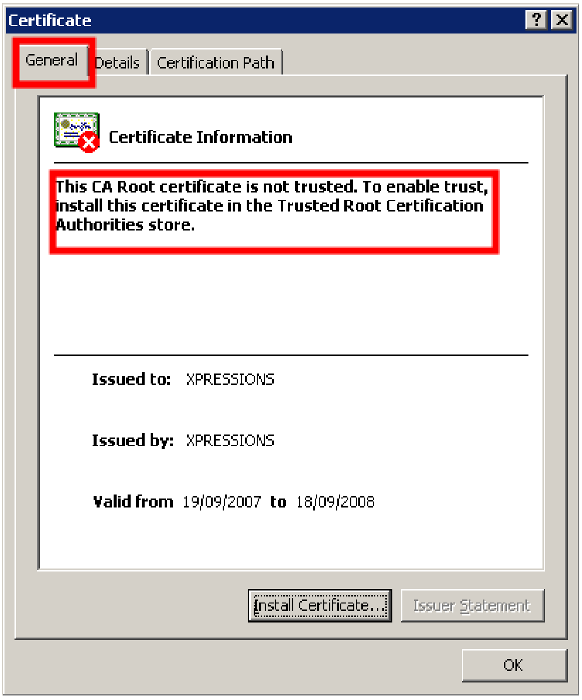
How to request certificates for HiPath Xpressions from a trusted CA

We all know the following error messages when we access Internet Sites or our HiPath applications or systems.

A security Alert appears. The homepage should not be trusted. We only press *Yes* to continue to the homepage but in fact we can easily go by accident to a phishing page.

A not trusted certificate can also mean that the CA (Certificate Authority) was hacked and people can read the passwords, emails or see whatever we do on this web site.



This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

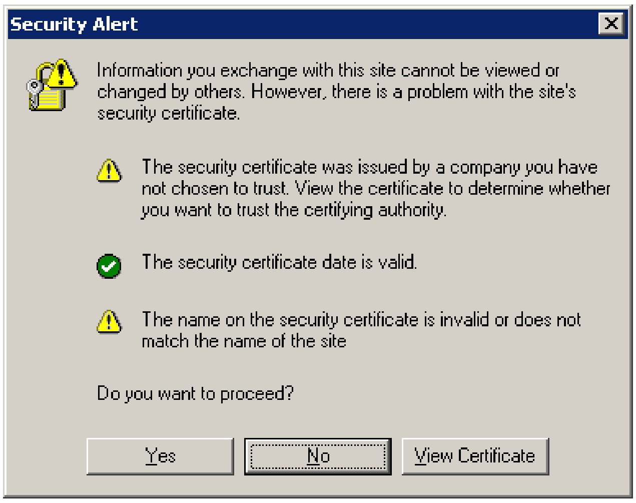
Issued to: XPRESSIONS

Issued by: XPRESSIONS

Valid from 19/09/2007 to 18/09/2008

It is an absolute must to have here the correct FQDN shown of the application shown

HiPath Xpressions WebApl is based on *OpenSSL* so it is fairly easy to create a new certificate with this open standard platform.



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

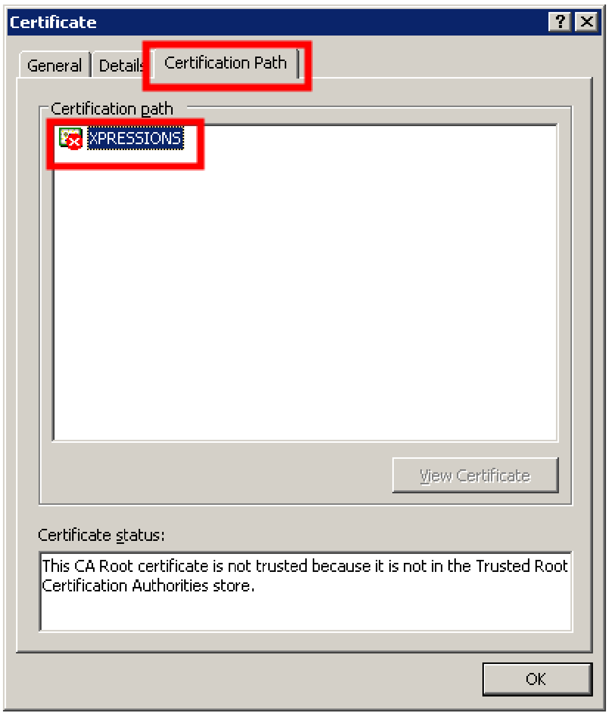
⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

For applications like HiPath Xpressions where you can access your email inbox if unified messaging is enabled absolutely critical!

By clicking onto *View Certificate* we can identify the reason why it is untrusted exactly. The example here shows the CA the cert was requested from a CA which is not trusted by us. We can either add the CA into our Trusted 3rd Party Certificate Store or request a proper certificate.

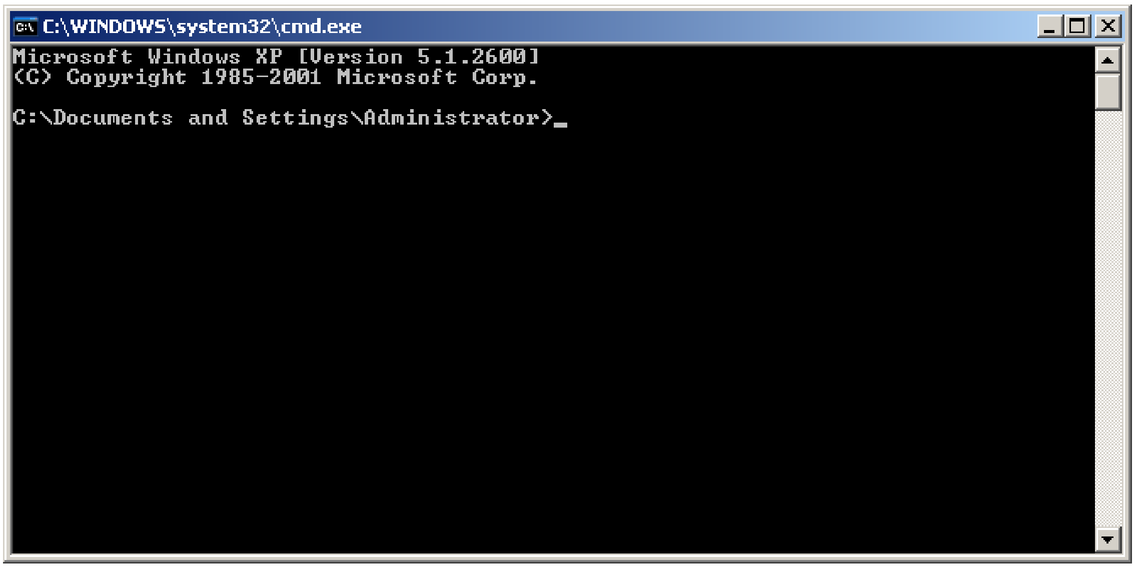
The *Certificate Path* shows us that the Root CA can not be found and the name of the application the certificate was issued to is invalid.



Certificate status:

This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store.

Open up the Command Prompt (Start – Run – CMD)

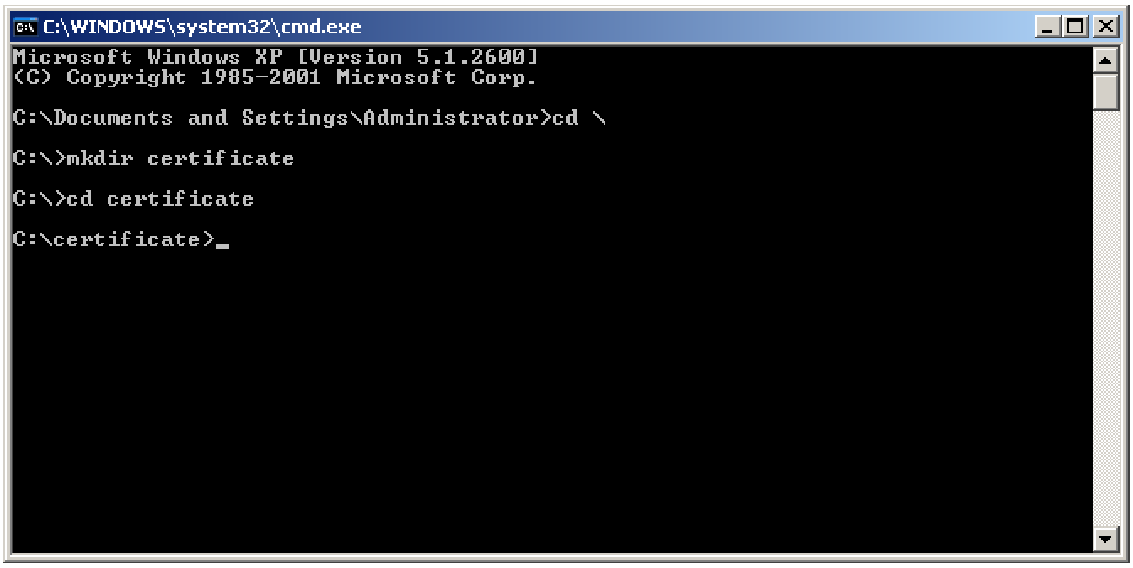


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>_
```

Browse to the root directory c:\ by typing *`cd \`*

Create a new directory maybe called certificate *`mkdir certificate`*

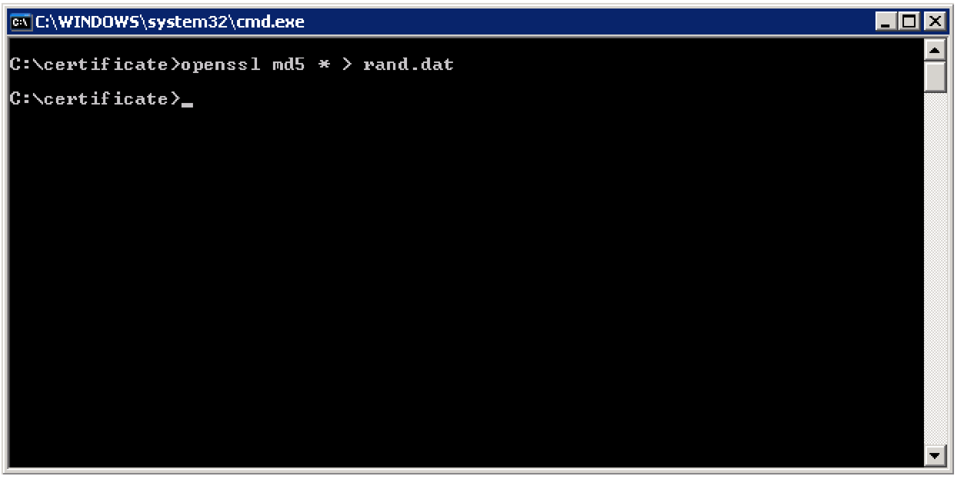
Browse into the certificate folder *`cd certificate`*



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd \

C:\>mkdir certificate

C:\>cd certificate

C:\certificate>_
```

