

## **Schlüsselverwaltung mit XCA für OpenVPN**

Dieses Dokument erläutert Ihnen die Zertifikate-Erstellung mit der Schlüsselverwaltung mit XCA - speziell zur Verwendung für OpenVPN.

### **Warum XCA ?**

OpenVPN bringt inzwischen eigene Scripte mit, mit welchen man die Zertifikate auch gut erstellen kann. Möglicherweise werden Sie diese Methode als einfacher empfinden und zumindest für die ersten Schritte bevorzugen. Wie dieses geht wird in einem eigenen Dokument unter der unten stehenden Adresse kurz beschrieben.

Mittels XCA Zertifikate zu erstellen bietet Ihnen im Gegensatz zu den Skripten eine größere Bandbreite an Einstellmöglichkeiten - beispielsweise bei der Gültigkeit der Zertifikate. Auch lassen sich die Zertifikate besser verwalten.

### **Vorwort:**

Ich freue mich, Ihnen die X Certificate Erstellung nahe bringen zu dürfen. XCA ist - man darf sich von der niedrigen Versionsnummer nicht irritieren lassen - sehr mächtig und vielfältig einsetzbar. Die Vielfalt irritiert einwenig, wenn man doch "nur" ein paar Zertifikate für OpenVPN erstellen möchte.

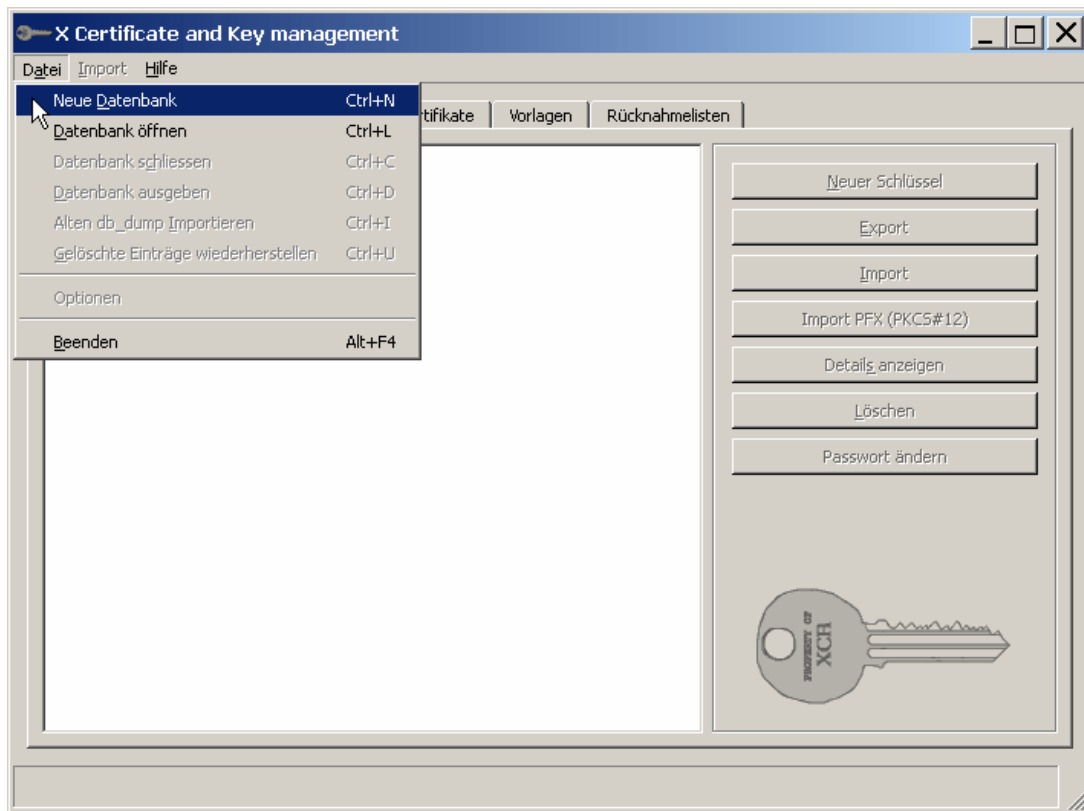
Grundlage für dieses Dokument war die Installation mit setup\_xca-0.6.4.exe

### **Hilfreiches:**

Hinweise können Sie auch diesem Wiki entnehmen:  
[http://wiki.openvpn.eu/index.php/Schlüsselverwaltung\\_mit\\_XCA](http://wiki.openvpn.eu/index.php/Schlüsselverwaltung_mit_XCA)

Downloadmöglichkeiten für Test-Zertifikate habe ich hier für Sie:  
<http://www.Optik-Berndt.de/xca-openvpn.html>

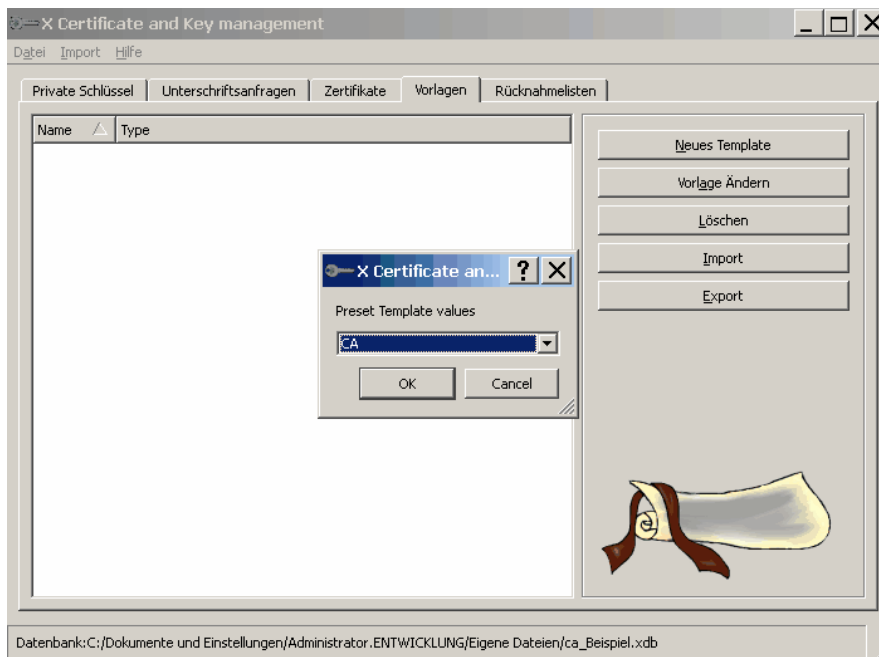
Nach dem Programmstart erstellen Sie sich eine neue Datenbank:



