

TECH NOTE 003

# Self Signed Certificates

X.509 Certificate Creation Using Easy-Rsa with OpenVPN



## AIM

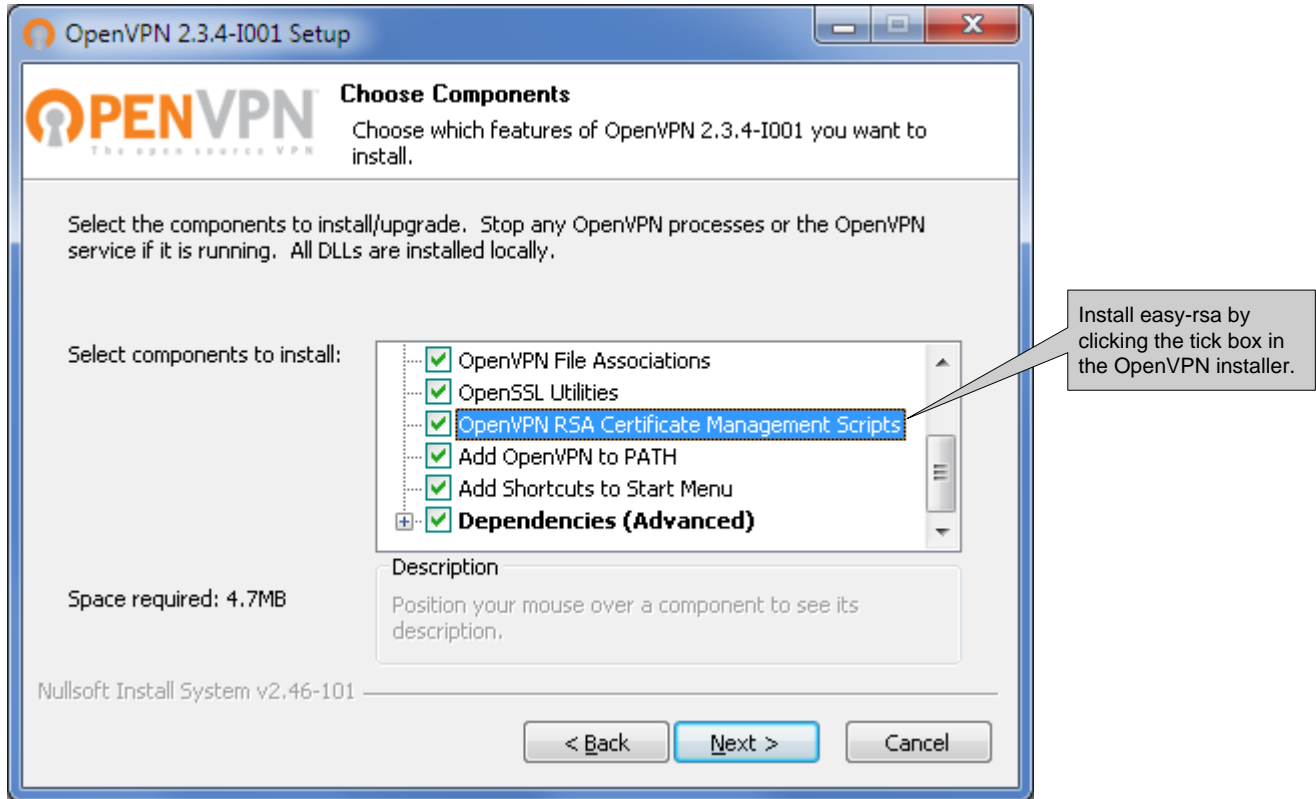
This Tech Note will show how to create X.509 certificates with easy-rsa in OpenVPN for MS Windows.

The certificates can be used to authenticate VPN tunnel end-points for both SSL and IPSec tunnels.

All examples in this note are made using MS Windows 7 Professional with Service Pack 1 and OpenVPN for MS Windows version 2.3.4-I001.

