvIkyDxomJ19AYCV0
NdCfoSqN5cOpFBICWE0G2ggrkT0jI+QFZkySz60L52aeTvbAvBU9Zqklifd1C+F3
eoKQrEJEz0V7iuy8WG5XcB9gwk5eIf8m6Lv0Ig==
-----END CERTIFICATE-----
```

You may select the "Download" option, and the certificate will be saved to disk.

Option two – Browser certificate request

Select "Web Browser" option under Certificate Retrieval. Selecting this option will automatically create a cryptographic key pair and request and install a certificate in the browser’s certificate store on the machine you are browsing from. As the creation of the certificate signing request is automated the only two pieces of information that need to be filled in are the registration (or reference) number and the authorization (or activation) code. There are options to change Cryptographic Service Provider if desired.



NHS Certificate Enrollment Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Go Links
Google Search No popups Check AutoLink AutoFill Options
NHS
Close
Home
Certificate Retrieval
Web Browser
Web Server
Computer,Device or Windows Server
ROOT CA and SUB CA Certficates
View ROOTCA cert (PEM format)
Install ROOTCA cert (DER format)
Install ROOTCA cert (PEM format)
View SUBCA cert (PEM format)
Install SUBCA cert (DER format)
Install SUBCA cert (PEM format)
Tasks
Certificate Policy
Help
SSL/TLS cert installation guide
User Guide
About
Done
Local intranet

Address: http://10.216.10.229/cda-cgi/clientcgi?action=start

NHS Certificate Enrollment Service

Browser Certificate Request

Please enter the reference number and authorization code that you received from the Administrator.

Reference Number : 05350464

Authorization Code : IAL4-LFF4-HDZX

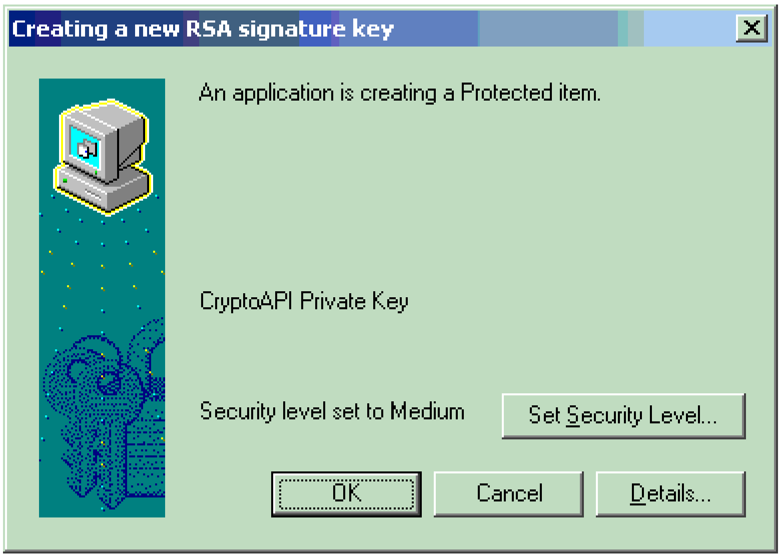
The appropriate Cryptographic Service Provider (CSP) should be selected automatically in the selection box below. In order to use a smart card reader, or other cryptographic add-on, select the appropriate CSP. When you switch to another CSP type, the CSP list will be updated with the providers of the specified type.

CSP type : RSA full

CSP : Microsoft Enhanced Cryptographic Provider v1.0

Submit Request | Start Over

Once the submit request button is pressed you may be prompted to create a key pair. E.g the following is the Internet Explorer prompt.



Creating a new RSA signature key

An application is creating a Protected item.