Ich darf Ihnen empfehlen, einen plausiblen Namen zu verwenden wie "ca\_Projekname" Diese Datenbank verschlüsseln Sie mit einem Passwort: verlieren Sie dieses bloss nicht !

Nun vereinfachen wir uns gleich zu Anfang das ganze mit der sinnvollen Erstellung einiger Vorlagen.

Wählt nun den Reiter Vorlagen aus und "neue Vorlage". Wählen Sie CA aus.



Als Interner Name empfehle ich Ihnen CA\_Template

Füllen Sie alle Felder außer CommonName aus !

The screenshot shows a window titled "X Certificate and Key management" with a sub-dialog "Create XCA template". The dialog has four tabs: "Besitzer", "Extensions", "Key Usage", and "Netscape". The "Besitzer" tab is active, showing a "Distinguished name" section with the following fields:

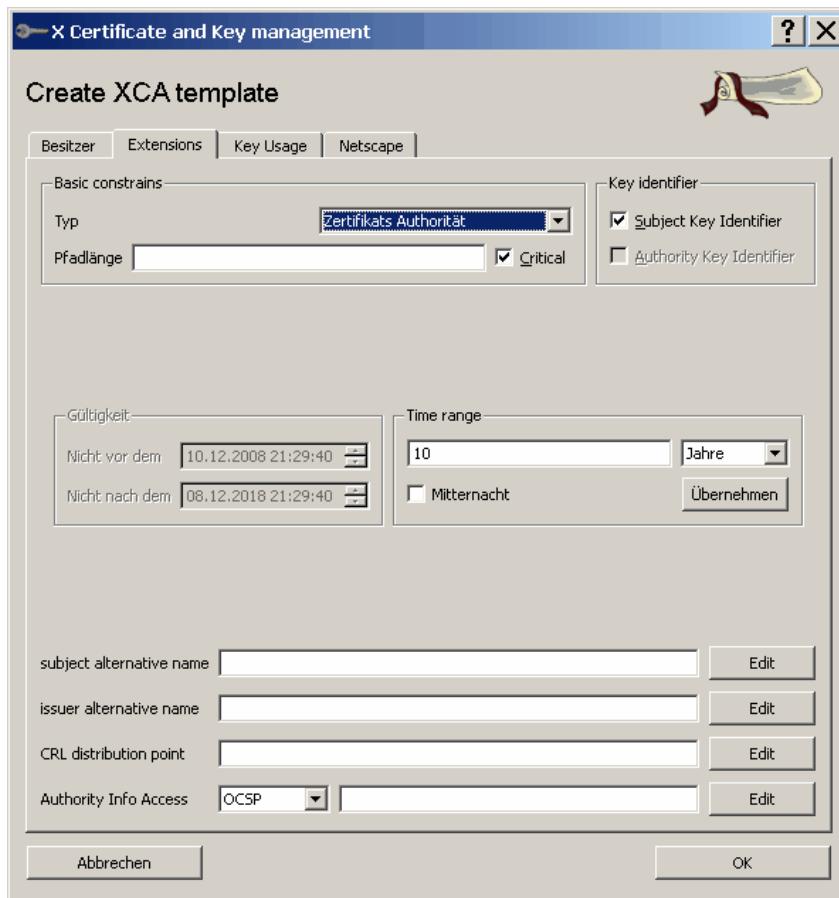
Interner Name	CA_Template	Firma	Muster
Länder code	DE	Firmenabteilung	EDV
Bundesland, Kreis	NRW	Üblicher Name	Frau Mustermann
Ort	Musterstadt	E-Mail Adresse	info@mustermal.de

Below these fields is a "commonName" dropdown menu, an empty text input field, and "Hinzufügen" and "Löschen" buttons. Underneath is a table with two columns: "Type" and "Content".

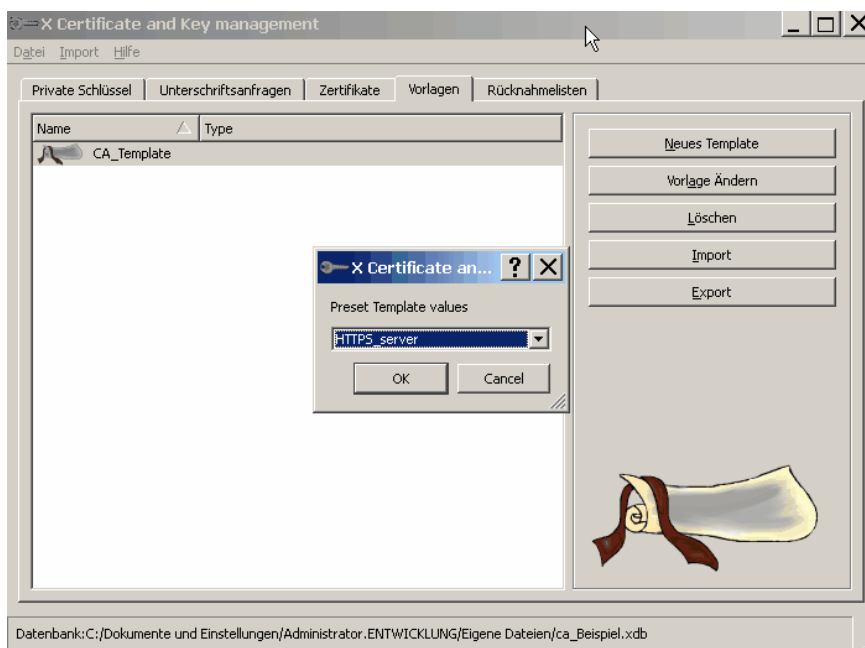
At the bottom, there is a "Privater Schlüssel" section with a dropdown menu, a checkbox labeled "Used keys too", and a button labeled "Erstelle einen neuen Schlüssel".