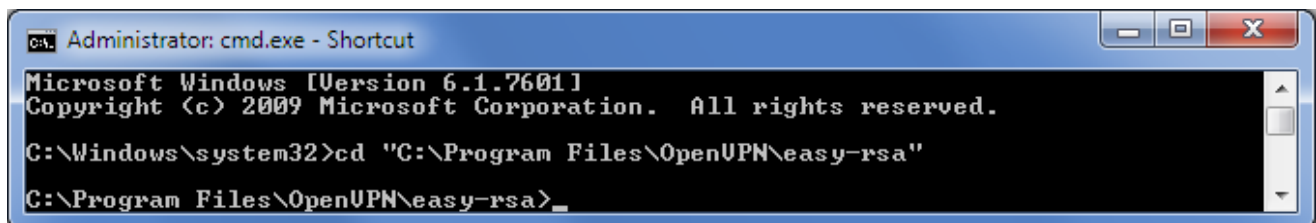
## Build Certificates with Easy-rsa

1. Make sure *easy-rsa* is installed with OpenVPN.

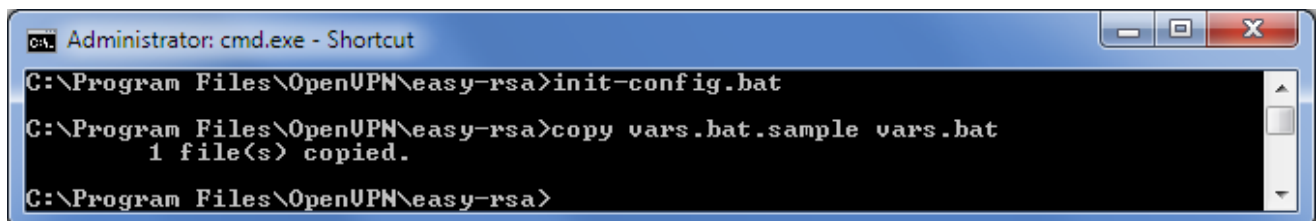


2. Use MS Windows Command Prompt to go to the *easy-rsa* folder. Default path is C:\Program Files\OpenVPN\easy-rsa.

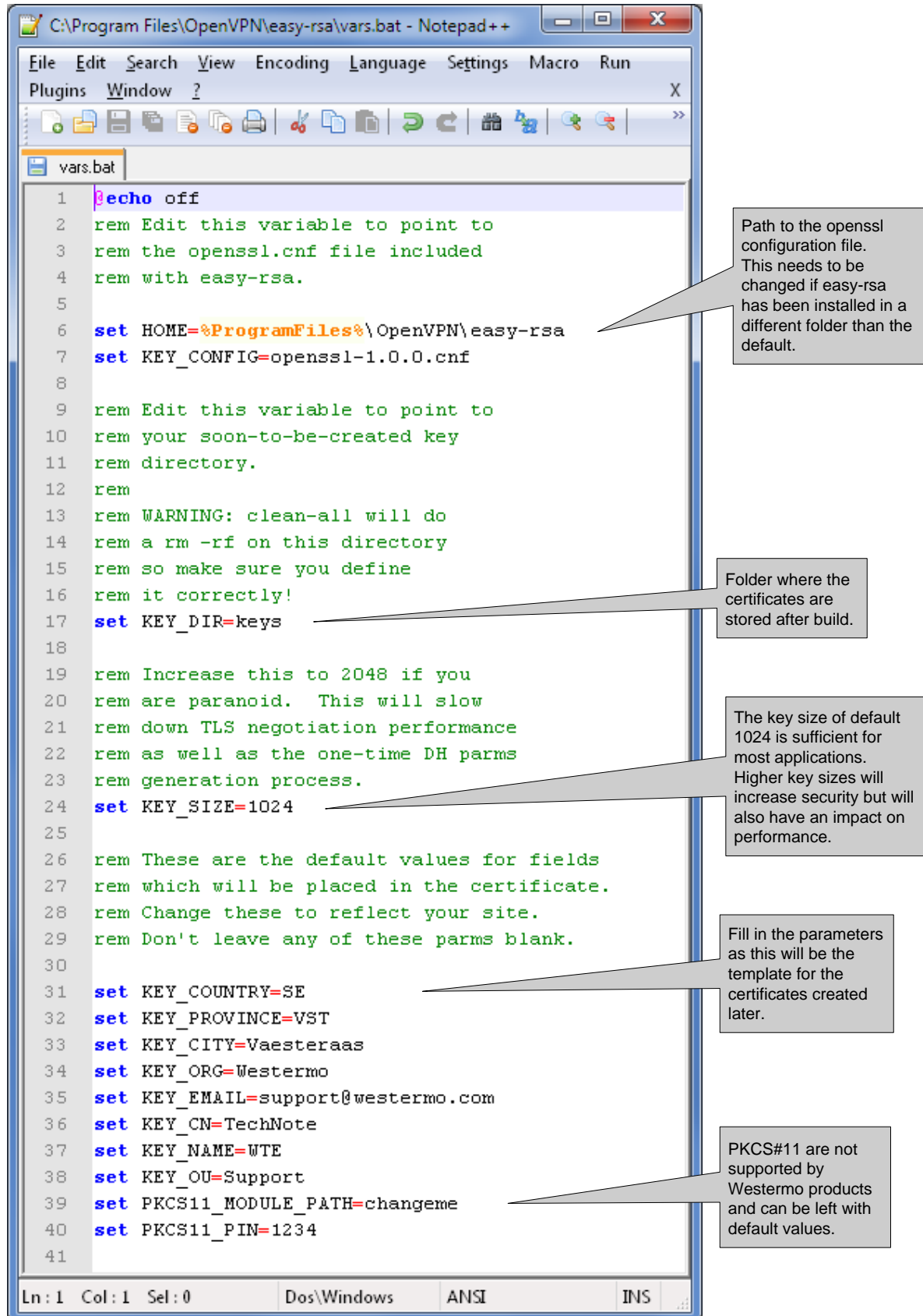
**Please Note! On MS Windows systems from Vista and onwards *easy-rsa* will have to be run with administrator rights.**



3. Start by running the *init-config.bat* script, this will copy configuration files into place (this will overwrite any preexisting *vars.bat* and *openssl.cnf* files).



4. Edit the *vars.bat* file with a text editor like Notepad++ with administrator rights or directly from the MS Windows Command Prompt if the MS-DOS command *edit* is installed.



```

1  echo off
2  rem Edit this variable to point to
3  rem the openssl.cnf file included
4  rem with easy-rsa.
5
6  set HOME=%ProgramFiles%\OpenVPN\easy-rsa
7  set KEY_CONFIG=openssl-1.0.0.cnf
8
9  rem Edit this variable to point to
10 rem your soon-to-be-created key
11 rem directory.
12 rem
13 rem WARNING: clean-all will do
14 rem a rm -rf on this directory
15 rem so make sure you define
16 rem it correctly!
17 set KEY_DIR=keys
18
19 rem Increase this to 2048 if you
20 rem are paranoid. This will slow
21 rem down TLS negotiation performance
22 rem as well as the one-time DH parms
23 rem generation process.
24 set KEY_SIZE=1024
25
26 rem These are the default values for fields
27 rem which will be placed in the certificate.
28 rem Change these to reflect your site.
29 rem Don't leave any of these parms blank.
30
31 set KEY_COUNTRY=SE
32 set KEY_PROVINCE=VST
33 set KEY_CITY=Vaesteraas
34 set KEY_ORG=Westermo
35 set KEY_EMAIL=support@westermo.com
36 set KEY_CN=TechNote
37 set KEY_NAME=WTE
38 set KEY_OU=Support
39 set PKCS11_MODULE_PATH=changeme
40 set PKCS11_PIN=1234
41
    
```

Path to the openssl configuration file. This needs to be changed if easy-rsa has been installed in a different folder than the default.

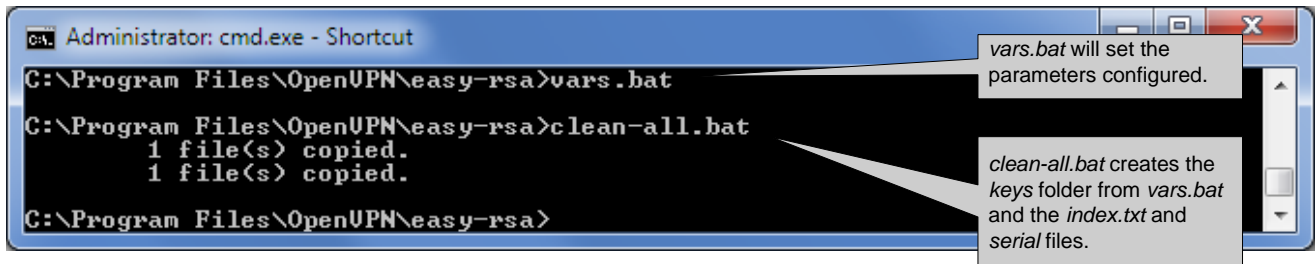
Folder where the certificates are stored after build.

The key size of default 1024 is sufficient for most applications. Higher key sizes will increase security but will also have an impact on performance.

Fill in the parameters as this will be the template for the certificates created later.

PKCS#11 are not supported by Westermo products and can be left with default values.

5. Run the *vars.bat* and *clean-all.bat* scripts to create the keys folder and the database files.

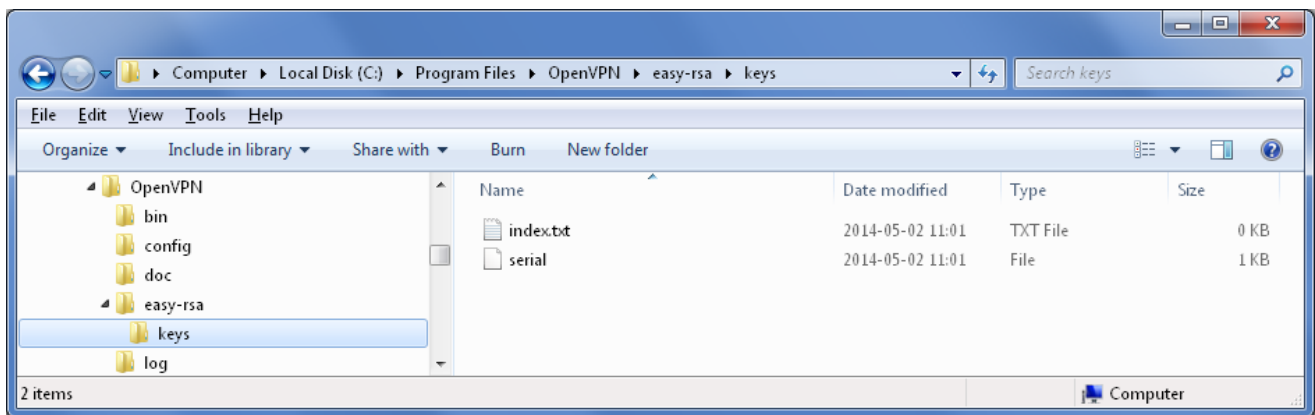


```
Administrator: cmd.exe - Shortcut
C:\Program Files\OpenVPN\easy-rsa>vars.bat
C:\Program Files\OpenVPN\easy-rsa>clean-all.bat
    1 file(s) copied.
    1 file(s) copied.
C:\Program Files\OpenVPN\easy-rsa>
```

*vars.bat* will set the parameters configured.

