INSYS icom

Industrial Data Communication

VPN with INSYS routers

Creating X509.v3 Certificates for VPNs with easy-rsa

Configuration Guide

Trademarks

The use of a trademark not shown below is not an indication that it is freely available for use.

MNP is a registered trademark of Microcom Inc.

IBM PC, AT, XT are registered trademarks of International Business Machine Corporation.

Windows™ is a registered trademark of Microsoft Corporation.

Linux is a registered trademark of Linus Torvalds.

INSYS ® is a registered trademark of INSYS icom GmbH.

The principles of this publication may be transferred to similar combinations. INSYS icom GmbH does not assume liability or provide support in this case. Moreover, it cannot be excluded that other effects or results than described here are produced, if other, similar components are combined and used.

INSYS icom GmbH is not liable for possible damages.

Publisher

INSYS icom GmbH
Hermann-Köhl-Str. 22
D-93049 Regensburg
Germany

Phone	+49 941 58692 0
Fax	+49 941 58692 45
E-mail	info@insys-icom.com
URL	http://www.insys-icom.com

Print	17. Jan. 2024
Item No.	-
Version	1.6
Language	EN

1 Introduction

General

The present publication refers to a combination of selected hardware and software components of INSYS icom GmbH as well as other manufacturers. All components have been combined with the target to realize certain results and effects for certain applications in the field of professional data transfer.

All components have been prepared, configured and used as described in this publication. Thus, the desired results and effects have been achieved.

The exact descriptions of all used components, to which this publication refers, are described in the tables *Hardware, Accessories* and *Software* at the end of this publication.

The symbols and formattings used in this publication are explained in the correspondent section at the end of this publication.

Some configurations or preparations, which are precondition in this publication, are described in other publications. Therefore, always refer to the related device manuals. INSYS devices with web interface provide you with helpful information about the configuration possibilities, if you click on "display help text" in the header.

Target of this Publication

An appropriate certificate structure is required for setting up a VPN network with certificate-based authentication.

You'll learn from this publication how to generate the key and certificate files for Certification Authority (CA), Server, and Clients as well as an optional Certificate Revocation List (CRL) required for this.

These files are necessary to set up an OpenVPN network. Refer to http://www.openvpn.eu for further information about OpenVPN.

Only the CA certificate and key and the certificates of the respective clients are required for setting up a VPN network with IPsec. The certificates for an IPsec participant are identical with those for the OpenVPN client. We refrain from a separate description of the creation of certificates and keys for an IPsec participant here.

The following figures show the distribution of the different keys and certificates across the different participants in the respective VPN networks. A Diffie Hellman parameter set exists by default on the INSYS router, but can also be replaced manually.

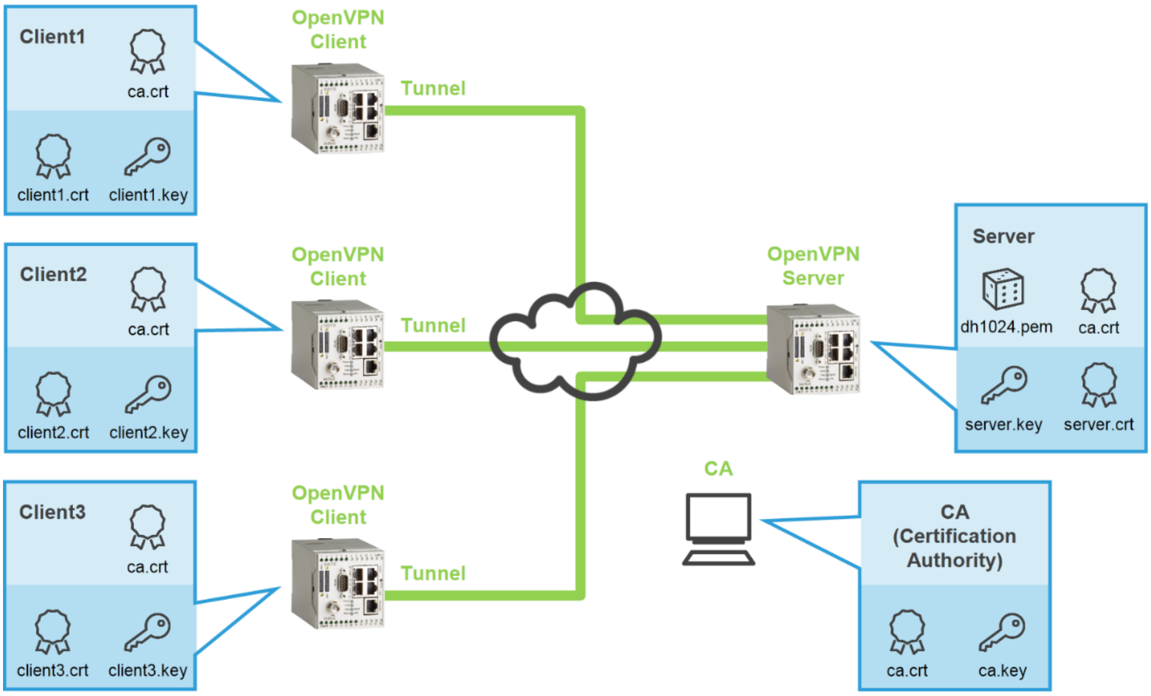


Figure 1: CA certificate structure for OpenVPN server and client with certificate-based authentication, here MoRoS as server and clients

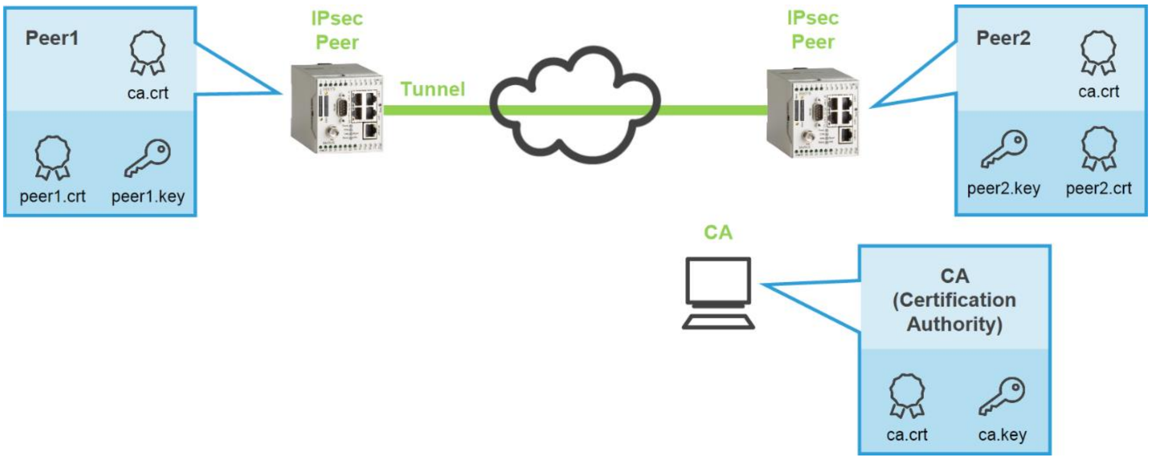


Figure 2: CA certificate structure for IPsec participant with certificate-based authentication, here MoRoS as participant

2 Summary

Generating Certificates and Keys

How to generate all required files for a certificate structure using the default settings. You will find detailed step by step instructions in the following section.