Create a new random CSR (Certificate Signing Request)

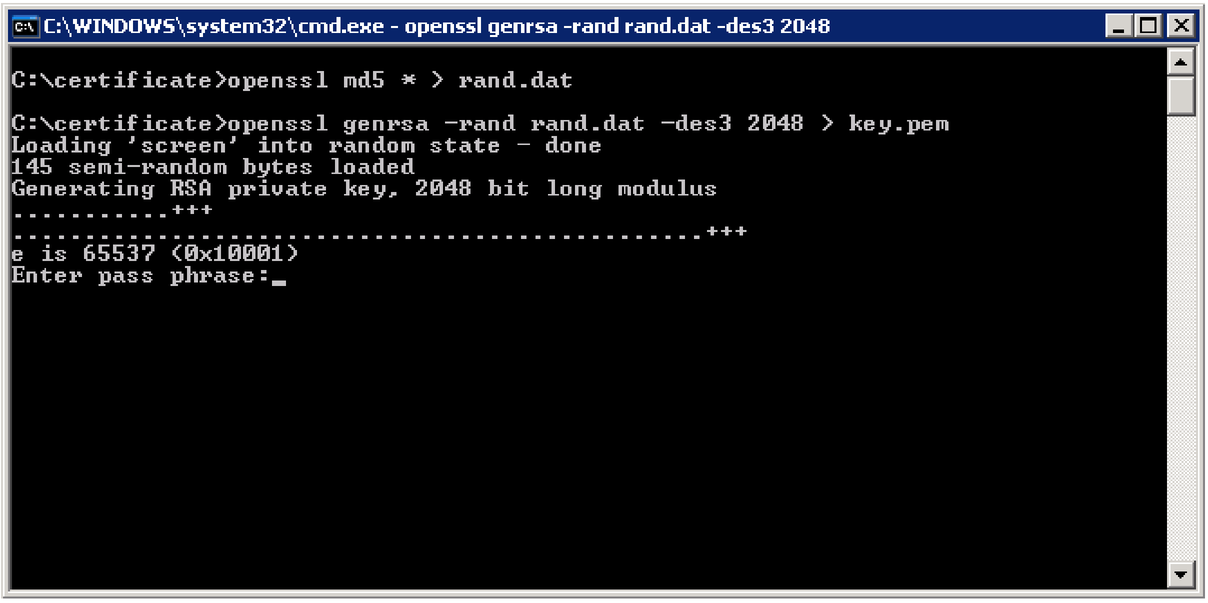
```
Openssl md5 * > rand.dat
```



```
C:\certificate>openssl md5 * > rand.dat

C:\certificate>_
```

With this random key file generate now an with DES3 encrypted private key. Simply type the command

`Openssl genrsa -rand rand.dat -des3 2048 > key.pem`

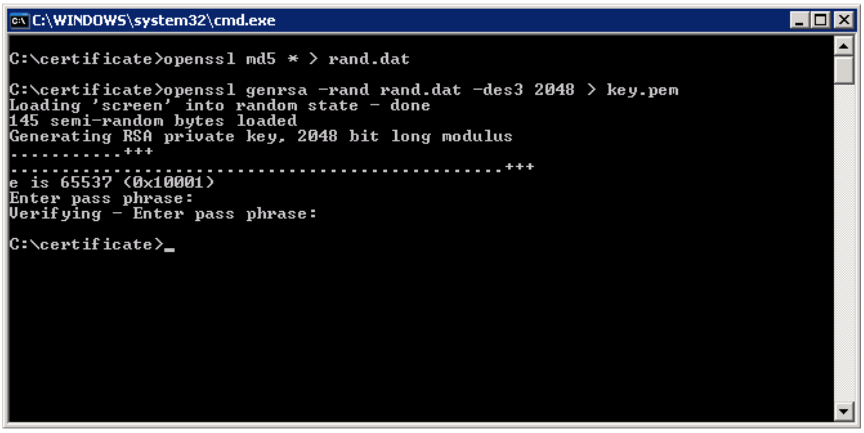

C:\WINDOWS\system32\cmd.exe - openssl genrsa -rand rand.dat -des3 2048

```
C:\certificate>openssl md5 * > rand.dat

C:\certificate>openssl genrsa -rand rand.dat -des3 2048 > key.pem
Loading 'screen' into random state - done
145 semi-random bytes loaded
Generating RSA private key, 2048 bit long modulus
...........+++
...................................................+++
e is 65537 (0x10001)
Enter pass phrase:_
```

You are now prompted to *enter a pass phrase*. This is the password that keeps the private key protected and should be as secure as possible. For example fill in a complete sentence like

Communication for the open minded

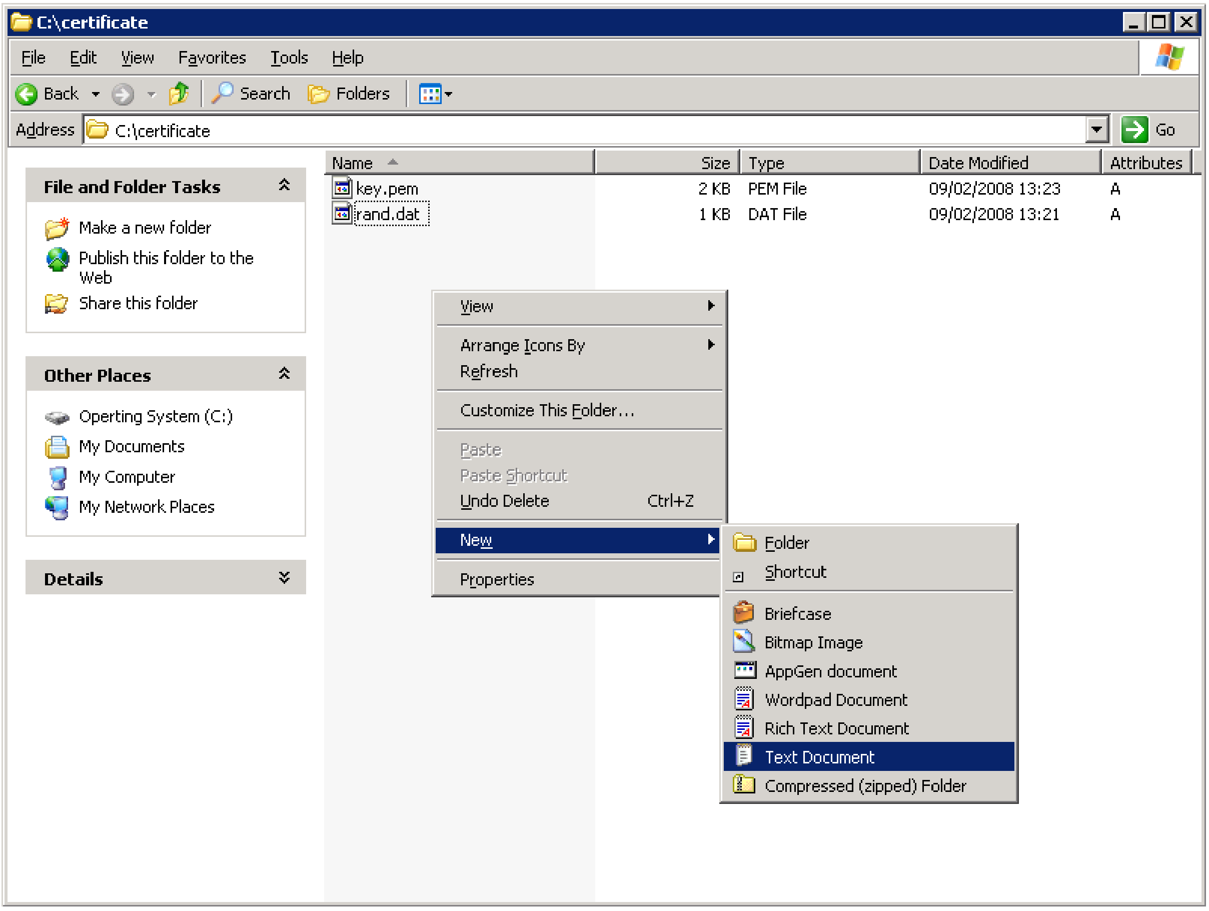
And verify the password



```
C:\certificate>openssl md5 * > rand.dat

C:\certificate>openssl genrsa -rand rand.dat -des3 2048 > key.pem
Loading 'screen' into random state - done
145 semi-random bytes loaded
Generating RSA private key, 2048 bit long modulus
...........+++
...................................................+++
e is 65537 (0x10001)
Enter pass phrase:
Verifying - Enter pass phrase:

C:\certificate>_
```

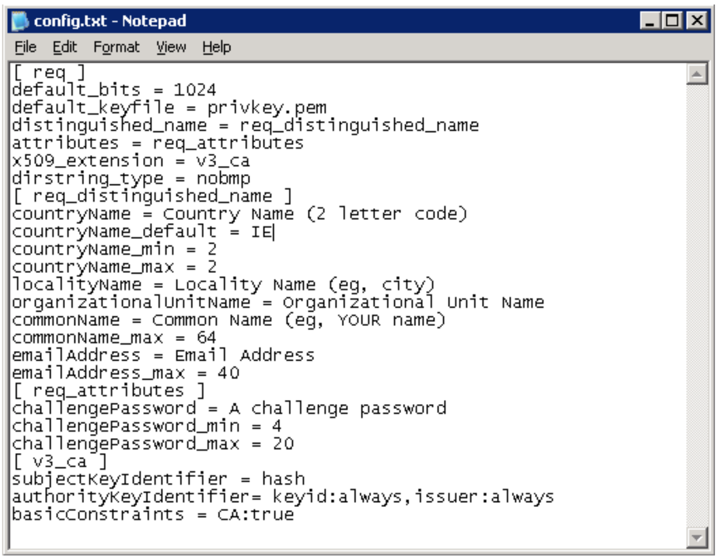
Now an OpenSSL configuration file has to be created.