*clean-all.bat* creates the keys folder from *vars.bat* and the *index.txt* and *serial* files.

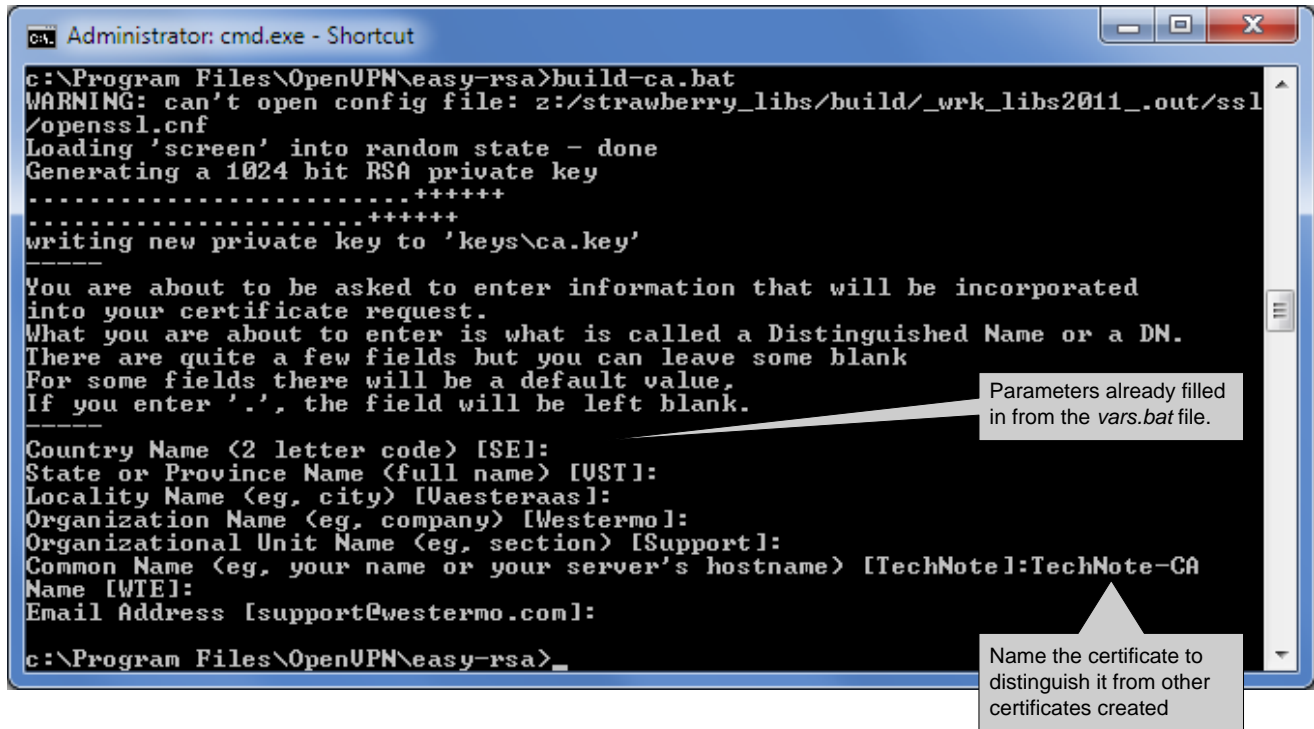
The following files should now be present in the KEY\_DIR folder (keys) as specified in *vars.bat*.  
*index.txt*  
*serial*



6. Now certificates can be generated.

Start by building the Certificate Authority (CA-certificate) which can create and sign client certificates and thereby authenticate connecting units.

Run the *build-ca.bat* script to build the CA-certificate.



```

Administrator: cmd.exe - Shortcut
c:\Program Files\OpenVPN\easy-rsa>build-ca.bat
WARNING: can't open config file: z:/strawberry_libs/build/_wrk_libs2011_.out/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'keys\ca.key'

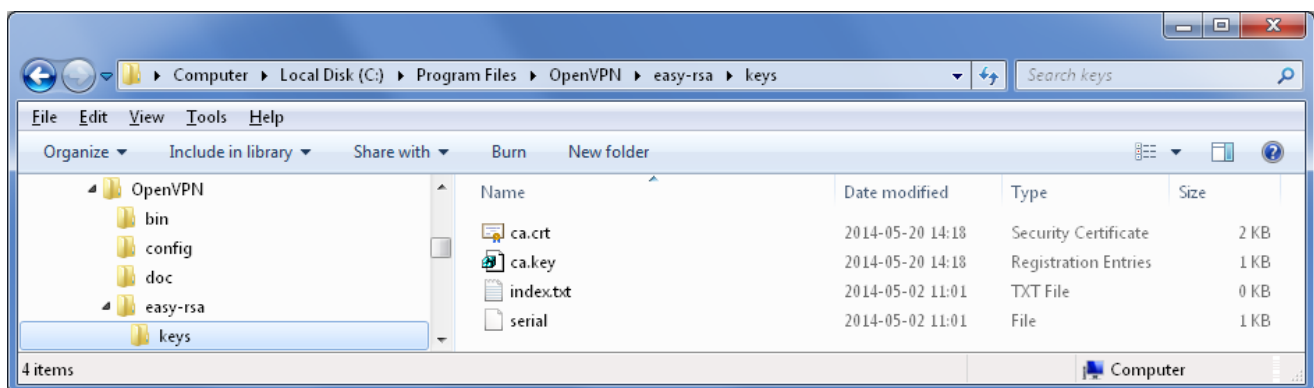
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [SE]:
State or Province Name (full name) [UT]:
Locality Name (eg, city) [Aesteraas]:
Organization Name (eg, company) [Westermo]:
Organizational Unit Name (eg, section) [Support]:
Common Name (eg, your name or your server's hostname) [TechNote-TechNote-CA
Name [WTE]:
Email Address [support@westermo.com]:
c:\Program Files\OpenVPN\easy-rsa>_
    
```

