

TECH NOTE 003

Self-Signed Certificates

X.509 Certificate Creation Using Easy-Rsa 2 with OpenVPN



AIM

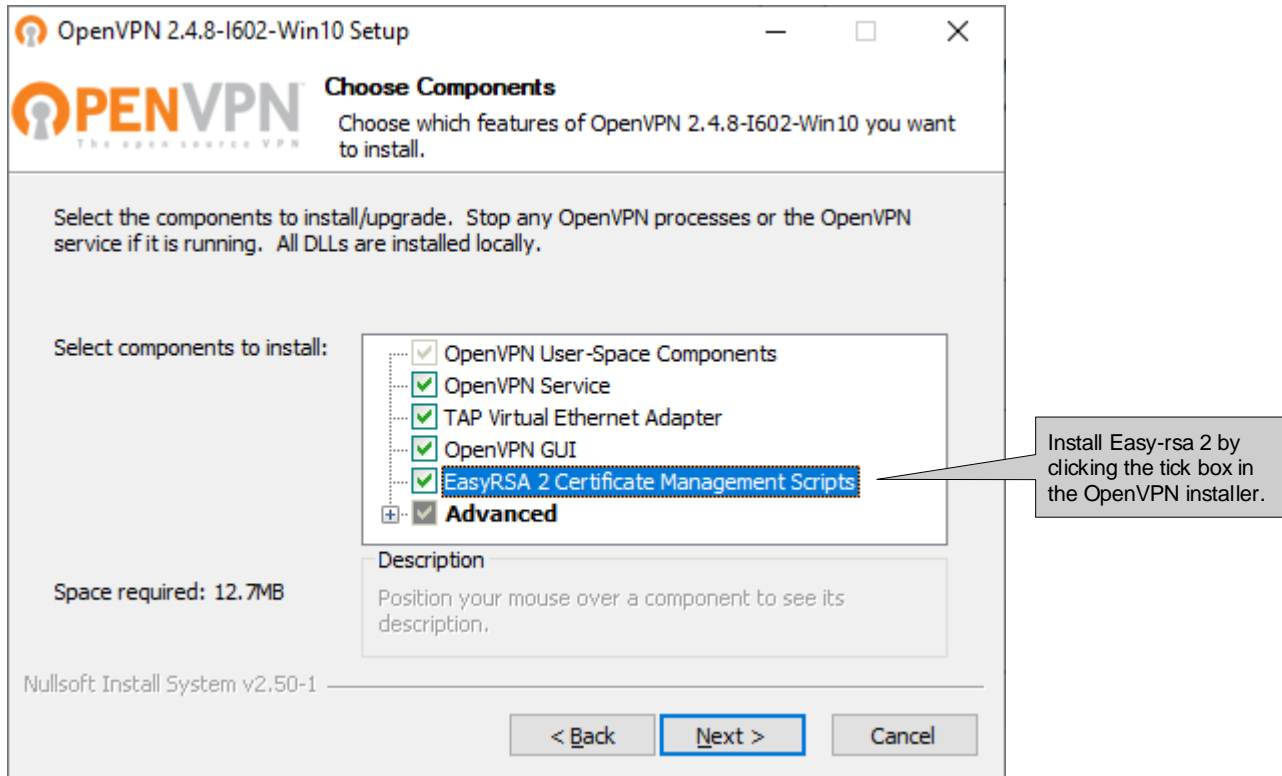
This Tech Note will show how to create X.509 certificates with Easy-rsa 2 in OpenVPN for Microsoft Windows.

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

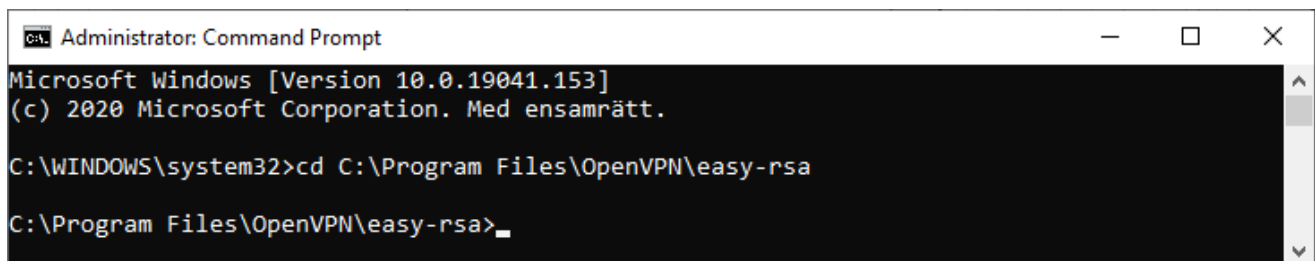
All examples in this Tech Note are made using MS Windows 10 Pro version 2004 and OpenVPN for MS Windows version 2.4.8-I602.

Build Certificates with Easy-rsa 2

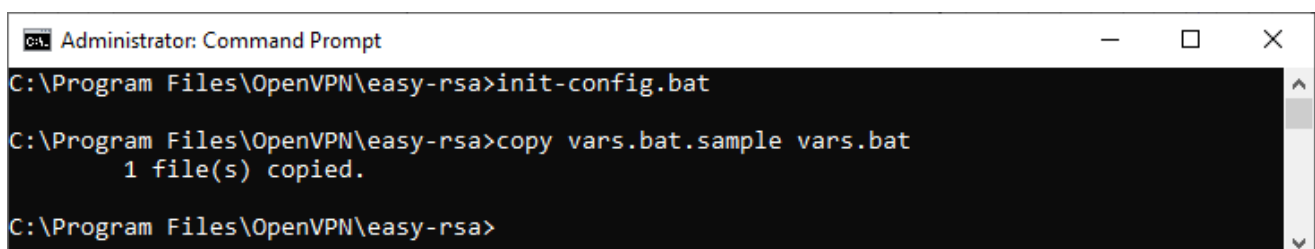
1. Make sure *easy-rsa 2* is installed with OpenVPN.



