

VPN mit INSYS-Routern

X509.v3-Zertifikate für VPNs
mit easy-rsa erzeugen

Copyright © 2024 INSYS icom GmbH

Jede Vervielfältigung dieser Publikation ist verboten. Alle Rechte an dieser Publikation und an den Geräten liegen bei INSYS icom GmbH, Regensburg.

Warenzeichen und Firmenzeichen

Die Verwendung eines hier nicht aufgeführten Waren- oder Firmenzeichens ist kein Hinweis auf die freie Verwendbarkeit desselben.

MNP ist ein eingetragenes Warenzeichen von Microcom, Inc.

IBM PC, AT, XT sind Warenzeichen von International Business Machine Corporation.

Windows™ ist ein Warenzeichen von Microsoft Corporation.

Linux ist ein eingetragenes Warenzeichen von Linus Torvalds.

INSYS® ist ein eingetragenes Warenzeichen der INSYS icom GmbH.

Die Prinzipien dieser Publikation können auf ähnliche Kombinationen übertragbar sein. In diesem Fall übernimmt INSYS icom GmbH weder Gewährleistung noch Support. Weiterhin kann nicht ausgeschlossen werden, dass andere als die beabsichtigten und hier beschriebenen Wirkungen oder Ergebnisse erzielt werden, wenn andere, ähnliche Komponenten kombiniert und verwendet werden. INSYS icom GmbH haftet nicht für etwaige, auftretende Schäden.

Herausgeber

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

Telefon +49 941 58692 0
Telefax +49 941 58692 45
E-Mail info@insys-icom.de
URL <http://www.insys-icom.de>

Druck 17. Jan. 2024
Artikel-Nr. -
Version 1.6
Sprache DE

1 Einführung

Allgemein

Die vorliegende Publikation bezieht sich auf eine Kombination von ausgewählten Hard- und Software-Komponenten der INSYS icom GmbH sowie anderer Hersteller. Alle Komponenten wurden mit dem Ziel kombiniert, bestimmte Ergebnisse und Wirkungen für bestimmte Anwendungen im Bereich der professionellen Datenübertragung zu realisieren.

Die genauen Bezeichnungen aller verwendeten Komponenten, auf die sich diese Publikation bezieht, sind in den Tabellen *Hardware*, *Zubehör* und *Software* am Ende dieser Publikation definiert.

Die in dieser Publikation verwendeten Symbole und Formatierungen sind im gleichnamigen Abschnitt im Gerätehandbuch näher erklärt.

Manche Konfigurationen oder Vorbereitungen, die in dieser Publikation vorausgesetzt werden, sind in anderen Publikationen beschrieben. Ziehen Sie daher auch immer die zugehörigen Geräte-Handbücher zu Rate. INSYS-Geräte mit Web-Interface zeigen Ihnen hilfreiche Informationen zu den Konfigurationsmöglichkeiten an, wenn Sie in der Kopfleiste auf „Hilfetexte anzeigen“ klicken.

Ziel dieser Publikation

Zum Aufbau eines VPN-Netzwerks mit zertifikatsbasierter Authentifizierung ist eine entsprechende Zertifikatsstruktur erforderlich.

In dieser Publikation erfahren Sie, wie Sie die dafür notwendigen Schlüssel- und Zertifikatsdateien für Certification Authority (CA, Zertifizierungsstelle), Server und Clients sowie eine optionale Certificate Revocation List (CRL, Zertifikatssperrliste) erzeugen.

Diese Dateien sind notwendig für den Aufbau eines OpenVPN-Netzwerks. Weitere Informationen zu OpenVPN finden Sie unter <http://www.openvpn.eu>.

Für den Aufbau eines VPN-Netzwerks mit IPsec sind nur das CA-Zertifikat und Schlüssel und Zertifikat der jeweiligen Clients erforderlich. Die Zertifikate für einen IPsec-Teilnehmer unterscheiden sich nicht von denen für den OpenVPN-Client. Auf eine gesonderte Beschreibung zum Erstellen von Zertifikaten und Schlüssel für einen IPsec-Teilnehmer wird hier verzichtet.

Folgende Abbildungen skizzieren dabei die Verteilung der verschiedenen Schlüssel und Zertifikate auf die verschiedenen Teilnehmer in den jeweiligen VPN-Netzwerken. Ein Diffie-Hellman-Parametersatz ist bereits werksseitig auf dem INSYS-Router geladen, kann aber auch manuell ersetzt werden.

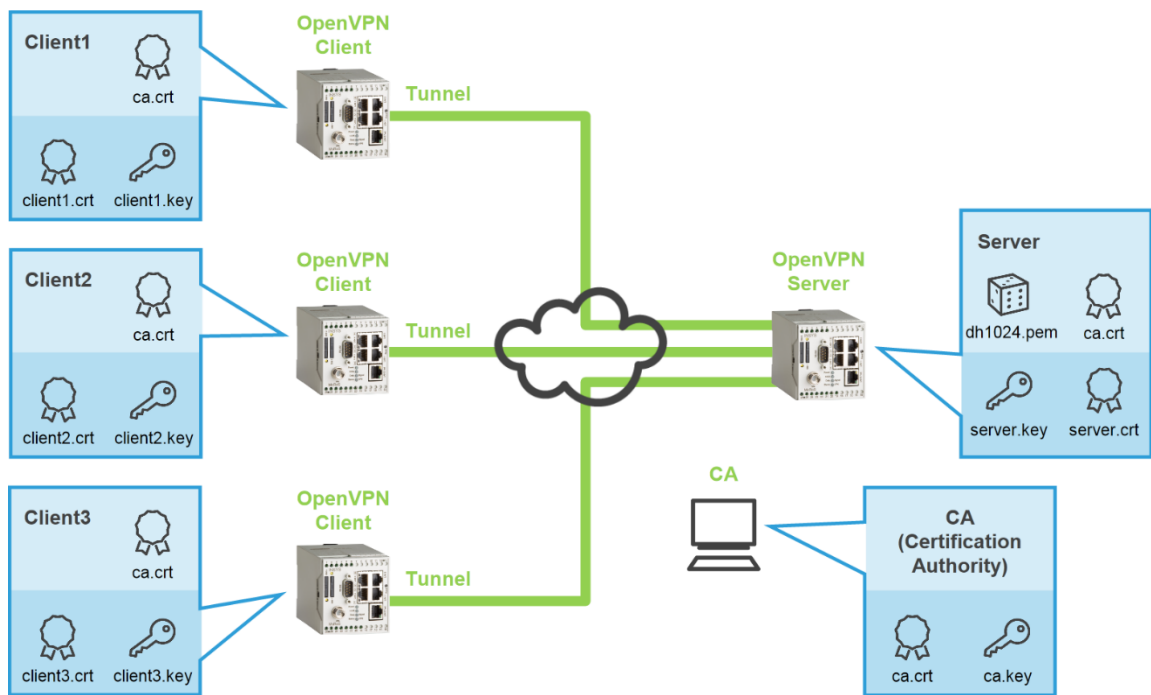


Abbildung 1: CA-Zertifikatsstruktur für OpenVPN-Server und -Client mit zertifikatsbasierter Authentifizierung, hier MoRoS als Server und als Clients