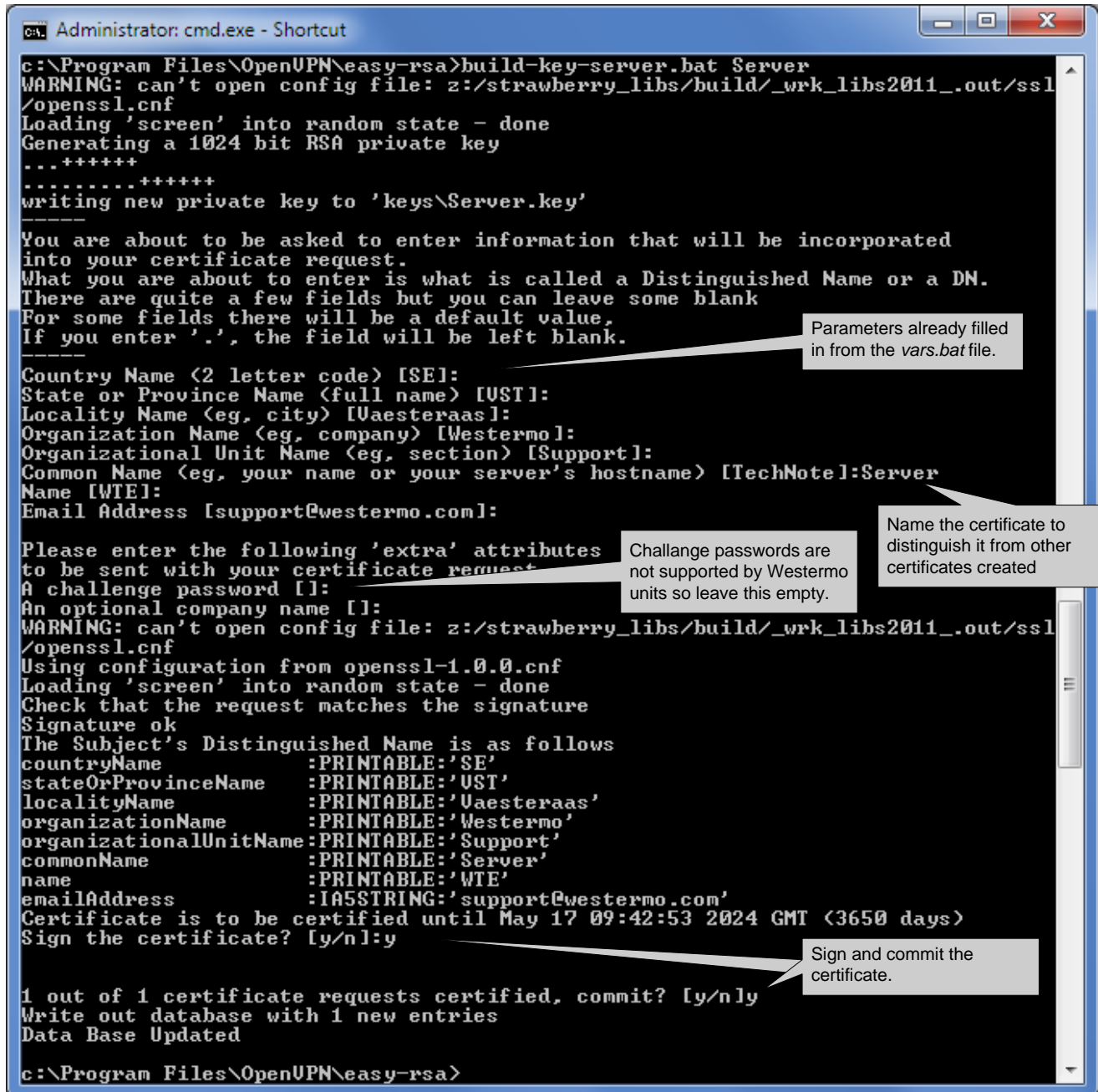
The following files should now be generated in the KEY\_DIR folder.

*ca.crt*

*ca.key*



7. Next build the server certificate by running the *build-key-server.bat* <server certificate file name> script.



```

Administrator: cmd.exe - Shortcut
c:\Program Files\OpenUPN\easy-rsa>build-key-server.bat Server
WARNING: can't open config file: z:/strawberry_libs/build/_wrk_libs2011_.out/ssl
/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
...+++++
.....+++++
writing new private key to 'keys\Server.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) [SE]:
State or Province Name (full name) [UST]:
Locality Name (eg, city) [Vaesteraas]:
Organization Name (eg, company) [Westermo]:
Organizational Unit Name (eg, section) [Support]:
Common Name (eg, your name or your server's hostname) [TechNote:Server
Name [WTE]:
Email Address [support@westermo.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: z:/strawberry_libs/build/_wrk_libs2011_.out/ssl
/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'SE'
stateOrProvinceName     :PRINTABLE:'UST'
localityName            :PRINTABLE:'Vaesteraas'
organizationName       :PRINTABLE:'Westermo'
organizationalUnitName  :PRINTABLE:'Support'
commonName              :PRINTABLE:'Server'
name                   :PRINTABLE:'WTE'
emailAddress            :IA5STRING:'support@westermo.com'
Certificate is to be certified until May 17 09:42:53 2024 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

c:\Program Files\OpenUPN\easy-rsa>
    
```

Parameters already filled in from the vars.bat file.

Challenge passwords are not supported by Westermo units so leave this empty.

Name the certificate to distinguish it from other certificates created

Sign and commit the certificate.

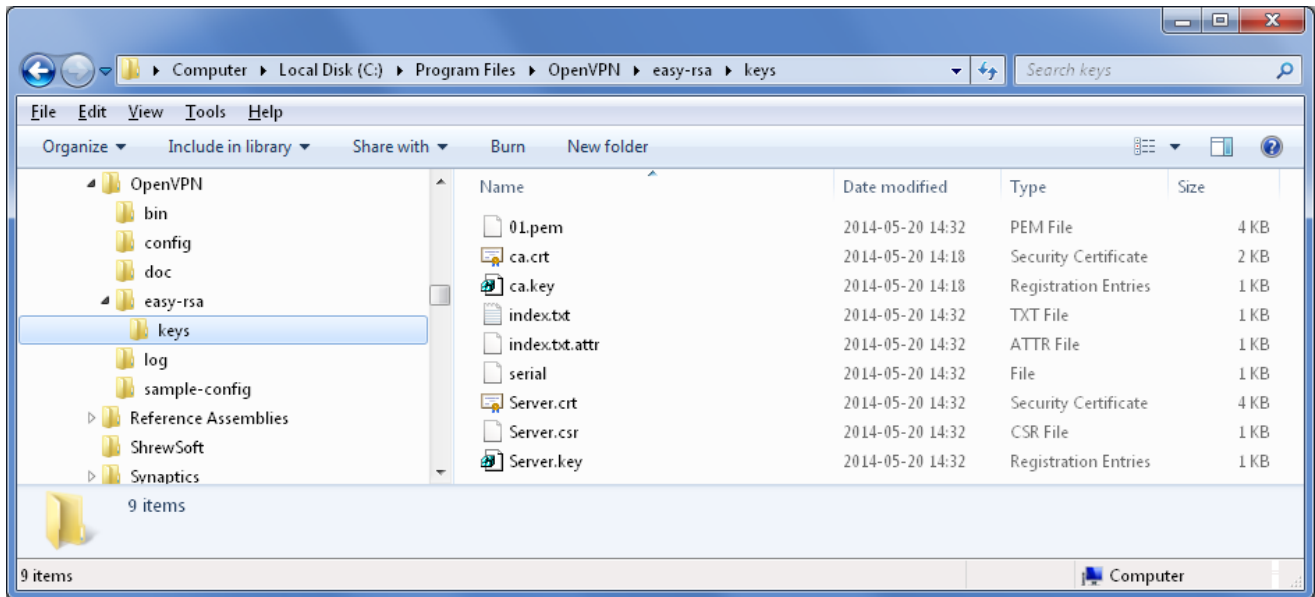
The following files should now be generated in the KEY\_DIR folder.