→ The system time of the PC is correct.

- **Preparing Key Directory**

```
C:\Program Files\OpenVPN\easy-rsa>vars
C:\Program Files\OpenVPN\easy-rsa>clean-all
```

- **Generating CA Certificate and Key**

```
C:\Program Files\OpenVPN\easy-rsa>vars
C:\Program Files\OpenVPN\easy-rsa>build-ca
…
Common Name (eg, your name or your server's hostname) []:ca
…
C:\Program Files\OpenVPN\easy-rsa>
```

- **Generating Certificate and Key for a Server**

```
C:\Program Files\OpenVPN\easy-rsa>vars
C:\Program Files\OpenVPN\easy-rsa>build-key-server server
…
Common Name (eg, your name or your server's hostname) []:server
…
Sign the certificate? [y/n]:y
…
1 out of 1 certificate requests certified, commit? [y/n]y
…
C:\Program Files\OpenVPN\easy-rsa>
```

- **Generating Certificate and Key for a Client**

```
C:\Program Files\OpenVPN\easy-rsa>vars
C:\Program Files\OpenVPN\easy-rsa>build-key client1
…
Common Name (eg, your name or your server's hostname) []:client1
…
Sign the certificate? [y/n]:y
…
1 out of 1 certificate requests certified, commit? [y/n]y
…
C:\Program Files\OpenVPN\easy-rsa>
```

- **Revoking a Certificate and Generating a Certificate Revocation List (if required)**

```
C:\Program Files\OpenVPN\easy-rsa>vars
C:\Program Files\OpenVPN\easy-rsa>revoke-full client1
…
certificate revoked
…
C:\Program Files\OpenVPN\easy-rsa>
```

✓ All files are generated with this.

3 Configuration

3.1 Provisions and Presettings

Provisions

Please prepare the following items before starting the configuration:

- **Downloading the OpenVPN Package**
- **Installing the OpenVPN Package on a Windows PC**
- **Initialising the OpenVPN Package on a Windows PC**

- **Downloading the OpenVPN Package**

  How to download the OpenVPN package from our website.

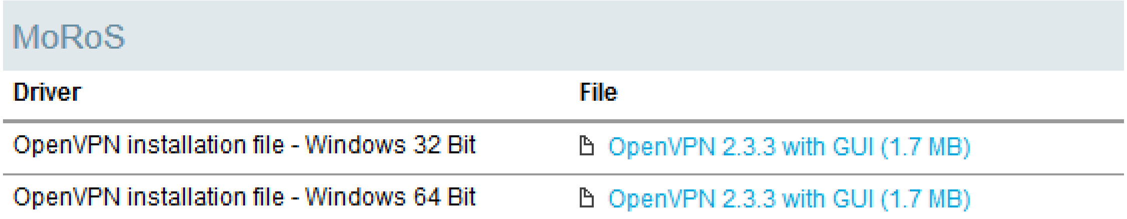
→ PC with approx. 1.5 MB free disk space

→ Web browser

→ Internet connection

1. Open http://www.insys-icom.com/driver/ to download the drivers.
2. Click on the link for your Windows version in the "MoRoS" section:

   ⓘ *Refer to Control Panel, System, System section and System type for your Windows version (32 or 64 bit).*



MoRoS

Driver	File
OpenVPN installation file - Windows 32 Bit	OpenVPN 2.3.3 with GUI (1.7 MB)
OpenVPN installation file - Windows 64 Bit	OpenVPN 2.3.3 with GUI (1.7 MB)

   ⓘ *If a more recent version is available, download this.*

3. Save the file on your PC.

   ✓ You have downloaded the OpenVPN package software with this.

Installing the OpenVPN Package on a Windows PC

How to install the OpenVPN GUI and the programs for creating the certificates and keys on your PC successfully.

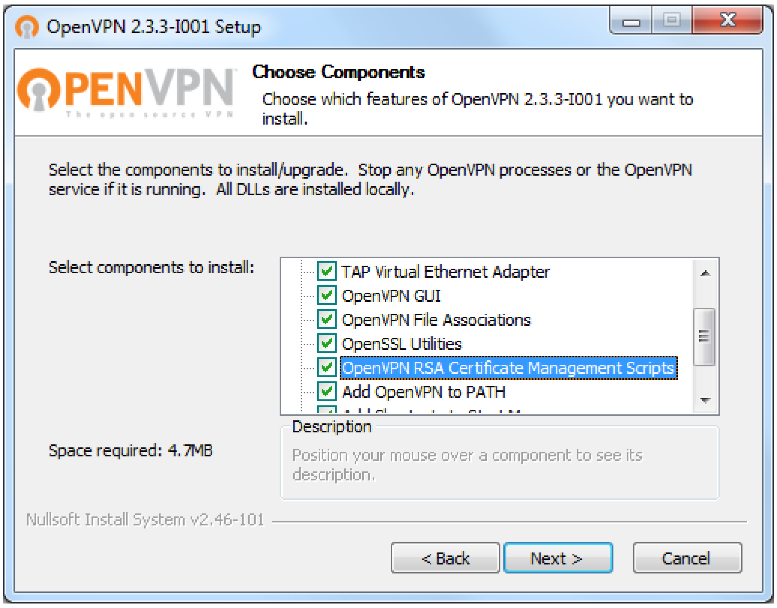
→ You have downloaded the OpenVPN packet (version 2.3.3 or higher) from the INSYS website (www.insys-icom.com/driver).

1. Execute the previously downloaded installation file

   ▶ *If Windows displays a security request, confirm it.*

2. Start the setup wizard and accept the license agreement.

   ✓ The component selection window appears.



OpenVPN 2.3.3-I001 Setup

Choose Components

Choose which features of OpenVPN 2.3.3-I001 you want to install.

Select the components to install/upgrade. Stop any OpenVPN processes or the OpenVPN service if it is running. All DLLs are installed locally.

Select components to install:

- ☑ TAP Virtual Ethernet Adapter
- ☑ OpenVPN GUI
- ☑ OpenVPN File Associations
- ☑ OpenSSL Utilities
- ☑ OpenVPN RSA Certificate Management Scripts
- ☑ Add OpenVPN to PATH

Space required: 4.7MB

Description

Position your mouse over a component to see its description.