At the very bottom of the dialog are "Abbrechen" and "OK" buttons.

Im Reiter Extensions kann man die Standard-Gültigkeitsdauer der Zertifikate anpassen. Wählen Sie tendenziell einen langen Zeitraum.



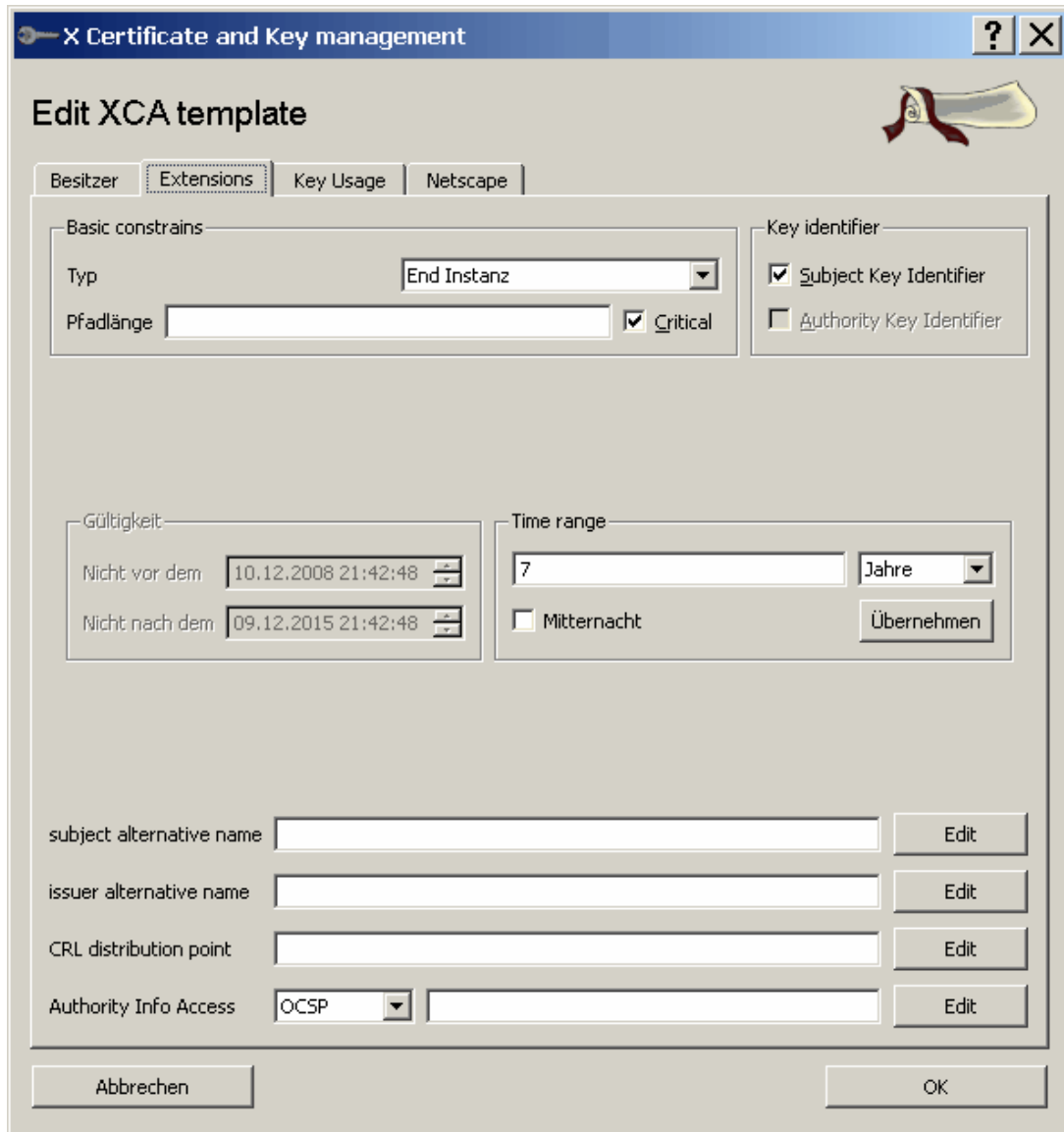
Wiederholt den Vorgang mit HTTPS\_server



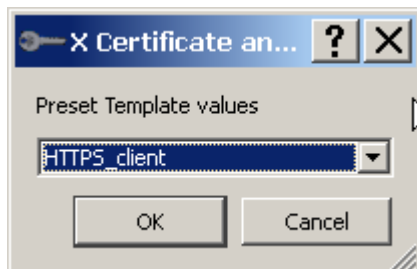
Als Internal Name empfiehlt sich etwas wie "OpenVPN\_Server\_Template". Die restlichen Werte wie beim CA-Template.