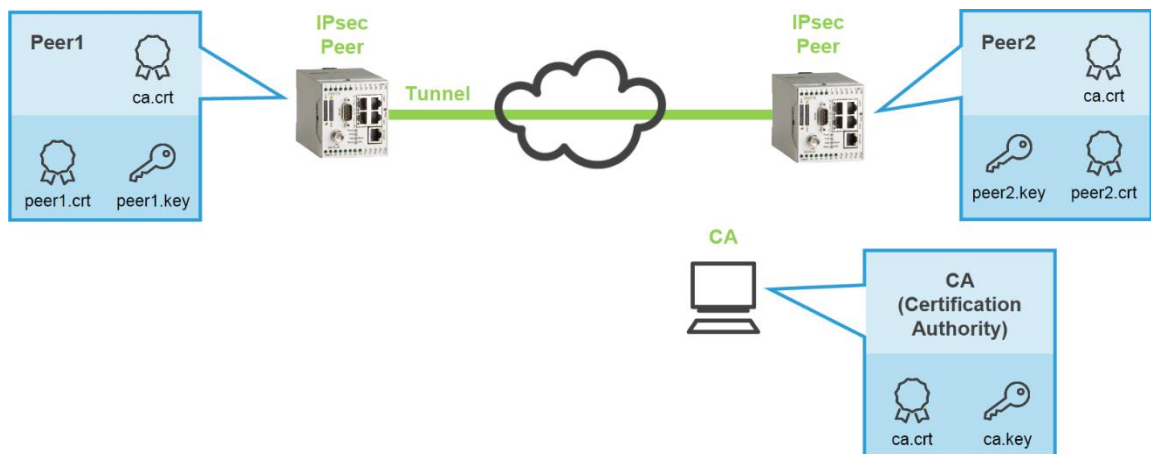


Abbildung 2: CA-Zertifikatsstruktur für IPsec-Teilnehmer mit zertifikatsbasierter Authentifizierung, hier MoRoS als Teilnehmer

2 Kurzfassung

Zertifikate und Schlüssel erzeugen

So erzeugen Sie mit den Standard-Einstellungen alle notwendigen Dateien für eine Zertifikatsstruktur. Detaillierte Schritt-für-Schritt-Anweisungen finden Sie im folgenden Kapitel.

→ Die Systemzeit im PC ist korrekt.

■ Schlüsselverzeichnis vorbereiten

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

■ CA-Zertifikat und Schlüssel erzeugen

```
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>
```

■ Zertifikat und Schlüssel für einen Server erzeugen

```
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>
```

■ Zertifikat und Schlüssel für einen Client erzeugen

```
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>
```

■ Zertifikat zurückrufen und Certificate Revocation List erzeugen (wenn erforderlich)

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

✓ Damit sind alle Dateien erzeugt.

3 Konfiguration

3.1 Vorbereitungen und Voreinstellungen

Vorbereitungen

Bevor Sie mit der Konfiguration beginnen, bereiten Sie bitte folgende Punkte vor:

- OpenVPN-Paket herunterladen
- OpenVPN-Paket auf Windows-PC installieren
- OpenVPN-Paket auf Windows-PC initialisieren

■ OpenVPN-Paket herunterladen

So laden Sie das OpenVPN-Paket von unserer Homepage herunter.

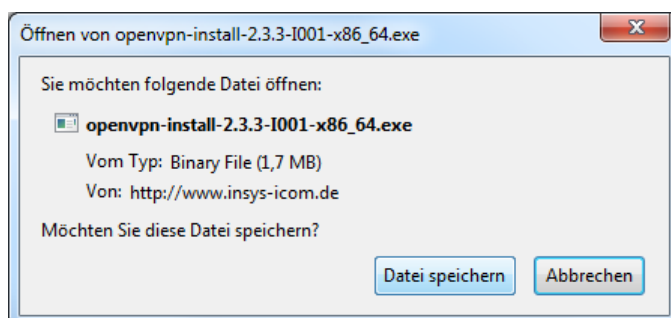
- PC mit ca. 1,5 MB freien Speicherplatz
- Webbrowser
- Internetverbindung

1. Öffnen Sie zum Download der Treiber <http://www.insys-icom.de/treiber/>.
2. Klicken Sie im Abschnitt „MoRoS“ auf den Link für Ihre Windows-Version:

i Ihre Windows-Version (32 oder 64 Bit) finden Sie in der Systemsteuerung auf der Seite System im Abschnitt System unter Systemtyp.

MoRoS	
Treiber	Datei
OpenVPN-Installationsdatei - Windows 32 Bit	OpenVPN 2.3.3 mit GUI (1,7 MB)
OpenVPN-Installationsdatei - Windows 64 Bit	OpenVPN 2.3.3 mit GUI (1,7 MB)

i Falls Ihnen eine aktuellere Version angeboten wird, wählen Sie diese.



3. Speichern Sie die Datei auf Ihrem PC.

✓ Damit haben Sie das OpenVPN-Paket herunter geladen.

■ OpenVPN-Paket auf Windows-PC installieren

So installieren Sie die OpenVPN-GUI und die Programme zum Erstellen der Zertifikate und Schlüssel erfolgreich auf Ihrem PC.

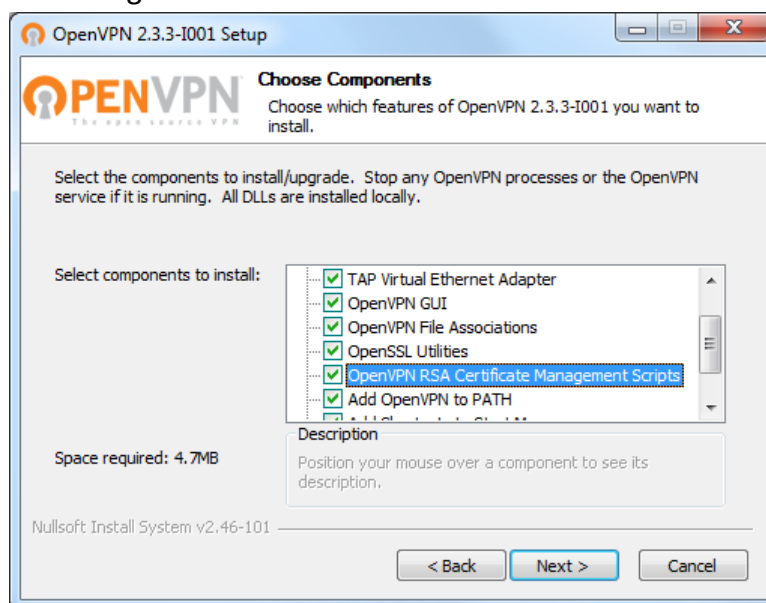
→ Sie haben das OpenVPN-Paket (Version 2.3.3 oder höher) von der INSYS Homepage www.insys-icom.de/treiber heruntergeladen.

1. Führen Sie die heruntergeladene Installationsdatei aus

▶ Falls eine Sicherheitsabfrage von Windows eingeblendet wird, bestätigen Sie diese.

2. Starten Sie den Setup Wizard und akzeptieren Sie die Lizenzhinweise.

✓ Das Fenster zur Auswahl der zu installierenden Komponenten wird angezeigt.



3. Markieren Sie die „OpenVPN RSA Certificate Management Scripts“, wählen Sie **Next >** und setzen Sie den Setup Wizard fort.

▶ Falls eine Warnung aus dem Windows-Log-Test eingeblendet wird, bestätigen Sie diese.

4. Klicken Sie nach dem Beenden der Installation zum Bestätigen **Finish**.

✓ Die OpenVPN-GUI, die SSL-Software und die Programme zum Erstellen der Zertifikate und Schlüssel befinden sich jetzt in den vorgegebenen Verzeichnissen (Standard: C:\Program Files\OpenVPN).

Name	Änderungsdatum	Typ	Größe
bin	04.06.2014 09:56	Dateiordner	
config	04.06.2014 09:56	Dateiordner	
doc	04.06.2014 09:56	Dateiordner	
easy-rsa	04.06.2014 09:56	Dateiordner	
log	04.06.2014 09:56	Dateiordner	
sample-config	04.06.2014 09:56	Dateiordner	
icon.ico	25.06.2012 10:46	IconView ICO File	22 KB
Uninstall.exe	04.06.2014 09:56	Anwendung	120 KB

Konfiguration

- ✓ Damit haben Sie das OpenVPN-Paket erfolgreich auf Ihrem PC installiert und die Vorbereitungen abgeschlossen.