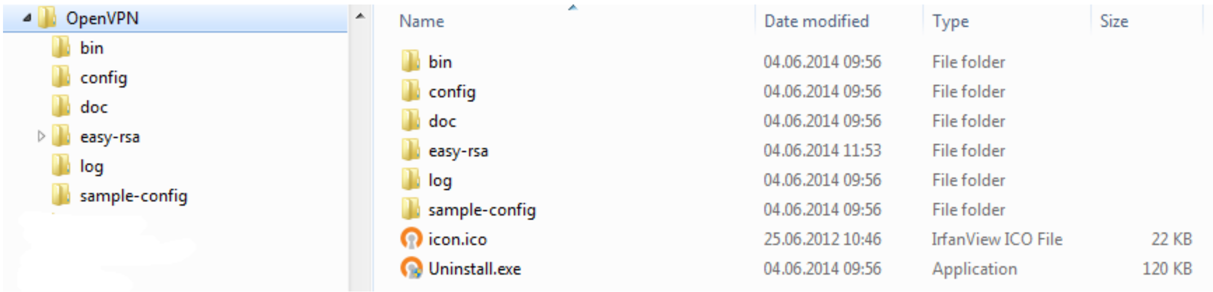
Nullsoft Install System v2.46-101

3. Check the "OpenVPN RSA Certificate Management Scripts", select Next > and continue the setup wizard.

   ▶ *If a Windows log test warning is displayed, confirm it.*

4. Click on Finish upon completion of the installation.

   ✓ The OpenVPN GUI, the SSL software and the programs for creating the certificates and keys are now in the specified directories (default: C:\Program Files\OpenVPN\).



Name	Date modified	Type	Size
bin	04.06.2014 09:56	File folder	
config	04.06.2014 09:56	File folder	
doc	04.06.2014 09:56	File folder	
easy-rsa	04.06.2014 11:53	File folder	
log	04.06.2014 09:56	File folder	
sample-config	04.06.2014 09:56	File folder	
icon.ico	25.06.2012 10:46	IrfanView ICO File	22 KB
Uninstall.exe	04.06.2014 09:56	Application	120 KB

✓ You have successfully installed the OpenVPN package on your PC and completed the provisions with this.

■ Initialising the OpenVPN Package on a Windows PC

How to initialise the OpenVPN package upon installation to be able to generate a certificate structure later.

➜ The OpenVPN package (version 2.0.9 or higher) is installed.

1. Open the command prompt as administrator (right-click on Start menu → All Programs → Accessories → Command Prompt and select "Run as administrator").

   ⓘ *It is necessary for further proceeding that you run the command prompt always as administrator!*

2. Change to the "easy-rsa" directory of the OpenVPN installation.

   ```
   D:\>c:
   C:\>cd program files\openvpn\easy-rsa
   ```

3. Start the batch file "init-config.bat" to to initialise the OpenVPN package

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

   ✓ You have initialised the OpenVPN package with this and are able to start with generating a certificate structure.

Presettings in the Batch Files

You'll later use several batch files for creating the keys and certificates in the "C:\Program Files\OpenVPN" directory.

Make the following presettings for the quick and accurate creation of key and certificate files:

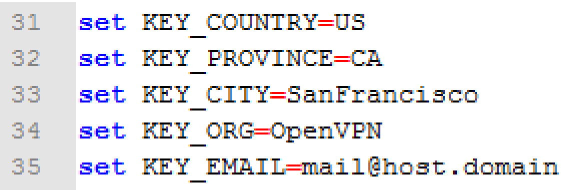
- **Editing the Presettings in "vars.bat"**
- **Specifying the Validity Period in "build-ca.bat"**
- **Specifying the Validity Period in "build-key-server.bat"**
- **Specifying the Validity Period in "build-key.bat"**

■ Editing the Presettings in "vars.bat"

The environment variables (KEY parameters) for the following batch files are defined by starting "vars.bat".

The KEY parameters must be identical in the complete certificate structure. It is therefore urgently recommended to do a one-time adjustment of the default values in "vars.bat" for your purposes to avoid typos and ease the complete process.

The following KEY parameters are set by default:



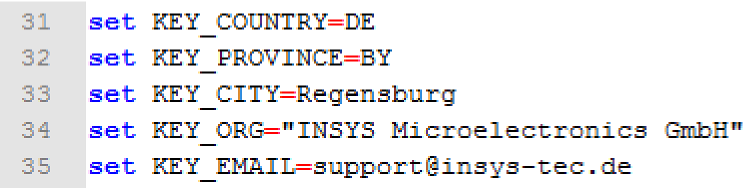
```
31  set KEY_COUNTRY=US
32  set KEY_PROVINCE=CA
33  set KEY_CITY=SanFrancisco
34  set KEY_ORG=OpenVPN
35  set KEY_EMAIL=mail@host.domain
```

Edit the file with a text editor as described in the following.

ⓘ *Text editor like "Notepad++" with syntax highlighting for example*

→ The OpenVPN packet (version 2.3.3 or higher) from the INSYS website (www.insys-icom.com/driver) is installed and ready for operation.

1. Create a backup copy of the file "vars.bat" in the directory "C:\Program Files\OpenVPN\easy-rsa".
2. Edit in "vars.bat" the lines 31 to 35, as shown in the following example.



```
31  set KEY_COUNTRY=DE
32  set KEY_PROVINCE=BY
33  set KEY_CITY=Regensburg
34  set KEY_ORG="INSYS Microelectronics GmbH"
35  set KEY_EMAIL=support@insys-tec.de
```

ⓘ *The maximum length of the default values is:*
2 characters for "KEY_COUNTRY"
e. g. two-digit country code as per ISO 3166-1 (alpha 2-Code)
64 characters for "KEY_PROVINCE"
64 characters for "KEY_CITY"
64 characters for "KEY_ORG"
40 characters for "KEY_EMAIL"

ⓘ *Use quotes for default values with blanks like for "INSYS MICROELECTRONIS GmbH".*
Capitalization is not ignored.

3. Save your modifications.

ⓘ *If you cannot save the edited file under Windows 7, save it to a different destination and copy it to the respective directory.*

✓ Editing of the default settings in "vars.bat" is completed with this.

■ Specifying the Validity Period in "build-ca.bat"

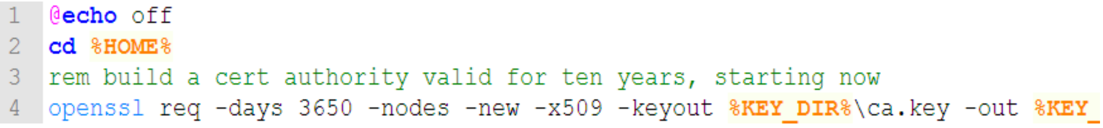
The batch file "build-ca.bat" described elsewhere in this guide generates an RSA key with a validity of 10 years for a CA by default. This validity period is controlled by the OpenSSL parameter "-days 3650".

▶ *Edit the file "build-ca.bat" if you want to modify the validity period of the generated keys and certificates.. Otherwise, proceed with the next section.*

Edit the file with a text editor, like Notepad++ for example, as described in the following.

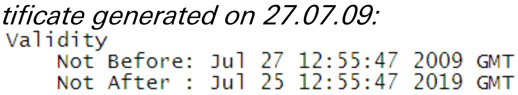
→ The OpenVPN packet (version 2.3.3 or higher) from the INSYS website (www.insys-icom.com/driver) is installed and ready for operation.