*01.pem*

*Server.crt*

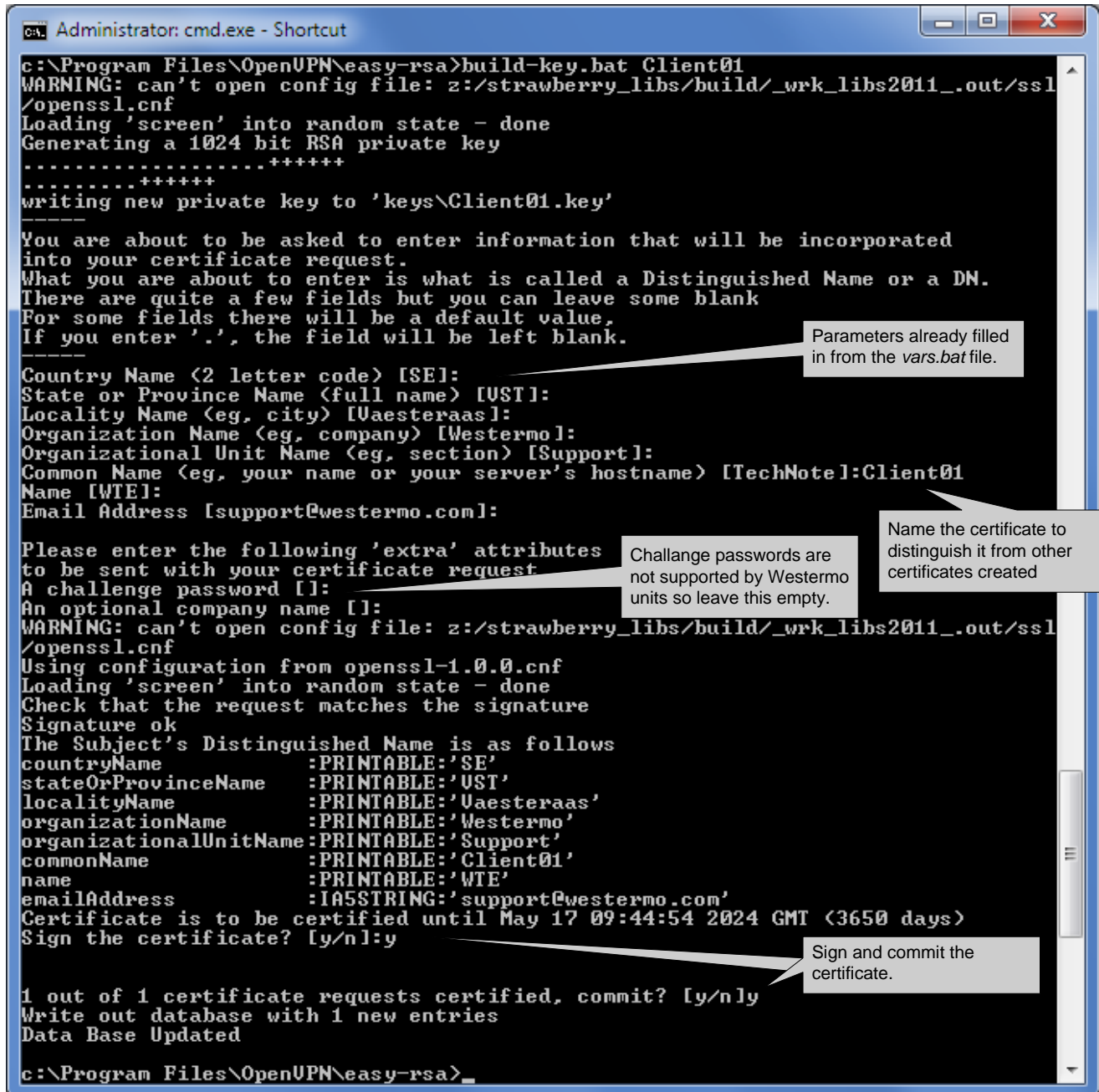
*Server.csr*

*Server.key*





6. Build client certificate/certificates by running the *build-key.bat* <client certificate file name> script.



```

Administrator: cmd.exe - Shortcut
c:\Program Files\OpenUPN\easy-rsa>build-key.bat Client01
WARNING: can't open config file: z:/strawberry_libs/build/_wrk_libs2011_.out/ssl
/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'keys\Client01.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) [SE]:
State or Province Name (full name) [UST]:
Locality Name (eg, city) [Vaesteraas]:
Organization Name (eg, company) [Westermo]:
Organizational Unit Name (eg, section) [Support]:
Common Name (eg, your name or your server's hostname) [TechNote:Client01
Name [WTE]:
Email Address [support@westermo.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: z:/strawberry_libs/build/_wrk_libs2011_.out/ssl
/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'SE'
stateOrProvinceName     :PRINTABLE:'UST'
localityName            :PRINTABLE:'Vaesteraas'
organizationName        :PRINTABLE:'Westermo'
organizationalUnitName  :PRINTABLE:'Support'
commonName              :PRINTABLE:'Client01'
name                   :PRINTABLE:'WTE'
emailAddress            :IA5STRING:'support@westermo.com'
Certificate is to be certified until May 17 09:44:54 2024 GMT (3650 days)
Sign the certificate? [y/n]:y

-----
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

c:\Program Files\OpenUPN\easy-rsa>_
    
```

Parameters already filled in from the vars.bat file.

Challenge passwords are not supported by Westermo units so leave this empty.

Name the certificate to distinguish it from other certificates created

Sign and commit the certificate.

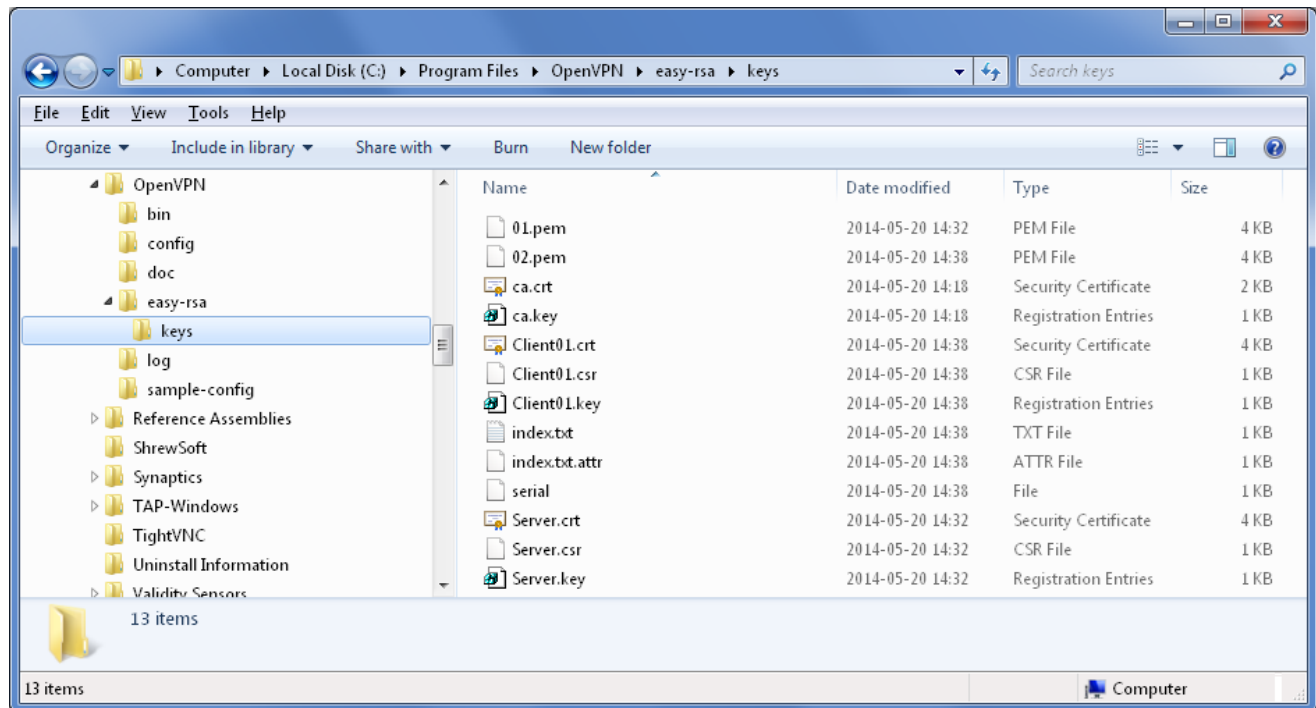
The following files should now be generated in the KEY\_DIR folder.