■ OpenVPN-Paket auf Windows-PC initialisieren

So initialisieren Sie das OpenVPN-Paket nach der Installation, um später eine Zertifikatsstruktur erstellen zu können.

→ Das OpenVPN-Paket (Version 2.0.9 oder höher) ist installiert.

1. Öffnen Sie die MS-DOS-Eingabeaufforderung als Administrator (Rechtsklick auf Start-Menü → Alle Programme → Zubehör → Eingabeaufforderung und „Als Administrator ausführen“ wählen).

ⓘ *Für den weiteren Verlauf ist es notwendig, dass Sie die Eingabeaufforderung immer als Administrator ausführen!*

2. Wechseln Sie in das Verzeichnis „easy-rsa“ der OpenVPN-Installation:

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

3. Starten Sie zum Initialisieren des OpenVPN-Pakets die Batch-Datei „init-config.bat“

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

- ✓ Damit ist das OpenVPN-Paket initialisiert und Sie können mit der Erstellung einer Zertifikatsstruktur beginnen.

Voreinstellungen in Stapelverarbeitungsdateien

Zum Erzeugen der Schlüssel und Zertifikate nutzen Sie später verschiedene Stapelverarbeitungsdateien im Verzeichnis „C:\Programme\OpenVPN“.

Führen Sie zum schnellen und fehlerfreien Erzeugen der Schlüssel- und Zertifikatsdateien folgende Voreinstellungen durch:

- Voreinstellungen in „vars.bat“ editieren
- Gültigkeitsdauer in „build-ca.bat“ festlegen
- Gültigkeitsdauer in „build-key-server.bat“ festlegen
- Gültigkeitsdauer in „build-key.bat“ festlegen

■ Voreinstellungen in „vars.bat“ editieren

Durch den Aufruf von „vars.bat“ legen Sie Umgebungsvariablen (KEY-Parameter) für die nachfolgenden Stapelverarbeitungsdateien fest.

Die KEY-Parameter müssen in der gesamten Zertifikatsstruktur identisch sein. Deshalb raten wir Ihnen zur Vermeidung von Tippfehlern und zur Vereinfachung des gesamten Ablaufs dringend, die Vorgabewerte in der Datei „vars.bat“ für Ihre Zwecke einmalig anzupassen.

Im Auslieferungszustand sind folgende KEY-Parameter gesetzt:

```
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
```


Bearbeiten Sie die Datei mit einem Texteditor wie nachfolgend beschrieben.

 *Texteditor wie z.B. „Notepad++“ mit Syntaxhervorhebung*

→ Das OpenVPN-Paket (Version 2.3.3 oder höher) von der INSYS Homepage www.insys-icom.de/treiber ist betriebsbereit installiert.

1. Erstellen Sie eine Sicherungskopie der Datei „vars.bat“ aus dem Verzeichnis „C:\Program Files\OpenVPN\easy-rsa“.
2. Bearbeiten Sie in „vars.bat“ die Zeilen 31 bis 35, wie in folgendem Beispiel gezeigt.

```
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
```

 *Die maximale Länge der Vorgabewerte ist:
2 Zeichen für „KEY_COUNTRY“
z. B. zweistelliger Ländercode nach ISO 3166-1 (alpha 2-Code)
64 Zeichen für „KEY_PROVINCE“*

64 Zeichen für „KEY_CITY“
64 Zeichen für „KEY_ORG“
40 Zeichen für „KEY_EMAIL“

- ❗ *Verwenden Sie für Vorgabewerte mit Leerzeichen wie bei „INSYS MICRO-ELECTRONIS GmbH“ Anführungszeichen. Groß- und Kleinschreibung wird unterschieden.*

3. Speichern Sie Ihre Änderungen

- ❗ *Wenn Sie die bearbeitete Datei unter Windows 7 nicht speichern können, speichern Sie sie an einem anderen Speicherort ab und kopieren Sie sie in das entsprechende Verzeichnis.*
- ✓ Die Bearbeitung der Voreinstellungen in „vars.bat“ ist damit abgeschlossen.

■ Gültigkeitsdauer in „build-ca.bat“ festlegen

Die an anderer Stelle beschriebene Stapelverarbeitungsdatei „build-ca.bat“ erzeugt per Voreinstellung einen RSA-Schlüssel mit 10-jähriger Gültigkeit für eine CA. Diese Gültigkeitsdauer wird über den OpenSSL-Parameter „-days 3650“ gesteuert.

- ▶ *Falls Sie die Gültigkeitsdauer der erzeugten Schlüssel und Zertifikate ändern möchten, editieren Sie die Datei „build-ca.bat“. Ansonsten weiter beim nächsten Abschnitt.*

Bearbeiten Sie die Datei mit einem Texteditor wie z. B. „Notepad++“, wie nachfolgend beschrieben.

- Das OpenVPN-Paket (Version 2.3.3 oder höher) von der INSYS Homepage www.insys-icom.de/treiber ist betriebsbereit installiert.

1. Erstellen Sie eine Sicherungskopie der Datei „build-ca.bat“ aus dem Verzeichnis „C:\Program Files\OpenVPN\easy-rsa“.
2. Bearbeiten Sie in „build-ca.bat“ in Zeile 4 den Wert des Parameters „-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_
```

- ❗ *Der Wert repräsentiert die Tage der Gültigkeit ab Erstellungsdatum und liegt zwischen 1 und x. Abhängig von Ausnahmen im Kalender (Schaltjahre, Tage im Februar) sind 3650 Tage nicht exakt 10 Jahre, wie aus dem am 27.07.09 erstellten Zertifikat ersichtlich ist:*

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

- ❗ *Falls Sie später ein Zertifikat widerrufen wollen, z.B. weil ein Mitarbeiter oder ein Gerät ausscheidet, können Sie ab der Firmware-Version 2.1.0 die „Certificate Revocation List“ nutzen. Dies ist eine Datei, welche die widerrufenen Zertifikate enthält, die zu einem bestimmten Root-Zertifikat ausgegeben wurden.*

3. Speichern Sie Ihre Änderungen

- ✓ Die Bearbeitung der Gültigkeitsdauer in „build-ca.bat“ ist damit abgeschlossen.

■ Gültigkeitsdauer in „build-key-server.bat“ festlegen

Die an anderer Stelle beschriebene Stapelverarbeitungsdatei „build-key-server.bat“ erzeugt per Voreinstellung einen RSA-Schlüssel mit 10-jähriger Gültigkeit für einen Server. Diese Gültigkeitsdauer wird über den OpenSSL-Parameter „-days 3650“ gesteuert.

- ▶ Falls Sie die Gültigkeitsdauer der erzeugten Schlüssel und Zertifikate ändern möchten, editieren Sie die Datei „build-key-server.bat“. Ansonsten weiter beim nächsten Abschnitt.

Bearbeiten Sie die Datei mit einem Texteditor wie z. B. „Notepad++“, wie nachfolgend beschrieben.

→ Das OpenVPN-Paket (Version 2.3.3 oder höher) von der INSYS Homepage www.insys-icom.de/treiber ist betriebsbereit installiert.

1. Erstellen Sie eine Sicherungskopie der Datei „build-key-server.bat“ aus dem Verzeichnis „C:\Program Files\OpenVPN\easy-rsa“.
2. Bearbeiten Sie in „build-key-server.bat“ in Zeile 4 und Zeile 6 den Wert des Parameters „-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

```

- ❗ Der Wert repräsentiert die Tage der Gültigkeit ab Erstellungsdatum und liegt zwischen 1 und x. Abhängig von Ausnahmen im Kalender (Schaltjahre, Tage im Februar) sind 3650 Tage nicht exakt 10 Jahre, wie aus dem am 27.07.09 erstellten Zertifikat ersichtlich ist:

```

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

```

- ❗ Falls Sie später ein Zertifikat widerrufen wollen, z.B. weil ein Mitarbeiter oder ein Gerät ausscheidet, können Sie ab der Firmware-Version 2.1.0 die „Certificate Revocation List“ nutzen. Dies ist eine Datei, welche die widerrufenen Zertifikate enthält, die zu einem bestimmten Root-Zertifikat ausgegeben wurden.