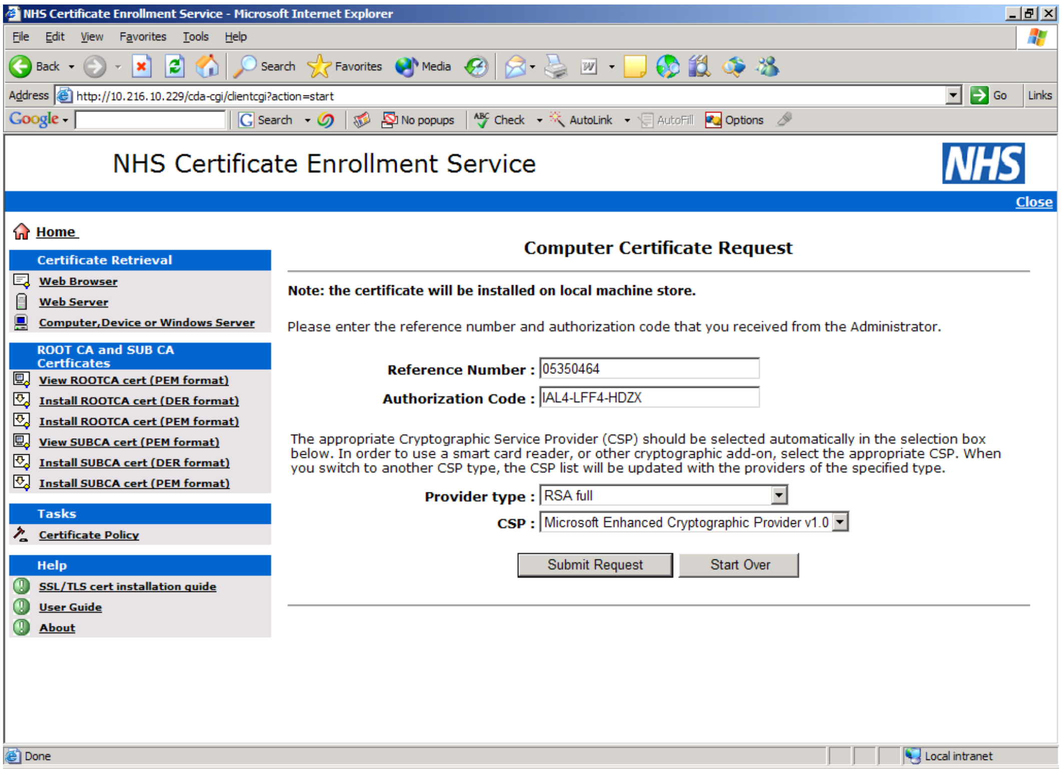
CryptoAPI Private Key

Security level set to Medium

Depending on the security settings of your browser you may be prompted to allow the installation of the certificate or other cryptographic actions. If so respond in the affirmative.

Option three – Create computer/Device certificate

Select "Computer, Device or Windows Server" option under Certificate Retrieval. Although very similar to the previous option this will automatically create a key pair and request and install a certificate in the Local Machine CAPI (certificate) store. Again only the reference number and authorization code are needed before the request is submitted.



NHS Certificate Enrollment Service - Microsoft Internet Explorer

Address: http://10.216.10.229/cda-cgi/clientcgi?action=start

NHS Certificate Enrollment Service

Home

Certificate Retrieval
- Web Browser
- Web Server
- Computer,Device or Windows Server

ROOT CA and SUB CA Certficates
- View ROOTCA cert (PEM format)
- Install ROOTCA cert (DER format)
- Install ROOTCA cert (PEM format)
- View SUBCA cert (PEM format)
- Install SUBCA cert (DER format)
- Install SUBCA cert (PEM format)

Tasks
- Certificate Policy

Help
- SSL/TLS cert installation guide
- User Guide
- About

Computer Certificate Request

Note: the certificate will be installed on local machine store.

Please enter the reference number and authorization code that you received from the Administrator.

Reference Number : 05350464

Authorization Code : IAL4-LFF4-HDZX

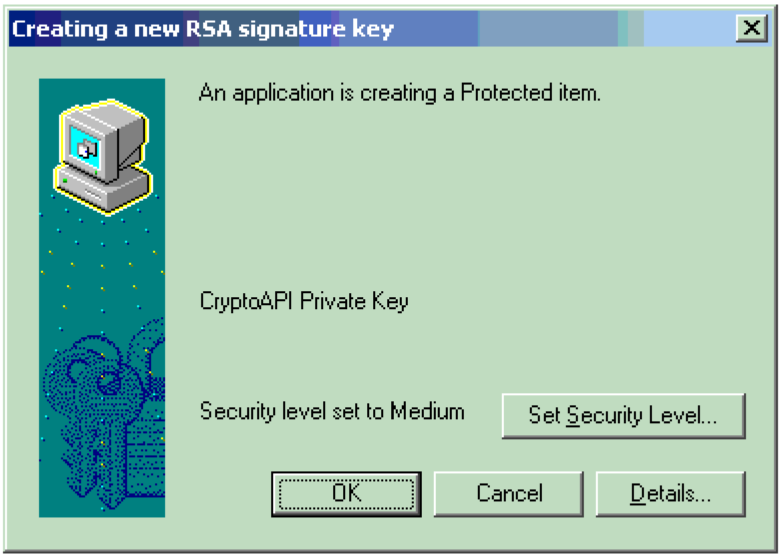
The appropriate Cryptographic Service Provider (CSP) should be selected automatically in the selection box below. In order to use a smart card reader, or other cryptographic add-on, select the appropriate CSP. When you switch to another CSP type, the CSP list will be updated with the providers of the specified type.