*02.pem*

*Client01.crt*

*Client01.csr*

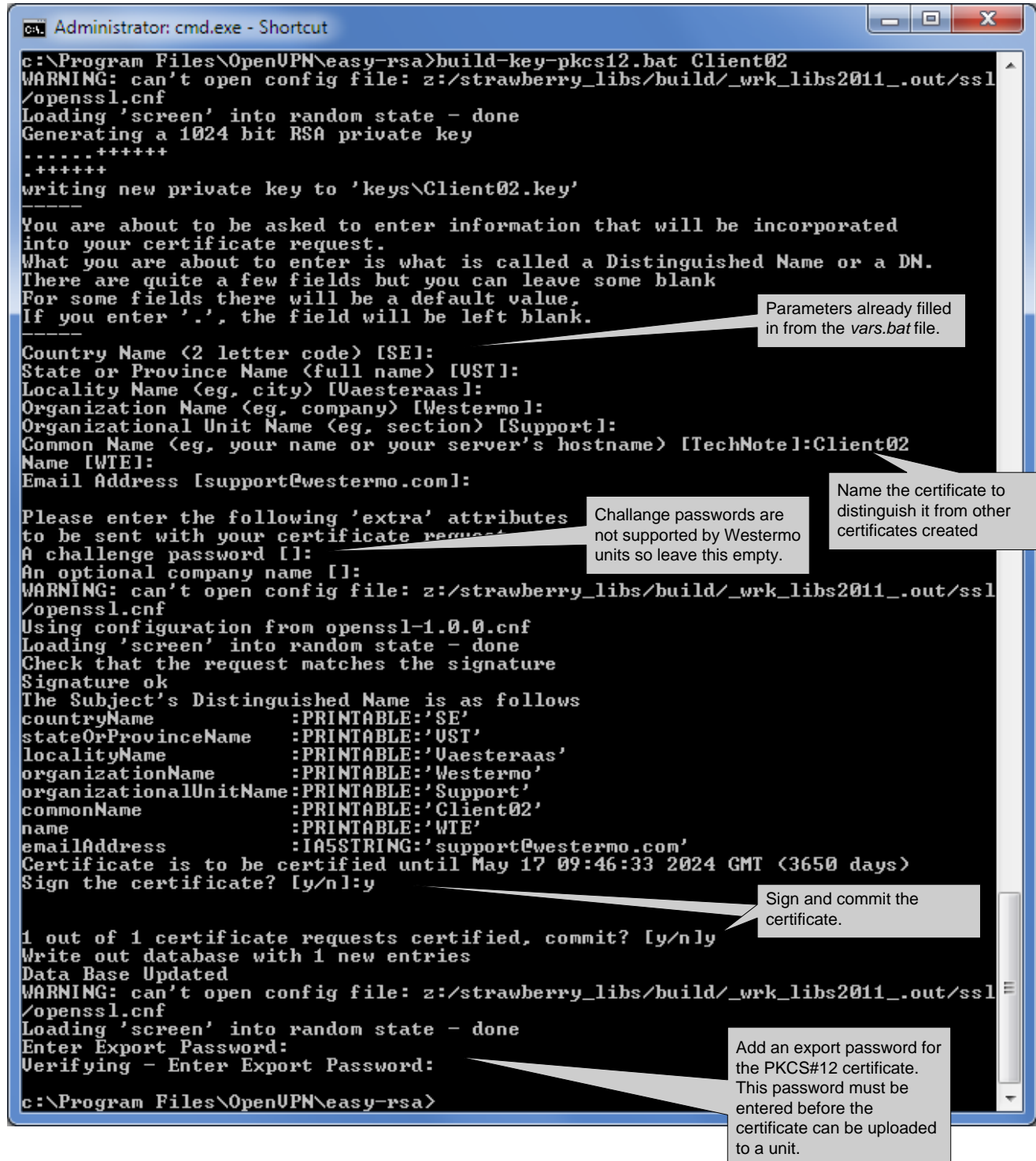
*Client01.key*



## The PKCS#12 format

If preferred the client certificates can also be created in the PKCS#12 format which basically bundles the three files *ca.crt*, *client.crt* and *client.key* into one file and password protects it. Run the *build-key-pkcs12.bat* <client certificate file name> script.

**Please Note!** This format is mandatory for the Westermo MRD-3xx 3G-routers.



```

Administrator: cmd.exe - Shortcut
c:\Program Files\OpenUPN\easy-rsa>build-key-pkcs12.bat Client02
WARNING: can't open config file: z:/strawberry_libs/build/_wrk_libs2011_.out/ssl
/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.+++++
writing new private key to 'keys\Client02.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) [SE]:
State or Province Name (full name) [UST]:
Locality Name (eg, city) [Vaesteraas]:
Organization Name (eg, company) [Westermo]:
Organizational Unit Name (eg, section) [Support]:
Common Name (eg, your name or your server's hostname) [TechNote:Client02]
Name [WTE]:
Email Address [support@westermo.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: z:/strawberry_libs/build/_wrk_libs2011_.out/ssl
/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'SE'
stateOrProvinceName   :PRINTABLE:'UST'
localityName          :PRINTABLE:'Vaesteraas'
organizationName      :PRINTABLE:'Westermo'
organizationalUnitName:PRINTABLE:'Support'
commonName            :PRINTABLE:'Client02'
name                  :PRINTABLE:'WTE'
emailAddress          :IA5STRING:'support@westermo.com'
Certificate is to be certified until May 17 09:46:33 2024 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
WARNING: can't open config file: z:/strawberry_libs/build/_wrk_libs2011_.out/ssl
/openssl.cnf
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:

c:\Program Files\OpenUPN\easy-rsa>
    
```

Parameters already filled in from the vars.bat file.

Name the certificate to distinguish it from other certificates created

Challenge passwords are not supported by Westermo units so leave this empty.