3. Speichern Sie Ihre Änderungen

- ✓ Die Bearbeitung der Gültigkeitsdauer in „build-key-server.bat“ ist damit abgeschlossen.

■ Gültigkeitsdauer in „build-key.bat“ festlegen

Die an anderer Stelle beschriebene Stapelverarbeitungsdatei „build-key.bat“ erzeugt per Voreinstellung einen RSA-Schlüssel mit 10-jähriger Gültigkeit für einen Client. Diese Gültigkeitsdauer wird über den OpenSSL-Parameter „-days 3650“ gesteuert.

- ▶ Falls Sie die Gültigkeitsdauer der erzeugten Schlüssel und Zertifikate ändern möchten, editieren Sie die Datei „build-key.bat“. Ansonsten weiter beim nächsten Abschnitt.

Bearbeiten Sie die Datei mit einem Texteditor wie z. B. „Notepad++“, wie nachfolgend beschrieben.

→ Das OpenVPN-Paket (Version 2.3.3 oder höher) von der INSYS Homepage www.insys-icom.de/treiber ist betriebsbereit installiert.

1. Erstellen Sie eine Sicherungskopie der Datei „build-key.bat“ aus dem Verzeichnis „C:\Program Files\OpenVPN\easy-rsa“.
2. Bearbeiten Sie in „build-key.bat“ in Zeile 4 und Zeile 6 den Wert des Parameters „-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
```

- ⓘ Der Wert repräsentiert die Tage der Gültigkeit ab Erstellungsdatum und liegt zwischen 1 und x. Abhängig von Ausnahmen im Kalender (Schaltjahre, Tage im Februar) sind 3650 Tage nicht exakt 10 Jahre, wie aus dem am 27.07.09 erstellten Zertifikat ersichtlich ist:

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

- ⓘ Falls Sie später ein Zertifikat widerrufen wollen, z.B. weil ein Mitarbeiter oder ein Gerät ausscheidet, können Sie ab der Firmware-Version 2.1.0 die „Certificate Revocation List“ nutzen. Dies ist eine Datei, welche die widerrufenen Zertifikate enthält, die zu einem bestimmten Root-Zertifikat ausgegeben wurden.

3. Speichern Sie Ihre Änderungen

- ✓ Die Bearbeitung der Gültigkeitsdauer in „build-key.bat“ ist damit abgeschlossen.

3.2 Zertifikate erzeugen

Zertifikatsstruktur unter Windows erzeugen

Eine Public Key Infrastructure (PKI, dt. Sicherheitsinfrastruktur) umfasst Services zur Verschlüsselung und digitalen Signatur auf Basis von Public-Key-Verfahren

Zunächst werden die Dateien für die CA (Certification Authority) erzeugt. Danach wird für den Server und für jeden Client ein Schlüsselpaar erzeugt. Für den Aufbau einer IPsec-Verbindung sind jeweils ein Schlüsselpaar für die beiden Clients (Teilnehmer) erforderlich. Diese Schlüsselpaare werden später auf die Geräte hochgeladen.

Weiterhin ist es für OpenVPN möglich, eine Certificate Revocation List (CRL, Zertifikatssperreliste oder Rücknahmelisten) zu erzeugen, die zurückgerufene Zertifikate enthält. Wenn Zertifikate vor ihrem Ablaufdatum zurückgerufen werden müssen (beispielsweise wegen missbräuchlicher Verwendung), können sie in diese Liste eingetragen werden. Die jeweils aktualisierte Liste muss dann auf das Gerät, das als OpenVPN-Server fungiert, hochgeladen werden.

- i** *Eine Certificate Revocation List kann nicht auf MoRoS 1.x hochgeladen werden und ist zum Aufbau eines OpenVPN-Netzwerks mit zertifikatsbasierter Authentifizierung nicht zwingend notwendig.*

Für den Aufbau eines OpenVPN-Netzwerks mit zertifikatsbasierter Authentifizierung benötigen Sie folgende Dateien:

Für den OpenVPN-Server:

Diffie-Hellman-Parametersatz (z.B. dh1024.pem)

CA-Zertifikat (z.B. ca.crt)

Server-Zertifikat (z.B. server.crt)

Server-Schlüssel (z.B. server.key)

Für jeden OpenVPN-Client (1-n):

CA-Zertifikat (z.B. ca.crt)

Client-Zertifikat (z.B. client1.crt)

Client-Schlüssel (z.B. client1.key)

- i** *Für jeden OpenVPN-Client ist ein separates Paar aus Zertifikat und Schlüssel erforderlich.*

- i** *Die jeweiligen Schlüssel sind geheim und dürfen neben der ausstellenden CA nur dem zugehörigen OpenVPN-Teilnehmer bekannt sein. Der CA-Schlüssel ist essentiell für die Sicherheit des OpenVPN-Netzwerks und muss von der CA streng gesichert werden.*

Für den Aufbau einer IPsec-Verbindung mit zertifikatsbasierter Authentifizierung benötigen Sie folgende Dateien:

Für jeden der beiden IPsec-Teilnehmer:

CA-Zertifikat (z.B. ca.crt)

Teilnehmer-Zertifikat (z.B. peer1.crt)

Teilnehmer-Schlüssel (z.B. peer1.key)

- i** *Die jeweiligen Schlüssel sind geheim und dürfen neben der ausstellenden CA nur dem zugehörigen VPN-Teilnehmer bekannt sein. Der CA-Schlüssel ist essentiell für die Sicherheit des VPN-Netzwerks und muss von der CA streng gesichert werden.*

Erzeugen Sie die Dateien in der Reihenfolge dieser Abschnitte:

- Schlüsselverzeichnis vorbereiten
- Diffie-Hellman-Parameter für einen Server erzeugen (wenn erforderlich)
- CA-Zertifikat und -Schlüssel erzeugen
- Zertifikat und Schlüssel für einen Server erzeugen
- Zertifikat und Schlüssel für einen Client erzeugen
- Zertifikat zurückrufen und Certificate Revocation List erzeugen (wenn erforderlich)

■ Schlüsselverzeichnis vorbereiten

So löschen Sie den kompletten Inhalt des Unterverzeichnisses „C:\Program Files\OpenVPN\easy-rsa\keys“.

- i** *Sichern Sie eventuell vorhandene Dateien aus anderen Projekten in diesem Verzeichnis, falls Sie diese noch benötigen.*

→ Das OpenVPN-Paket (Version 2.3.3 oder höher) ist installiert.

1. Öffnen Sie die MS-DOS-Eingabeaufforderung als Administrator (Rechtsklick auf Start-Menü → Alle Programme → Zubehör → Eingabeaufforderung und „Als Administrator ausführen“ wählen).

- i** *Für den weiteren Verlauf ist es notwendig, dass Sie die Eingabeaufforderung immer als Administrator ausführen!*

2. Wechseln Sie in das Verzeichnis „easy-rsa“ der OpenVPN-Installation:

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

3. Starten Sie zum Setzen der Umgebungsvariablen und der Vorgabewerte die Batch-Datei „vars.bat“

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

4. Starten Sie zum Vorbereiten des Unterverzeichnisses „C:\Program Files\OpenVPN\easy-rsa\keys“ die Batch-Datei „clean-all.bat“

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

- i** *Die Batch-Datei „clean-all.bat“ löscht den gesamten Inhalt des Ordners „C:\Program Files\OpenVPN\easy-rsa\keys“.*

- ✓ Im Unterverzeichnis „C:\Program Files\OpenVPN\easy-rsa\keys“ befinden sich jetzt die beiden Dateien „index.txt“ und „serial“ mit 0 und 1 kB Dateigröße. „index.txt“ ist leer, in „serial“ steht „01“ als Vorgabewert für die laufende Nummerierung der PEM-Dateien und wird mit jeder erzeugten PEM-Datei um 1 inkrementiert; siehe Abschnitt „Zertifikat und Schlüssel für einen Server erzeugen“.

■ Diffie-Hellman-Parameter für einen Server erzeugen

So erzeugen Sie die Diffie-Hellman-Parameter. Die Erzeugung kann, je nach Rechenleistung des PCs, bis zu mehreren Minuten dauern.

- ▶ *Ein Diffie-Hellmann-Parametersatz ist im Auslieferungszustand eines INSYS-Routers bereits geladen. Wenn Sie einen neuen Parametersatz erzeugen wollen, absolvieren Sie die folgenden Schritte. Andernfalls können Sie diesen Abschnitt überspringen.*

i *Diffie-Hellman-Parameter werden nur vom OpenVPN-Server benötigt, nicht von den OpenVPN-Clients.*

→ Das OpenVPN-Paket (Version 2.3.3 oder höher) ist installiert.

1. Öffnen Sie die MS-DOS-Eingabeaufforderung als Administrator (Rechtsklick auf Start-Menü → Alle Programme → Zubehör → Eingabeaufforderung und „Als Administrator ausführen“ wählen).

i *Für den weiteren Verlauf ist es notwendig, dass Sie die Eingabeaufforderung immer als Administrator ausführen!*

2. Wechseln Sie in das Verzeichnis „easy-rsa“ der OpenVPN-Installation:

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

3. Starten Sie zum Setzen der Umgebungsvariablen und der Vorgabewerte die Batch-Datei „vars.bat“

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

4. Starten Sie zum Erzeugen der Diffie-Hellmann-Parameter die Batch-Datei „build-dh.bat“

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

- ✓ Während der Erzeugung wird folgender Dialog eingeblendet:

```
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>
```

- ✓ Damit ist die Erzeugung der Diffie-Hellmann-Parameter abgeschlossen. Im Unterverzeichnis „C:\Program Files\OpenVPN\easy-rsa\keys“ befindet sich jetzt die Datei „dh1024.pem“.

■ CA-Zertifikat und -Schlüssel erzeugen

So erzeugen Sie die Zertifikatsstruktur Ihrer eigenen Zertifizierungsstelle (CA, Certificate Authority). Die CA-Zertifikatsstruktur besteht aus den beiden Dateien „ca.key“ (geheimer Schlüssel) und „ca.crt“ (öffentliches Zertifikat).

- Das OpenVPN-Paket (Version 2.3.3 oder höher) ist installiert.
- Die Vorgabewerte in „vars.bat“ sind angepasst.
- Die Gültigkeitsdauer ist definiert; Standardeintrag ist 3650 Tage = 10 Jahre.

1. Prüfen Sie die Einstellung von Uhrzeit und Datum im PC

i *Zertifikate haben ein Gültigkeitsdatum. Eine falsche Systemzeit (Uhrzeit und Datum) sind häufige Fehlerquellen. Achten Sie deshalb auf die korrekte Systemzeit sowohl im PC bei der Erstellung als auch im INSYS-Router bei der Inbetriebnahme des VPN-Servers oder -Clients.*

2. Öffnen Sie die MS-DOS-Eingabeaufforderung als Administrator (Rechtsklick auf Start-Menü → Alle Programme → Zubehör → Eingabeaufforderung und „Als Administrator ausführen“ wählen).

i *Für den weiteren Verlauf ist es notwendig, dass Sie die Eingabeaufforderung immer als Administrator ausführen!*

3. Wechseln Sie in das Verzeichnis „easy-rsa“ der OpenVPN-Installation:

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

4. Starten Sie zum Setzen der Umgebungsvariablen und der Vorgabewerte die Batch-Datei „vars.bat“:

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

i *Die Umgebungsvariablen sind nur so lange gültig, wie die Eingabeaufforderung geöffnet ist. „vars.bat“ muss nur dann nochmals ausgeführt werden, wenn in der Zwischenzeit das DOS-Fenster geschlossen wurde.*

5. Starten Sie zum Erstellen des öffentlichen CA-Zertifikats „ca.crt“ und des öffentlichen Schlüssels „ca.key“ die Batch-Datei „build-ca.bat“:

```
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'  
-----
```

✓ Der RSA-Schlüssel wurde erzeugt.
Im Unterverzeichnis „C:\Program Files\OpenVPN\easy-rsa\keys“ befindet sich jetzt eine Datei mit dem Namen „ca.key“ und 0 kB Dateigröße.

i *Die Dateinamen „ca.crt“ und „ca.key“ sind fest definiert. Eine spätere Änderung führt zu Funktionsverlust!*

i *Mit den folgenden Angaben wird der Server identifiziert. Außer dem „Common Name“ müssen alle Angaben bei allen Zertifikaten innerhalb einer Zertifikatsstruktur identisch sein! Der „Common Name“ muss bei allen Zertifikaten unterschiedlich sein!*

✓ Sie werden nun aufgefordert, Ihre Voreinstellungen wie „[DE]“ zu bestätigen:

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. Bestätigen Sie Ihre Voreinstellungen mit **Return**.

Der Wert für „Organizational Unit Name“ kann leer bleiben.

- ✓ Sie werden nun aufgefordert, einen „Common Name“ einzugeben:

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

- i** Dieses Feld dürfen Sie auf keinem Fall leer lassen. Mit dieser Angabe unterscheidet der Server später die verschiedenen Clients und Clientnetze. Der „Common Name“ muss in der gesamten Zertifikatsstruktur eindeutig sein und darf maximal 63 Zeichen lang sein.

- i** Ersetzen Sie Leerzeichen mit Unterstrichen wie z. B. „VPN_HOSTNAME“. Achten Sie auf Groß-/Kleinschreibung und verwenden Sie am besten durchgängig nur eine dieser Möglichkeiten. Verwenden Sie keine länderspezifischen Zeichen wie Umlaute.

7. Verwenden Sie als „Common Name“ z. B. „ca“.

- ✓ Sie werden nun aufgefordert, einen Namen einzugeben:

Name [changeme]:

8. Bestätigen Sie Ihre Voreinstellung mit **Return**.

Der Wert für „Name“ kann leer bleiben.

- ✓ Sie werden nun aufgefordert, Ihre voreingestellte Email-Adresse zu bestätigen:

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

9. Bestätigen Sie Ihre Voreinstellung mit **Return**.

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

- ✓ Damit ist die Erzeugung der CA-Zertifikatsstruktur abgeschlossen. Im Unterverzeichnis „C:\Program Files\OpenVPN\easy-rsa\keys“ befinden sich jetzt die beiden Dateien „ca.key“ und „ca.crt“ mit ca. 1 bis 2 kB Dateigröße.

Anhang: Inhalt des Eingabefensters (Ablauf der Skripte)

i Ihre Eingaben sind blau markiert.