Provider type : RSA full

CSP : Microsoft Enhanced Cryptographic Provider v1.0

File Edit View Favorites Tools Help
Back Search Favorites Media
Go Links
Google Search No popups Check AutoLink AutoFill Options
NHS
Close
Submit Request
Start Over
Done
Local intranet

Once the submit request button is pressed you may be prompted to create a key pair. The following is the Internet Explorer prompt.



Creating a new RSA signature key

An application is creating a Protected item.

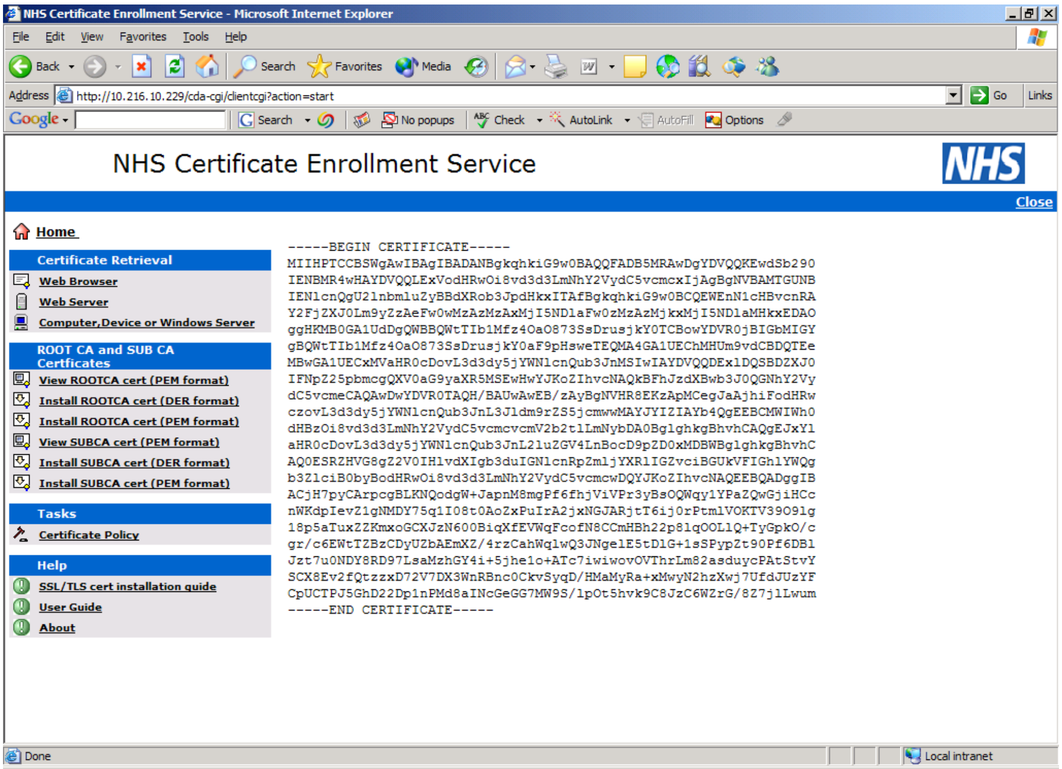
CryptoAPI Private Key

Security level set to Medium

Depending on the security settings of your browser you may be prompted to allow the installation of the certificate or other cryptographic actions. If so respond in the affirmative.