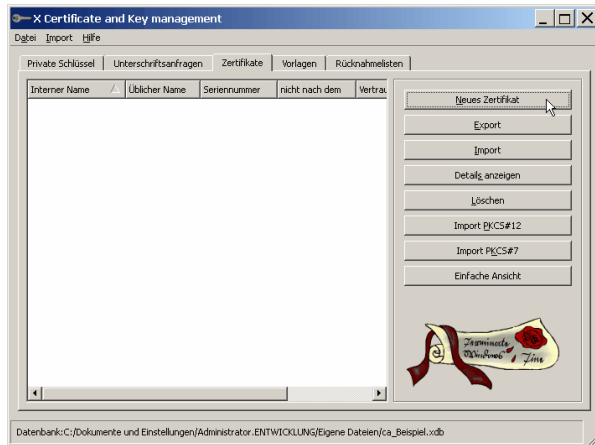
Besondere Aufmerksamkeit sollte die Gültigkeit des Zertifikates haben. Da man

Zertifikate in der Praxis nicht wirklich zurück rufen kann, könnte es zweckmäßig sein diese auch einmal auslaufen zu lassen. Sonst wählen Sie einen möglichst langen Zeitraum:



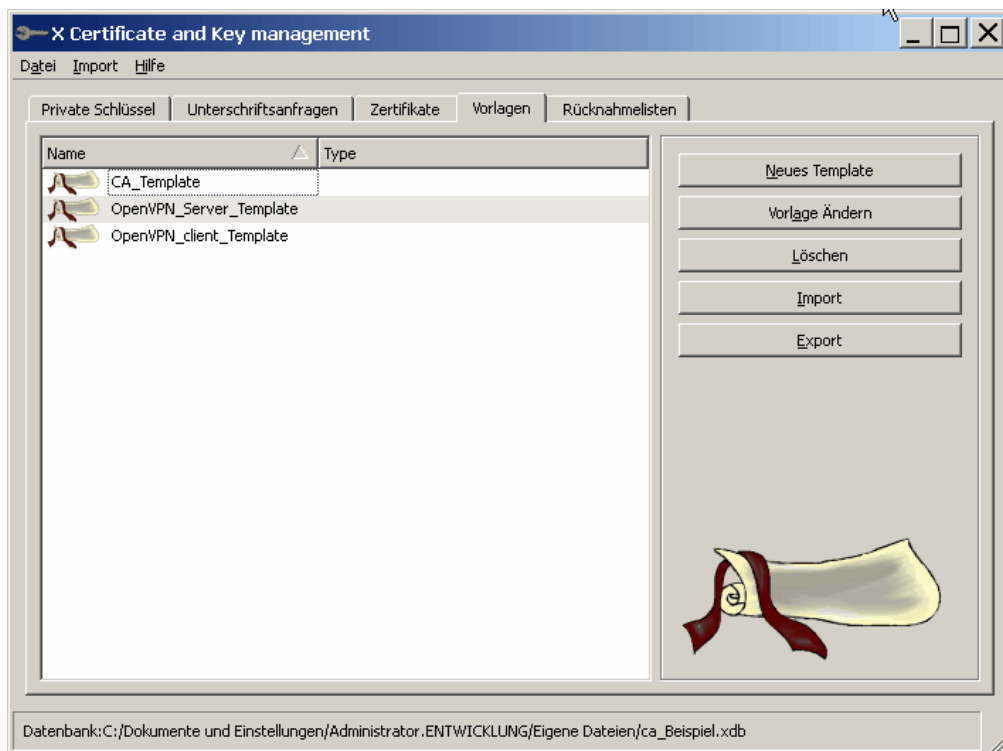
Erzeugt ein drittes Template mit Preset HTTPS\_client.





Nehmt die selben Werte wie beim Server-Template und der CA, nur wieder einen anderen internen Namen (z.B. OpenVPN\_client\_Template).

Prima, damit hätten wir dieses erledigt.