1. Create a backup copy of the file "build-ca.bat" in the directory "C:\Program Files\OpenVPN\easy-rsa".
2. Edit in "build-ca.bat" in line 4 the value of the parameter "-days".



```
1  @echo off
2  cd %HOME%
3  rem build a cert authority valid for ten years, starting now
4  openssl req -days 3650 -nodes -new -x509 -keyout %KEY_DIR%\ca.key -out %KEY_
```

ⓘ *The value represents the validity period in days from the date of generation and is between 1 and x. Due to calender exceptions (leap years, days in February), 3650 days are not exactly 10 years, as it is obvious from the certificate generated on 27.07.09:*



```
Validity
    Not Before: Jul 27 12:55:47 2009 GMT
    Not After : Jul 25 12:55:47 2019 GMT
```

ⓘ *If you want to revoke a certificate later, because an employee or device retires for example, you can use the "Certificate Revocation List" from firmware version 2.1.0. This is a file, which contains the revoked certificates issued to certain root certificate.*

3. Save your modifications.

✓ Editing of the validity period in "build-ca.bat" is completed with this.

■ Specifying the Validity Period in "build-key-server.bat"

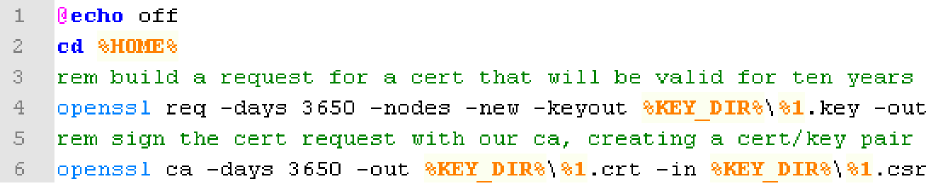
The batch file "build-key-server.bat" described elsewhere in this guide generates an RSA key with a validity of 10 years for a server by default. This validity period is controlled by the OpenSSL parameter "-days 3650".

▶ *Edit the file "build-key-server.bat" if you want to modify the validity period of the generated keys and certificates.. Otherwise, proceed with the next section.*

Edit the file with a text editor, like Notepad++ for example, as described in the following.

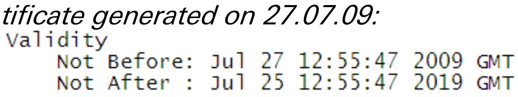
→ The OpenVPN packet (version 2.3.3 or higher) from the INSYS website (www.insys-icom.com/driver) is installed and ready for operation.

1. Create a backup copy of the file "build-key-server.bat" in the directory "C:\Program Files\OpenVPN\easy-rsa".
2. Edit in "build-key-server.bat" in line 4 and line 6 the value of the parameter "-days".



```
1  @echo off
2  cd %HOME%
3  rem build a request for a cert that will be valid for ten years
4  openssl req -days 3650 -nodes -new -keyout %KEY_DIR%\%1.key -out
5  rem sign the cert request with our ca, creating a cert/key pair
6  openssl ca -days 3650 -out %KEY_DIR%\%1.crt -in %KEY_DIR%\%1.csr
```

ⓘ *The value represents the validity period in days from the date of generation and is between 1 and x. Due to calender exceptions (leap years, days in February), 3650 days are not exactly 10 years, as it is obvious from the certificate generated on 27.07.09:*



```
Validity
    Not Before: Jul 27 12:55:47 2009 GMT
    Not After : Jul 25 12:55:47 2019 GMT
```

ⓘ *If you want to revoke a certificate later, because an employee or device retires for example, you can use the "Certificate Revocation List" from firmware version 2.1.0. This is a file, which contains the revoked certificates issued to certain root certificate.*

3. Save your modifications.

✓ Editing of the validity period in "build-key-server.bat" is completed with this.

■ Specifying the Validity Period in "build-key.bat"

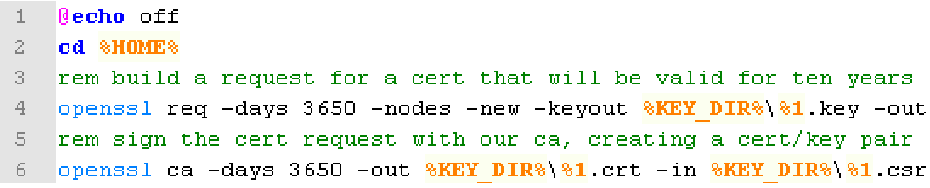
The batch file "build-key.bat" described elsewhere in this guide generates an RSA key with a validity of 10 years for a client by default. This validity period is controlled by the OpenSSL parameter "-days 3650".

▶ *Edit the file "build-key.bat" if you want to modify the validity period of the generated keys and certificates.. Otherwise, proceed with the next section.*

Edit the file with a text editor, like Notepad++ for example, as described in the following.

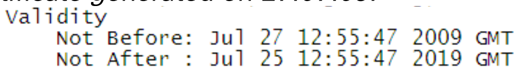
→ The OpenVPN packet (version 2.3.3 or higher) from the INSYS website (www.insys-icom.com/driver) is installed and ready for operation.

1. Create a backup copy of the file "build-key.bat" in the directory "C:\Program Files\OpenVPN\easy-rsa".
2. Edit in "build-key.bat" in line 4 and line 6 the value of the parameter "-days".



```
1  @echo off
2  cd %HOME%
3  rem build a request for a cert that will be valid for ten years
4  openssl req -days 3650 -nodes -new -keyout %KEY_DIR%\%1.key -out
5  rem sign the cert request with our ca, creating a cert/key pair
6  openssl ca -days 3650 -out %KEY_DIR%\%1.crt -in %KEY_DIR%\%1.csr
```

ⓘ *The value represents the validity period in days from the date of generation and is between 1 and x. Due to calender exceptions (leap years, days in February), 3650 days are not exactly 10 years, as it is obvious from the certificate generated on 27.07.09:*



```
Validity
    Not Before: Jul 27 12:55:47 2009 GMT
    Not After : Jul 25 12:55:47 2019 GMT
```

ⓘ *If you want to revoke a certificate later, because an employee or device retires for example, you can use the "Certificate Revocation List" from firmware version 2.1.0. This is a file, which contains the revoked certificates issued to certain root certificate.*

3. Save your modifications.

   ✓ Editing of the validity period in "build-key.bat" is completed with this.

3.2 Creating Certificates

Creating a Certificate Structure Under Windows

A Public Key Infrastructure (PKI) comprises services for encryption and digital signature on the basis of public key procedures.

First, the files for the CA (Certification Authority) are generated. Then, a key pair is generated for the server and each client. One key pair for both clients (participants) is necessary for setting up an IPsec connection. These key pairs will be uploaded to the devices later.

Moreover, it is possible to create a Certificate Revocation List (CRL) for OpenVPN, which contains the revoked certificates. If certificates have to be revoked before their expiry (due to misuse for example), they can be entered into this list. Every updated list must then be uploaded to the device, which acts as OpenVPN server.