Other uses of ESW

ESW also allows anybody on N3 to retrieve the Root and Subordinate CA certificates for that environment. For example if you select the “Install ROOTCA cert (PEM format)” link in the left hand pane you will get the following screen:


NHS Certificate Enrollment Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.216.10.229/cda-cgi/clientcgi?action=start
Go Links
Google Search No popups Check AutoLink AutoFill Options
NHS Certificate Enrollment Service
NHS
Close
Home
Certificate Retrieval
Web Browser
Web Server
Computer,Device or Windows Server
ROOT CA and SUB CA Certficates
View ROOTCA cert (PEM format)
Install ROOTCA cert (DER format)
Install ROOTCA cert (PEM format)
View SUBCA cert (PEM format)
Install SUBCA cert (DER format)
Install SUBCA cert (PEM format)
Tasks
Certificate Policy
Help
SSL/TLS cert installation guide
User Guide
About
Done
Local intranet

```
-----BEGIN CERTIFICATE-----
MIIHPTCCBSWgAwIBAgIBADANBgkqhkiG9w0BAQQFADB5MRAwDgYDVQQKEwdSb290
IENBMR4wHAYDVQQLExVodHRwOi8vd3d3LmNhY2VydC5vcmcxIjAgBgNVBAMTGUNB
IENlcnQgU2lnbmluZyBBdXRob3JpdHkxITAfBgkqhkiG9w0BCQEWEnN1cHBvcnRA
Y2FjZXJ0Lm9yZzAeFw0wMzAzMzAxMjI5NDlaFw0zMzAzMjkxMjI5NDlaMHkxEDAO
ggHKMB0GA1UdDgQWBBQWtTIb1Mfz4OaO873SsDrusjkY0TCBowYDVR0jBIGbMIGY
gBQWtTIb1Mfz4OaO873SsDrusjkY0aF9pHsweTEQMA4GA1UEChMHUm9vdCBDQTEe
MBwGA1UECxMVaHR0cDovL3d3dy5jYWNlcnQub3JnMSIwIAYDVQQDExlDQSBDZXJ0
IFNpZ25pbmcgQXV0aG9yaXR5MSEwHwYJKoZIhvcNAQkBFhJzdXBwb3J0QGNhY2Vy
dC5vcmeCAQAwDwYDVR0TAQH/BAUwAwEB/zAyBgNVHR8EKzApMCegJaAjhiFodHRw
czovL3d3dy5jYWNlcnQub3JnL3J1dm9rZS5jcmwwMAYJYIZIAYb4QgEEBCMWIWh0
dHBzOi8vd3d3LmNhY2VydC5vcmcvcmV2b2tlLmNybDA0BglghkgBhvhCAQgEJxYl
aHR0cDovL3d3dy5jYWNlcnQub3JnL2luZGV4LnBocD9pZD0xMDBWBglghkgBhvhC
AQ0ESRZHVG8gZ2V0IHlvdXIgb3duIGNlcnRpZmljYXRlIGZvciBGUkVFIGhlYWQg
b3ZlciB0byBodHRwOi8vd3d3LmNhY2VydC5vcmcwDQYJKoZIhvcNAQEEBQADggIB
ACjH7pyCArpcgBLKNQodgW+JapnM8mgPf6fhjViVPr3yBsOQWqy1YPaZQwGjiHCc
nWKdpIevZ1gNMDY75q1I08t0AoZxPuIrA2jxNGJARjtT6ij0rPtmlVOKTV39O9lg
18p5aTuxZZKmxoGCXJzN600BiqXfEVWqFcofN8CCmHBh22p8lqOOLlQ+TyGpkO/c
gr/c6EWtTZBzCDyUZbAEmXZ/4rzCahWqlwQ3JNgelE5tDlG+1sSPypZt90Pf6DBl
Jzt7u0NDY8RD97LsaMzhGY4i+5jhe1o+ATc7iwiwovOVThrLm82asduycPAtStvY
SCX8Ev2fQtzzxD72V7DX3WnRBnc0CkvSyqD/HMaMyRa+xMwyN2hzXwj7UfdJUzYF
CpUCTPJ5GhD22Dp1nPMd8aINcGeGG7MW9S/lpOt5hvk9C8JzC6WZrG/8Z7jlLwum
-----END CERTIFICATE-----
```

The root certificate can be cut and pasted from this screen.

Troubleshooting ESW

ESW is a simple system that is easy and reliable to use once the initial learning curve has been completed. There are times however when a submitted request may fail. Error messages are intentionally obscure to ensure few clues as to the problem with the submission are communicated to unauthorised users.

The following problems (in order of prevalence) will cause failure of an ESW submission and should be used as a simple checklist for initial troubleshooting.

- An incorrect Registration Number or Activation Code.
- Activation Codes have expired. As a security feature activation codes have a limited lifetime. This is currently set at six weeks.

- An incorrectly created PKCS#10. The PKCS#10 *must* be created with the Common Name set to the Registration Number that is communicated to you by the Endpoint Registration Team.
- A poorly formatted PKCS#10. Typically, spurious characters can be introduced into the body of the PKCS#10 text whilst cutting and pasting into/from files. This is dependent on the text editors used for the purpose, and whether text is pasted in email bodies etc. It is recommended that the simplest text editors are used for the purpose and if the created PKCS#10 is transported by email it is sent as a file rather than a text string in the body of the mail. NB The delimiters "---begin new certificate request-------" and "---------end new certificate request---------" must be present at the start and end of the encoded text string.
- Incorrect Cryptographic Provider for key pair generation (RSA 1024 should be used).

If a problem still occurs after these potential causes have been investigated please contact the Endpoint Registration Team on 0845 600 2956.

End of Document.