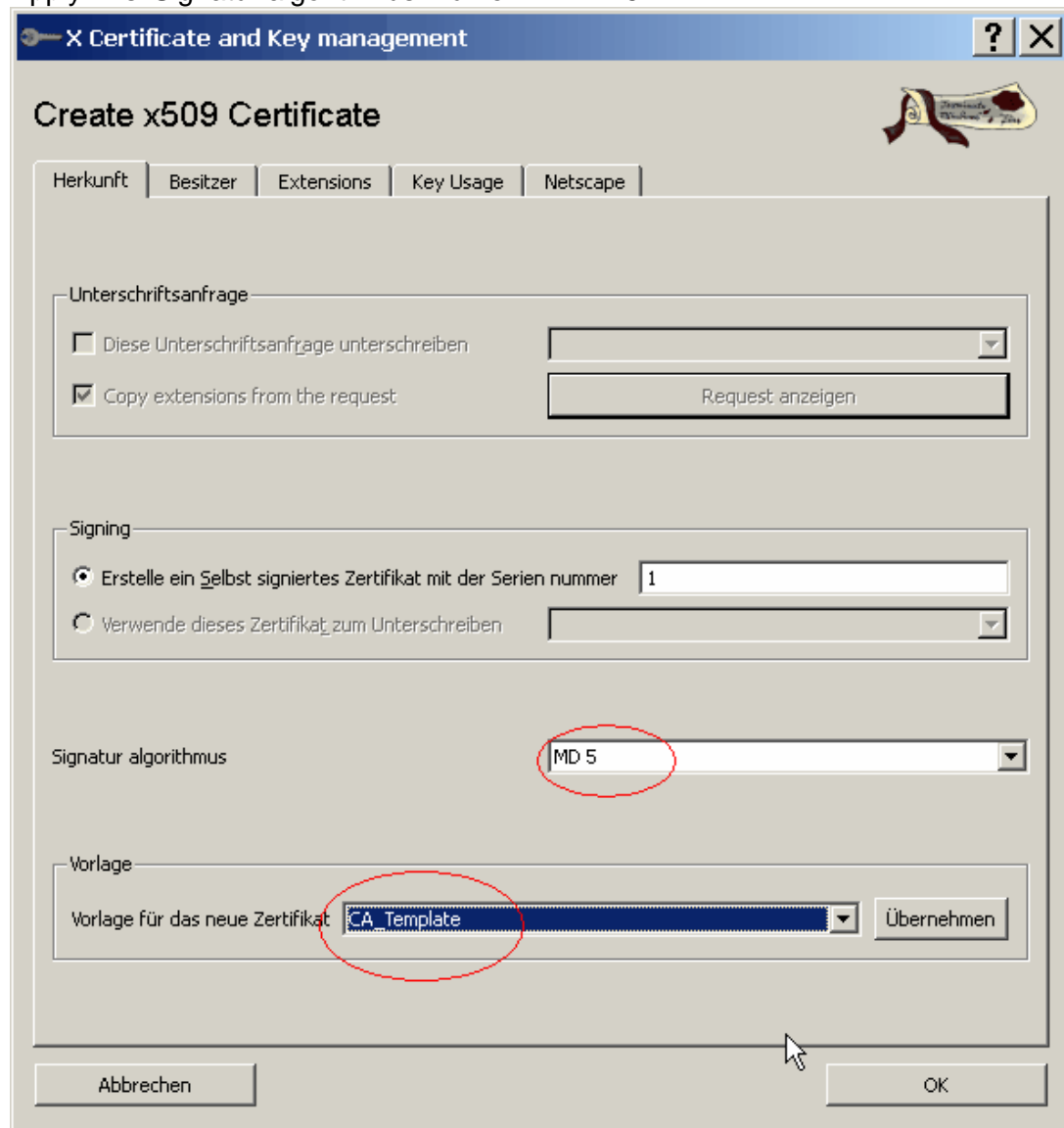


## Erzeugen einer CA

Nun können wir eine CA aus dem Template erzeugen.

Gehen Sie nach Zertifikate - Neues Zertifikat

Im Reiter Source wählen Sie Ihr CA-Template aus ("CA\_Template") und klickt auf Apply. Als 'Signatur algorithmus' wählen wir 'MD5'.



The screenshot shows a Windows dialog box titled "Certificate and Key management" with a sub-title "Create x509 Certificate". The dialog has several tabs: "Herkunft", "Besitzer", "Extensions", "Key Usage", and "Netscape". The "Herkunft" tab is selected. In the "Unterschriftenanfrage" section, there are two checkboxes: "Diese Unterschriftenanfrage unterschreiben" (unchecked) and "Copy extensions from the request" (checked). A "Request anzeigen" button is next to the second checkbox. In the "Signing" section, there are two radio buttons: "Erstelle ein Selbst signiertes Zertifikat mit der Seriennummer" (selected) and "Verwende dieses Zertifikat zum Unterschreiben". The "Erstelle ein Selbst signiertes Zertifikat mit der Seriennummer" option has a text input field containing "1". In the "Signatur algorithmus" section, a dropdown menu is set to "MD 5", which is circled in red. In the "Vorlage" section, a dropdown menu is set to "CA\_Template", which is also circled in red. There is an "Übernehmen" button next to the dropdown. At the bottom of the dialog, there are "Abbrechen" and "OK" buttons. A mouse cursor is pointing at the "OK" button.

Im Reiter Subject gebt ihr der CA nun einen Common Name. Beispiel: OpenVPN\_CA. Die restlichen Felder sollten aus dem Template übernommen worden sein.

**Klicken Sie bitte auf übernehmen.**

Im Reiter *Besitzer* gebt ihr der CA nun einen *Common Name*. Ich darf Ihnen empfehlen: OpenVPN\_CA. Die restlichen Felder sollten automatisch aus dem Template übernommen worden sein.

**Create x509 Certificate**

Herkunft | **Besitzer** | Extensions | Key Usage | Netscape

Distinguished name

Interner Name:  Firma:

Länder code:  Firmenabteilung:

Bundesland, Kreis:  Üblicher Name:

Ort:  E-Mail Adresse:

commonName:

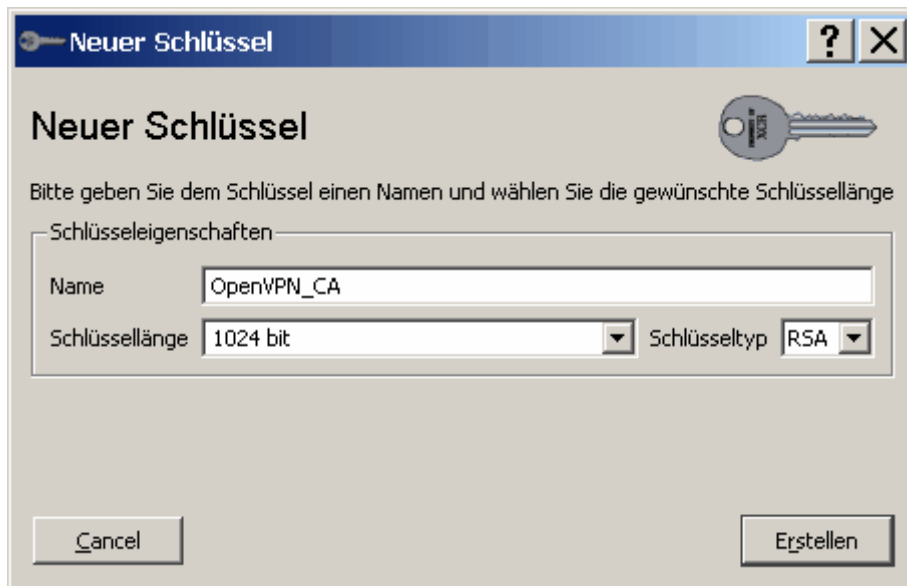
	Type	Content
1	commonName	OpenVPN_CA

Privater Schlüssel

Used keys too

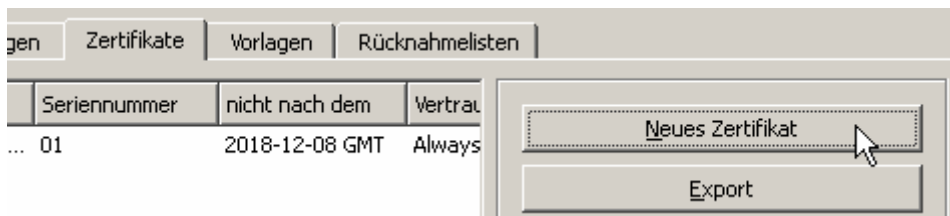
Danach klicken Sie auf "Erstelle einen neuen Schlüssel." Gebt dem Key am besten den selben Namen wie der *Common Name* der CA, also in unserem Beispiel "OpenVPN\_CA"

Die Schlüssellänge wählen Sie nach Ihrem Sicherheitsbedürfnis - wobei hohe Schlüssellängen dem Rechner Performance kosten: man sollte es auch nicht übertreiben. 1024 bit erscheinen in der Regel als einen angemessenen Wert.