Open the windows explorer and browse to the `c:\certificates` directory and *create a* `text file`



Name	Size	Type	Date Modified	Attributes
key.pem	2 KB	PEM File	09/02/2008 13:23	A
rand.dat	1 KB	DAT File	09/02/2008 13:21	A

Name it *config.txt* and fill in the following information



```
[ req ]
default_bits = 1024
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name
attributes = req_attributes
x509_extension = v3_ca
dirstring_type = nobmp
[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = IE
countryName_min = 2
countryName_max = 2
localityName = Locality Name (eg, city)
organizationalUnitName = Organizational Unit Name
commonName = Common Name (eg, YOUR name)
commonName_max = 64
emailAddress = Email Address
emailAddress_max = 40
[ req_attributes ]
challengePassword = A challenge password
challengePassword_min = 4
challengePassword_max = 20
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier= keyid:always,issuer:always
basicConstraints = CA:true
```

The file will look like in this example and has to be saved.

```
[ req ]
default_bits = 1024
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name
attributes = req_attributes
x509_extension = v3_ca
dirstring_type = nobmp
[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = IE
countryName_min = 2
countryName_max = 2
localityName = Locality Name (eg, city)
organizationalUnitName = Organizational Unit Name
commonName = Common Name (eg, YOUR name)
commonName_max = 64
emailAddress = Email Address
emailAddress_max = 40
[ req_attributes ]
challengePassword = A challenge password
challengePassword_min = 4
challengePassword_max = 20
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier= keyid:always,issuer:always
basicConstraints = CA:true
```

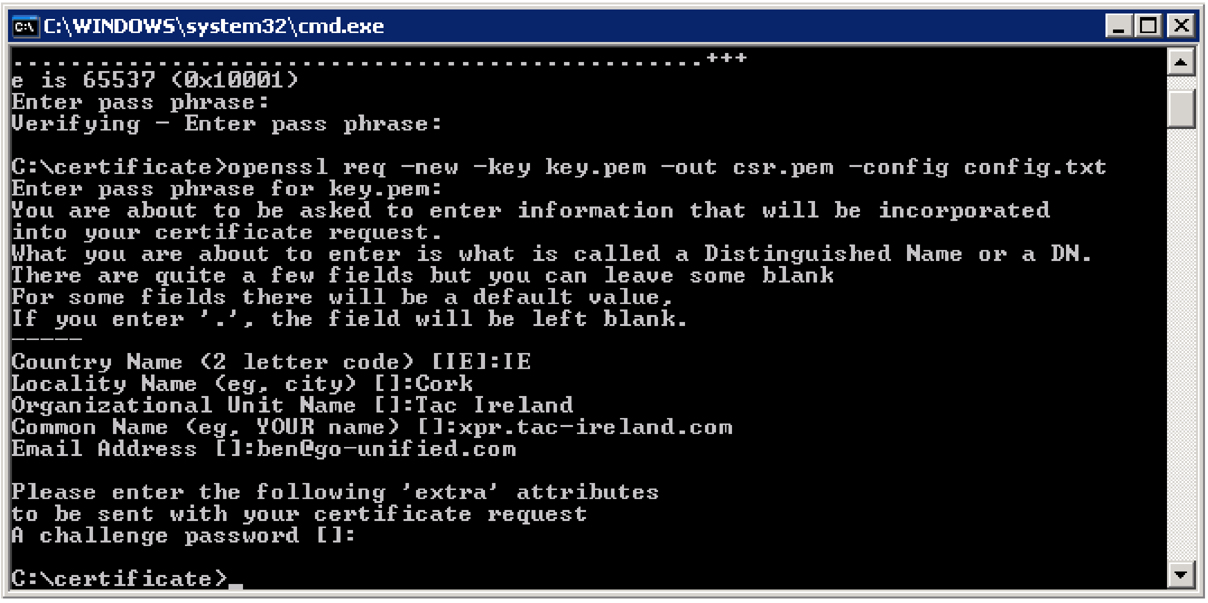
Back in the command prompt create the certificate request file that you send to your root CA.

Just type openssl req -new -key key.pem -out csr.pem -config config.txt

Enter the *password* which you specified beforehand for the private key

Now you have to enter some certificate specific details as specified in the configuration file.

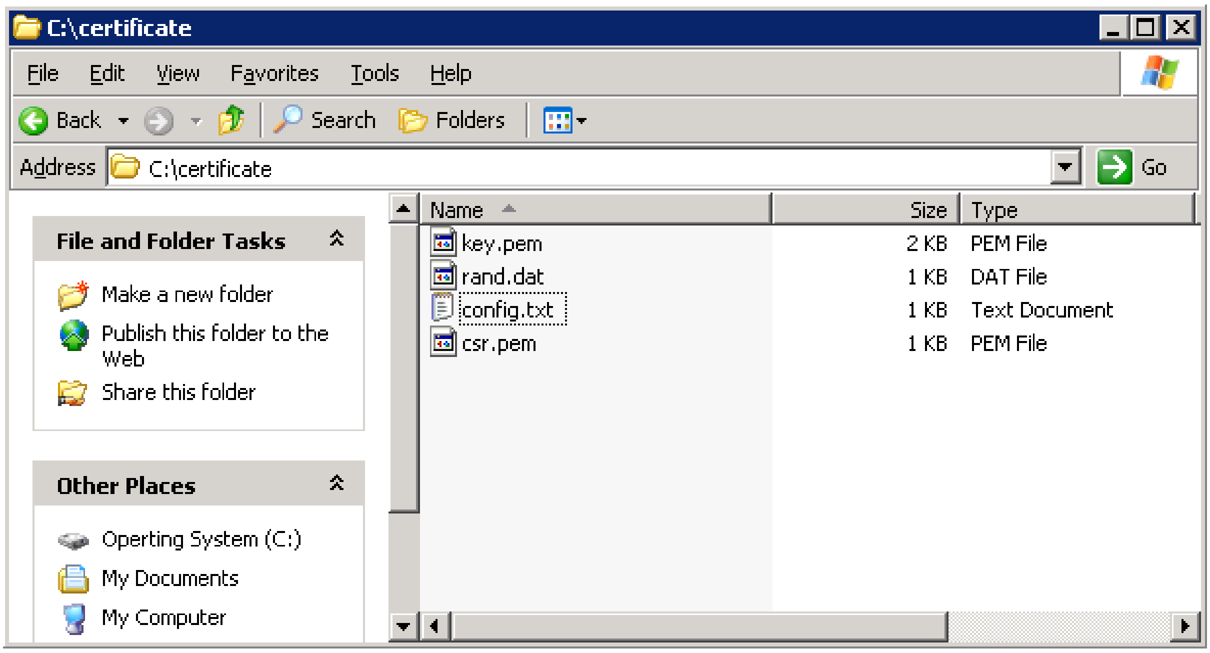
Country Name (2 letter code) [IE]:	*IE*
Locality Name (eg, city) []:	*Cork*
Organizational Unit Name []:	*TAC Ireland*
Common Name (eg, YOUR name) []:	*xpr.tac-ireland.com – This is the server FQDN and it has to be correct in this step*
Email Address []:	*ben@go-unified.com*
Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:	*Just press Enter to skip this field*



```
.............................................................+++
e is 65537 (0x10001)
Enter pass phrase:
Verifying - Enter pass phrase:

C:\certificate>openssl req -new -key key.pem -out csr.pem -config config.txt
Enter pass phrase for key.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [IE]:IE
Locality Name (eg, city) []:Cork
Organizational Unit Name []:Tac Ireland
Common Name (eg, YOUR name) []:xpr.tac-ireland.com
Email Address []:ben@go-unified.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:

C:\certificate>_
```

In the Windows Explorer window you will now see four files.

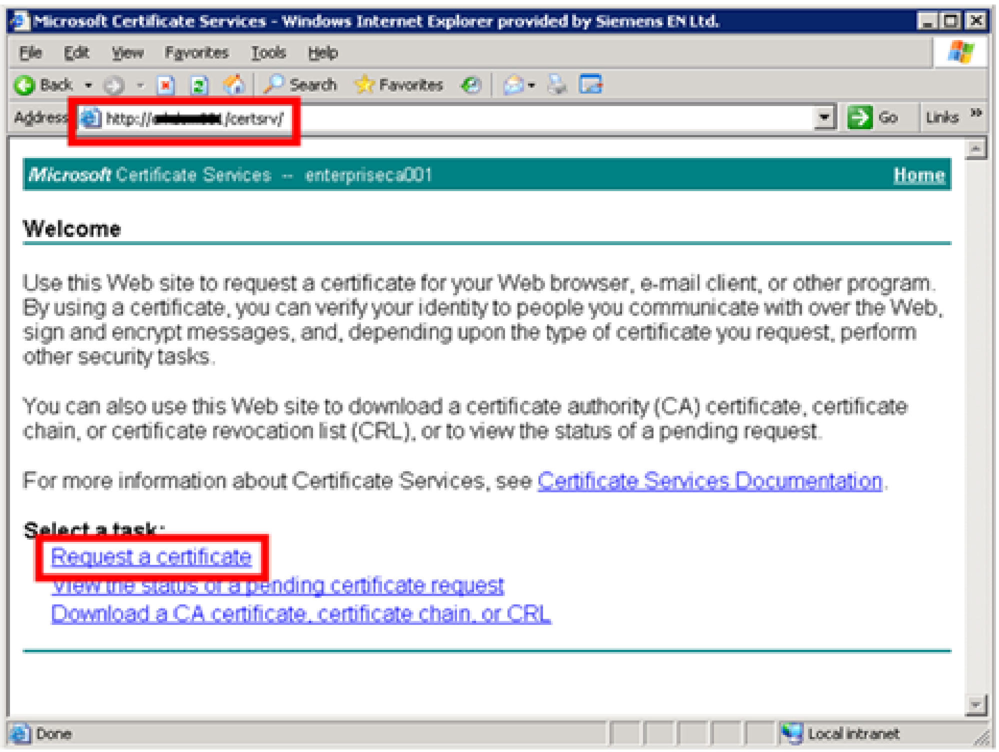
`key.pem`	The private key file
`Rand.dat`	The random md5 hash file
`Config.txt`	The OpenSSL configuration file
`Csr.pem`	The Certificate request file



Name	Size	Type
key.pem	2 KB	PEM File
rand.dat	1 KB	DAT File
config.txt	1 KB	Text Document
csr.pem	1 KB	PEM File

Request the certificate using a Microsoft Root CA

Open the Internet explorer and browse to your certificate authority's homepage. In Microsoft this is `http(s)://<servername>/certsrv`
Here you click on *Request a certificate*


Microsoft Certificate Services - Windows Internet Explorer provided by Siemens EN Ltd.
File Edit View Favorites Tools Help
Back Search Favorites
Address http://[redacted]/certsrv/
Go Links
Done
Local intranet

