

How to configure NGS for with certificate chain

Contents

How to configure NGS for with certificate chain	1
Idea:	1
Setup:	1
Configuration steps:.....	1
Test login with client and verify certificate chain	10

NOTE: This is not a official Cisco document and you use it on your own risk.

**Best regards
Roger Nobel**

Idea:

These instructions are of relevance if you have a server certificate for the Guest Server for installation that has been issued by an intermediate CA. These instructions are valid for Guest Server 2.0.x only. NGS use certificate from intermediate CA server but client managing NGS only has root CA certificate trust installed. Hence NGS will have to send the full certificate chain to allow client validate the server NGS certificate.

Setup:

NGS 2.0.2

DC's are MS server 2003

DC01 (root CA – domain : wlaaan.ch)

DC03 (subCA - child domain: child1.wlaaan.ch)

Configuration steps:

- 1.) NGS does certificate request

NGS (admin) > Server > SSL Settings > Certificate Signing Request > Create CSR



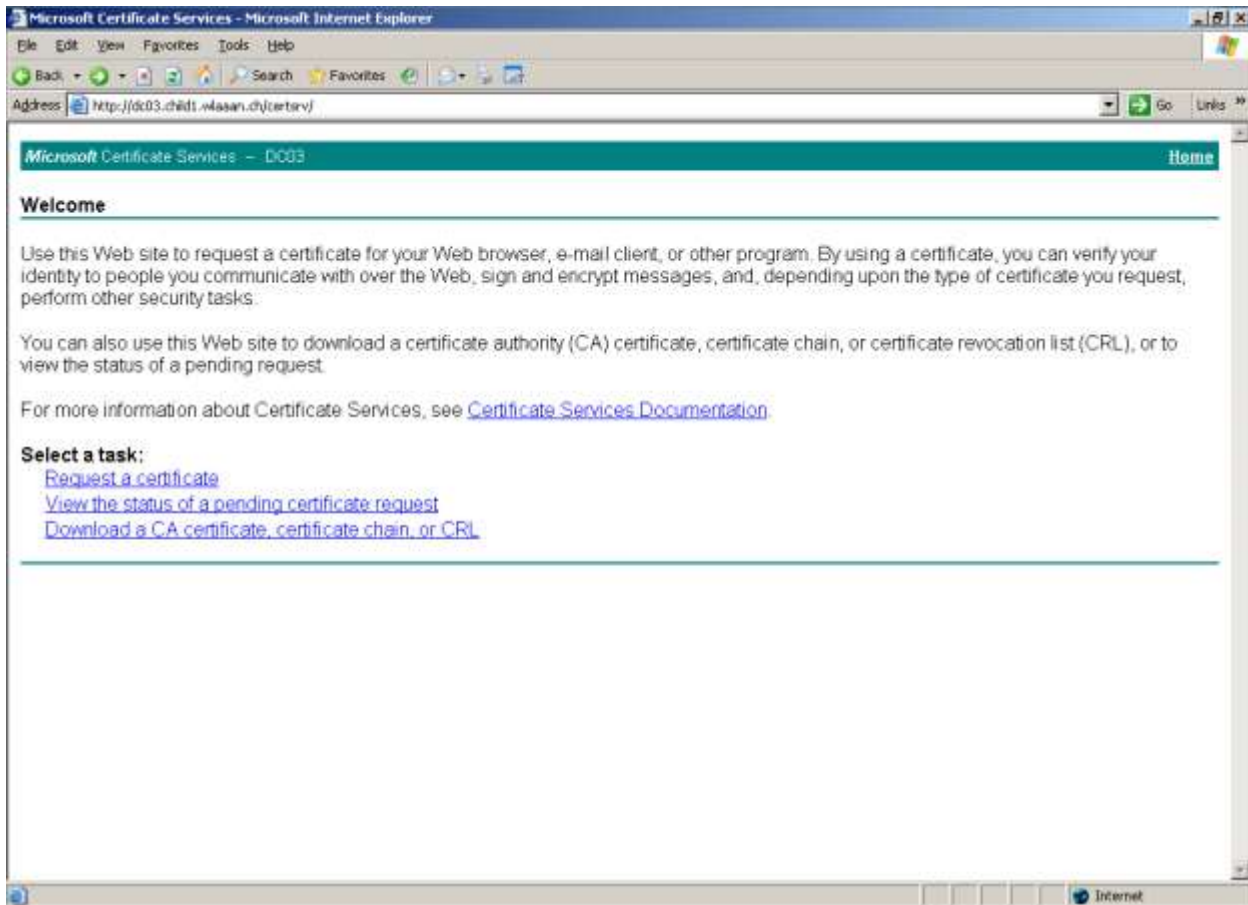
Create
Download CSR

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

```
MIIBqzCCARQCAQAwazELMAkGA1UEBhMCQ0gxJDAiBgNVBAMTG2NodGFjLWd1ZXN0
LTaxLmNjYS1jaHRhYy5jaDELMAkGA1UECBMCemgxZzAJBgNVBACtAnpoMQ4wDAYD
VQQKEwVjaHRhYzEMMAoGA1UECxMDdGFjMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQDPnC+A7oVx9MsMnSWMYwUk8POj7LDKmxRDHMsZAmG3loZdAHM3g/3nxM2V
pCMmw5vLOJzigPHbc8P7MGDcw15x1ZgDGnLJoS6PmgR6uJmJkdBHKCrjBnSQmVp1
m3cWwuzM3r0dMabJSNhG7uZXmkgetjvD3wP3DOGHX/ogRlwj0QIDAQABoAAwDQYJ
KoZlhvcNAQEFBQADgYEAioh1BR7VZKC1h82FZ67tRrmkGoHU2Bp17ULVi2uzKu8
GSj7fQ29E74f3r+nBTTuPrHaGKyQqUIXhH3OLYfKXN7VQXifBZtl/Gsk7leTW72
dzdgy2KmvhypBlGE+7bzNrgPEgdxpDXfOgZJGd4bppY3/8FaYU7TqVoruEDbQ6g=
```