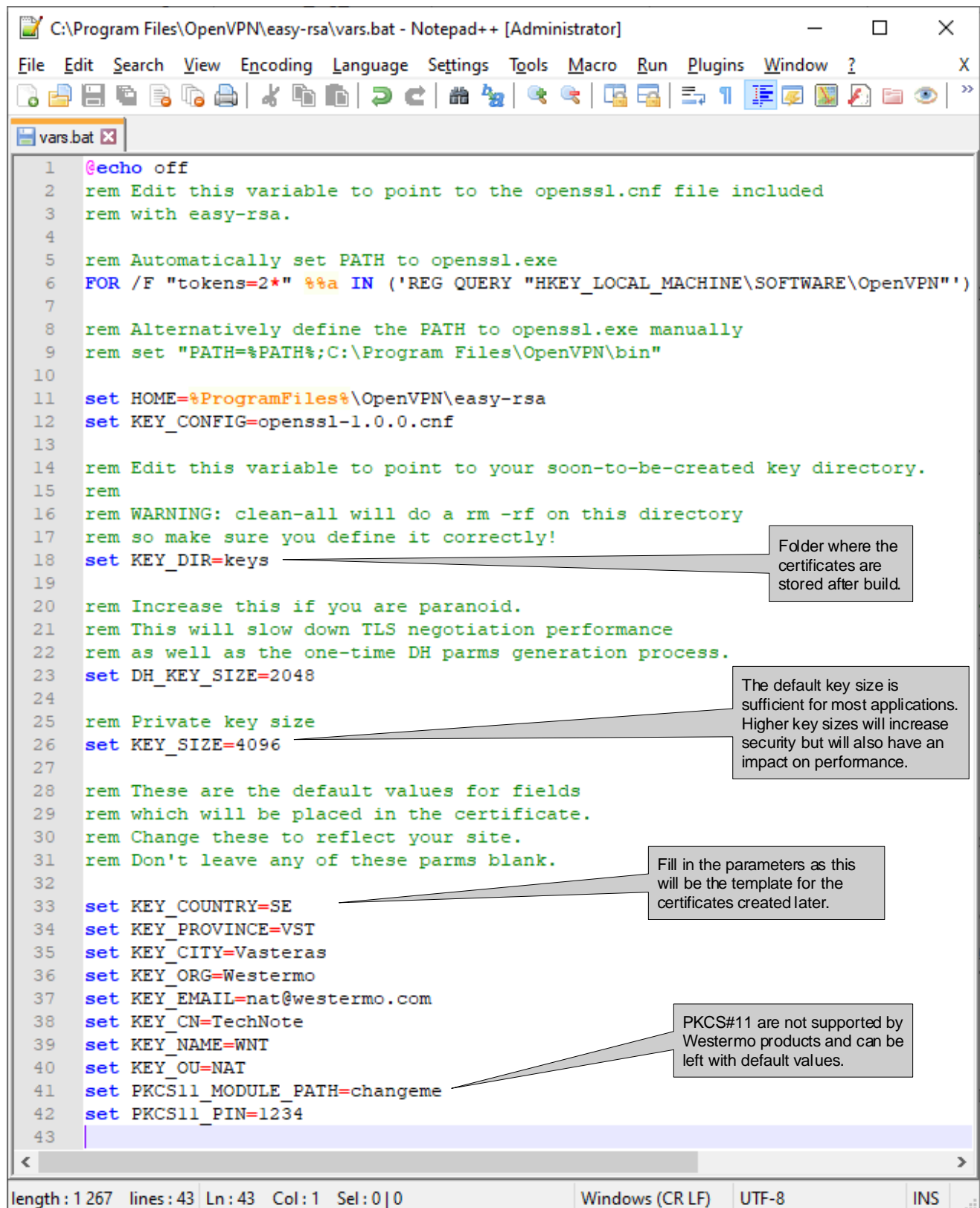
2. Use MS Windows Command Prompt to go to the *easy-rsa* folder. Default path for the 64-bit version is `C:\Program Files\OpenVPN\easy-rsa`. **Please Note! On MS Windows systems *easy-rsa 2* will have to be run with administrator rights.**