```
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>
```

■ Zertifikat und Schlüssel für einen Server erzeugen

So erzeugen Sie den geheimen Schlüssel (z.B. server.key) und das öffentliche Zertifikat (z.B. server.crt) für einen Server.

Für die Erzeugung ist ein „Common Name“ erforderlich. Der „Common Name“ ist der einzigartige Mitgliedsname eines VPN-Teilnehmers im gesicherten Netzwerk und wird z. B. zum Routing in die Clientnetze verwendet. Der „Common Name“ darf nur für einen Teilnehmer verwendet werden und ist nach der Erzeugung unveränderlich. Achten Sie beim „Common Name“ auf Groß-/Kleinschreibung und verwenden Sie am besten durchgängig nur Groß- oder Kleinschreibung.

Wir empfehlen denselben Eintrag für den „Dateinamen“ und den „Common Name“. Ihr Vorteil: Sie erkennen den „Common Name“ des Zertifikates bereits am Dateinamen. Falls dies aus Sicherheitsgründen verschleiert werden soll, wählen Sie unterschiedliche Einträge.

i Die maximale Länge des „Common Name“ für alle INSYS-Router beträgt 29 Zeichen (für den MoRoS 1.3 sind es 15 Zeichen).

i Am Ende dieses Abschnitts ist der Inhalt des Eingabefensters (Ablauf der Skripte) zusammenhängend als Anhang abgebildet.

- Das OpenVPN-Paket (Version 2.3.3 oder höher) ist installiert.
- Die CA-Zertifikatsstruktur ist erzeugt (Dateien „ca.key“ und „ca.crt“).
- Die Vorgabewerte in „vars.bat“ müssen unbedingt dieselben sein, wie bei der Erzeugung der CA-Zertifikatsstruktur!
- In diesem Beispiel ist der Dateiname „server“; der „Common Name“ ist ebenfalls „server“.

1. Prüfen Sie die Einstellung von Uhrzeit und Datum im PC

- i** *Zertifikate haben ein Gültigkeitsdatum. Eine falsche Systemzeit (Uhrzeit und Datum) sind häufige Fehlerquellen. Achten Sie deshalb auf die korrekte Systemzeit sowohl im PC bei der Erstellung als auch im INSYS-Router bei der Inbetriebnahme des Servers oder Clients.*

2. Öffnen Sie die MS-DOS-Eingabeaufforderung als Administrator (Rechtsklick auf Start-Menü → Alle Programme → Zubehör → Eingabeaufforderung und „Als Administrator ausführen“ wählen).

- i** *Für den weiteren Verlauf ist es notwendig, dass Sie die Eingabeaufforderung immer als Administrator ausführen!*

3. Wechseln Sie in das Verzeichnis „easy-rsa“ der OpenVPN-Installation:

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

4. Starten Sie zum Setzen der Umgebungsvariablen und der Vorgabewerte die Batch-Datei „vars.bat“:

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

- i** *Die Umgebungsvariablen sind nur so lange gültig, wie die Eingabeaufforderung geöffnet ist. „vars.bat“ muss nur dann nochmals ausgeführt werden, wenn in der Zwischenzeit das DOS-Fenster geschlossen wurde.*

5. Starten Sie zum Erzeugen von Zertifikat und Schlüssel die Batch-Datei „build-key-server“ und geben Sie als Parameter den gewünschten Dateinamen an, z.B. „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.
-----
```

- ✓ Es wurde 1 Datei angelegt.
Im Unterverzeichnis „C:\Program Files\OpenVPN\easy-rsa\keys“ befindet sich jetzt die Datei „server.key“ mit 0 kB Dateigröße.
- ✓ Sie werden nun aufgefordert, Ihre Voreinstellungen wie „[DE]“ zu bestätigen.

- i** Jeder Teilnehmer im VPN-Netzwerk wird z. B. beim Verbindungsaufbau u. a. mit den Angaben „Country Name“, „State or Province Name“, „Locality Name“, „Organization Name“, „Organizational Unit Name“ identifiziert. Deshalb müssen diese Angaben (DN, Distinguished Names) bei allen Zertifikaten innerhalb eines VPN-Netzwerkes identisch sein!
Um Fehler bei der Erzeugung auszuschließen und der Ablauf zu beschleunigen, haben Sie die Vorgabewerte in der Datei „vars.bat“ bereits vor der Erzeugung der Zertifizierungsstelle (CA-Zertifikatsstruktur) festgelegt.

6. Bestätigen Sie Ihre Voreinstellungen mit **Return**.

Der Wert für „Organizational Unit Name“ kann leer bleiben.

```
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]:
```

- ✓ Sie werden nun aufgefordert, einen „Common Name“ einzugeben:

- i** Dieses Feld dürfen Sie auf keinem Fall leer lassen!

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

- i** Ersetzen Sie Leerzeichen durch Unterstriche. Achten Sie auf Groß-/Kleinschreibung und verwenden Sie am besten durchgängig nur eine dieser Möglichkeiten. Verwenden Sie keine länderspezifischen Zeichen wie z.B. Umlaute. Verwenden Sie nicht mehr als 29 Zeichen, um die Kompatibilität zu allen INSYS-Routern zu gewährleisten (15 Zeichen für den MoRoS 1.3).

7. Verwenden Sie in diesem Beispiel als „Common Name“ z.B. „server“.

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

- ✓ Sie werden nun aufgefordert, einen Namen einzugeben:

```
Name [changeme]:
```

8. Bestätigen Sie Ihre Voreinstellung mit **Return**.

Der Wert für „Name“ kann leer bleiben.

- ✓ Sie werden nun aufgefordert, Ihre voreingestellte Email-Adresse zu bestätigen:

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

9. Bestätigen Sie Ihre Voreinstellung mit **Return**.

- ✓ Sie werden nun aufgefordert, weitere Angaben zu machen:

- i** Der Wert für „challenge password“ muss leer bleiben, damit der VPN-Tunnel automatisch aufgebaut werden kann!
Der Wert für „optional company name“ kann leer bleiben.

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

10. Bestätigen Sie die leeren Voreinstellungen mit **Return**.

- ✓ Nach einer Prüfung und Zusammenfassung der Angaben werden Sie aufgefordert, das Zertifikat zu signieren:

```
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

```

✓ Bisher wurden 3 Dateien angelegt.

Im Unterverzeichnis „C:\Program Files\OpenVPN\easy-rsa\keys“ befinden sich jetzt die Dateien „server.key“ und „server.csr“ mit je 1 kB Dateigröße sowie die Datei „server.crt“ mit 0 kB.

11. Bestätigen Sie mit y.

✓ Sie werden nun aufgefordert, Ihre eigene Zertifikatsanfrage zu bestätigen:

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

12. Bestätigen Sie mit y.

```

write out database with 1 new entries
Data Base Updated

```

✓ Das Zertifikat wurde erstellt und als Datei gespeichert.

Die Dateien „index.txt“ und „serial“ (Data Base) im Verzeichnis „C:\Program Files\OpenVPN\easy-rsa\keys“ wurden aktualisiert.

i Die upgedatete „Data Base“ ist die Datei „serial“, diese enthält einen dezimalen Zahlenwert wie z. B. „01“. Dieser Wert wird bei jeder erfolgreichen Zertifikats-/Schlüsselerstellung um 1 erhöht.
Die Datei „index.txt“ enthält jetzt einen ersten Eintrag in der Form:
V 190726143431Z 01 unknown /C=DE/ST=BY/O="INSYS MICRO-ELECTRONICS GmbH"/CN=server/emailAddress=support@insys-tec.de. Dabei ist „190726143431“ das Datum, ab dem das Zertifikat ungültig ist: 2019/07/26 ab 14:34:31 Uhr. Bei CN steht der von Ihnen vergebene Common Name, hier „server“. Der Wert „01“ danach ist die laufende Nummer der PEM-Datei; s. u.


```
C:\Programme\OpenVPN\easy-rsa>
```

✓ Damit ist die Erzeugung des geheimen Schlüssels und des öffentlichen Zertifikates für einen Server abgeschlossen.
Im Unterverzeichnis „C:\Program Files\OpenVPN\easy-rsa\keys“ befinden sich jetzt die vier neuen Dateien „server.key“, „server.crt“, „server.csr“ und „01.pem“ mit ca. 1 bis 4 kB Dateigröße.

i Die CSR-Datei, hier „server.csr“, ist für die hier beschriebenen Zwecke nicht notwendig. CSR steht für „Certificate Signing Request“. Nachdem Sie mit OpenSSL Ihre eigene Zertifizierungsstelle sind und oben Ihre Zertifikatsanfrage selbst bestätigt haben, können Sie die Datei „server.csr“ jederzeit löschen. Diese wäre nur erforderlich, wenn Sie die Zertifizierung bei einer fremden Zertifizierungsstelle (CA, Certificate Authority) beantragen würden; in diesem Fall würden Sie die Datei „x.csr“ zur Zertifizierungsstelle senden und eine zertifizierte „x.crt“ zurück bekommen.

i Die PEM-Datei, hier „01.pem“, ist für die hier beschriebenen Zwecke nicht notwendig. Eine PEM-Datei ist ein Base64-kodiertes Zertifikat. Die Datei wird fortlaufend nummeriert, z. B. „01.pem“ usw. und ist eine Kopie des ausgestellten Zertifikats, in diesem Beispiel von „server.crt“. In der Datei „index.txt“ führt OpenSSL Buch über die ausgestellten Zertifikate.