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

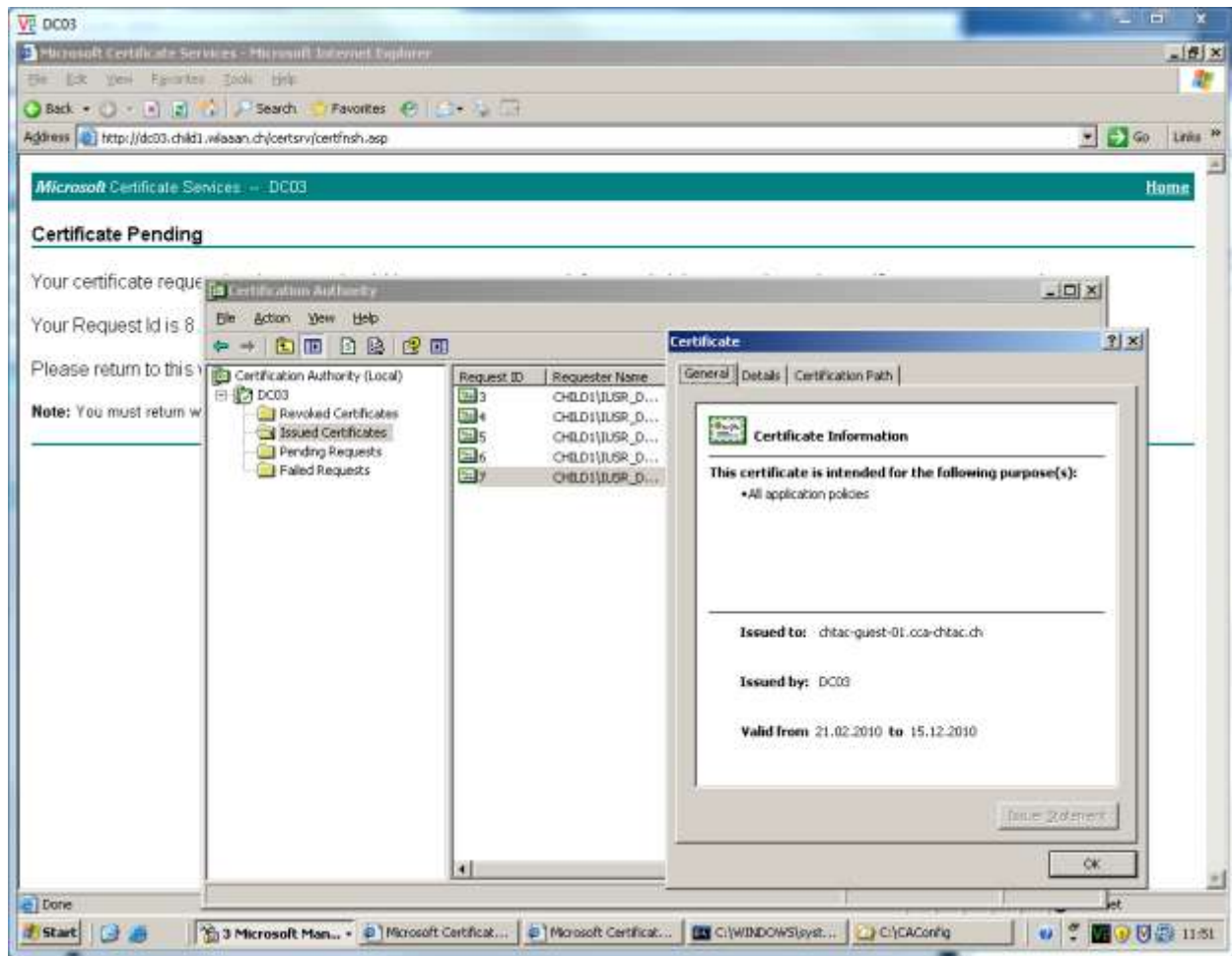
2.) Request certificate for NGS and DC03 and DC01



