

# Technical Note

Auteur: Wim van Ommen  
Gemaakt op: 31 Oktober 2008



## SSL Certicaten en de NetASQ

Deze technote beschrijft de hele procedure om een SSL certicaat van Comodo te maken en op de NetASQ Firewall te gebruiken voor de captive portal. De werkwijze is voor andere leveranciers van certificaten zo goed als gelijk.

Maak een csr aan via openssl (voor Windows kan [Win32 OpenSSL v0.9.8i Light](#) gebruikt worden):

```
openssl req -new -nodes -keyout myserver.key -out server.csr
```

voor Windows:

```
c:\openssl\bin\openssl req -new -nodes -keyout myserver.key -out server.csr
```

```
Generating a 1024 bit RSA private key
..+++++
.....+++++
unable to write 'random state'
writing new private key to 'myserver.key'
```

```
-----
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) [AU]:NL
State or Province Name (full name) [Some-State]:UT
Locality Name (eg, city) []:Soest
Organization Name (eg, company) [Internet Widgits Pty Ltd]:TopIT
Organizational Unit Name (eg, section) []:TopIT
Common Name (eg, YOUR name) []:www.topit.nl
Email Address []:wim@topit.nl
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
```

```
A challenge password []:12345
```

```
An optional company name []:Topit
```

Let op dat bij Common Name de naam van server moet staan!!!!

## Vervolgens is het heel belangrijk om het bestand myserver.key goed te bewaren!!!

Open het bestand server.csr, al het goed is ziet dat er ongeveer zo uit:

```
---BEGIN CERTIFICATE REQUEST---  
MIIB7TCCAUYCAQAwfjELMAkGA1UEBhMCTkwxCzAJBgNVBAGTAIVUMQ4wDAYDVQQH  
H  
EwVTb2VzdDEOMAwGA1UEChMFVGV9wSVQxDjAMBgNVBAAsTBVRvcEIUMRUwEwYDV  
QQD  
Ewx3d3cudG9waXQubmwxGzAZBgkqhkiG9w0BCQEWDHdpbUB0b3BpdC5ubDCBnzAN  
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAog/0OyZrNtpIkIB7VpubXf83jeoBJZK  
jllZy7sJJ5KI2hJQ8Z+2Rzla8GtpUENF+p8ANEAP5aFg/Oi6GDT7URwGkc9DfUT  
pTFbvyGSR+YIHkgFSZD7bjVfX8qp1PWDN0dyYOa/c2IYpERq7JToTsz+tnCgdDEs  
AtmmBaogm8UCAwEAAaAvMBQGCSqGSIb3DQEJAJEHEwVUub3BJVDAXBgkqhkiG9w0  
B  
CQCxChMIMTlzNDU2NzgwDQYJKoZIhvcNAQEEBQADgYEANStH+Ln6Ney6ll2RRCSO  
E/FtoZ69tByWPKINPndQzzwEMnVXqQkzcv6AcUthg9CycUpr24T9FwqO2NhSYoef  
61o2We4resAFVtYi3nGC+q+Ny3Lr93uPUm0LGehmcCp196pdM/0cEHalyr/tMxsp  
UzH24I6bl41c4Xp8LQJyR6w=  
---END CERTIFICATE REQUEST---
```

Plak deze code in de aanvraag voor Comodo.

Volg dan de procedure tot Comodo de certificaat bestanden mailt.

Pak de zipfile uit.

Daar staan een aantal belangrijke bestanden in:

AddTrustExternalCARoot.crt

EssentialSSLCA\_2.crt

www\_topit\_nl.crt (als het goed is, is dit de naam van het domein waarvoor dit certificaat aangevraagd is).

Ga in de manager naar de Captive Portal en kies Web Portal, klik op private key certificate en kies Add.

Geef een naam op (bijvoorbeeld TopIT) kies private key en klik next.

Klik op certificate file name en ga naar de map waar de certificaten staan en kies bij bestandstype alle bestanden en kies www\_topit\_nl (deze heeft uiteraard een andere naam!).

Klik vervolgens private key en ga naar de map waar de private key staat en kies deze.

Klik vervolgens op finish.

Klik vervolgens bij certificate chain op add en voeg daar als certificate authority de AddTrustExternalCARoot.crt, EssentialSSLA\_2.crt en ComodoUTNSGCCA.crt toe.

Nu zou het certificaat actief moeten zijn.