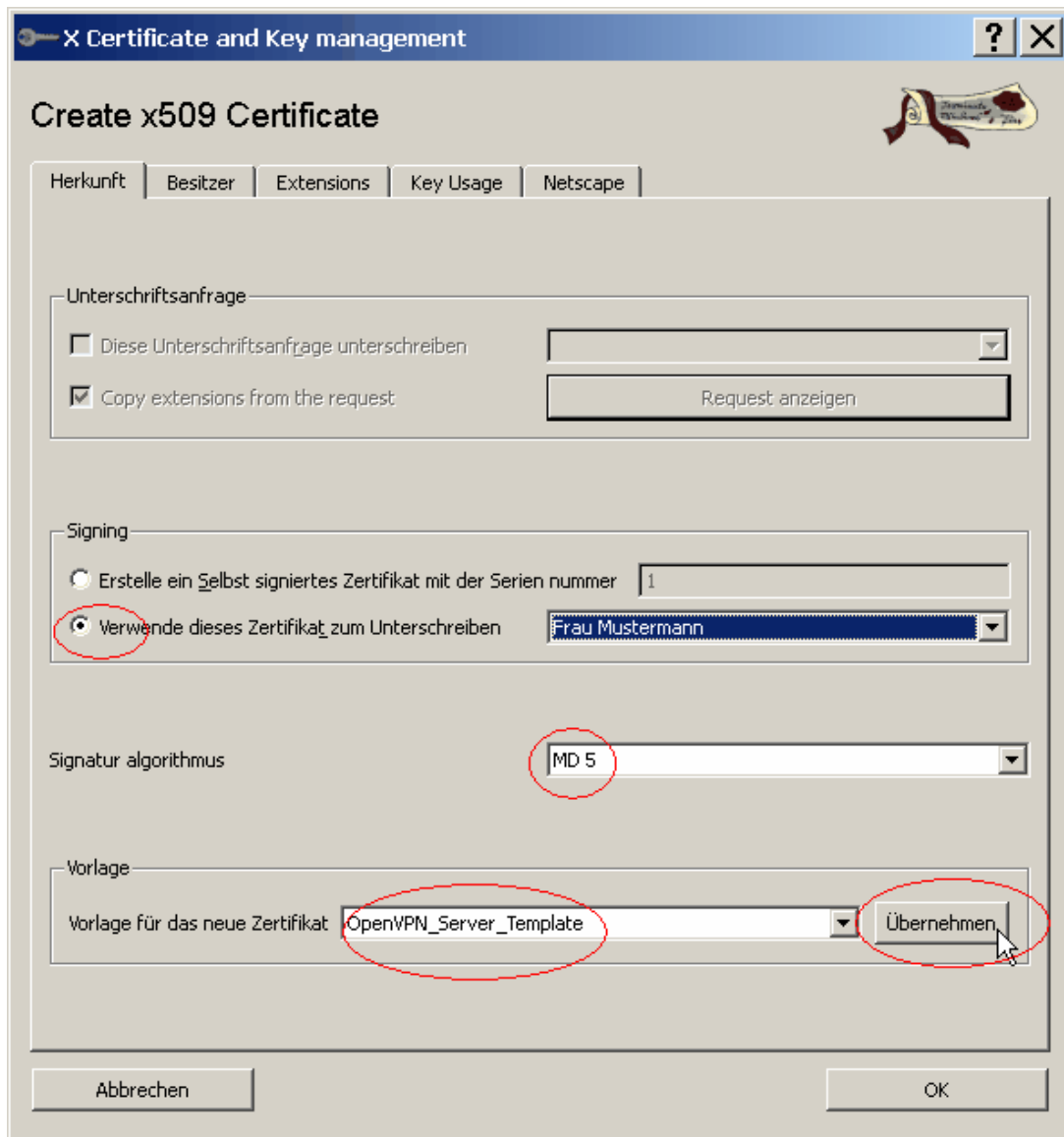
### Erzeugen eines Server-Zertifikats

Wieder geht es zum neuen Zertifikat.

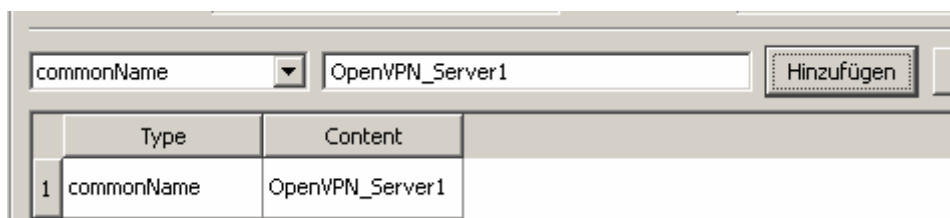


Als 'Signatur algorithmus' wählen wir 'MD5'. Beim Unterpunkt Signing wählen Sie das vorherige Zertifikat zur Unterschrift.

Als Vorlage dient diesmal das Server-Template: **unbedingt auf Übernehmen** klicken.