Anhang: Inhalt des Eingabefensters (Ablauf der Skripte)

 Ihre Eingaben sind blau markiert.

```
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>
```

■ Zertifikat und Schlüssel für einen Client erzeugen

So erzeugen Sie den geheimen Schlüssel (z.B. client1.key) und das öffentliche Zertifikat (z.B. client1.crt) für einen Client.

Für die Erzeugung ist ein „Common Name“ erforderlich. Der „Common Name“ ist der einzigartige Mitgliedsname eines VPN-Teilnehmers im gesicherten Netzwerk und wird z.B. zum Routing in die Clientnetze verwendet. Der „Common Name“ darf nur für einen Teilnehmer verwendet werden und ist nach der Erzeugung unveränderlich. Achten Sie beim „Common Name“ auf Groß-/Kleinschreibung und verwenden Sie am besten durchgängig nur Groß- oder Kleinschreibung.

Wir empfehlen denselben Eintrag für den „Dateinamen“ und „Common Name“. Ihr Vorteil: Sie erkennen den „Common Name“ des Zertifikates bereits am Dateinamen. Falls dies aus Sicherheitsgründen verschleiert werden soll, wählen Sie unterschiedliche Einträge.

i *Die maximale Länge des „Common Name“ für alle INSYS-Router beträgt 29 Zeichen (für den MoRoS 1.3 sind es 15 Zeichen).*

i *Am Ende dieses Abschnitts ist der Inhalt des Eingabefensters (Ablauf der Skripte) zusammenhängend als Anhang abgebildet.*

- Das OpenVPN-Paket (Version 2.3.3 oder höher) ist installiert.
- Die CA-Zertifikatsstruktur ist erzeugt (Dateien „ca.key“ und „ca.crt“).
- Die Vorgabewerte in „vars.bat“ müssen unbedingt dieselben sein, wie bei der Erzeugung der CA-Zertifikatsstruktur!
- In diesem Beispiel ist der Dateiname „client1“; der „Common Name“ ist ebenfalls „client1“.

1. Prüfen Sie die Einstellung von Uhrzeit und Datum im PC

i *Zertifikate haben ein Gültigkeitsdatum. Eine falsche Systemzeit (Uhrzeit und Datum) sind häufige Fehlerquellen. Achten Sie deshalb auf die korrekte Systemzeit sowohl im PC bei der Erstellung als auch im INSYS-Router bei der Inbetriebnahme des Servers oder Clients.*

2. Öffnen Sie die MS-DOS-Eingabeaufforderung als Administrator (Rechtsklick auf Start-Menü → Alle Programme → Zubehör → Eingabeaufforderung und „Als Administrator ausführen“ wählen).

i *Für den weiteren Verlauf ist es notwendig, dass Sie die Eingabeaufforderung immer als Administrator ausführen!*

3. Wechseln Sie in das Verzeichnis „easy-rsa“ der OpenVPN-Installation:

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

4. Starten Sie zum Setzen der Umgebungsvariablen und der Vorgabewerte die Batch-Datei „vars.bat“:

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

i *Die Umgebungsvariablen sind nur so lange gültig, wie die Eingabeaufforderung geöffnet ist. „vars.bat“ muss nur dann nochmals ausgeführt werden, wenn in der Zwischenzeit das DOS-Fenster geschlossen wurde.*

5. Starten Sie zum Erzeugen von Zertifikat und Schlüssel die Batch-Datei „build-key.bat“ und geben Sie als Parameter den gewünschten Dateinamen an, z.B. „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.
-----
```

- ▶ *Ab Version 2.1.1 des OpenVPN-Pakets können Sie hier alternativ die Batch-Datei „build-key-pkcs12“ starten. Damit wird zusätzlich ein PKCS12-Container mit CA-Zertifikat sowie Zertifikat und Schlüssel des Client angelegt. Die weitere Vorgehensweise ist analog zu dieser Beschreibung. Am Ende haben Sie noch die Möglichkeit, den Container mit einem Passwort zu versehen. PKCS12-Container können nicht auf MoRoS 1.x geladen werden. Eine Passwordeingabe ist erst ab FW 2.3.0 möglich.*
- ✓ Es wurde 1 Datei angelegt.
Im Unterverzeichnis „C:\Program Files\OpenVPN\easy-rsa\keys“ befindet sich jetzt die Datei „client1.key“ mit 0 kB Dateigröße.
- ✓ Sie werden nun aufgefordert, Ihre Voreinstellungen wie „[DE]“ zu bestätigen.
- ⓘ *Jeder Teilnehmer im VPN-Netzwerk wird z. B. beim Verbindungsaufbau u. a. mit den Angaben „Country Name“, „State or Province Name“, „Locality Name“, „Organization Name“, „Organizational Unit Name“ identifiziert. Deshalb müssen diese Angaben (DN, Distinguished Names) bei allen Zertifikaten innerhalb eines VPN-Netzwerkes identisch sein!
Um Fehler bei der Erzeugung auszuschließen und der Ablauf zu beschleunigen, haben Sie die Vorgabewerte in der Datei „vars.bat“ bereits vor der Erzeugung der Zertifizierungsstelle (CA-Zertifikatsstruktur) festgelegt.*

6. Bestätigen Sie Ihre Voreinstellungen mit **Return**.

Der Wert für „Organizational Unit Name“ kann leer bleiben.

```
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]:
```

- ✓ Sie werden nun aufgefordert, einen „Common Name“ einzugeben:

- ⓘ *Dieses Feld dürfen Sie auf keinem Fall leer lassen!*

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

- ⓘ *Ersetzen Sie Leerzeichen durch Unterstriche. Achten Sie auf Groß-/Kleinschreibung und verwenden Sie am besten durchgängig nur eine dieser Möglichkeiten. Verwenden Sie keine länderspezifischen Zeichen wie z. B. Umlaute. Verwenden Sie nicht mehr als 29 Zeichen, um die Kompatibilität zu allen INSYS-Routern zu gewährleisten (15 Zeichen für den MoRoS 1.3).*

7. Verwenden Sie in diesem Beispiel als „Common Name“ z. B. „client1“.

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


- ✓ Sie werden nun aufgefordert, einen Namen einzugeben:

```
Name [changeme]:
```

- Bestätigen Sie Ihre Voreinstellung mit .

Der Wert für „Name“ kann leer bleiben.

- ✓ Sie werden nun aufgefordert, Ihre voreingestellte Email-Adresse zu bestätigen:

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

- Bestätigen Sie Ihre Voreinstellung mit .

- ✓ Sie werden nun aufgefordert, weitere Angaben zu machen:

- i** *Der Wert für „challenge password“ muss leer bleiben, damit der VPN-Tunnel automatisch aufgebaut werden kann!*

Der Wert für „optional company name“ kann leer bleiben.

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

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

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

- Bestätigen Sie die leeren Voreinstellungen mit .

- ✓ Nun werden Ihre Angaben geprüft und zusammengefasst:

```
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
```

- ✓ Bisher wurden 3 Dateien angelegt.

Im Unterverzeichnis „C:\Program Files\OpenVPN\easy-rsa\keys“ befinden sich jetzt die Dateien „client1.key“ und „client1.csr“ mit je 1 kB Dateigröße sowie die Datei „client1.crt“ mit 0 kB.

- Bestätigen Sie Aufforderung zum Signieren des Zertifikates mit .

- ✓ Sie werden nun aufgefordert, Ihre eigene Zertifikatsanfrage zu bestätigen:

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

- Bestätigen Sie mit .