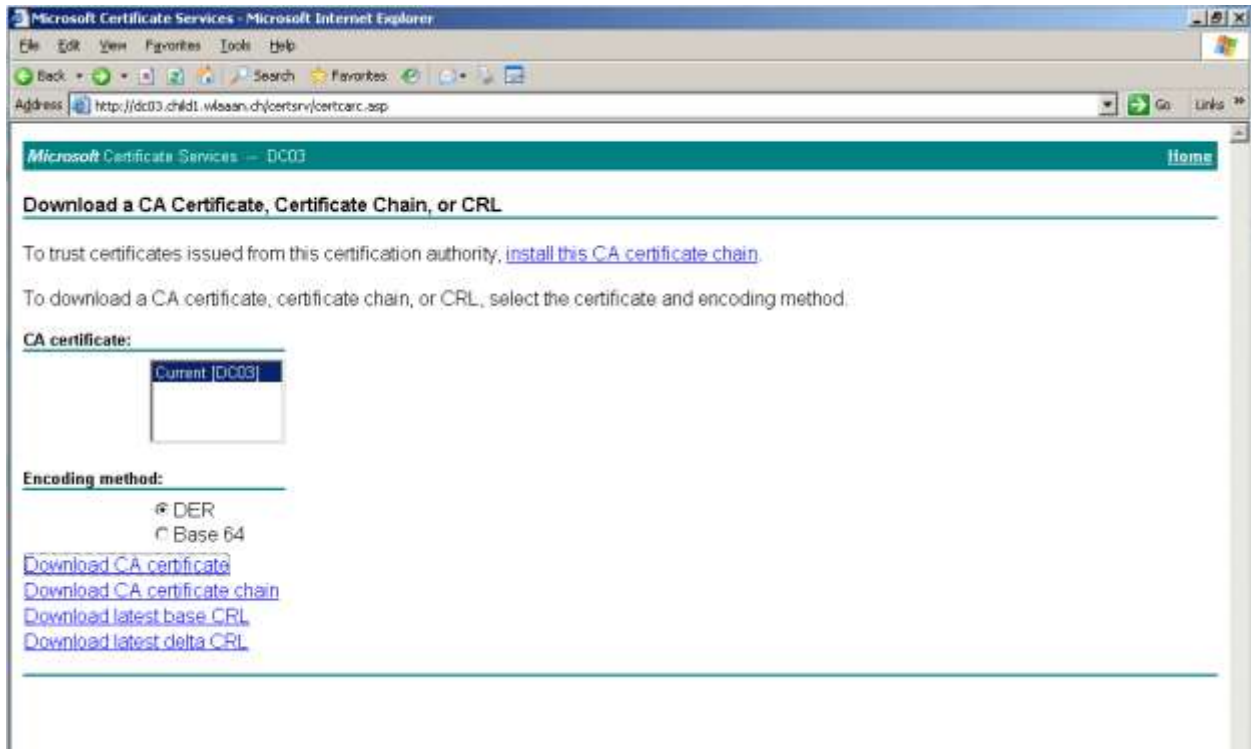
Open IE for <http://dc03.child1.wlaan.ch/certsrv/>

- a.) Request a certificate
- b.) Advanced certificate request
- c.) Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file, or submit a renewal by using a base-64-encoded PKCS#7 file.
- d.) Paste the CSR from NGS to "Save Request:" -> Submit

Now get the certificate from the CA Authority in base-64-encoded format



Also collect certificate for DC01 and DC03

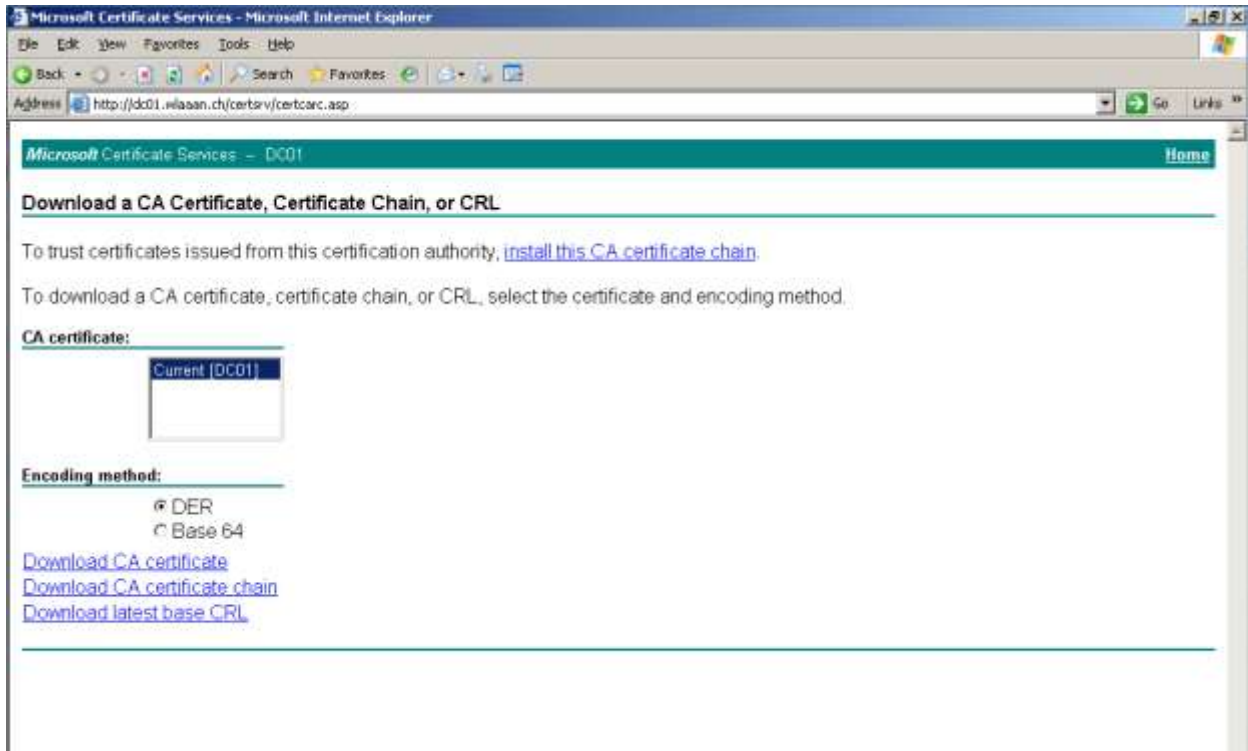


<http://dc03.child1.wlaaan.ch/certsrv/>

a.) Download a CA certificate, certificate chain, or CRL

b.) Download CA certificate

=> RootSubCA-DC03.cer



<http://dc01.wlaaan.ch/certsrv/>

- a.) Download a CA certificate, certificate chain, or CRL
- b.) Download CA certificate