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++ using 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 the openssl.cnf file included
3 rem with easy-rsa.
4
5 rem Automatically set PATH to openssl.exe
6 FOR /F "tokens=2*" %%a IN ('REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\OpenVPN"')
7
8 rem Alternatively define the PATH to openssl.exe manually
9 rem set "PATH=%PATH%;C:\Program Files\OpenVPN\bin"
10
11 set HOME=%ProgramFiles%\OpenVPN\easy-rsa
12 set KEY_CONFIG=openssl-1.0.0.cnf
13
14 rem Edit this variable to point to your soon-to-be-created key directory.
15 rem
16 rem WARNING: clean-all will do a rm -rf on this directory
17 rem so make sure you define it correctly!
18 set KEY_DIR=keys
19
20 rem Increase this if you are paranoid.
21 rem This will slow down TLS negotiation performance
22 rem as well as the one-time DH parms generation process.
23 set DH_KEY_SIZE=2048
24
25 rem Private key size
26 set KEY_SIZE=4096
27
28 rem These are the default values for fields
29 rem which will be placed in the certificate.
30 rem Change these to reflect your site.
31 rem Don't leave any of these parms blank.
32
33 set KEY_COUNTRY=SE
34 set KEY_PROVINCE=VST
35 set KEY_CITY=Vasteras
36 set KEY_ORG=Westermo
37 set KEY_EMAIL=nat@westermo.com
38 set KEY_CN=TechNote
39 set KEY_NAME=WNT
40 set KEY_OU=NAT
41 set PKCS11_MODULE_PATH=changeme
42 set PKCS11_PIN=1234
43
```

Folder where the certificates are stored after build.

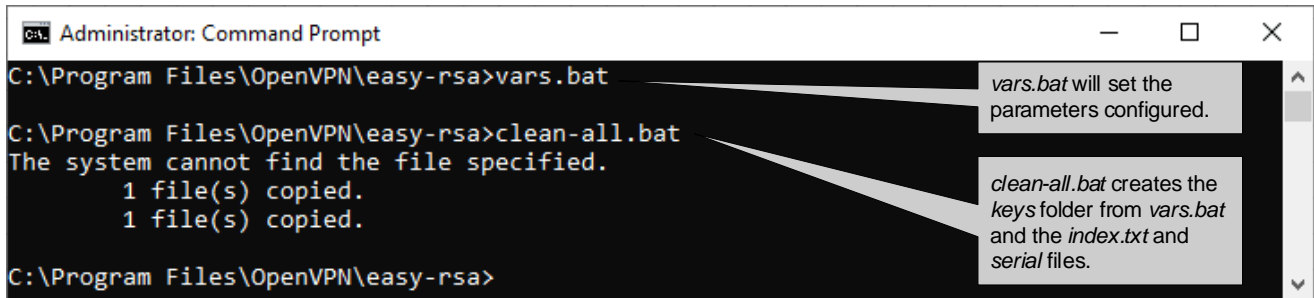
The default key size is sufficient for most applications. Higher key sizes will increase security but will also have an impact on performance.

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.

length : 1 267 lines : 43 Ln : 43 Col : 1 Sel : 0 | 0 Windows (CR LF) UTF-8 INS

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

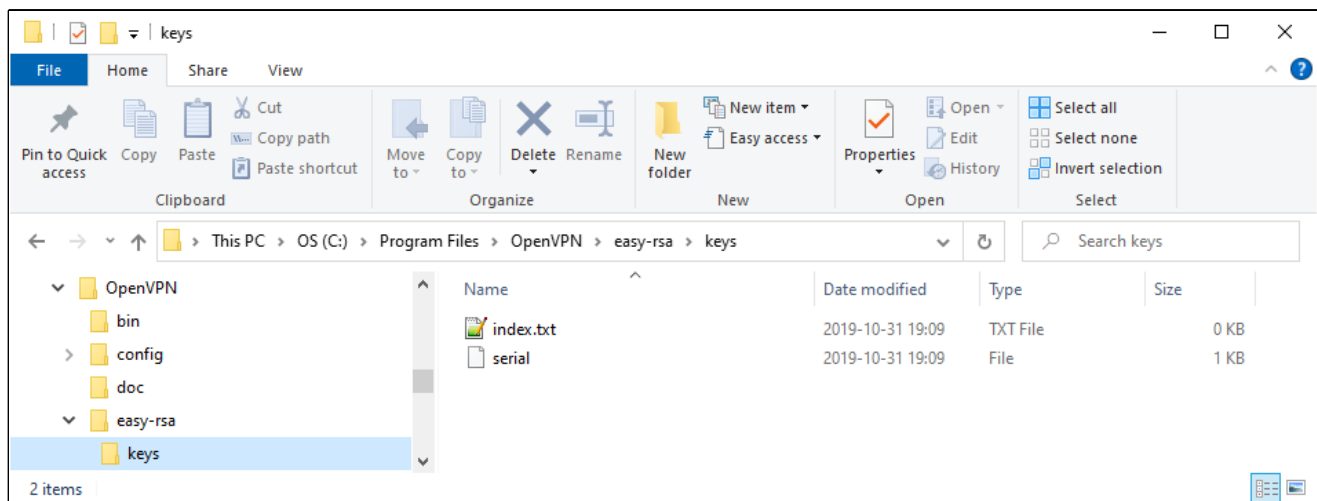