ⓘ *A Certificate Revocation List can not be uploaded to MoRoS 1.x and is not essential for setting up an OpenVPN network with certificate-based authentication.*

You will need the following files for setting up an OpenVPN network with certificate-based authentication:

For the OpenVPN server:

Diffie-Hellman parameter set (e.g. dh1024.pem)

CA certificate (e.g. ca.crt)

Server certificate (e.g. server.crt)

Server key (e.g. server.key)

For each OpenVPN client (1-n):

CA certificate (e.g. ca.crt)

Client certificate (e.g. client1.crt)

Client key (e.g. client1.key)

ⓘ *A separate pair of certificate and key is necessary for each OpenVPN client.*

ⓘ *The respective keys are secret and may only be known by the related OpenVPN participant besides the issuing CA. The CA key is essential for the security of the OpenVPN network and must be kept top secret by the CA.*

You will need the following files for setting up an IPsec connection with certificate-based authentication:

For each of both IPsec participants:

CA certificate (e.g. ca.crt)

Participant certificate (e.g. peer1.crt)

Participant key (e.g. peer1.key)

ⓘ *The respective keys are secret and may only be known by the related VPN participant besides the issuing CA. The CA key is essential for the security of the VPN network and must be kept top secret by the CA.*

Generate the files in the sequence of the following sections:

- **Preparing Key Directory**
- **Generating Diffie-Hellman Parameters for a Server (if required)**
- **Generating CA Certificate and Key**
- **Generating Certificate and Key for a Server**
- **Generating Certificate and Key for a Client**
- **Revoking a Certificate and Generating a Certificate Revocation List (if required)**

Preparing Key Directory

How to delete the complete content of the subdirectory "C:\Program Files\OpenVPN\easy-rsa\keys".

ⓘ *Save possibly existing files from other projects in this directory if you still need them.*

→ The OpenVPN package (version 2.3.3 or higher) is installed.

1. Open the command prompt as administrator (right-click on Start menu → All Programs → Accessories → Command Prompt and select "Run as administrator").

   ⓘ *It is necessary for further proceeding that you run the command prompt always as administrator!*

2. Change to the "easy-rsa" directory of the OpenVPN installation.

```
D:\>c:
C:\>cd program files\openvpn\easy-rsa
```

3. Start the batch file "vars.bat" for setting the environment variables and default values.

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

4. Start the batch file "clean-all.bat" to prepare the subdirectory "C:\Programme\OpenVPN\easy-rsa\keys"

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

   ⓘ *The batch file "clean-all.bat" deletes the complete content of the "C:\Program Files\OpenVPN\easy-rsa\keys" directory.*

   ✓ The two files with the name "index.txt" and "serial" with a file size of approx. 0 and 1 kb are now in the subdirectory "C:\Program Files\OpenVPN\easy-rsa\keys". "index.txt" is empty and "serial" contains "01" as default value for the consecutive numbering of the PEM files and will be incremented by 1 with each generated PEM file; see section "Generating Certificate and Key for a Server".

■ Generating Diffie-Hellman Parameters for a Server

How to generate the Diffie-Hellman parameters. Generating the parameters can take several minutes, depending on the processing power of the PC.

▶ *A Diffie-Hellmann parameter set is already loaded in the default state of an INSYS router. Execute the following steps if you want to generate a new parameter set. Otherwise, you can skip this section.*

ⓘ *Diffie-Hellman parameters are only used by the OpenVPN server, not by the OpenVPN clients.*

→ The OpenVPN package (version 2.3.3 or higher) is installed.

1. Open the command prompt as administrator (right-click on Start menu → All Programs → Accessories → Command Prompt and select "Run as administrator").

   ⓘ *It is necessary for further proceeding that you run the command prompt always as administrator!*

2. Change to the "easy-rsa" directory of the OpenVPN installation.

```
D:\>c:
C:\>cd program files\openvpn\easy-rsa
```

3. Start the batch file "vars.bat" for setting the environment variables and default values.

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

4. Start the batch file "build--dh.bat" to generate the Diffie-Hellmann parameters

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

   ✓ The following dialogue is displayed during generation:

```
Loading 'screen' into random state - done
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
............................................................+....
...+........................................................+....
.+...............................................+...............
........................+.........++*++*++*
C:\Program Files\OpenVPN\easy-rsa>
```

   ✓ The Diffie-Hellmann parameter generation is completed with this. The file "dh1024.pem" is now in the subdirectory "C:\Program Files\OpenVPN\easy-rsa\keys".

■ Generating CA Certificate and Key

How to generate the certificate structure of your own certification authority (CA). The CA certificate structure consists of the two files "ca.key" (secret key) and "ca.crt" (public certificate).

→ The OpenVPN package (version 2.3.3 or higher) is installed.

→ The default values in "vars.bat" are modified.

→ The validity period is defined; default entry is 3650 days = 10 years.

1. Check the time and date setting of the PC

ⓘ *Certificates have an expiry date. A wrong system time (time and date) is a frequent failure source. Therefore, ensure that the system time of the PC and the INSYS router is correct when creating as well as commissioning the VPN server or clients.*

2. Open the command prompt as administrator (right-click on Start menu → All Programs → Accessories → Command Prompt and select "Run as administrator").

   ⓘ *It is necessary for further proceeding that you run the command prompt always as administrator!*

3. Change to the "easy-rsa" directory of the OpenVPN installation.

```
D:\>c:
C:\>cd program files\openvpn\easy-rsa
```

4. Start the batch file "vars.bat" for setting the environment variables and default values:

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

   ⓘ *The environment variables are valid as long as the command prompt window is open. "vars.bat" must be executed again if the DOS window has been closed in the meantime.*

5. Start the batch file "build-ca".bat" to generate the public CA certificate "ca.crt" and the secret key "ca.key":

```
C:\Program Files\OpenVPN\easy-rsa>build-ca
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
...........................++++++
..++++++
writing new private key to 'keys\ca.key'
-----
```

   ✓ The RSA key has been created.
   A file with the name "ca.key" and a file size of 0 kb is now in the subdirectory "C:\Program Files\OpenVPN\easy-rsa\keys".

   ⓘ *The file names "ca.crt" and "ca.key" are fixed. A later modification leads to a function loss!*

   ⓘ *The server is identified with the following information. All information must be identical for all certificates within a certificate structure except the "Common Name"! The "Common Name" must be different for all certificates!*

   ✓ You are now prompted to confirm your presettings, like "[DE]":

```
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) [DE]:
State or Province Name (full name) [BY]:
Locality Name (eg, city) [Regensburg]:
Organization Name (eg, company) ["INSYS MICROELECTRONICS GmbH"]:
Organizational Unit Name (eg, section) [changeme]:
```

6. Confirm your presettings with Enter.
   The value for "Organizational Unit Name" can be left empty.

   ✓ You will now be prompted to enter a "Common Name".

```
Common Name (eg, your name or your server's hostname) []:ca
```

ⓘ *This field may never be empty. With this information, the server will later distinguish the various clients and client networks. The "Common Name" must be biunique in the complete certificate structure and have a maximum length of 63 characters.*

ⓘ *Replace blanks with underscores, like for example "VPN_HOSTNAME". Observe the capitalization and preferably use only one of these possibilities consistently. Do not use country-specific characters like umlauts.*

7. Use as "Common Name" e.g. "ca".

   ✓ You will now be prompted to enter a Name.

```
Name [changeme]:
```

8. Confirm your presetting with Enter.
   The value for "Name" can be left empty.

   ✓ You are now prompted to confirm your preset e-mail address

```
Email Address [support@insys-tec.de]:
```

9. Confirm your presetting with Enter.

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

✓ The CA certificate structure generation is completed with this.
The two files with the name "ca.key" and "ca.crt" with a file size of approx. 1 to 2 kb are now in the subdirectory "C:\Program Files\OpenVPN\easy-rsa\keys".