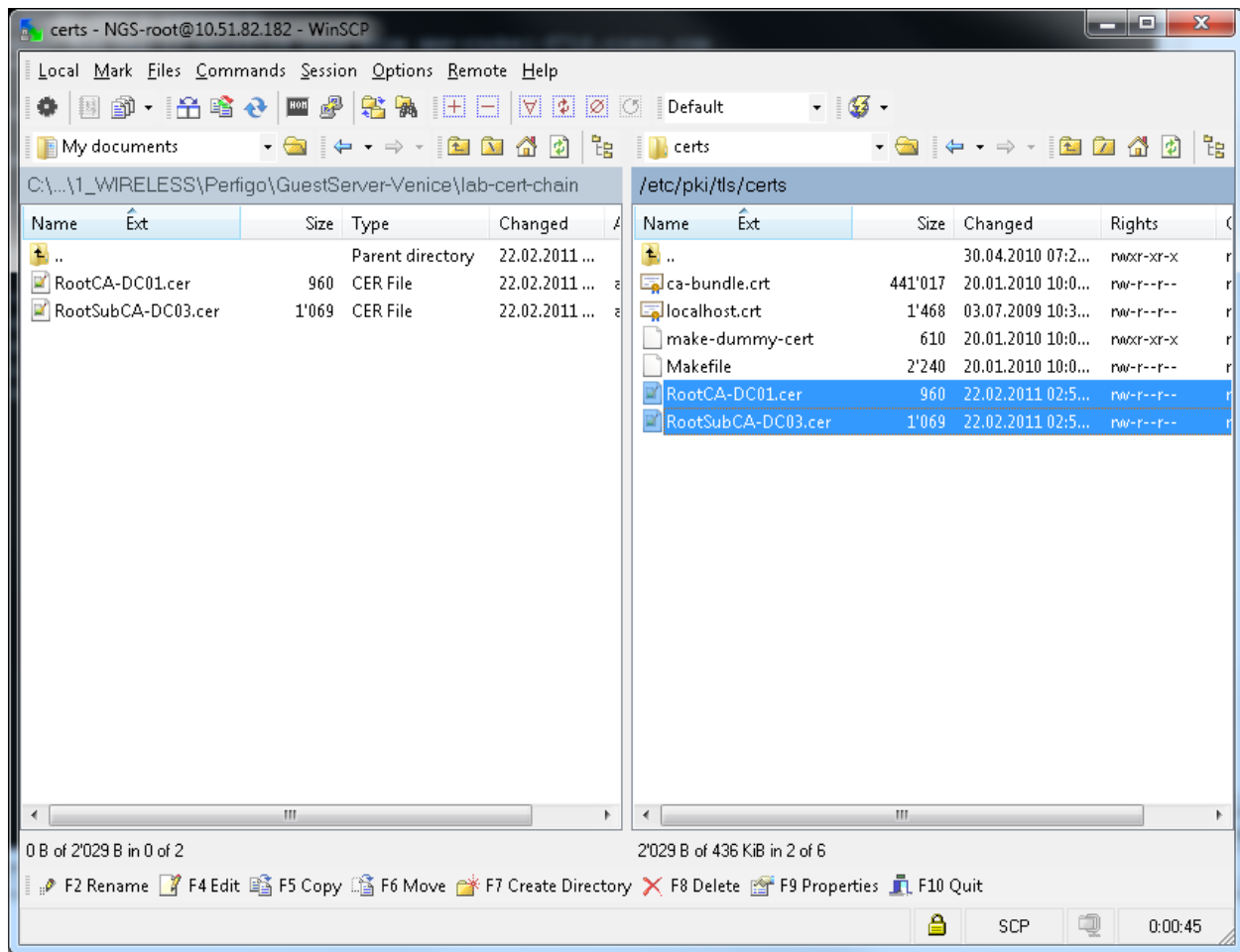
=> RootCA-DC01.cer

3.) Create server certificate chain

A cert is in PEM format if it contains the text "-----BEGIN CERTIFICATE-----". If the file is in binary (DER) format it can be converted to PEM using:

```
openssl x509 -in cert.der -inform DER -out cert.pem -outform PEM
```

- 1.) Using sftp or scp upload the intermediate and root certs to /etc/pki/tls/certs.



Since we did get all the certificate from DC01 and DC03 – convert it to PEM.

```
openssl x509 -in RootCA-DC01.cer -inform DER -out root.pem -outform PEM
openssl x509 -in RootSubCA-DC03.cer -inform DER -out intermediate.pem -outform PEM
```

2.)In a root shell:

```
cd /etc/pki/tls/certs
chmod 666 *.pem
cp intermediate.pem localhost.chain.crt
cat root.pem >> localhost.chain.crt
```

e.g

```
[root@chtac-guest-01 certs]# ls -al
total 488
drwxr-xr-x 2 root root 4096 Sep 13 01:42 .
drwxr-xr-x 5 root root 4096 Apr 30 07:25 ..
```

```
-rw-r--r-- 1 root root 441017 Jan 20 2010 ca-bundle.crt
-rw-rw-rw- 1 root root 1505 Sep 13 01:42 intermediate.pem
-rw-r--r-- 1 root root 2859 Sep 13 01:42 localhost.chain.crt
-rw-r--r-- 1 root root 1468 Jul 3 2009 localhost.crt
-rwxr-xr-x 1 root root 610 Jan 20 2010 make-dummy-cert
-rw-r--r-- 1 root root 2240 Jan 20 2010 Makefile
-rw-r--r-- 1 root root 960 Feb 22 2011 RootCA-DC01.cer
-rw-rw-rw- 1 root root 1354 Sep 13 01:42 root.pem
-rw-r--r-- 1 root root 1069 Feb 22 2011 RootSubCA-DC03.cer
[root@chtac-guest-01 certs]#
```

3.) Edit /etc/httpd/conf.d/ssl.conf – e.g use VI

```
Find the line starting:#SSLCertificateChainFile
Uncomment the line and change it to read:
SSLCertificateChainFile /etc/pki/tls/certs/localhost.chain.crt
```

4.) In the admin interface upload the server cert ("Upload this Server's SSL Certificate")

on Server -> SSL Settings).