Sign and commit the certificate.

Add an export password for the PKCS#12 certificate. This password must be entered before the certificate can be uploaded to a unit.

The following files should now be generated in the KEY\_DIR folder.

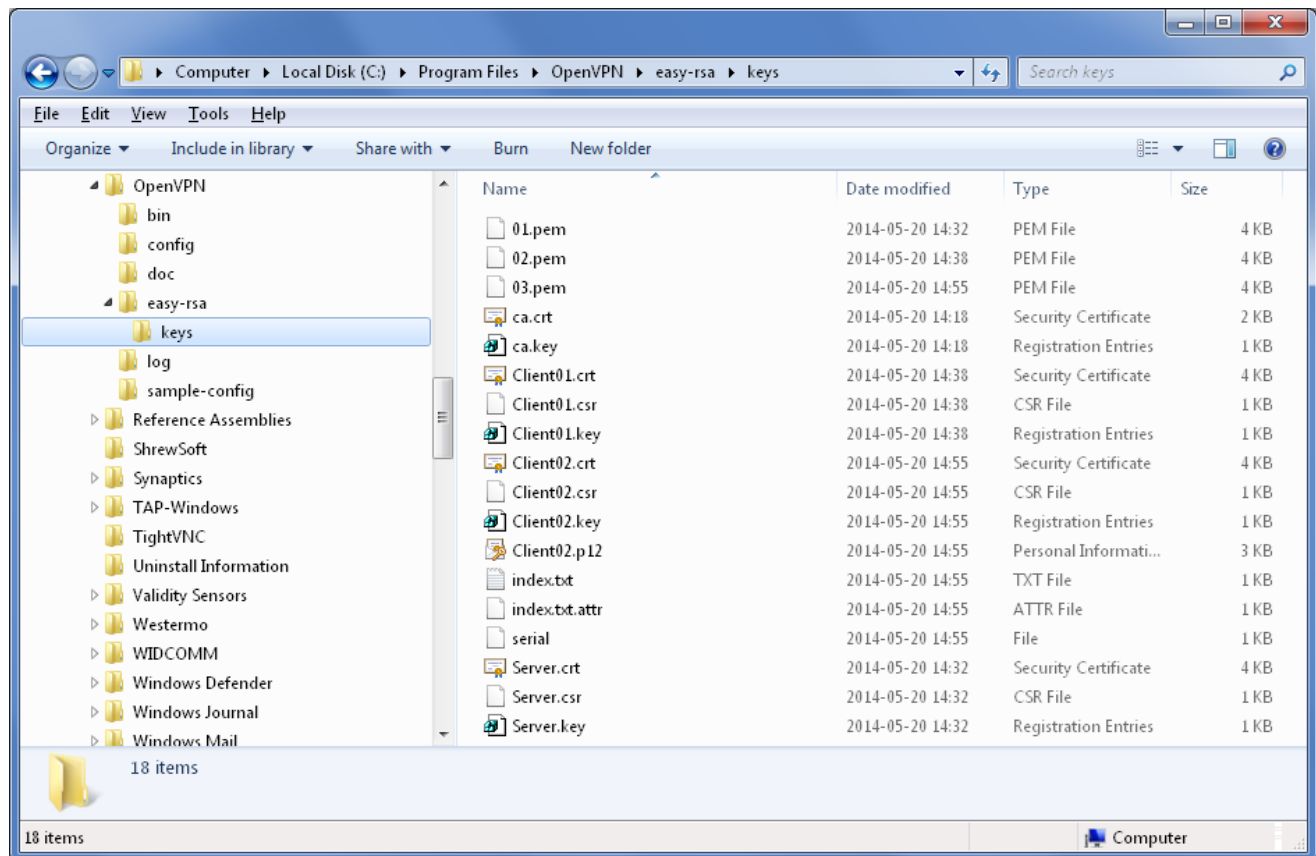
*03.pem*

*Client02.crt*

*Client02.csr*

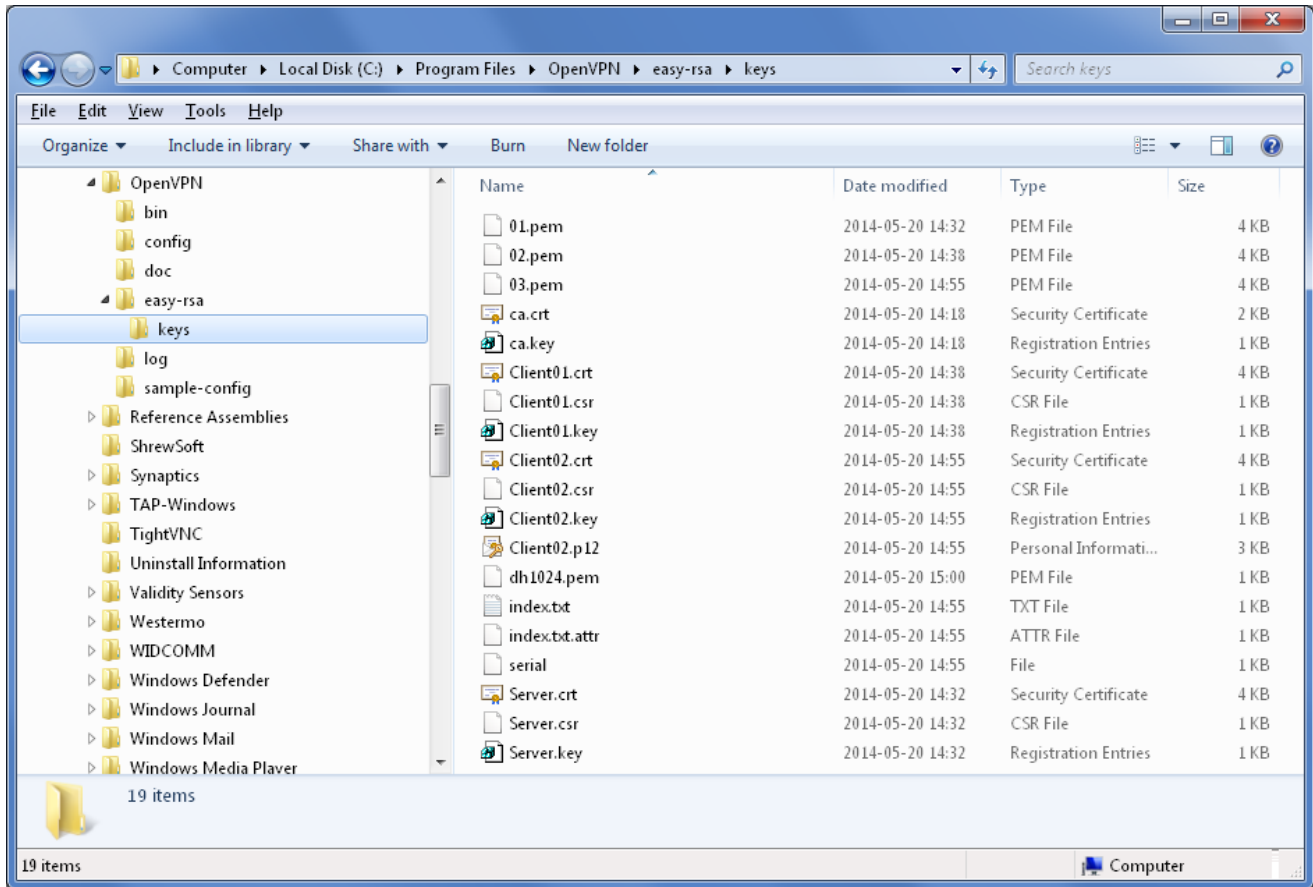
*Client02.key*

*Client02.p12*





The following file should now be generated in the KEY\_DIR folder.  
*dh1024.pem*



## WeOS IPSec Certificates

When generating certificates for IPSec VPN tunnels that should be used with WeOS units an additional conversion is needed. Generate certificates as usual following this Tech Note. When the needed certificates have been generated the private key files for the server and client needs to be converted into the .pem format.