Appendix: Content of the command prompt window (process of the scripts)

ⓘ *Your inputs are highlighted in blue.*

```
D:\>c:
C:\>cd program files\openvpn\easy-rsa
C:\Program Files\OpenVPN\easy-rsa>vars
C:\Program Files\OpenVPN\easy-rsa>build-ca
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) [DE]:
State or Province Name (full name) [BY]:
Locality Name (eg, city) [Regensburg]:
Organization Name (eg, company) ["INSYS MICROELECTRONICS GmbH"]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) []:ca
Name [changeme]:
Email Address [support@insys-tec.de]:
C:\Program Files\OpenVPN\easy-rsa>
```

■ Generating Certificate and Key for a Server

How to generate the private key (e.g. server.key) and the public certificate (e.g. server.crt) for a server.

A "Common Name" is required for the generation. The "Common Name" is the unique member name of a VPN participant in the secured network and is used for routing into the client networks for example. The "Common Name" must only be used for one participant and cannot be changed any more after the generation. Observe the capitalization for the "Common Name" and preferably use upper or lower case consistently.

The same entry for "file name" and "Common Name" is recommended. Your benefit: You can already tell the "Common Name" of the certificate by the file name. Select different entries if this is to be disguised due to security reasons.

ⓘ *The maximum length of the "Common Name" is 29 characters for all INSYS routers (15 characters for MoRoS 1.3).*

ⓘ *The content of the command prompt window A(process of the scripts) is shown completely as appendix at the end of this section.*

→ The OpenVPN package (version 2.3.3 or higher) is installed.

→ The CA certificate structure is generated (files "ca.key" and "ca.crt").

→ The default values in "vars.bat" must definitely be the same as for the generation of the CA certificate structure!

→ The file name is "server" in this example; the "Common Name" is also "server".

1. Check the time and date setting of the PC

   ⓘ *Certificates have an expiry date. A wrong system time (time and date) is a frequent failure source. Therefore, ensure that the system time of the PC and the INSYS router is correct when creating as well as commissioning the server or clients.*

2. Open the command prompt as administrator (right-click on Start menu → All Programs → Accessories → Command Prompt and select "Run as administrator").

   ⓘ *It is necessary for further proceeding that you run the command prompt always as administrator!*

3. Change to the "easy-rsa" directory of the OpenVPN installation.

```
D:\>c:
C:\>cd program files\openvpn\easy-rsa
```

4. Start the batch file "vars.bat" for setting the environment variables and default values:

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

   ⓘ *The environment variables are valid as long as the command prompt window is open. "vars.bat" must be executed again if the DOS window has been closed in the meantime.*

5. Start the batch file "build--key--server.bat" to generate certificate and key and enter as parameter the desired file name, e.g. "server":

```
C:\Program Files\OpenVPN\easy-rsa>build-key-server server
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.
-----
```

✓ One file has been created.
The file "server.key" with a file size of 0 kb is now in the subdirectory "C:\Program Files\OpenVPN\easy-rsa\keys".

✓ You are now prompted to confirm your presettings, like "[DE]".

ⓘ *Each participant in the VPN network is identified with the information "Country Name", "State or Province Name", "Locality Name", "Organization Name", "Organizational Unit Name" among others for example when establishing a connection.*
Therefore, this information (DN, Distinguished Names) must be identical for all certificates within a VPN network!
In order to avoid mistakes and speed up the process, you have already specified the default values in the file "vars.bat" before creating the certification authority (CA).

6. Confirm your presettings with Enter.
   The value for "Organizational Unit Name" can be left empty.

```
Country Name (2 letter code) [DE]:
State or Province Name (full name) [BY]:
Locality Name (eg, city) [Regensburg]:
Organization Name (eg, company) ["INSYS MICROELECTRONICS GmbH"]:
Organizational Unit Name (eg, section) [changeme]:
```

✓ You will now be prompted to enter a "Common Name".

ⓘ *This field may never be empty!*

```
Common Name (eg, your name or your server's hostname) []:
```

ⓘ *Replace blanks with underscores. Observe the capitalization and preferably use only one of these possibilities consistently. Do not use country-specific characters like umlauts. Don't use more than 29 characters to ensure compatibility with all INSYS routers (15 characters for MoRoS 1.3).*

7. Use in this example as "Common Name" e.g. "server".

```
Common Name (eg, your name or your server's hostname) []:server
```

✓ You will now be prompted to enter a Name.

```
Name [changeme]:
```

8. Confirm your presetting with Enter.
   The value for "Name" can be left empty.

✓ You are now prompted to confirm your preset e-mail address

```
Email Address [support@insys-tec.de]:
```

9. Confirm your presetting with Enter.

✓ You are now prompted to make further specifications:

ⓘ *The value for "challenge password" must remain empty that the VPN tunnel can be established automatically!*
The value for "optional company name" can be left empty.

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

10. Confirm the empty presettings with Enter.

✓ You are prompted to sign the certificate after checking and summarising the specifications:

```
Using configuration from openssl.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:'DE'
stateOrProvinceName   :PRINTABLE:'BY'
localityName          :PRINTABLE:'Regensburg'
organizationName      :T61STRING:'"INSYS MICROELECTRONICS GmbH"'
organizationalUnitName:PRINTABLE:'changeme'
commonName            :PRINTABLE:'server'
name                  :PRINTABLE:'changeme'
emailAddress          :IA5STRING:'support@insys-tec.de'
Certificate is to be certified until Jul 26 14:34:31 2019 GMT (3650 days)
Sign the certificate? [y/n]:y
```

✓ Three files have been created up to now.
The files "server.key" and "server.csr" each with a file size of 1 kb and the file "server.crt" with a file size of 0 kb are now in the subdirectory "C:\Program Files\OpenVPN\easy-rsa\keys".

11. Confirm with y.

✓ You are now prompted to confirm your own certificate request:

```
1 out of 1 certificate requests certified, commit? [y/n]y
```

12. Confirm with y.

```
Write out database with 1 new entries
Data Base Updated
```

✓ The certificate has been created and saved as file.
The files "index.txt" and "serial" (database) in the directory "C:\Program Files\OpenVPN\easy-rsa\keys" have been updated.

ⓘ *The updated "database" is the file "serial", which contains a decimal figure, like e.g. "01". This value is increased by 1 with each successful certificate/key generation.*
The file "index.txt" contains now an entry in the form:
V   190726143431Z   01   unknown   /C=DE/ST=BY/O="INSYS MICROELECTRONICS GmbH"/CN=server/emailAddress=support@insys-tec.de. The entry "190726143431" is the date from which the certificate is invalid here: 2019/07/26 from 14:34:31. The Common Name specified by you is indicated for CN, here "server". The following value "01" is the sequence number of the PEM file; see below

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

✓ The generation of the secret key and the public certificate for a server is completed with this.
The four new files "server.key", "server.crt", "server.csr" and "01.pem" with a file size of approx. 1 to 4 kb are now in the subdirectory "C:\Program Files\OpenVPN\easy-rsa\keys".