The screenshot shows the Cisco NAC Guest Server Administration interface. The left sidebar contains a navigation menu with the following items: Authentication, Guest Policy, Devices, User Interface, Hotspot, and Server. The Server menu is expanded, showing sub-items: Network Settings, Date/Time Settings, Access Restrictions, SSL Settings (highlighted), Backup, System Logs, Licensing, Replication Settings, and SNMP. The main content area is titled "SSL Settings" and features a green checkmark icon with the text "CSR Created". Below this, there are three sections: "HTTPS and HTTP" with radio buttons for "Allow Only HTTPS", "Allow Only HTTP", "Allow HTTPS and HTTP" (selected), and "Allow Only HTTPS (with HTTP Redirected to HTTPS)", along with "Save Settings" and "Cancel" buttons; "Certificate Signing Request" with links for "Create CSR", "Create Temporary Certificate from CSR", and "Download CSR", and a "Reboot Server" button; and "Download Certificate" with a link for "Download Current SSL Certificate". At the bottom, the "Upload Certificates" section includes two "Browse..." buttons for uploading the server's SSL certificate and a root CA certificate, and "Upload" and "Cancel" buttons.

The notification box is titled "SSL Settings" and contains a green checkmark icon followed by the text "Server SSL Certificate Uploaded" and "You must reboot the server to use the new Certificate".

5.)Recreate the cert structure and reboot server:

```
c_rehash  
reboot
```

e.g

```
[root@htac-guest-01 conf.d]# c_rehash
```

```
Doing /etc/pki/tls/certs
root.pem => d391afe4.0
intermediate.pem => 9d6f598b.0
```

```
s_ [root@htac-guest-01 conf.d]# reboot
Broadcast message from root (pts/0) (Mon Sep 13 21:24:36 2010):
The system is going down for reboot NOW!
[root@htac-guest-01 conf.d]#
```

Test login with client and verify certificate chain

From another machine running openssl you can test using:

```
openssl s_client -connect x.x.x.x:443 -showcerts
```

This will list all certificates that would be supplied to a client.
Replace x.x.x.x with the NGS IP address.

```
[root@htac-profiler-02 ~]# openssl s_client -connect 10.51.82.182:443 -showcerts
CONNECTED(00000003)
depth=2 /DC=ch/DC=wlaaan/CN=DC01
verify error:num=19:self signed certificate in certificate chain
verify return:0
---
Certificate chain
0 s:/C=CH/ST=zh/L=zh/O=chtac/OU=tac/CN=chtac-guest-01.cca-htac.ch
i:/DC=ch/DC=wlaaan/DC=child1/CN=DC03
-----BEGIN CERTIFICATE-----
MIIEOzCCA6SgAwIBAgIKf8b8wAAAAAACjANBgkqhkiG9w0BAQUFADBTRiwEAYK
CZImiZPYLQGBGRYCY2gxFjAUBgoJkiaJk/lsZAEZFgZ3bGFhYW4xZjAUBgoJkiaJ
k/lsZAEZFgZjaGlzZDEwDTALBgNVBAMTBERTMDMwHhcNMTAwMjlyMDMzOTEwWhcN
MTAxMjE1MTAyNTAzWjBrMQswCQYDVQQGEwJDSDELMAkGA1UECBMCemgxZjAUBgNV
BACTAnpoMQ4wDAYDVQQKEwVjaHRhYzEMMAoGA1UECmMDdGFjMSQwIlgYDVQQDEExtj
aHRhYy1ndWVzdC0wMS5jY2EtY2h0YWMuY2gwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQQDvPBPIbutHvQZ/CS20D7Aw4JCLyVNrW847d+KumTR7v/TKqpAV
MiZoA4M1D2NyG9rebsa9DJTfqIH2fk2KKGF2g9aGFLIYkoqASnjWaGlbFm73aK2I
US4d6piykQv0GgvZ0esB0kFaPIHmx1oaXOnud/q5I6yCEykRruplKonuQIRRtYy7
dmQKbiWNz9/kBjX94NGnqDyhFETBltd90qU4rOafW4QXDHtdDvYxvJNSorBCZl/B
XmcuZfZNNZ+6PMteTiCOs2u1o/MK8KHdFiscvEkkj/FMfkHoxMB85ome1m+7prBa
mc2pZHLvpxmZ5ARbPYTvZFWQ73yLwrImGoA1AgMBAAGjggF4MIIbDAdBgNVHQ4E
FgQUMoUHGIj3jF70RNIP0MP9q3F7LswHwYDVR0jBBgwFoAUUvwLIKZBisSHyIdJA
OK98Gfx7QFEwdQYDVR0fBG4wbDBqoGigZoYwaHR0cDovL2RjMDMuY2hpbGQxLnds
YWFhbi5jaC9DZXJ0RW5yb2xsL0RDMDMuY3JshjJmaWxloI8vXFxEQzAzLmNoaWxk
MS53bGFhYW4uY2h0Y2VudEVucm9sbFxEQzAzLmNyYDcBvYkYkYBBQUHAQEgA0w
```

gaowUgYIKwYBBQUHMAKGRmh0dHA6Ly9kYzAzLmNoaWxkMS53bGFhYW4uY2gvQ2Vy
dEVucm9sbC9EQzAzLmNoaWxkMS53bGFhYW4uY2hfREMwMy5jcnQwVAYIKwYBBQUH
MAKGSZpbGU6Ly9cXERDMDMuY2hpbGQxLndsYWFhbi5jaF9EQzAzLmNydDANBgkqhkiG9w0BAQUFAAOBgQBQ
MDMuY2hpbGQxLndsYWFhbi5jaF9EQzAzLmNydDANBgkqhkiG9w0BAQUFAAOBgQBQ
9GmWeOLwxMVJKN6thyw8FvSfr3BToz8xsAkScsE4DKYpe0mdYNxiSkozBCHMBDA2
jQzcRedal2eUkdyqDgO6GBzvn8vt7S1rNYnITURXBqTk9Z/k0woVi5spM4HC2O6g
l1qfm1jP6YtMNFfMHlcDuvN8bthdlchTPrk+Da9wg==
-----END CERTIFICATE-----