Microsoft Certificate Services -- enterpriseca001 **Home**

Welcome

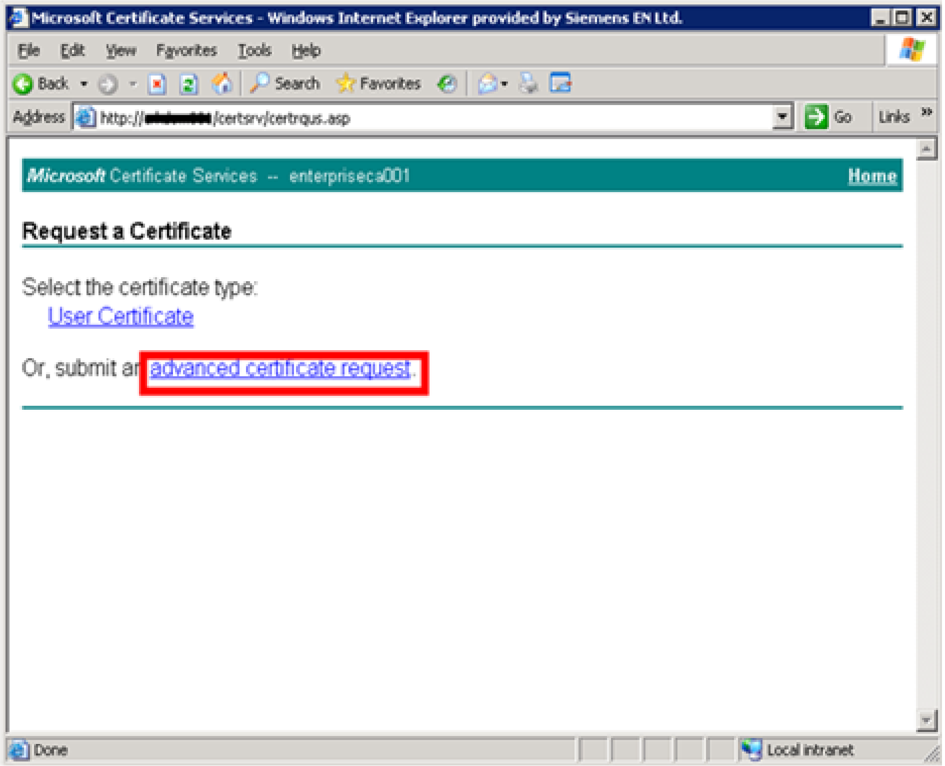
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Press on `advanced certificate request`


Microsoft Certificate Services - Windows Internet Explorer provided by Siemens EN Ltd.
File Edit View Favorites Tools Help
Back Search Favorites
Address http://[redacted]/certsrv/certrqus.asp
Go Links
Done
Local intranet

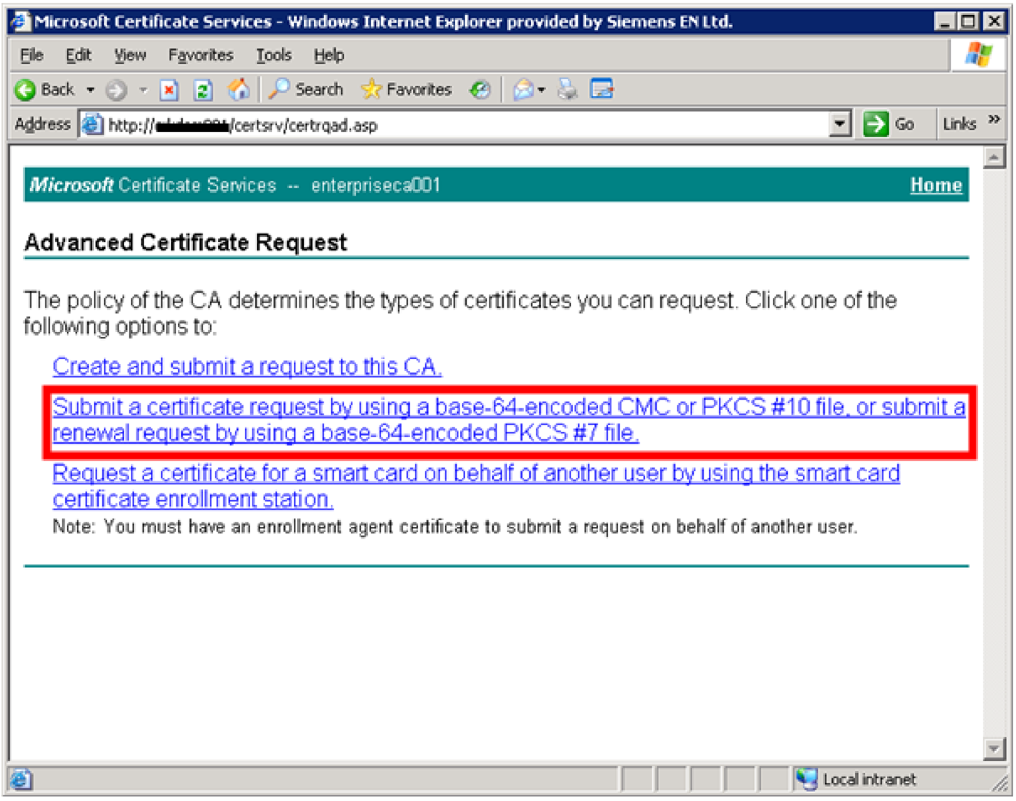
Microsoft Certificate Services -- enterpriseca001 **Home**

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

Select `Submit a certificate request by using a base 4 encoded CMC`


Microsoft Certificate Services - Windows Internet Explorer provided by Siemens EN Ltd.
File Edit View Favorites Tools Help
Back Search Favorites
Address http://[redacted]/certsrv/certrqad.asp
Go Links
Local intranet

Microsoft Certificate Services -- enterpriseca001 Home

Advanced Certificate Request

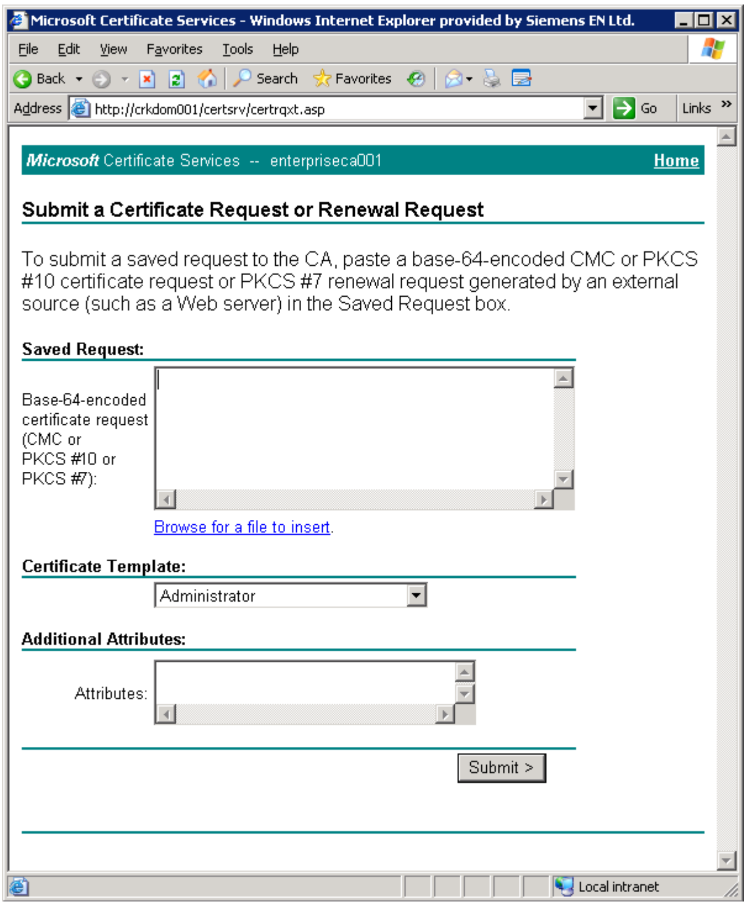
The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.
Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

`Please enter the certificate details here`


Microsoft Certificate Services - Windows Internet Explorer provided by Siemens EN Ltd.
File Edit View Favorites Tools Help
Back Search Favorites
Address http://crkdom001/certsrv/certrqxt.asp
Go Links
Local intranet

Microsoft Certificate Services -- enterpriseca001 Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Browse for a file to insert.

Certificate Template:

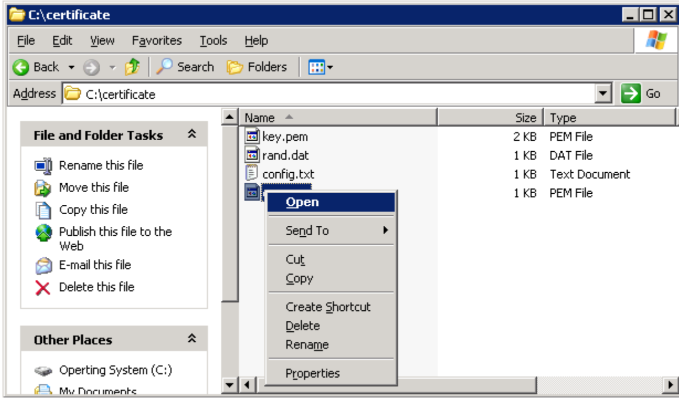
Administrator

Additional Attributes:

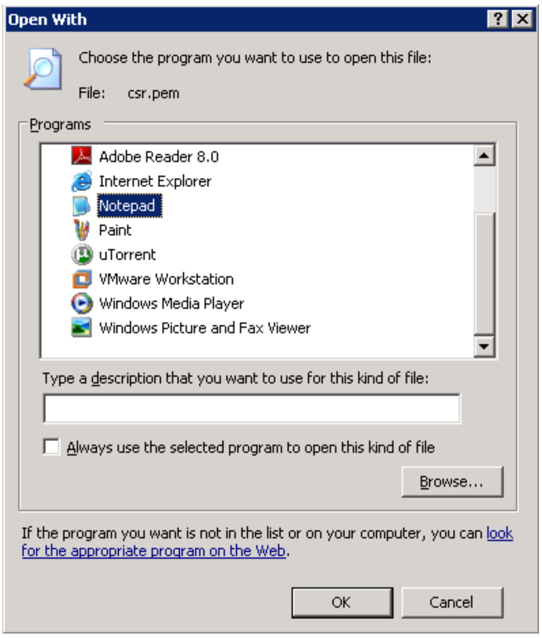
Attributes:

Submit >

Browse to the `c:\certificate` folder and open the file `csr.pem` with a `text editor`



Name	Size	Type
key.pem	2 KB	PEM File
rand.dat	1 KB	DAT File
config.txt	1 KB	Text Document
	1 KB	PEM File