```
write out database with 1 new entries
```

```
Data Base updated
```

- ✓ Das Zertifikat wurde erstellt und als Datei gespeichert.


Die Dateien „index.txt“ und „serial“ (Data Base) im Verzeichnis „C:\Program Files\OpenVPN\easy-rsa\keys“ wurden aktualisiert.

- ❗ Die upgedatete „Data Base“ ist die Datei „serial“, diese enthält einen dezimalen Zahlenwert wie z. B. „02“. Dieser Wert wird bei jeder erfolgreichen Zertifikats-/Schlüsselerstellung um 1 erhöht.
Die Datei „index.txt“ enthält jetzt einen zweiten Eintrag in der Form:
V 190728161024Z 02 unknown /C=DE/ST=BY/O="INSYS MICRO-ELECTRONICS GmbH"/CN=client1/emailAddress=support@insys-tec.de.
Dabei ist „190728161024“ das Datum, ab dem das Zertifikat ungültig ist: 2019/07/28 ab 16:10:24 Uhr. Bei CN steht der von Ihnen vergebene Common Name, hier „client1“. Der Wert „01“ danach ist die laufende Nummer der PEM-Datei; s. u.

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

- ✓ Damit ist die Erzeugung des geheimen Schlüssels und des öffentlichen Zertifikates für einen Client abgeschlossen.
- ▶ Wenn Sie alternativ die Batch-Datei „build-key-pkcs12“ gestartet haben, müssen Sie an dieser Stelle noch ein Passwort für den PKCS12-Container festlegen. Wenn Sie die Eingabeaufforderung ohne Passwortheingabe abschließen, wird kein Passwort vergeben. Eine Passwortheingabe ist erst ab FW 2.3.0 möglich.
- ❗ Zum Erzeugen eines Zertifikats und Schlüssels für einen weiteren Client müssen Sie nur die Schritte in diesem Abschnitt wiederholen. Die Vorgehensweise zum Erzeugen von Zertifikaten und Schlüsseln für eine CA oder einen Server müssen bzw. dürfen nicht wiederholt werden.
- ✓ Im Unterverzeichnis „C:\Program Files\OpenVPN\easy-rsa\keys“ befinden sich jetzt die vier neuen Dateien „client1.key“, „client1.crt“, „client1.csr“ und „02.pem“ mit ca. 1 bis 4 kB Dateigröße.
- ❗ Die CSR-Datei, hier „client1.csr“, ist für die hier beschriebenen Zwecke nicht notwendig. CSR steht für „Certificate Signing Request“. Nachdem Sie mit OpenSSL Ihre eigene Zertifizierungsstelle sind und oben Ihre Zertifikatsanfrage selbst bestätigt haben, können Sie die Datei „client1.csr“ jederzeit löschen. Diese wäre nur erforderlich, wenn Sie die Zertifizierung bei einer fremden Zertifizierungsstelle (CA, Certificate Authority) beantragen würden; in diesem Fall würden Sie die Datei „x.csr“ zur Zertifizierungsstelle senden und eine zertifizierte „x.crt“ zurück bekommen.
- ▶ Wenn Sie alternativ die Batch-Datei „build-key-pkcs12“ gestartet haben, wurde noch eine Datei „client1.p12“ angelegt. Dieser PKCS12-Container enthält das CA-Zertifikat sowie Zertifikat und Schlüssel des Client. Damit können Sie mit einem einmaligen Vorgang CA-Zertifikat sowie Zertifikat und Schlüssel des Client hochladen.
- ❗ Die PEM-Datei, hier „02.pem“, ist für die hier beschriebenen Zwecke nicht notwendig. Eine PEM-Datei ist ein Base64-kodiertes Zertifikat. Die Datei wird fortlaufend nummeriert, z. B. „01.pem“ usw. und ist eine Kopie des ausgestellten Zertifikats, in diesem Beispiel von „client1.crt“. In der Datei „index.txt“ führt OpenSSL Buch über die ausgestellten Zertifikate.

Anhang: Inhalt des Eingabefensters (Ablauf der Skripte)

 Ihre Eingaben sind blau markiert.

```
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>
```

■ Zertifikat zurückrufen und Certificate Revocation List erzeugen (wenn erforderlich)

So rufen Sie ein Zertifikat vor seinem Ablaufdatum zurück (beispielsweise wegen missbräuchlicher Verwendung) und erzeugen eine Certificate Revocation List.

i *Eine Certificate Revocation List kann nicht auf MoRoS 1.x hochgeladen werden und ist zum Aufbau eines OpenVPN-Netzwerks mit zertifikatsbasierter Authentifizierung nicht zwingend notwendig.*

- Das OpenVPN-Paket (Version 2.3.3 oder höher) ist installiert.
- Die CA-Zertifikatsstruktur ist erzeugt (Dateien „ca.key“ und „ca.crt“).
- Client- bzw. Server-Zertifikate wurden bereits erzeugt.
- Die Vorgabewerte in „vars.bat“ müssen unbedingt dieselben sein, wie bei der Erzeugung der CA-Zertifikatsstruktur und der Zertifikate!

1. Öffnen Sie die MS-DOS-Eingabeaufforderung als Administrator (Rechtsklick auf Start-Menü → Alle Programme → Zubehör → Eingabeaufforderung und „Als Administrator ausführen“ wählen).

i *Für den weiteren Verlauf ist es notwendig, dass Sie die Eingabeaufforderung immer als Administrator ausführen!*

2. Wechseln Sie in das Verzeichnis „easy-rsa“ der OpenVPN-Installation:

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

3. Starten Sie zum Setzen der Umgebungsvariablen und der Vorgabewerte die Batch-Datei „vars.bat“:

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

i *Die Umgebungsvariablen sind nur so lange gültig, wie die Eingabeaufforderung geöffnet ist. „vars.bat“ muss nur dann nochmals ausgeführt werden, wenn in der Zwischenzeit das DOS-Fenster geschlossen wurde.*

4. Starten Sie zum Zurückrufen eines Zertifikats die Batch-Datei „revoke-full.bat“ und geben Sie als Parameter den „Common Name“ des zurückzurufenden Zertifikats an, z.B. „client1“:

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

- ✓ Die Certificate Revocation List, die alle bislang zurückgerufenen Zertifikate dieser CA enthält, wurde erstellt bzw. aktualisiert und als Datei gespeichert.
Im Unterverzeichnis „C:\Program Files\OpenVPN\easy-rsa\keys“ befindet sich jetzt die Datei „crl.pem“ mit 1 kB Dateigröße.

4 Verwendete Komponenten

Software

Bezeichnung	Hersteller	Typ	Version
OpenVPN-Paket	Open Source	OpenVPN mit GUI	2.3.3
Betriebssystem	Microsoft	Windows	7

Tabelle 1: Verwendete Software

Deutschland

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

Telefon +49 941 58692 0
Telefax +49 941 58692 45
E-Mail info@insys-icom.de
URL www.insys-icom.de

Czech Republic

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

Telefon +420 377 429 952
Telefax +420 377 429 952
Mobil +420 777 651 188
E-Mail info@insys-icom.cz
URL www.insys-icom.cz