1 s:/DC=ch/DC=wlaaan/DC=child1/CN=DC03
i:/DC=ch/DC=wlaaan/CN=DC01

-----BEGIN CERTIFICATE-----
MIIKTCCAxGgAwIBAgIKe25meAAAAAADTANBgkqhkiG9w0BAQUFADA7MRIwEAYK
CZImiZPYLGBGRYCY2gxFjAUBgoJkiaJk/IsZAEZFgZ3bGFhYW4xDTALBgNVBAMT
BERDMDEwHhcNMDkxMjE1MTAxNTAzWhcnMTAxMjE1MTAyNTAzWjBTMRIwEAYKCYIm
iZPYLGBGRYCY2gxFjAUBgoJkiaJk/IsZAEZFgZ3bGFhYW4xDTALBgNVBAMTBERDM
ZAEZFgZjaGlzZDEwDTALBgNVBAMTBERDMDEwZ8wDQYJKoZIhvcNAQEBBQADgYOA
MIGJAoGBAL79kZKjuVMBT1O9TqWfVAOngVasFvHV+/hjStCanoUCEG1XpmYMIV5S
fO6oL4zpeviYp+PXOb3xfNon6L+2UwVjYkv1WrMJAp1UGmFEEeb8O07XP3p40qb
N00e6liddWvcb4d0Hpdqs5OouiU5pV+ZIAelmqC+q78RCaSbf2jc1AgMBAAGjggGZ
MIIIBITAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBS/AsgpkGKxIfh0kA4r3wZ
/HtAUTALBgNVHQ8EBAMCAYYwEAYJKwYBBAGCNxUBBAMCAQAwGQYJKwYBBAGCNxQC
BAweCgBTAHUAYgBDAEEwHwYDVR0jBBgwFoAUYOlg1AeZjhN2KQ9ZV15CUJrNkuAw
ZwYDVR0fBGAwXjBcoFqgWlYpaHR0cDovL2RjMDEud2xhYW5uLmNoL0NlcnRFbnJv
bGwvREMwMS5jcmYgK2ZpbGU6Ly9cXERDMDEud2xhYW5uLmNoXENlcnRFbnJvbGxw
REMwMS5jcmwZ4GCCsGAQUFBwEBBIBGRMIGOMEQGCCsGAQUFBzACHjodHRwOi8v
ZGMwMS53bGFhYW4uY2gvQ2VydEVucm9sbC9EQzAxLndsYWFhbi5jaF9EQzAxLmNy
dDBGBggrBgEFBQcwAoY6ZmlsZTovL1xcREMwMS53bGFhYW4uY2hcQ2VydEVucm9s
bFxEQzAxLndsYWFhbi5jaF9EQzAxLmNydDANBgkqhkiG9w0BAQUFAAOCAQEAIMOC
bXM3tg/NVpPDnIRvKpoiKAvPrciCkuCQeis6uOA2Z73qTVA11V5OkH8sD08SG5d9
UrZkry5XE7DqpalVHsL0Ades3SQhnQnXqEP1AJj6KUuDFg6UvRdp1xv8k5KpuPkc
ywL1gWfIc9j/rjmsU9FMkWNTqAMxNj0Kn4XBoTPCQZEs7x0nKCFQF2NzdV9uBzaJ
Yi0txJXlfZywJfO72k8JDBmDaO0xw/vHSN9yb2FSjBJTMAHGWMkK0I5nH4WQJ/q
suEzf912ly3fWr1LkP8J/kv15bnDAcwPDUkHZhpmFJdTbVNpLlIkvoH5r8DyCrV
Es57uTtt+AlktiRQQ==
-----END CERTIFICATE-----