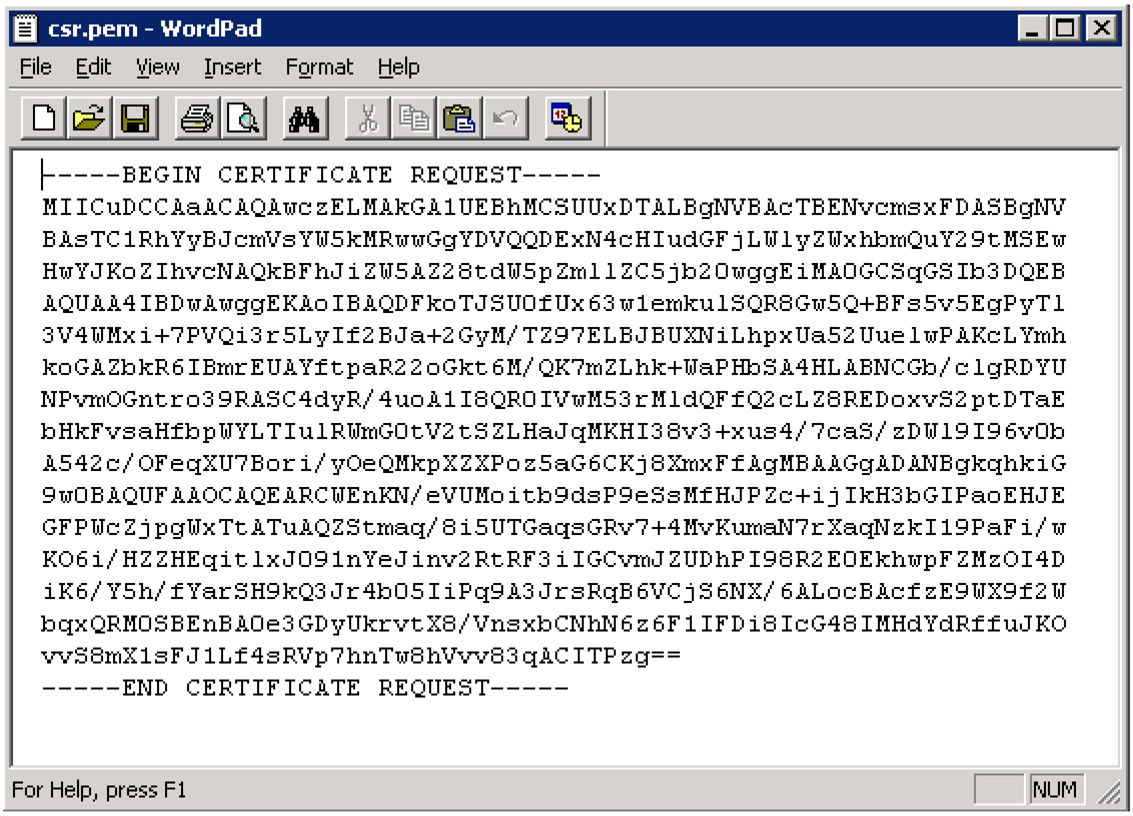
Choose the program you want to use to open this file:

File: csr.pem

Type a description that you want to use for this kind of file:

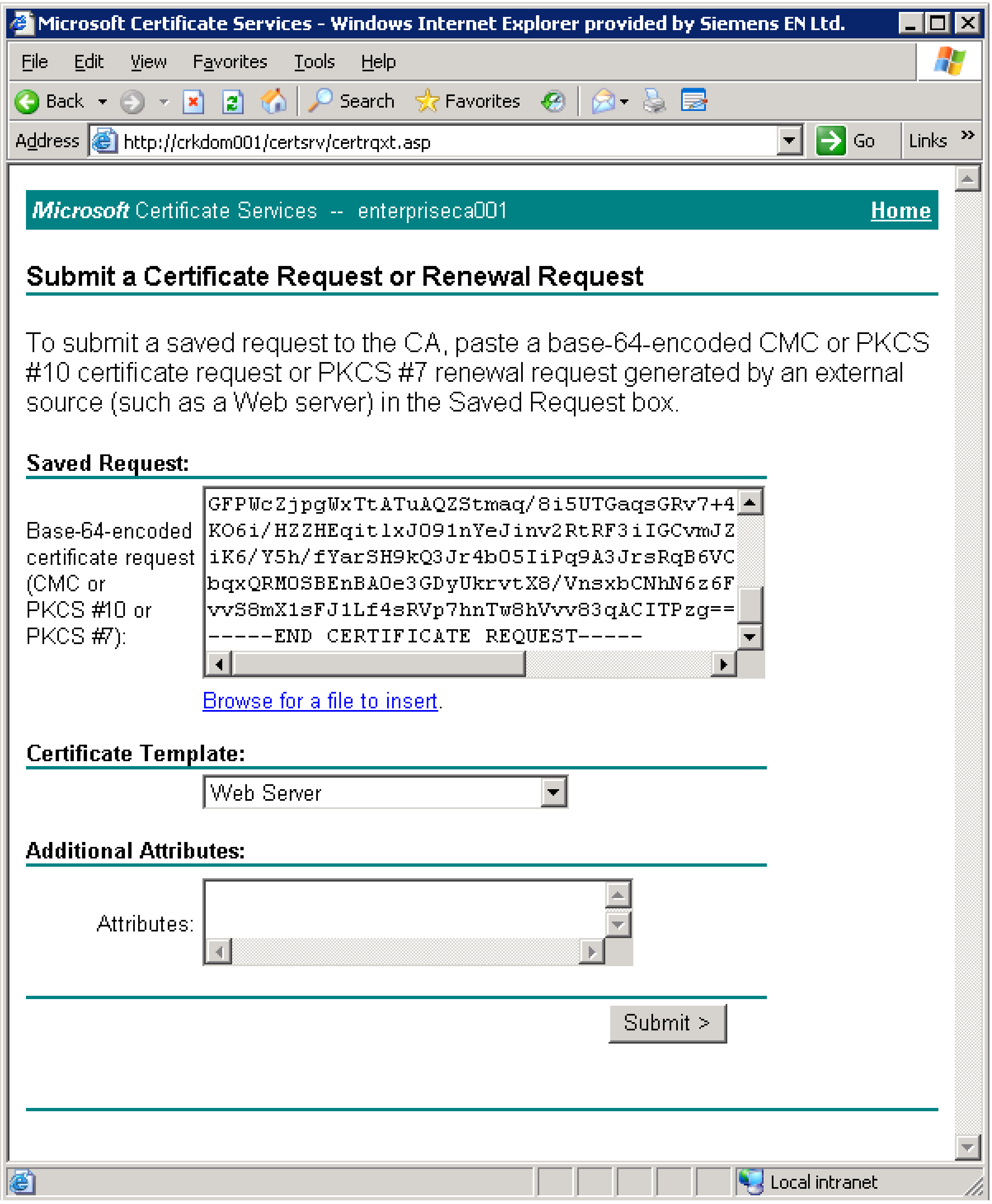
□ Always use the selected program to open this kind of file

If the program you want is not in the list or on your computer, you can look for the appropriate program on the Web.



```
-----BEGIN CERTIFICATE REQUEST-----
MIICuDCCAaACAQAwczELMAkGA1UEBhMCSUUxDTALBgNVBAcTBENvcmsxFDASBgNV
BAsTC1RhYyBJcmVsYW5kMRwwGgYDVQQDExN4cHIudGFjLWlyZWxhbmQuY29tMSEw
HwYJKoZIhvcNAQkBFhJiZW5AZ28tdW5pZmllZC5jb20wggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDFkoTJSU0fUx63w1emkulSQR8Gw5Q+BFs5v5EgPyTl
3V4WMxi+7PVQi3r5LyIf2BJa+2GyM/TZ97ELBJBUXNiLhpxUa52UuelwPAKcLYmh
koGAZbkR6IBmrEUAYftpaR22oGkt6M/QK7mZLhk+WaPHbSA4HLABNCGb/clgRDYU
NPvmOGntro39RASC4dyR/4uoA1I8QR0IVwM53rMldQFfQ2cLZ8REDoxvS2ptDTaE
bHkFvsaHfbpWYLTIulRWmG0tV2tSZLHaJqMKHI38v3+xus4/7caS/zDWl9I96v0b
A542c/OFeqXU7Bori/yOeQMkpXZXPoz5aG6CKj8XmxFfAgMBAAGgADANBgkqhkiG
9w0BAQUFAAOCAQEARCWEnKN/eVUMoitb9dsP9eSsMfHJPZc+ijIkH3bGIPaoEHJE
GFPWcZjpgWxTtATuAQZStmaq/8i5UTGaqsGRv7+4MvKumaN7rXaqNzkI19PaFi/w
KO6i/HZZHEqitlxJO91nYeJinv2RtRF3iIGCvmJZUDhPI98R2EOEkhwpFZMzOI4D
iK6/Y5h/fYarSH9kQ3Jr4bO5IiPq9A3JrsRqB6VCjS6NX/6ALocBAcfzE9WX9f2W
bqxQRMOSBEnBAOe3GDyUkrvtX8/VnsxbCNhN6z6F1IFDi8IcG48IMHdYdRffuJKO
vvS8mX1sFJ1Lf4sRVp7hnTw8hVvv83qACITPzg==
-----END CERTIFICATE REQUEST-----
```

`Copy – Paste` the information into the Request window, select Certificate Template: `Web Server` and `submit` the request


Microsoft Certificate Services - Windows Internet Explorer provided by Siemens EN Ltd.
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://crkdom001/certsrv/certrqxt.asp
Go
Links
Local intranet