ⓘ *The CSR file, here "server.csr", is not required for the purposes described here. CSR stands for "Certificate Signing Request". You can easily delete the file "server.csr" since you are your own certification authority with OpenSSL and have confirmed your certificate request yourself. This would only be necessary, if you would request the certification from a foreign certification authority (CA); you would send the file "x.csr" to the certification authority and receive a certified "x.crt" again.*

ⓘ *The PEM file, here "01.pem", is not required for the purposes described here. A PEM file is a Base64-encoded certificate. The file is enumerated consecutively, e.g "01.pem" etc. and is a copy of the issued certificate, in this example of "server.crt". OpenSSL keeps an account about the issued certificates in the file "index.txt".*

Appendix: Content of the command prompt window (process of the scripts)

ⓘ *Your inputs are highlighted in blue.*

```
D:\>c:
C:\>cd program files\openvpn\easy-rsa
C:\Program Files\OpenVPN\easy-rsa>vars
C:\Program Files\OpenVPN\easy-rsa>build-key-server server
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) [DE]:
State or Province Name (full name) [BY]:
Locality Name (eg, city) [Regensburg]:
Organization Name (eg, company) ["INSYS MICROELECTRONICS GmbH"]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) []:server
Name [changeme]:
Email Address [support@insys-tec.de]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl.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:'DE'
stateOrProvinceName   :PRINTABLE:'BY'
localityName          :PRINTABLE:'Regensburg'
organizationName      :T61STRING:'"INSYS MICROELECTRONICS GmbH"'
organizationalUnitName:PRINTABLE:'changeme'
commonName            :PRINTABLE:'server'
name                  :PRINTABLE:'changeme'
emailAddress          :IA5STRING:'support@insys-tec.de'
Certificate is to be certified until Jul 28 14:03:36 2019 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>
```

■ Generating Certificate and Key for a Client

How to generate the private key (e.g. client1.key) and the public certificate (e.g. client1.crt) for a client.

A "Common Name" is required for the generation. The "Common Name" is the unique member name of a VPN participant in the secured network and is used for routing into the client networks for example. The "Common Name" must only be used for one participant and cannot be changed any more after the generation. Observe the capitalization for the "Common Name" and preferably use upper or lower case consistently.

The same entry for "file name" and "Common Name" is recommended. Your benefit: You can already tell the "Common Name" of the certificate by the file name. Select different entries if this is to be disguised due to security reasons.

ⓘ *The maximum length of the "Common Name" is 29 characters for all INSYS routers (15 characters for MoRoS 1.3).*

ⓘ *The content of the command prompt window A(process of the scripts) is shown completely as appendix at the end of this section.*

→ The OpenVPN package (version 2.3.3 or higher) is installed.

→ The CA certificate structure is generated (files "ca.key" and "ca.crt").

→ The default values in "vars.bat" must definitely be the same as for the generation of the CA certificate structure!

→ The file name is "client1" in this example; the "Common Name" is also "client1".

1. Check the time and date setting of the PC

   ⓘ *Certificates have an expiry date. A wrong system time (time and date) is a frequent failure source. Therefore, ensure that the system time of the PC and the INSYS router is correct when creating as well as commissioning the server or clients.*

2. Open the command prompt as administrator (right-click on Start menu → All Programs → Accessories → Command Prompt and select "Run as administrator").

   ⓘ *It is necessary for further proceeding that you run the command prompt always as administrator!*

3. Change to the "easy-rsa" directory of the OpenVPN installation.

```
D:\>c:
C:\>cd program files\openvpn\easy-rsa
```

4. Start the batch file "vars.bat" for setting the environment variables and default values:

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

   ⓘ *The environment variables are valid as long as the command prompt window is open. "vars.bat" must be executed again if the DOS window has been closed in the meantime.*

5. Start the batch file "build--key.bat" to generate certificate and key and enter as parameter the desired file name, e.g. "client1":

```
C:\Program Files\OpenVPN\easy-rsa>build-key client1
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
..........++++++
.........++++++
writing new private key to 'keys\client1.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.
-----
```

▶ *Starting with version 2.1.1 of the OpenVPN package, you can alternatively start the batch file "build-key-pkcs12" here. A PKCS12 container with CA certificate as well as certificate and key of the client will be created with this. The further proceeding is the same as in this description. It is possible at the end to protect the container with a password. PKCS12 containers cannot be uploaded to MoRoS 1.x. Entering a password is only possible from FW 2.3.0.*

✓ One file has been created.
The file "client1.key" with a file size of 0 kb is now in the subdirectory "C:\Program Files\OpenVPN\easy-rsa\keys".

✓ You are now prompted to confirm your presettings, like "[DE]".

ⓘ *Each participant in the VPN network is identified with the information "Country Name", "State or Province Name", "Locality Name", "Organization Name", "Organizational Unit Name" among others for example when establishing a connection.*
Therefore, this information (DN, Distinguished Names) must be identical for all certificates within a VPN network!
In order to avoid mistakes and speed up the process, you have already specified the default values in the file "vars.bat" before creating the certification authority (CA).

6. Confirm your presettings with Enter.
   The value for "Organizational Unit Name" can be left empty.

```
Country Name (2 letter code) [DE]:
State or Province Name (full name) [BY]:
Locality Name (eg, city) [Regensburg]:
Organization Name (eg, company) ["INSYS MICROELECTRONICS GmbH"]:
Organizational Unit Name (eg, section) [changeme]:
```

✓ You will now be prompted to enter a "Common Name".

ⓘ *This field may never be empty!*

```
Common Name (eg, your name or your server's hostname) []:
```

ⓘ *Replace blanks with underscores. Observe the capitalization and preferably use only one of these possibilities consistently. Do not use country-specific characters like umlauts. Don't use more than 29 characters to ensure compatibility with all INSYS routers (15 characters for MoRoS 1.3).*

7. Use in this example as "Common Name" e.g. "client1".

```
Common Name (eg, your name or your server's hostname) []:client1
```

✓ You will now be prompted to enter a Name.

```
Name [changeme]:
```

8. Confirm your presetting with Enter.
   The value for "Name" can be left empty.

✓ You are now prompted to confirm your preset e-mail address

```
Email Address [support@insys-tec.de]:
```

9. Confirm your presetting with Enter.

✓ You are now prompted to make further specifications:

ⓘ *The value for "challenge password" must remain empty that the VPN tunnel can be established automatically!*
The value for "optional company name" can be left empty.