2 s:/DC=ch/DC=wlaaan/CN=DC01
i:/DC=ch/DC=wlaaan/CN=DC01

-----BEGIN CERTIFICATE-----
MIIIDvDCCAqSgAwIBAgIQb16ZPgiJHI5G0ra5Jn9DXTANBgkqhkiG9w0BAQUFADA7
MRIwEAYKCYImiZPYLGBGRYCY2gxFjAUBgoJkiaJk/IsZAEZFgZ3bGFhYW4xDTAL
BgNVBAMTBERDMDEwHhcNMDkxMjE1MTAxNTAzWhcnMTAxMjE1MTAyNTAzWjBTMRIw
EAYKCYImiZPYLGBGRYCY2gxFjAUBgoJkiaJk/IsZAEZFgZ3bGFhYW4xDTALBgNV
BAMTBERDMDEwZ8wDQYJKoZIhvcNAQEBBQADgYOAQwGQYJKwYBBAGCNxUBBAMCAQAw
wfOtlRqTwQdvq/rAUvzGg+UORrcKO7BzRBz/sP2E8fpEY6NtduoouJZVCG5W+8NA
PLSEdoAmpaLESjbe0dEE93f5YJajfV3wlelzsCRTR8tqYEVrgsC0t9TbATCYCSFr
png/aFkls+4OTUaxvKgZSI10x+ypz3Zri5ikQtZ2i1HUaXmw+tUjMHsgqDzDermB
x2F1x3WtGJq832Rk72hdzsjw130+9bexXJGTVHLVrr3v7LOu2HSyrOgqXJCWwgwz
MVPBVfvBu7WxvmXH/WT1nKFFn/74dCkhtgf7yQM+fM+kk91e0pboGksj09ztY6Hh

```
XldYhaWZMBmrAgMBAAGjbswgbgwCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQFMAMB
Af8wHQYDVR0OBBYEFGDiiNQHM4TdikPWVdeQICazZLgMGcGA1UdHwRgMF4wXKBa
oFiGKWh0dHA6Ly9kYzAxLndsYWZhbi5jaC9DZXJ0RW5yb2xsL0RDMDEuY3Jshitm
aWxIOi8vXFxEQzAxLndsYWZhbi5jaFxDZXJ0RW5yb2xsXERDMDEuY3JsbGAGCSsG
AQQBgjcVAQQDAgEAMA0GCSqGSIB3DQEBBQUAA4IBAQAz6nn/KKzen1QJEXE3vJV/
4x7ykrRBpzZVGd6Y04eSammbjgxpqUe9bKbewHwW4rJXzcSkYlvS2uXqF72GU8ly
QkY8vPXoMV9vA7I8+IlykPwubdm6AFdV44+SOR469CQx5WVgbMOdWvswpQO/SDX1
cZC45QO7mp5EqT4YxgqvoophPhZvpX+xsR/9oYzquB23lqJsaeqxBsktLZ0+hRt7
5eWi9vbCTHSR8TfIEKmPiv0scQTrs15Eq+GXmX3D4TtkE69pKxst+8/BLHv7Ow/
mG5WG7b/5VVXrMY7IOSM365977eAB3gAcjrxNJXlnUxocA1K9yClwARCBYivu94
-----END CERTIFICATE-----
```

Server certificate

```
subject=/C=CH/ST=zh/L=zh/O=chtac/OU=tac/CN=chtac-guest-01.cca-chtac.ch
issuer=/DC=ch/DC=wlaaan/DC=child1/CN=DC03
```

No client certificate CA names sent

SSL handshake has read 3814 bytes and written 334 bytes

New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA

Server public key is 2048 bit

Compression: NONE

Expansion: NONE

SSL-Session:

```
Protocol : TLSv1
Cipher   : DHE-RSA-AES256-SHA
Session-ID: CC199168FE8774E32A24FAB644D9B1C050A34E4C3DC7EA4688FA1D19713B67E5
Session-ID-ctx:
Master-Key:
4D373D55E036C9836387DF14ED6B7B177EDB8E71C10595EE168EF0ADB582109C56877B2E6684C94847
05B8E6BD884417
Key-Arg  : None
Start Time: 1298372073
Timeout  : 300 (sec)
Verify return code: 19 (self signed certificate in certificate chain)
```

Or directly from NGS CLI:>

```
openssl s_client -connect localhost:443 -state -debug
```

```
.....
read from 0x95bfe90 [0x95c543d] (48 bytes => 48 (0x30))
0000 - 7a 5e f4 a5 45 68 ad 84-46 a8 af ab bd 30 42 69  z^..Eh..F....0Bi
0010 - d5 a6 be 4e 22 82 2b 22-c4 d2 be f8 0f d7 a0 a2  ...N".+".....
0020 - f2 5b 53 57 24 39 39 21-f4 77 58 50 3d 9b d4 64  .[SW$99!.wXP=..d
```

SSL_connect:SSLv3 read finished A

Certificate chain

0 s:/C=CH/ST=zh/L=zh/O=chtac/OU=tac/CN=chtac-guest-01.cca-chtac.ch
i:/DC=ch/DC=wlaaan/DC=child1/CN=DC03
1 s:/DC=ch/DC=wlaaan/DC=child1/CN=DC03
i:/DC=ch/DC=wlaaan/CN=DC01
2 s:/DC=ch/DC=wlaaan/CN=DC01
i:/DC=ch/DC=wlaaan/CN=DC01