```
Administrator: Command Prompt
C:\Program Files\OpenVPN\easy-rsa>vars.bat
C:\Program Files\OpenVPN\easy-rsa>clean-all.bat
The system cannot find the file specified.
1 file(s) copied.
1 file(s) copied.
C:\Program Files\OpenVPN\easy-rsa>
```

vars.bat will set the parameters configured.

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

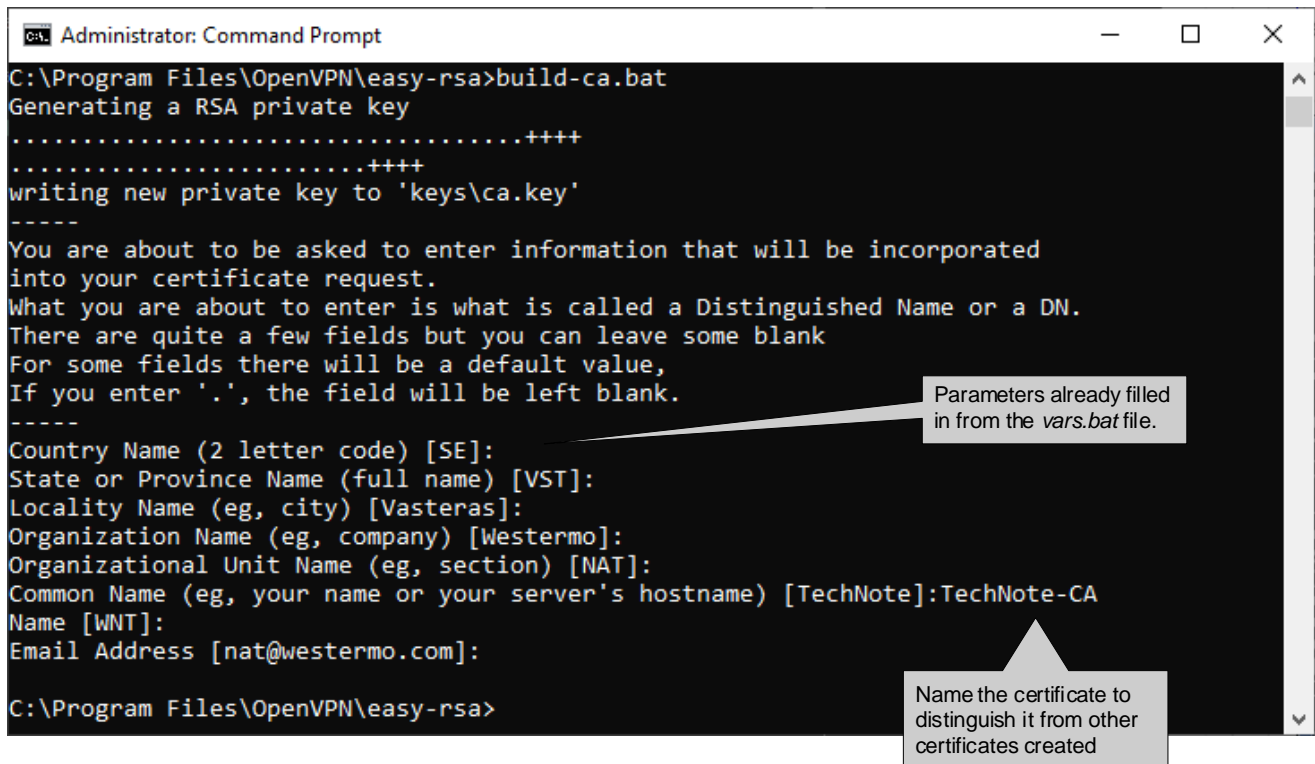
The following files should now be present in the KEY_DIR folder (*keys*) as specified in *vars.bat*.
index.txt
serial



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: Command Prompt
C:\Program Files\OpenVPN\easy-rsa>build-ca.bat
Generating a 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) [VST]:
Locality Name (eg, city) [Vasteras]:
Organization Name (eg, company) [Westermo]:
Organizational Unit Name (eg, section) [NAT]:
Common Name (eg, your name or your server's hostname) [TechNote]:TechNote-CA
Name [WNT]:
Email Address [nat@westermo.com]:

C:\Program Files\OpenVPN\easy-rsa>
```

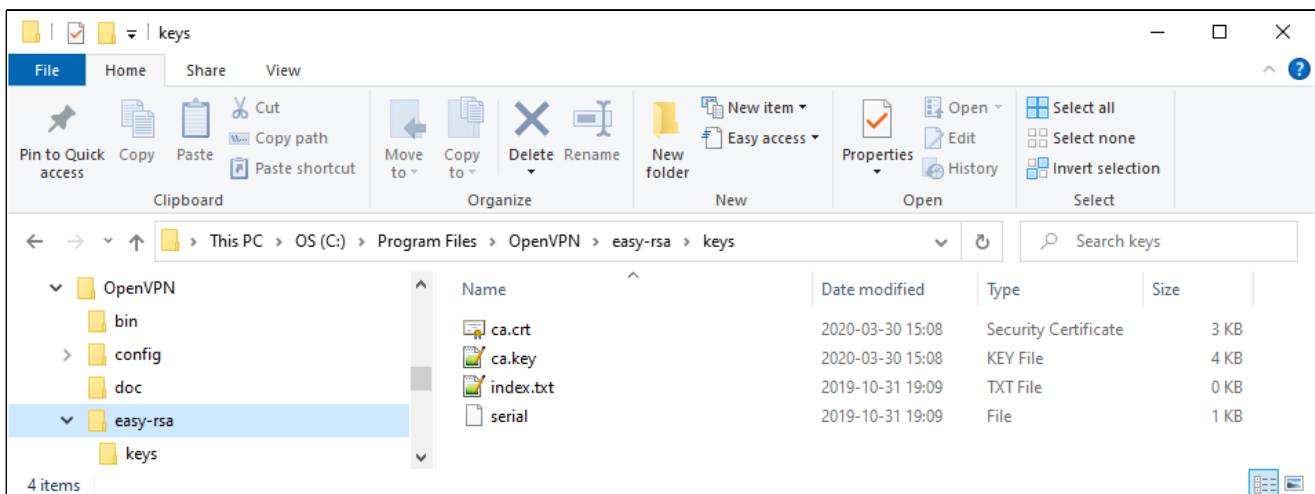
Parameters already filled in from the *vars.bat* file.

Name the certificate to distinguish it from other certificates created

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: Command Prompt
C:\Program Files\OpenVPN\easy-rsa>build-key-server.bat Server
Generating a 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) [VST]:
Locality Name (eg, city) [Vasteras]:
Organization Name (eg, company) [Westermo]:
Organizational Unit Name (eg, section) [NAT]:
Common Name (eg, your name or your server's hostname) [TechNote]:Server
Name [WNT]:
Email Address [nat@westermo.com]:

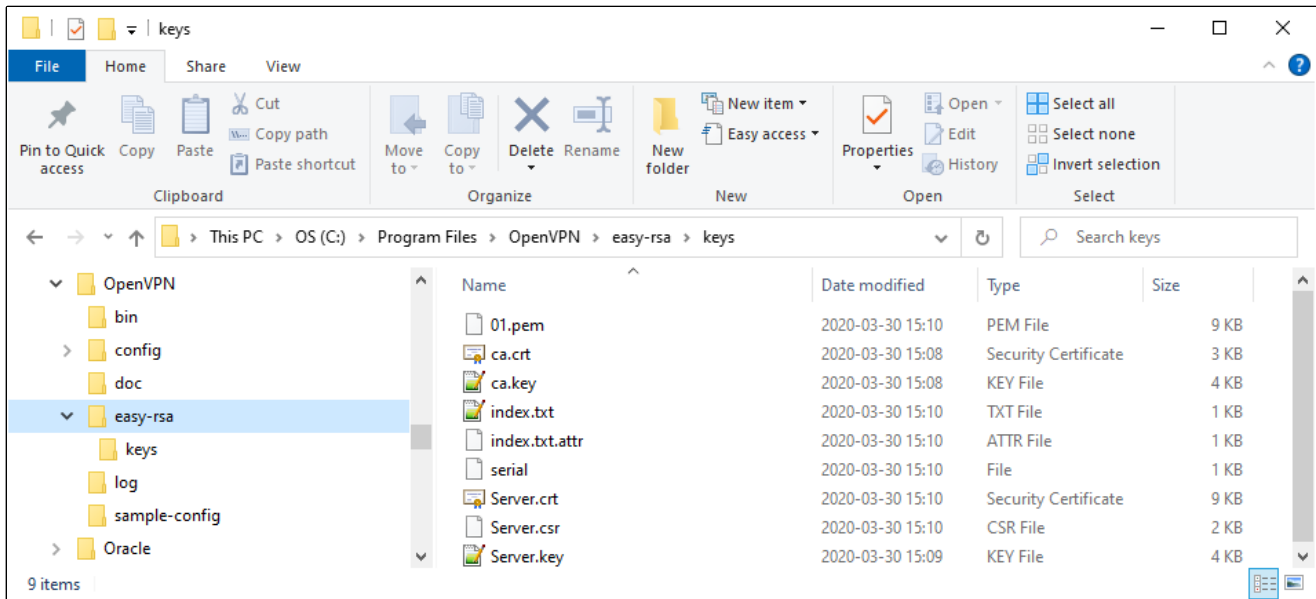
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl-1.0.0.cnf
Can't open keys/index.txt.attr for reading, No such file or directory
15800:error:02001002:system library:fopen:No such file or directory:crypto/bio/bss_file.c
:74:fopen('keys/index.txt.attr','r')
15800:error:2006D080:BIIO routines:BIIO_new_file:no such file:crypto/bio/bss_file.c:81:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'SE'
stateOrProvinceName :PRINTABLE:'VST'
localityName      :PRINTABLE:'Vasteras'
organizationName  :PRINTABLE:'Westermo'
organizationalUnitName:PRINTABLE:'NAT'
commonName       :PRINTABLE:'Server'
name             :PRINTABLE:'WNT'
emailAddress      :IA5STRING:'nat@westermo.com'
Certificate is to be certified until Mar 28 13:10:08 2030 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\OpenVPN\easy-rsa>_
```

The following files should now be generated in the KEY_DIR folder.

- 01.pem
- Index.txt.attr
- Server.crt
- Server.csr
- Server.key



8. Client certificates can be built either with the *build-key.bat* <client certificate file name> script or by generating PKCS#12 format certificates instead. This will create all the files that *build-key.bat* does but also the PKCS#12 file format. Which bundles the ca.crt, client.crt and client.key files into one password protected file.

Use the *build-key-pkcs12.bat* <client certificate file name> script for the creation.

Please Note! PKCS#12 format is the preferred choice of the Westermo MRD/BRD routers.