The private keys generated starts and ends with these headers:

```
-----BEGIN PRIVATE KEY-----  
.  
.  
-----END PRIVATE KEY-----
```

But the IPSec implementation in WeOS only allows these headers of the .pem file format:

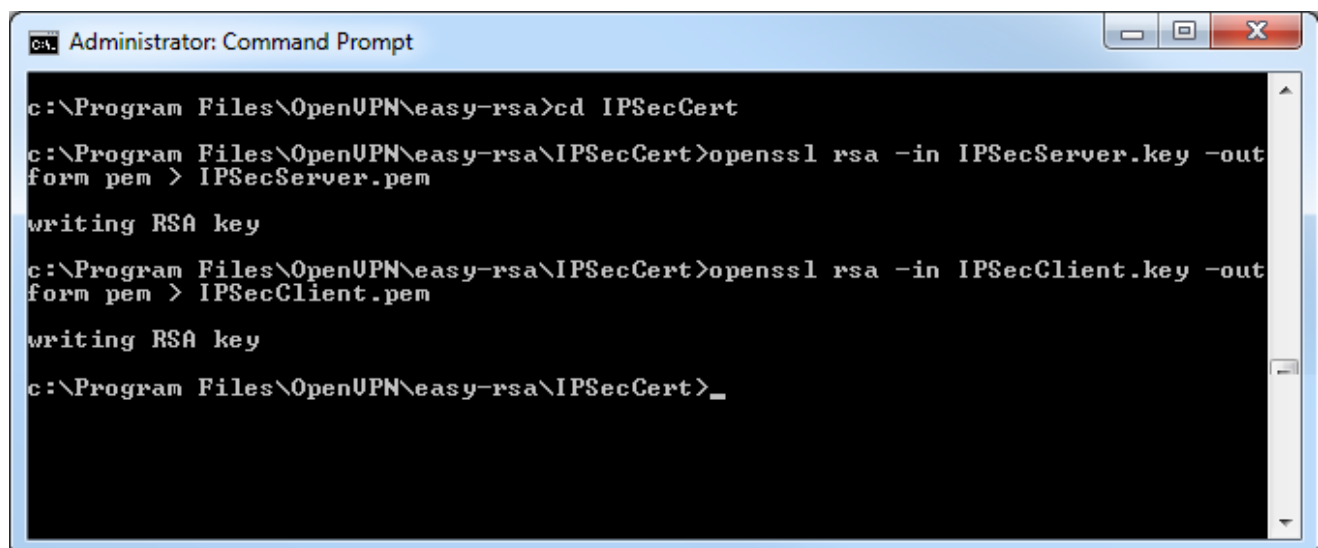
```
-----BEGIN RSA PRIVATE KEY-----  
.  
.  
-----END RSA PRIVATE KEY-----
```

The easiest way to make the certificates work with IPSec is to simply convert the already generated .key files into .pem files and this is done with easy-rsa as well.

In the cmd window go to the folder where the newly generated SSL VPN certificates are stored using the `cd <Folder>` command.

Then issue the below stated commands for the server and client keys to convert them to the .pem format.

```
openssl rsa -in <nameofserverkey>.key -outform pem > <nameofserverkey>.pem  
openssl rsa -in <nameofclientkey>.key -outform pem > <nameofclientkey>.pem
```



```
Administrator: Command Prompt  
c:\Program Files\OpenVPN\easy-rsa>cd IPsecCert  
c:\Program Files\OpenVPN\easy-rsa\IPsecCert>openssl rsa -in IPsecServer.key -out  
form pem > IPsecServer.pem  
writing RSA key  
c:\Program Files\OpenVPN\easy-rsa\IPsecCert>openssl rsa -in IPsecClient.key -out  
form pem > IPsecClient.pem  
writing RSA key  
c:\Program Files\OpenVPN\easy-rsa\IPsecCert>_
```

## The Files Created

<u>File</u>	<u>Security</u>	<u>Description</u>
01.pem	public	Same file as Server.crt but different file ending.
02.pem	public	Same file as Client01.crt but different file ending.
03.pem	public	Same file as Client02.crt but different file ending.
ca.crt	public	CA certificate, must be available on both client and server.
ca.key	<b>secret!</b>	CA key, must be kept very secret and <u>only</u> on the CA.
Server.crt	public	Signed certificate for the server, must be on the VPN server.
Server.key	<b>secret!</b>	Private RSA key of the client, must be on the VPN server.
Server.csr		<i>Certificate signing request not needed.</i>
Client01.crt	public	Signed certificate for the client, must be on the VPN client.
Client01.key	<b>secret!</b>	Private RSA key of the client, must be on the VPN client.
Client01.csr		<i>Certificate signing request not needed.</i>
Client02.p12	<b>secret!</b>	Only the .p12 file is needed on the VPN client.
Client02.crt	public	Also generated with the PKCS#12 build command.
Client02.key	<b>secret!</b>	Also generated with the PKCS#12 build command.
Client02.csr		<i>Also generated with the PKCS#12 build command.</i>
dh1024.pem	public	Contains the Diffie-Hellman key, must be on the VPN server.
index.txt		Easy-rsa database file.
index.txt.attr		Easy-rsa database file.
serial		Easy-rsa database file.

### File types needed by Westermo WeOS products:

#### Server:

ca.crt  
dh1024.pem  
server.crt  
server.key / server.pem

#### Clients:

ca.crt  
client.crt  
client.key / client.pem  
or  
client.p12

### File types needed by Westermo MRD-3xx 3G-routers

client.p12







## Revision history for version 2.0

Revision	Rev by	Revision note	Date
00	ML	First version	150518
01			
02			
03			
04			
05			
06			
07			



**H E A D   O F F I C E**

**Sweden**

Westermo  
SE-640 40 Stora Sundby  
Tel: +46 (0)16 42 80 00  
Fax: +46 (0)16 42 80 01  
info@westermo.se  
www.westermo.com

**Sales Units**

Westermo Data Communications

**China**

sales.cn@westermo.com  
www.cn.westermo.com

**France**

infos@westermo.fr  
www.westermo.fr

**Germany**

info@westermo.de  
www.westermo.de

**North America**

info@westermo.com  
www.westermo.com

**Singapore**

sales@westermo.com.sg  
www.westermo.com

**Sweden**

info.sverige@westermo.se  
www.westermo.se

**United Kingdom**

sales@westermo.co.uk  
www.westermo.co.uk

**Other Offices**



*For complete contact information, please visit our website at [www.westermo.com/contact](http://www.westermo.com/contact) or scan the QR code with your mobile phone.*