Server certificate

-----BEGIN CERTIFICATE-----

```
MIIEOzCCA6SgAwIBAgIKIf8b8wAAAAAACjANBgkqhkiG9w0BAQUFADBTMRIwEAYK
CZImiZPyLQBGRYCY2gxFjAUBgoJkiaJk/lsZAEZFgZ3bGFhYW4xZjAUBgoJkiaJ
k/lsZAEZFgZjaGlzZDExDTALBgNVBAMTBERTMDMwHhcNMTAwMjlyMDMzOTE0WhcN
MTAxMjE1MTAyNTAzWjBrMQswCQYDVQQGEwJDSDELMAkGA1UECBMCemgxZjAUBgNV
BACTAnpoMQ4wDAYDVQQKEwVjaHRhYzEMMAoGA1UECXMdZGFjMSQwYjYDVQQDExtj
aHRhYy1ndWVzdC0wMMSjY2EtY2h0YWMuY2gwgEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQDvPBPIbutHvQZ/CS20D7Aw4JCLyVNrw847d+KumTR7v/TKqpAV
MiZoA4M1D2NyG9rebsa9DJTfqIH2fk2KKGf2g9aGFLIYkoqASnjWaGlbFm73aK2I
US4d6piykQv0GgvZ0esB0kFaPIHMx1oaXOnud/q5I6yCEyKRruplKonuQIRRtYy7
dmQkblWNz9/kBjX94NGnqDyhFETBltd90qU4rOafW4QXDHtDdVyxvJNSorBCZl/B
XmcuZfZNNZ+6PMeTiLCOs2u1o/MK8KHdFIScVekKj/FMfkHoxMB85ome1m+7prBa
mc2pZHLvpxmZ5ARbPYTvZFWQ73yLwrimGoA1AgMBAAGjggF4MIIBDAdBgNVHQ4E
FgQUMoUHGidJ3jF70RNIP0MP9q3F7LswHwYDVR0jBBgwFoAUUvwLIKZBisSHyldJA
OK98Gfx7QFEwdQYDVR0fBG4wbDBqoGigZoYwaHR0cDovL2RjMDMuY2hpbGQxLnds
YWFhbi5jaC9DZXJ0RW5yb2xsL0RDMDMuY2hpbGQxLndsYWFhbi5jaF9EQzAzLmNoaWxk
MS53bGFhYW4uY2hcQ2VydEVucm9sbFxEQzAzLmNybDcBugYIKwYBBQUHAQEEdga0w
gaowUgYIKwYBBQUHMAKGRmh0dHA6Ly9kYzAzLmNoaWxkMS53bGFhYW4uY2gV2VydEVucm9sbC9EQzAzLmNoaWxkMS53bGFhYW4uY2hfREMwMy5jcnQwVAYIKwYBBQUH
MAKGSZGZpbGU6Ly9cXERDMDMuY2hpbGQxLndsYWFhbi5jaF9EQzAzLmNydDANBgkqhkiG9w0BAQUFAAOBgQBQ
9GmWeOLwxMVJKN6thyw8FvSfr3BToz8xsAkScsE4DKYpe0mdYNxiSkozBCHMBDA2
jQzcRedal2eUkdyqDgO6GBzvn8vt7S1rNYnITURXBqTk9Z/k0woVi5spM4HC2O6g
l1qfm1jP6YtMNFfMHlcDuvN8bthdlchTPIrk+Da9wg==
```

-----END CERTIFICATE-----

subject=/C=CH/ST=zh/L=zh/O=chtac/OU=tac/CN=chtac-guest-01.cca-chtac.ch
issuer=/DC=ch/DC=wlaaan/DC=child1/CN=DC03

Now on the client workstation you can validate using sniffer trace (wireshark)

The image shows a Wireshark capture of a TLS handshake. The packet list pane shows the following packets:

No.	Time	Source	Destination	Protocol	Info
20	2011-02-22 12:06:30.372156	10.55.142.138	10.51.82.182	TLSv1	Client Hello
21	2011-02-22 12:06:30.428548	10.51.82.182	10.55.142.138	TCP	https > 53861 [ACK] seq=1 Ack=121 win=5888 Len=0
22	2011-02-22 12:06:30.446233	10.51.82.182	10.55.142.138	TLSv1	Server Hello
23	2011-02-22 12:06:30.446943	10.51.82.182	10.55.142.138	TCP	[TCP segment of a reassembled PDU]
24	2011-02-22 12:06:30.446993	10.55.142.138	10.51.82.182	TCP	53861 > https [ACK] Seq=121 Ack=2521 win=66780 Len=0
25	2011-02-22 12:06:30.490753	10.51.82.182	10.55.142.138	TLSv1	Certificate, Server Key Exchange, Server Hello Done
40	2011-02-22 12:06:30.700350	10.55.142.138	10.51.82.182	TCP	53861 > https [ACK] Seq=121 Ack=1756 win=65544 Len=0

The packet details pane for packet 25 shows the following structure:

- Frame 25: 1289 bytes on wire (10312 bits), 1289 bytes captured (10312 bits) on interface 11
- Ethernet II, Src: Cisco_19:29:70 (00:1e:4a:19:29:70), Dst: Usf_69:b5:0d (00:17:13:69:b5:0d)
- Internet Protocol, Src: 10.51.82.182 (10.51.82.182), Dst: 10.55.142.138 (10.55.142.138)
- Transmission Control Protocol, Src Port: https (443), Dst Port: https (53861), Seq: 2521, Ack: 121, Len: 1235
- [Reassembled TCP segments (3676 bytes): #22(118L), #23(1260), #25(1235)]
- Secure Socket Layer
 - TLSv1 Record Layer: Handshake Protocol: Certificate
 - Content Type: Handshake (12)
 - Version: TLS 1.0 (0x0301)
 - Length: 3132
 - Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 3128
 - Certificates Length: 3125
 - Certificates (3125 bytes)
 - Certificate Length: 1087
 - Certificate (1d-at-commonname=cttac-guest-01.cca-cttac.ch, 1d-at-organizationalunitname=tac, 1d-at-organizationname=cttac, 1d-at-localityname=zh, 1d-at-countryname=ch)
 - Certificate Length: 1069
 - Certificate (1d-at-commonname=dc01.dc=ch1d1, dc=wlaaan, dc=ch)
 - Certificate Length: 950
 - Certificate (1d-at-commonname=dc01.dc=wlaaan, dc=ch)
 - TLSv1 Record Layer: Handshake Protocol: Server Key Exchange
 - Content Type: Handshake (12)
 - Version: TLS 1.0 (0x0301)
 - Length: 525
 - Handshake Protocol: Server Key Exchange
 - Handshake Type: Server Key Exchange (12)
 - Length: 521
 - TLSv1 Record Layer: Handshake Protocol: Server Hello Done
 - Content Type: Handshake (12)
 - Version: TLS 1.0 (0x0301)
 - Length: 4
 - Handshake Protocol: Server Hello Done

The packet bytes pane shows the raw data of the certificate, including the 'Certificate' field.

Note: certificate for DC01 / DC03 and cttac-guest-01.cca-cttac.ch