Microsoft Certificate Services -- enterpriseca001 **Home**

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
GFPWcZjpgWxTtATuAQZStmaq/8i5UTGaqsGRv7+4
KO6i/HZZHEqitlxJO91nYeJinv2RtRF3iIGCvmJZ
iK6/Y5h/fYarSH9kQ3Jr4bO5IiPq9A3JrsRqB6VC
bqxQRMOSBEnBAOe3GDyUkrvtX8/VnsxbCNhN6z6F
vvS8mX1sFJ1Lf4sRVp7hnTw8hVvv83qACITPzg==
-----END CERTIFICATE REQUEST-----
```

Browse for a file to insert.

Certificate Template:

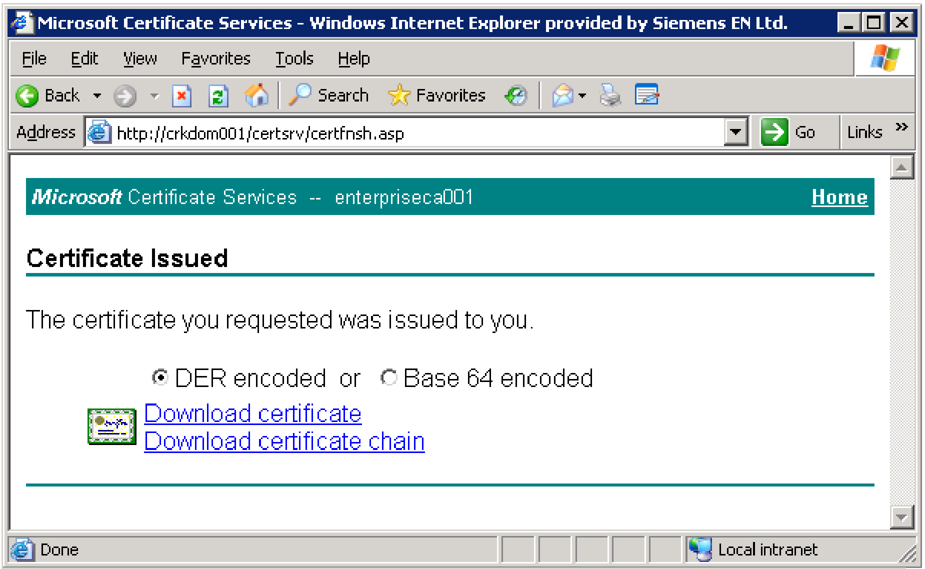
Web Server

Additional Attributes:

Attributes:

Submit >

Download the Certificate *DER* encoded and save it in the `c:\certificate` folder


Microsoft Certificate Services - Windows Internet Explorer provided by Siemens EN Ltd.
File Edit View Favorites Tools Help
Back Search Favorites
Go Links
Done
Local intranet

Address: http://crkdom001/certsrv/certfnsh.asp

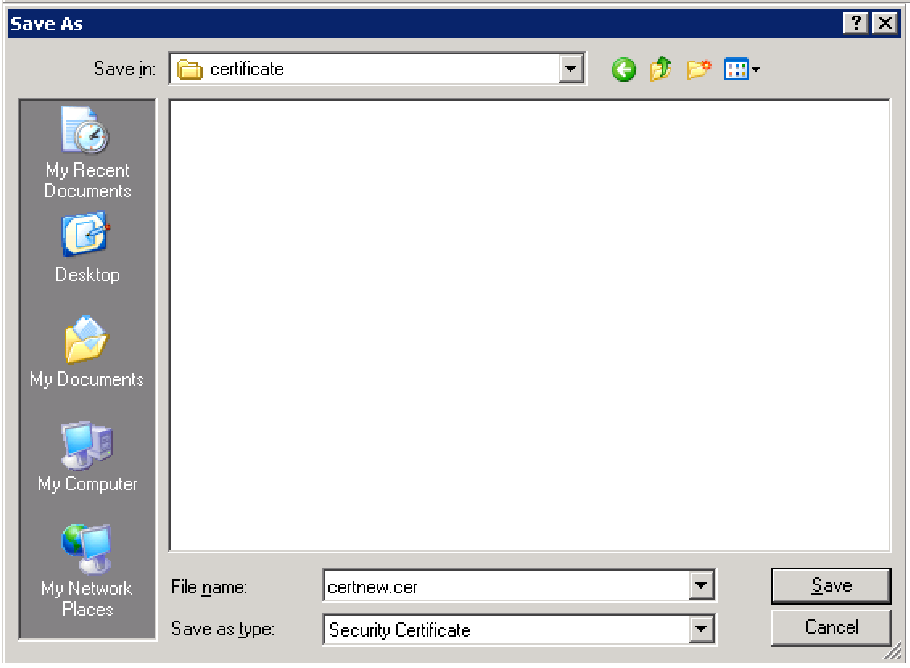
Microsoft Certificate Services -- enterpriseca001 **Home**

Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

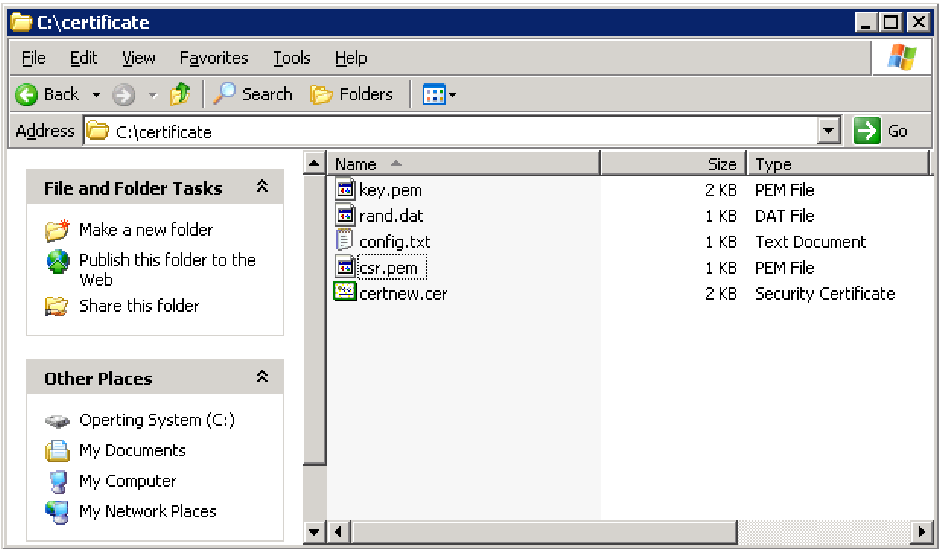
Download certificate
Download certificate chain



Save in: certificate

File name: certnew.cer

Save as type: Security Certificate

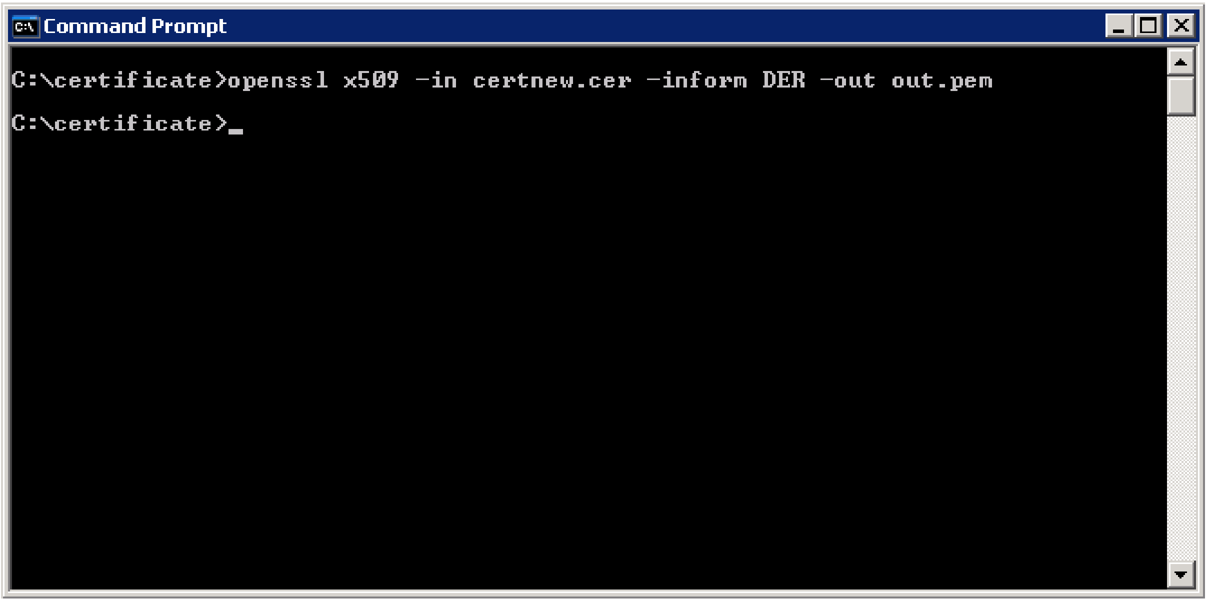


Address: C:\certificate

Name	Size	Type
key.pem	2 KB	PEM File
rand.dat	1 KB	DAT File
config.txt	1 KB	Text Document
csr.pem	1 KB	PEM File
certnew.cer	2 KB	Security Certificate

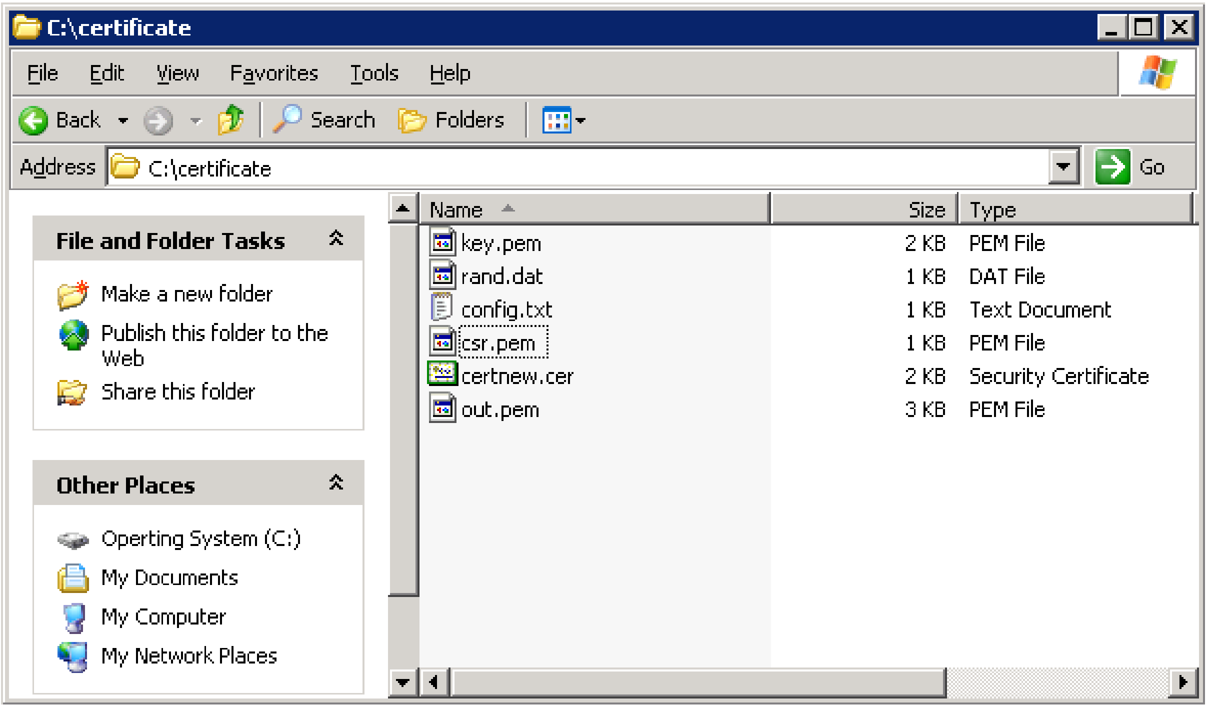
Back in the command prompt translate the certnew.cer file into the PEM OpenSSL file format