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

10. Confirm the empty presettings with Enter.

✓ Your specifications are checked and summarised now:

```
Using configuration from openssl.cnf
Loading 'screen' into random state - done
DEBUG[load_index]: unique_subject = "yes"
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'DE'
stateOrProvinceName   :PRINTABLE:'BY'
localityName          :PRINTABLE:'Regensburg'
organizationName      :T61STRING:'"INSYS MICROELECTRONICS GmbH"'
organizationalUnitName:PRINTABLE:'changeme'
commonName            :PRINTABLE:'client1'
name                  :PRINTABLE:'changeme'
emailAddress          :IA5STRING:'support@insys-tec.de'
Certificate is to be certified until Jul 28 16:10:24 2019 GMT (3650 days)
Sign the certificate? [y/n]:y
```

✓ Three files have been created up to now.
The files "client1.key" and "client1.csr" each with a file size of 1 kb and the file "client1.crt" with a file size of 0 kb are now in the subdirectory "C:\Program Files\OpenVPN\easy-rsa\keys".

11. Confirm the prompt for signing the certificate with y.

✓ You are now prompted to confirm your own certificate request:

```
1 out of 1 certificate requests certified, commit? [y/n]y
```

12. Confirm with y.

```
Write out database with 1 new entries
Data Base Updated
```

✓ The certificate has been created and saved as file.
The files "index.txt" and "serial" (database) in the directory "C:\Program Files\OpenVPN\easy-rsa\keys" have been updated.

ⓘ *The updated "database" is the file "serial", which contains a decimal figure, like e.g. "02". This value is increased by 1 with each successful certificate/key generation.*
The file "index.txt" contains now a second entry in the form:
V 190728161024Z 02 unknown /C=DE/ST=BY/O="INSYS MICROELECTRONICS GmbH"/CN=client1/emailAddress=support@insys-tec.de. The entry "190728161024" is the date from which the certificate is invalid here: 2019/07/28 from 16:10:24. The Common Name specified by you is indicated for CN, here "client1". The following value "01" is the sequence number of the PEM file; see below

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

✓ The generation of the secret key and the public certificate for a client is completed with this.

▶ *If you have started the batch file "build-key-pkcs12" alternatively, you must specify a password for the PKCS12 container at this stage. No password will be applied if you complete the command prompt without entering a password. Entering a password is only possible from FW 2.3.0.*

ⓘ *You only have to repeat the steps in this section for generating a certificate and key for another client. The proceeding for generating certificates and keys for a CA or server must not be repeated.*

✓ The four new files "client1.key", "client1.crt", "client1.csr" and "02.pem" with a file size of approx. 1 to 4 kb are now in the subdirectory "C:\Program Files\OpenVPN\easy-rsa\keys".

ⓘ *The CSR file, here "client1.csr", is not required for the purposes described here. CSR stands for "Certificate Signing Request". You can easily delete the file "client1.csr" since you are your own certification authority with OpenSSL and have confirmed your certificate request yourself. This would only be necessary, if you would request the certification from a foreign certification authority (CA); you would send the file "x.csr" to the certification authority and receive a certified "x.crt" again.*

▶ *If you have started the batch file "build-key-pkcs12" alternatively, a file "client1.p12" has been created. This PKCS12 container contains the CA certificate as well as certificate and key of the client. You can upload the CA certificate as well as certificate and key of the client in one go with this.*

ⓘ *The PEM file, here "02.pem", is not required for the purposes described here. A PEM file is a Base64-encoded certificate. The file is enumerated consecutively, e.g "01.pem" etc. and is a copy of the issued certificate, in this example of "client1.crt". OpenSSL keeps an account about the issued certificates in the file "index.txt".*

Appendix: Content of the command prompt window (process of the scripts)

Your inputs are highlighted in blue.

```
D:\>c:
C:\>cd program files\openvpn\easy-rsa
C:\Program Files\OpenVPN\easy-rsa>vars
C:\Program Files\OpenVPN\easy-rsa>build-key client1
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
...........++++++
.........++++++
writing new private key to 'keys\client1.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) [DE]:
State or Province Name (full name) [BY]:
Locality Name (eg, city) [Regensburg]:
Organization Name (eg, company) ["INSYS MICROELECTRONICS GmbH"]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) []:client1
Name [changeme]:
Email Address [support@insys-tec.de]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl.cnf
Loading 'screen' into random state - done
DEBUG[load_index]: unique_subject = "yes"
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'DE'
stateOrProvinceName   :PRINTABLE:'BY'
localityName          :PRINTABLE:'Regensburg'
organizationName      :T61STRING:'"INSYS MICROELECTRONICS GmbH"'
organizationalUnitName:PRINTABLE:'changeme'
commonName            :PRINTABLE:'client1'
name                  :PRINTABLE:'changeme'
emailAddress          :IA5STRING:'support@insys-tec.de'
Certificate is to be certified until Jul 28 16:10:24 2019 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>
```

■ Revoking a Certificate and Generating a Certificate Revocation List (if required)

How to revoke a certificate before its expiry date (due to misuse for example) and generate a Certificate Revocation List.

ⓘ *A Certificate Revocation List cannot be uploaded to MoRoS 1.x and is not essential for setting up an OpenVPN network with certificate-based authentication.*

→ The OpenVPN package (version 2.3.3 or higher) is installed.

→ The CA certificate structure is generated (files "ca.key" and "ca.crt").

→ Client or server certificates have already been created.

→ The default values in "vars.bat" must definitely be the same as for the generation of the CA certificate structure and the certificates!

1. Open the command prompt as administrator (right-click on Start menu → All Programs → Accessories → Command Prompt and select "Run as administrator").

   ⓘ *It is necessary for further proceeding that you run the command prompt always as administrator!*

2. Change to the "easy-rsa" directory of the OpenVPN installation.

```
D:\>c:
C:\>cd program files\openvpn\easy-rsa
```

3. Start the batch file "vars.bat" for setting the environment variables and default values:

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

   ⓘ *The environment variables are valid as long as the command prompt window is open. "vars.bat" must be executed again if the DOS window has been closed in the meantime.*

4. Start the batch file "revoke-full.bat" to revoke a certificate and enter as parameter the Common Name of the certificate to be revoked, e.g. "client1":

```
C:\Program Files\OpenVPN\easy-rsa>revoke-full client1
Using configuration from openssl.cnf
Revoking Certificate 02.
Data Base Updated
...
certificate revoked
```

   ✓ The Certificate Revocation List, that contains all certificates of this CA revoked up to now, has been generated or updated, respectively, and saved as file.
   The file "crl.pem" with a file size of 1 kb is now in the subdirectory "C:\Program Files\OpenVPN\easy-rsa\keys".

4 Used Components

Software

Description	Manufacturer	Type	Version
OpenVPN package	Open Source	OpenVPN with GUI	2.3.3
Operating system	Microsoft	Windows	7

Table 1: Used software

Notes

Germany

INSYS icom GmbH
Hermann-Köhl-Str. 22
93049 Regensburg
Germany

Phone	+49 941 58692 0
Fax	+49 941 58692 45
E-mail	info@insys-icom.com
URL	www.insys-icom.com

Czech Repulic

INSYS icom CZ, s.r.o.
Slovanská alej 1993 / 28a
326 00 Plzen-Východní Předměstí
Czech Republic

Phone	+420 377 429 952
Fax	+420 377 429 952
Mobile	+420 777 651 188
E-mail	info@insys-icom.cz
URL	www.insys-icom.cz