```
Administrator: Command Prompt
C:\Program Files\OpenVPN\easy-rsa>build-key-pkcs12.bat Client01
Generating a 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) [VST]:
Locality Name (eg, city) [Vasteras]:
Organization Name (eg, company) [Westermo]:
Organizational Unit Name (eg, section) [NAT]:
Common Name (eg, your name or your server's hostname) [TechNote]:Client01
Name [WNT]:
Email Address [nat@westermo.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'SE'
stateOrProvinceName  :PRINTABLE:'VST'
localityName         :PRINTABLE:'Vasteras'
organizationName     :PRINTABLE:'Westermo'
organizationalUnitName:PRINTABLE:'NAT'
commonName           :PRINTABLE:'Client01'
name                 :PRINTABLE:'WNT'
emailAddress         :IA5STRING:'nat@westermo.com'
Certificate is to be certified until Mar 28 13:53:15 2030 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
Enter Export Password:
Verifying - Enter Export Password:
```

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 bundle. This password must be entered before the file can be uploaded to a unit.

The following files should now be generated in the KEY_DIR folder.

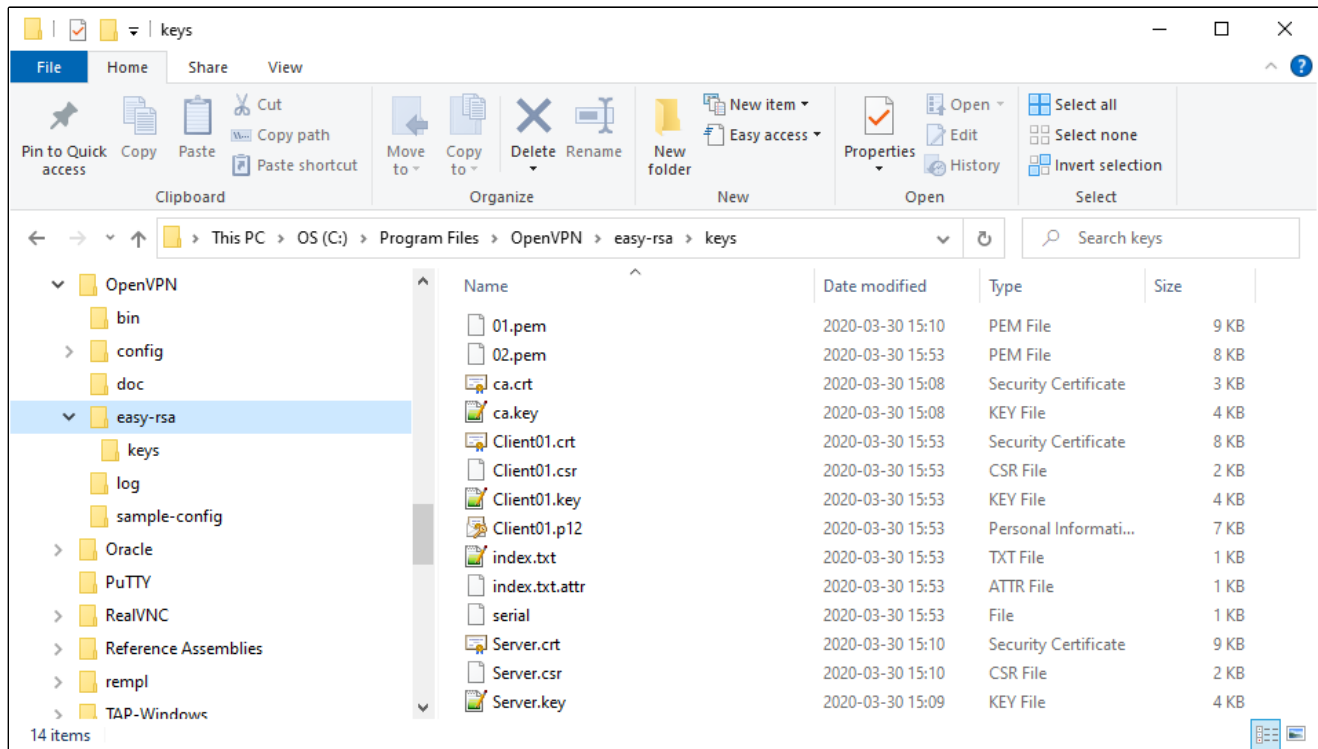
02.pem

Client01.crt

Client01.csr

Client01.key

Client01.p12



TLS Authentication

By using TLS Authentication another layer of protection from unwanted connection attempts can be added to the SSL VPN Server. Rouge connection attempts may very well be part of a DDoS attack causing the SSL Server to become unreachable for allowed VPNs.

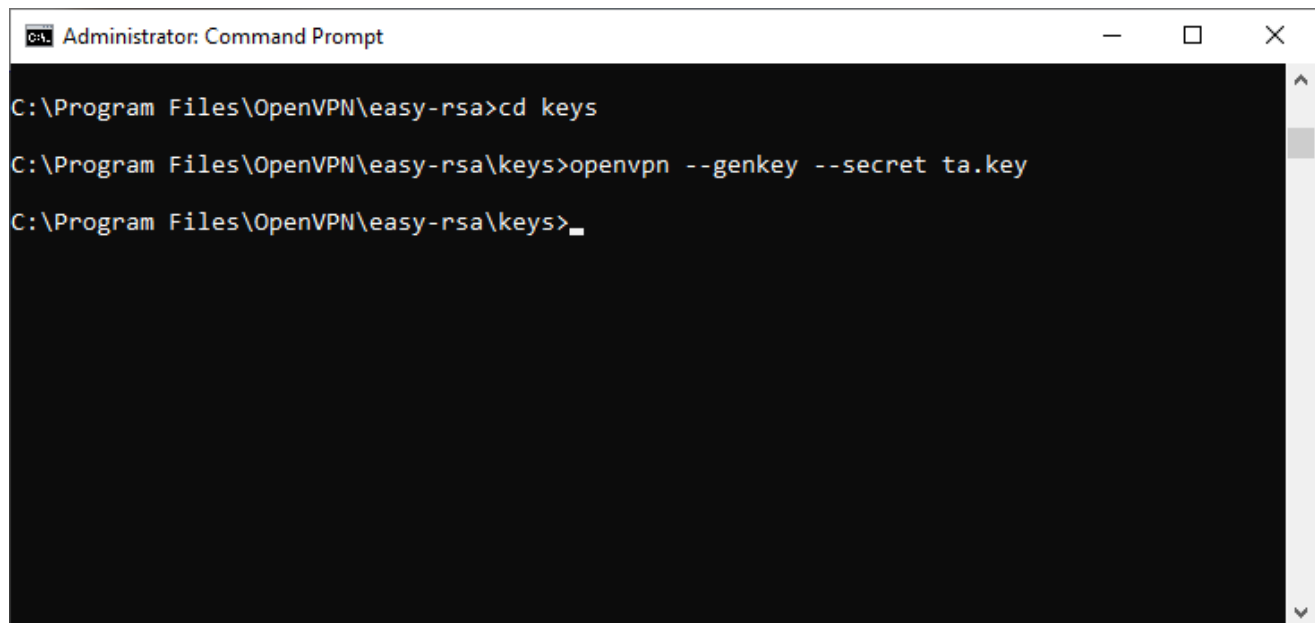
TLS Authentication is achieved by adding a TLS key to both the SSL Client and Server. If the expected key is not present in the connection attempt the initiation packet will be silently dropped without any further processing (with the UDP version of the tunnel).

TLS Authentication is available on both WeOS Layer 3 products and the MRD/BRD routers. On the MRD/BRD routers the TLS key must to be part of an .ovpn configuration file that is uploaded to these units.

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

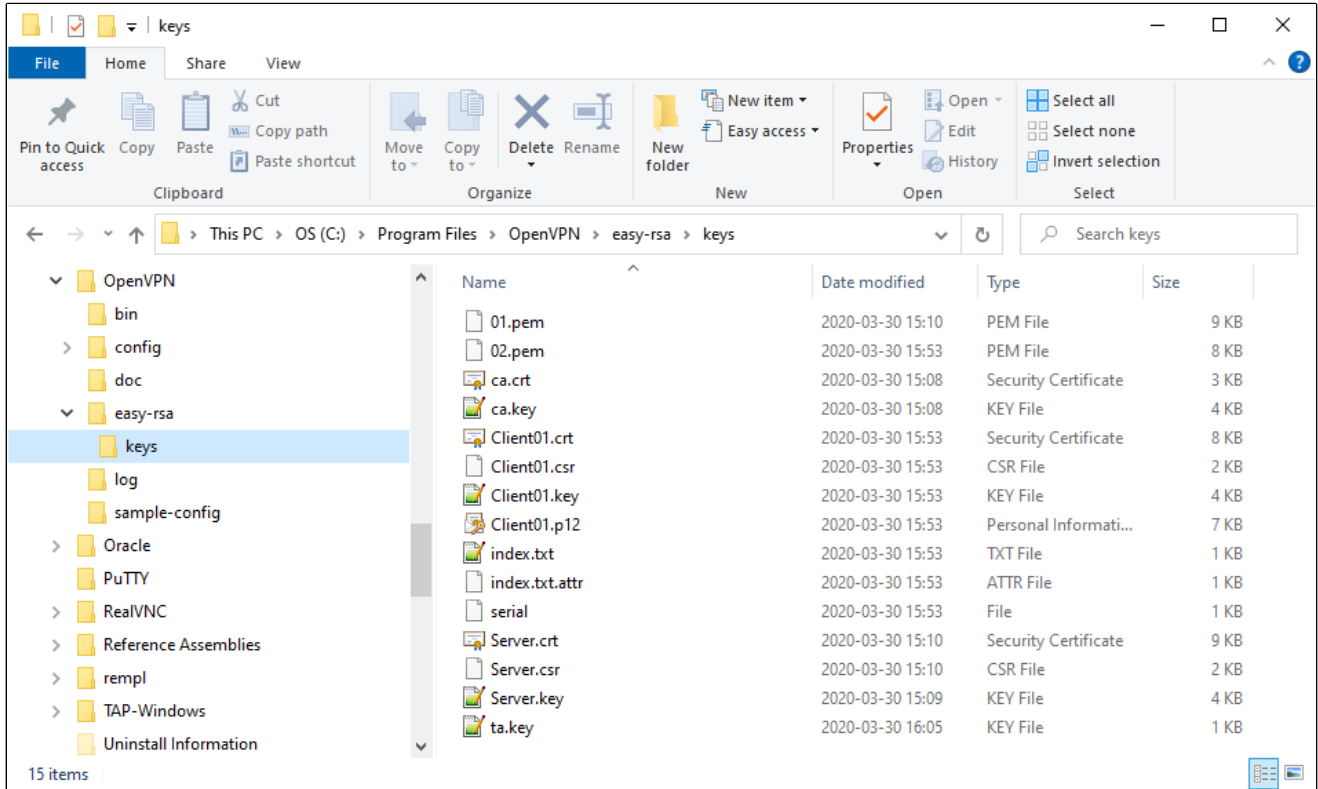
The TLS key is a static key file that is generated with OpenVPN by issuing this command:

```
openvpn --genkey --secret <nameofstatickey>.key
```



```
Administrator: Command Prompt
C:\Program Files\OpenVPN\easy-rsa>cd keys
C:\Program Files\OpenVPN\easy-rsa\keys>openvpn --genkey --secret ta.key
C:\Program Files\OpenVPN\easy-rsa\keys>_
```

The following file should now be generated in the KEY_DIR folder.
Ta.key



WeOS IPSec Certificates

When generating certificates for IPSec VPN tunnels that should be used with WeOS units an additional conversion is needed. Create certificates as usual following this Tech Note. When the needed certificates have been built 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:

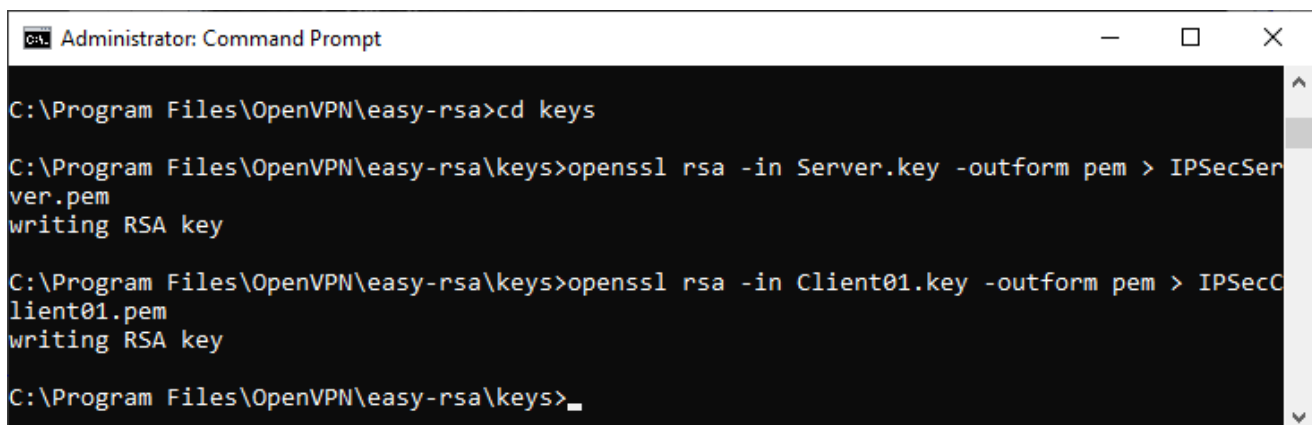
```
-----BEGIN RSA PRIVATE KEY-----  
.  
.  
-----END RSA PRIVATE KEY-----
```

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 also done with easy-rsa.

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

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

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

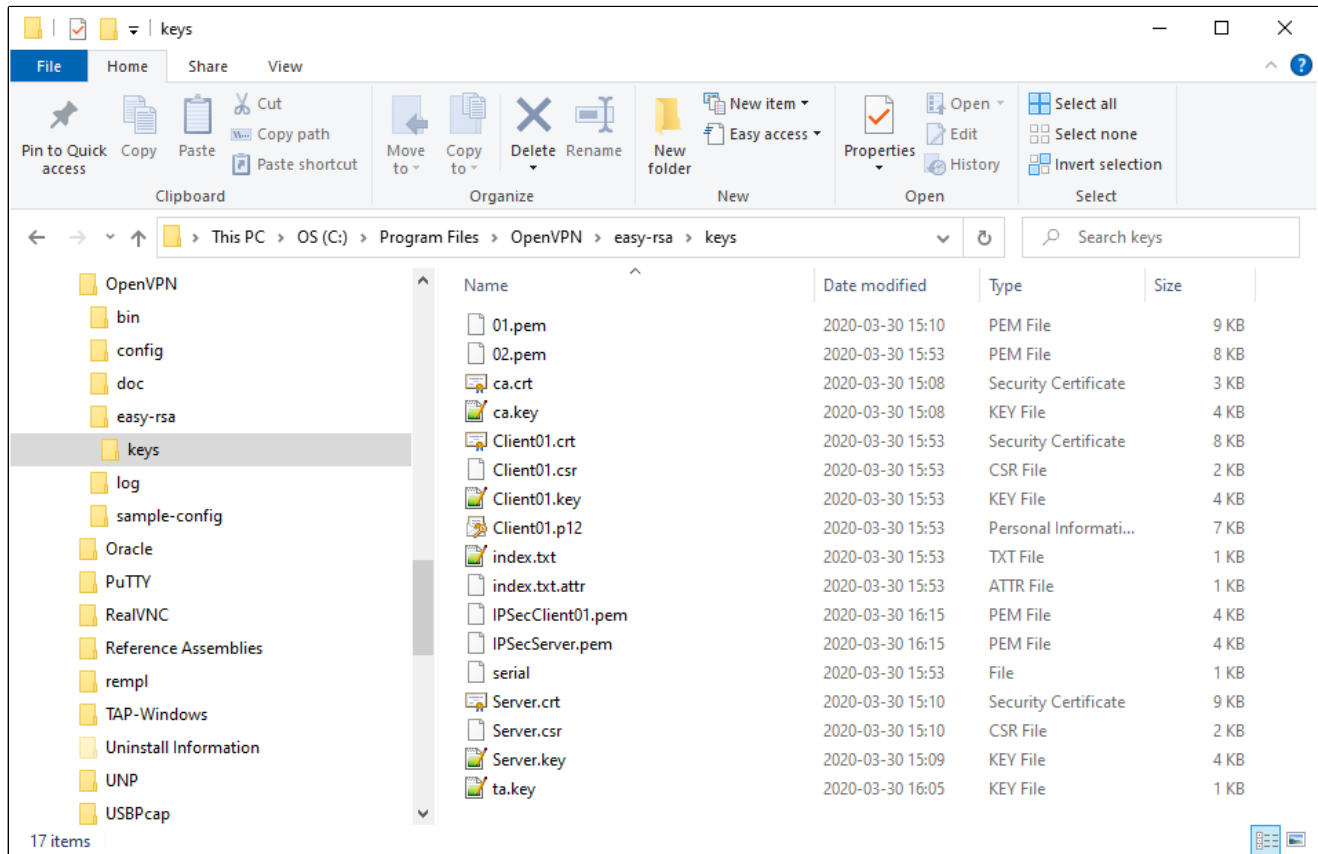


```
Administrator: Command Prompt  
C:\Program Files\OpenVPN\easy-rsa>cd keys  
C:\Program Files\OpenVPN\easy-rsa\keys>openssl rsa -in Server.key -outform pem > IPsecServer.pem  
writing RSA key  
C:\Program Files\OpenVPN\easy-rsa\keys>openssl rsa -in Client01.key -outform pem > IPsecClient01.pem  
writing RSA key  
C:\Program Files\OpenVPN\easy-rsa\keys>_
```

The following files should now be generated in the KEY_DIR folder.

IPSecClient01.pem

IPSecServer.pem



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.
ca.crt	public	CA certificate, must be available on both client and server.
ca.key	secret!	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	secret!	Private RSA key of the server, must be on the VPN server.
Server.csr		<i>Certificate signing request, not needed.</i>
Client01.p12	secret!	Only the .p12 file is needed on the VPN client.
Client01.crt	public	Signed certificate for the client, must be on the VPN client.
Client01.key	secret!	Private RSA key of the client, must be on the VPN client.
Client01.csr		<i>Certificate signing request, not needed.</i>
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
server.crt
ta.key
server.key / server.pem

Clients:

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

File types needed by Westermo MRD and BRD routers

client.p12 (with TLS-auth an .ovpn config file containing the ta.key file)

Revision history for version 3.0

Revision	Rev by	Revision note	Date
00	ML	First version	200331
01			
02			
03			
04			
05			
06			
07			



Westermo Network Technologies AB

SE-635 35 Stora Sundby, Sweden

Phone: +46 16 42 80 00

info@westermo.com

www.westermo.com

Sales Units

Australia

info@westermo.net.au

www.westermo.net.au

Finland

info@westermo.fi

www.westermo.fi

Singapore

sales@westermo.com.sg

www.westermo.com.sg

Austria

info@westermo.at

www.westermo.at

France

infos@westermo.fr

www.westermo.fr

Sweden

info.sverige@westermo.se

www.westermo.se

Belgium

info.belgique@westermo.fr

www.westermo.be

Germany

info@westermo.de

www.westermo.de

Switzerland

info@westermo.ch

www.westermo.ch

China

sales.cn@westermo.com

www.westermocn.com

North America

info.wus@westermo.com

www.westermo.us

United Kingdom

sales@westermo.co.uk

www.westermo.co.uk