```
openssl x509 -in certnew.cer -inform DER -out out.pem
```



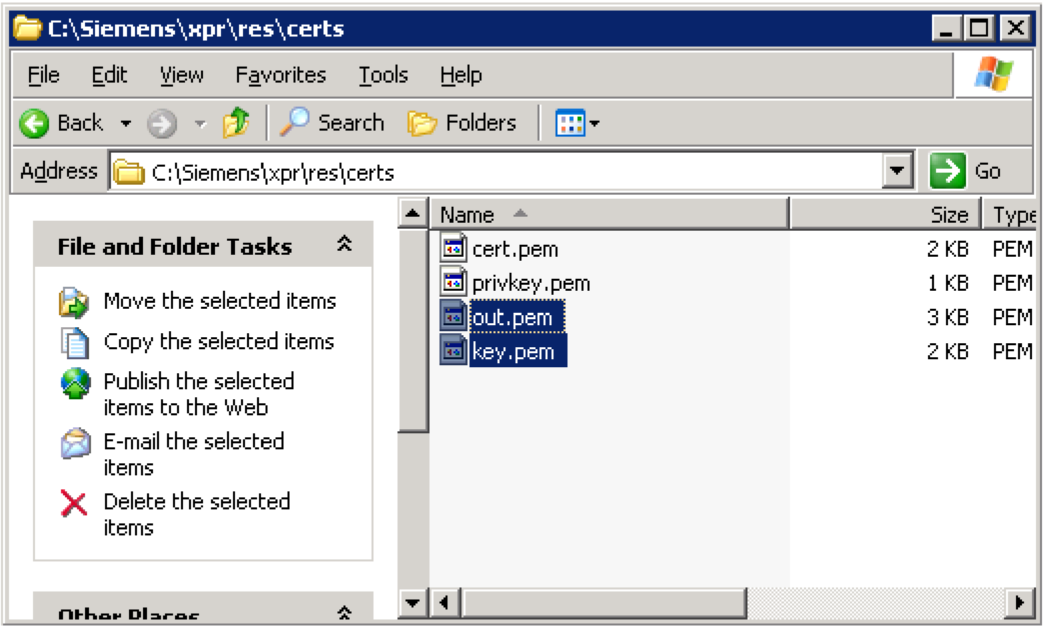
```
C:\certificate>openssl x509 -in certnew.cer -inform DER -out out.pem

C:\certificate>_
```

The content of your `c:\certificate` folder should look like in this example



Name	Size	Type
key.pem	2 KB	PEM File
rand.dat	1 KB	DAT File
config.txt	1 KB	Text Document
csr.pem	1 KB	PEM File
certnew.cer	2 KB	Security Certificate
out.pem	3 KB	PEM File

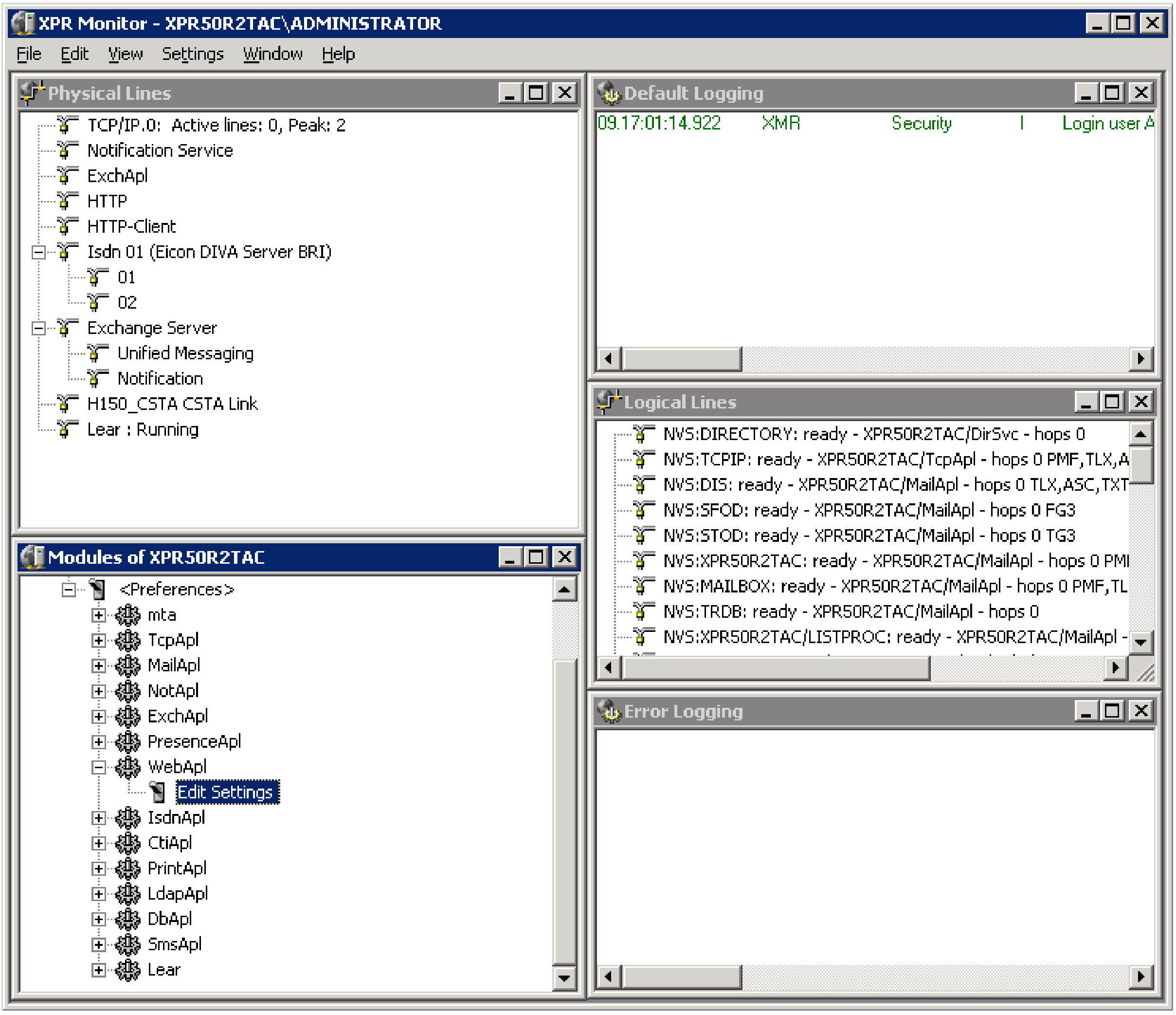
Mark the two .pem files *`key.pem and out.pem`* and *copy* them into the HiPath Xpressions certificate store *`<XPR Installation Dir>\res\certs`*



Address: C:\Siemens\xpr\res\certs

Name	Size	Type
cert.pem	2 KB	PEM
privkey.pem	1 KB	PEM
out.pem	3 KB	PEM
key.pem	2 KB	PEM

Open the MRS Monitor and `Edit the Webpl's settings`



Physical Lines:

```
TCP/IP.0:  Active lines: 0, Peak: 2
Notification Service
ExchApl
HTTP
HTTP-Client
Isdn 01 (Eicon DIVA Server BRI)
    01
    02
Exchange Server
    Unified Messaging
    Notification
H150_CSTA CSTA Link
Lear : Running
```

Default Logging:

```
09.17:01:14.922    XMR    Security    I    Login user A
```

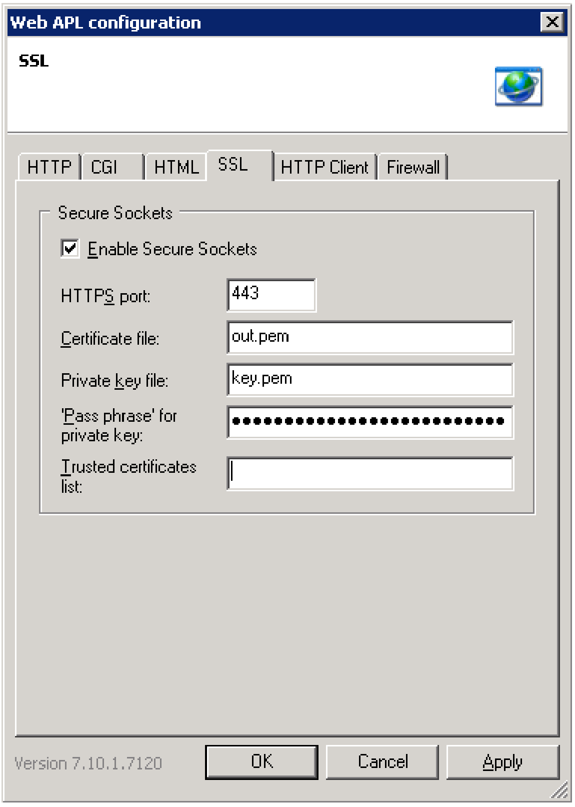
Logical Lines:

```
NVS:DIRECTORY: ready - XPR50R2TAC/DirSvc - hops 0
NVS:TCPIP: ready - XPR50R2TAC/TcpApl - hops 0 PMF,TLX,A
NVS:DIS: ready - XPR50R2TAC/MailApl - hops 0 TLX,ASC,TXT
NVS:SFOD: ready - XPR50R2TAC/MailApl - hops 0 FG3
NVS:STOD: ready - XPR50R2TAC/MailApl - hops 0 TG3
NVS:XPR50R2TAC: ready - XPR50R2TAC/MailApl - hops 0 PMI
NVS:MAILBOX: ready - XPR50R2TAC/MailApl - hops 0 PMF,TL
NVS:TRDB: ready - XPR50R2TAC/MailApl - hops 0
NVS:XPR50R2TAC/LISTPROC: ready - XPR50R2TAC/MailApl -
```

Modules of XPR50R2TAC:

```
<Preferences>
    mta
    TcpApl
    MailApl
    NotApl
    ExchApl
    PresenceApl
    WebApl
        Edit Settings
    IsdnApl
    CtiApl
    PrintApl
    LdapApl
    DbApl
    SmsApl
    Lear
```

On the SSL tab make sure SSL is enabled and the default port `443` is selected.
The certificate file is named `out.pem` and the private key is called `key.pem` in our example. As Pass Phrase please enter the string you entered to secure the private key in our example *"Communication for the open minded"*



Secure Sockets

☑ Enable Secure Sockets

HTTPS port: 443

Certificate file: out.pem

Private key file: key.pem

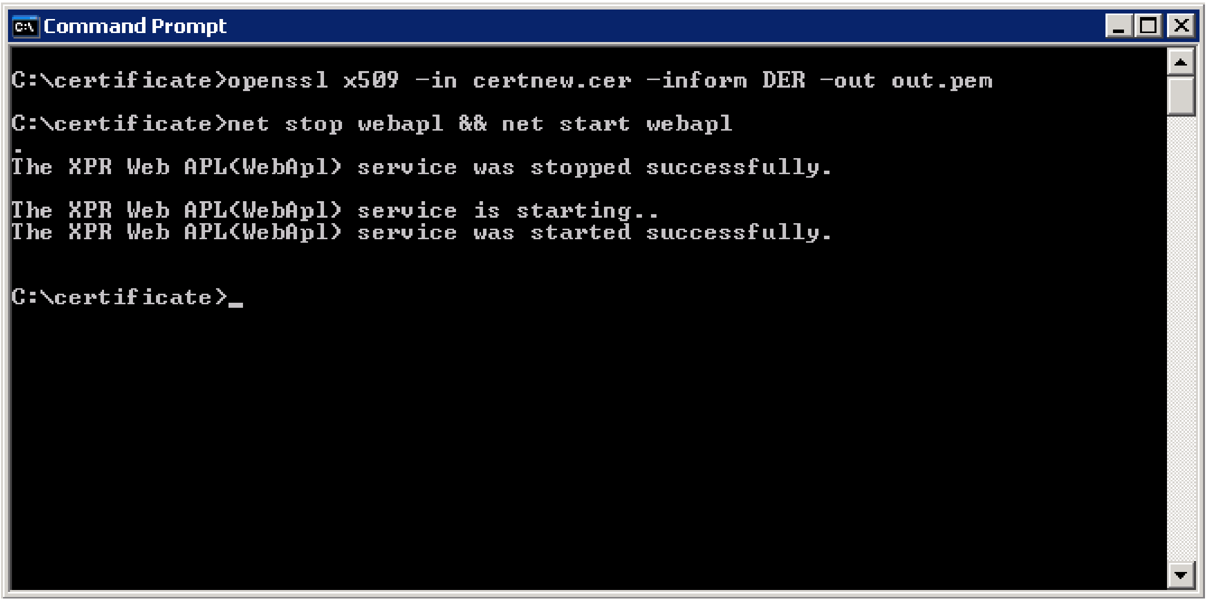
'Pass phrase' for private key: ••••••••••••••••••••••••••

Trusted certificates list:

Version 7.10.1.7120

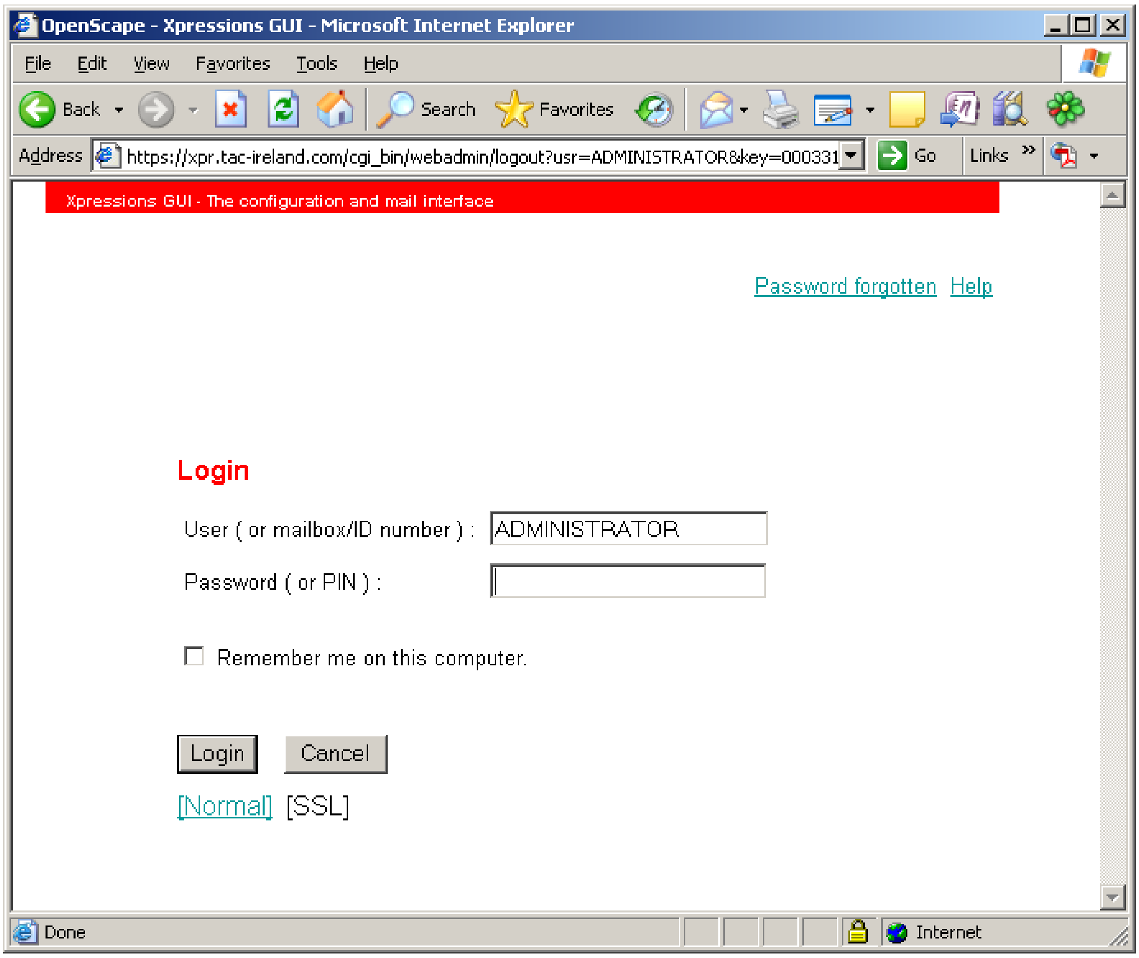
For the changes to apply simply restart the WebApl using the command prompt

Net stop webapl && net start webapl



```
C:\certificate>openssl x509 -in certnew.cer -inform DER -out out.pem

C:\certificate>net stop webapl && net start webapl

The XPR Web APL(WebApl) service was stopped successfully.

The XPR Web APL(WebApl) service is starting..
The XPR Web APL(WebApl) service was started successfully.


C:\certificate>_
```

Now *browse* to the HiPath Xpressions Web Assistant URL (*https://<FQDN>*) and you will not see any certificate error message anymore. ***Job done!***



OpenScape - Xpressions GUI - Microsoft Internet Explorer

Address https://xpr.tac-ireland.com/cgi_bin/webadmin/logout?usr=ADMINISTRATOR&key=000331

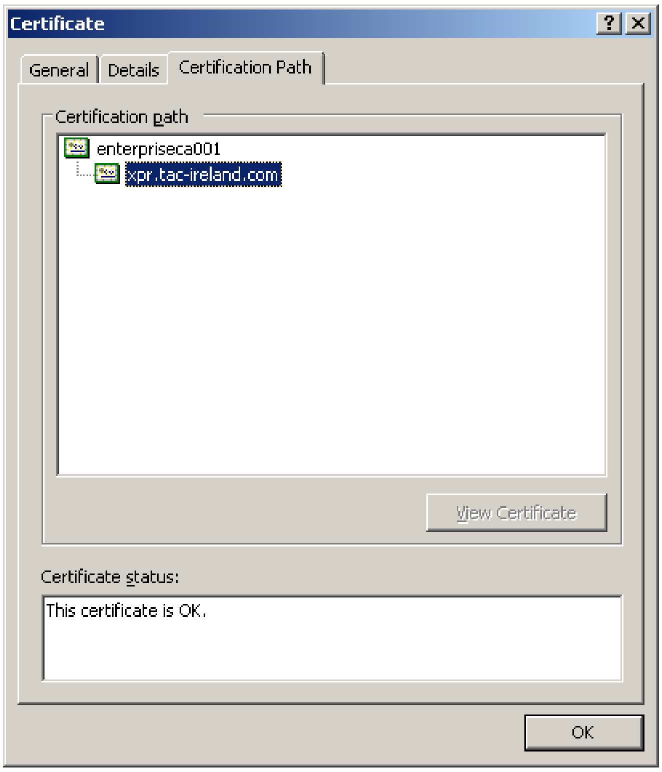
Xpressions GUI - The configuration and mail interface

Login

User (or mailbox/ID number) : ADMINISTRATOR

Password (or PIN) :

□ Remember me on this computer.



Certificate

Certification path

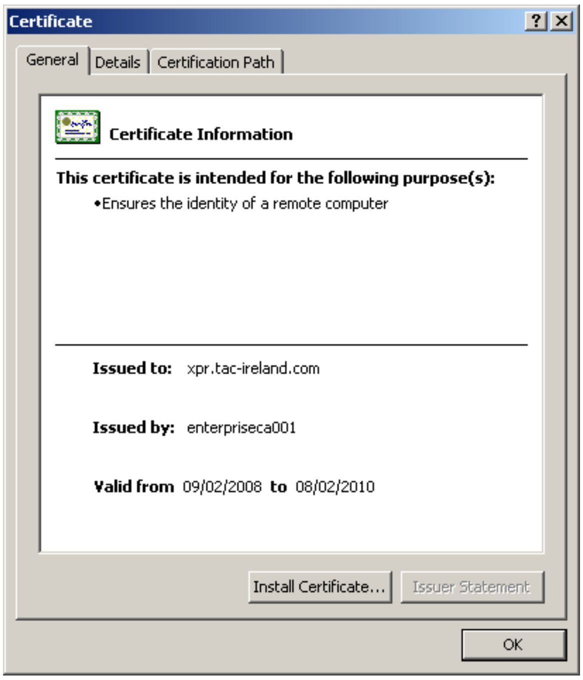
enterpriseca001

xpr.tac-ireland.com

Certificate status:

This certificate is OK.

Details about the certificate can be gained by pressing on the lock icon in the IE.



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

•Ensures the identity of a remote computer

Issued to: xpr.tac-ireland.com

Issued by: enterpriseca001

Valid from 09/02/2008 **to** 08/02/2010