Weiter geht es wieder zum Besitzer: man kann beispielsweise "OpenVPN\_Server1" eintragen. Die anderen Felder sollten vom Template automatisch übernommen worden sein.

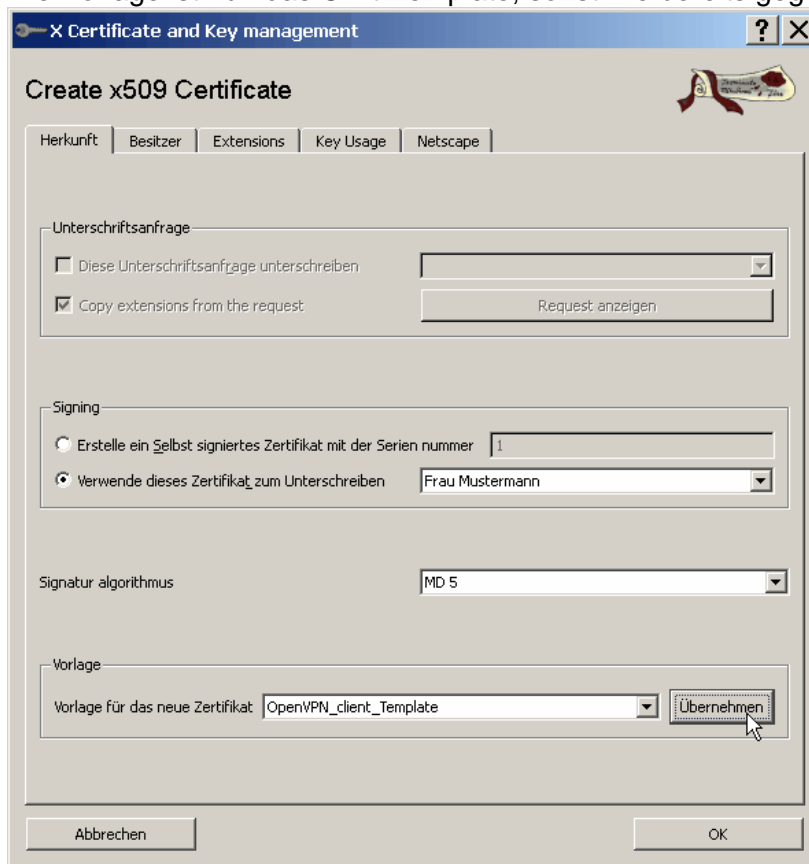


Erzeugt nun für dieses Zertifikate einen neuen Schlüssel und nennt ihn wie der Common Name des Zertifikats.



### Erzeugen der Client-Zertifikate

Für jeden Client muß ein eigenes Zertifikat erstellt werden. Die Vorlage ist nun das Client-Template, sonst wie bereits gegeben:



Ganz wichtig: die Common Names müssen immer eindeutig sein. Beispiel: OpenVPN\_Client1, OpenVPN\_Client2, etc.

**Create x509 Certificate**

Herkunft | Besitzer | Extensions | Key Usage | Netscape

Distinguished name

Interner Name:  Firma:

Länder code:  Firmenabteilung:

Bundesland, Kreis:  Üblicher Name:

Ort:  E-Mail Adresse:

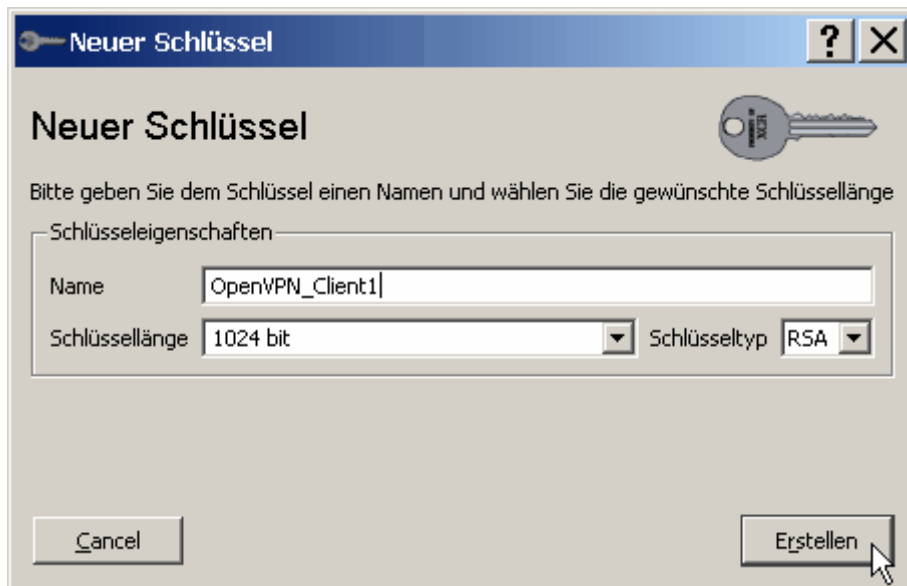
commonName:

	Type	Content
1	commonName	OpenVPN_Client1

Privater Schlüssel

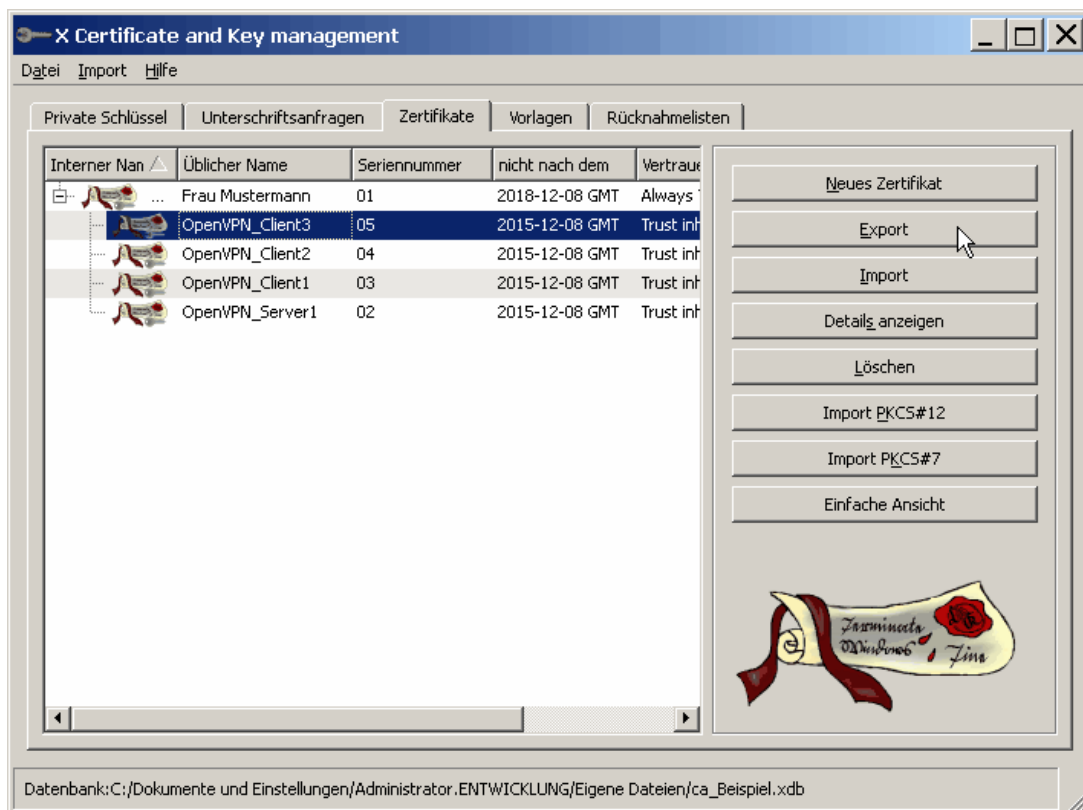
Used keys too

Natürlich wieder einen Schlüssel für jeden Client erzeugen. (Name = Common Name)



### Exportieren als PKCS#12-Dateien

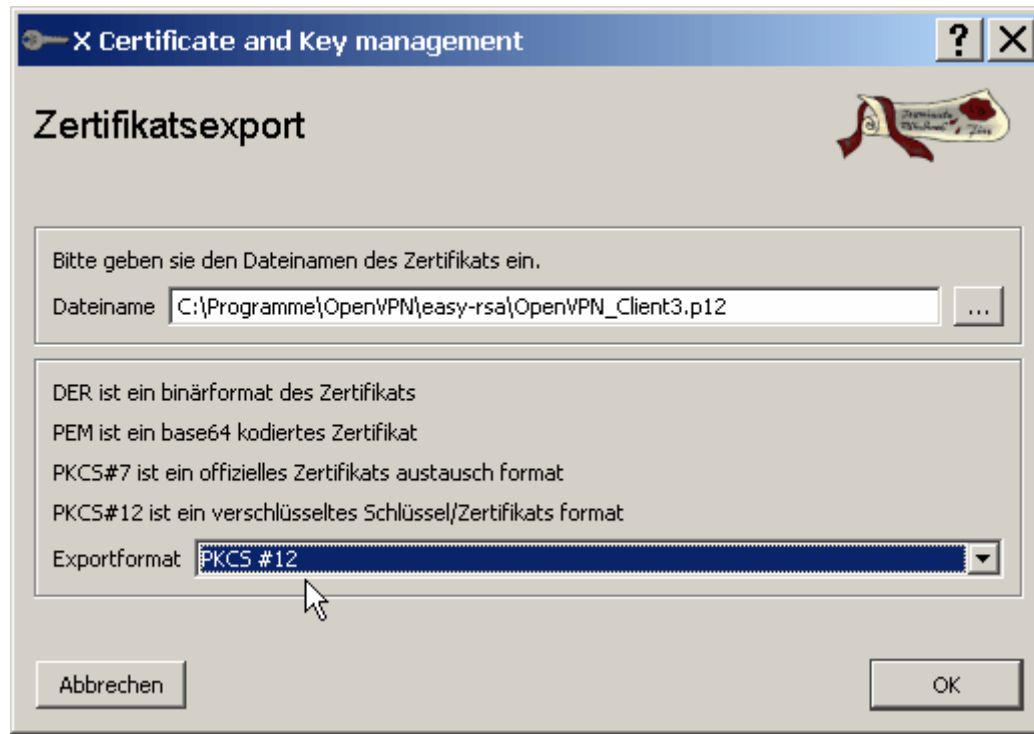
Damit die Schlüsselpaare in OpenVPN verwendet werden können, kann man sie kompakt in eine PKCS#12-Datei exportieren.



Wählen Sie nacheinander Clints und Server aus und exportieren Sie diese.

Dabei wählen Sie p12 Dateien.

Achtung Änderung: beim Export muss das Format "PKCS #12 with Certificate Chain" (Danke an Walter Laub)



Es wird nach einem Passwort gefragt, welches den privaten Schlüssel in der PKCS#12-Datei schützt. Beim Server wird normalerweise - damit dort ein Autostart möglich ist - kein Passwort verwendet. Bei den Clients sind Passwörter jedoch empfehlenswert: beachten Sie aber bitte, dass der Nutzer diese dann auch stets eingeben muss um sich mit dem Netzwerk zu verbinden.

Es kann möglicherweise sinnvoll sein, die Felder leer zu lassen und kein Passwort zu vergeben. Der Nutzer kann sich damit automatisierter mit dem Server verbinden was vielleicht handlicher ist und den Supportaufwand kleiner hält. Vielleicht wollen Sie unerwünschte Nutzung eher durch eine Limitierung der zeitlichen Gültigkeit des Zertifikates begrenzen ?

kleine Randnotiz zur Schonung des Servers: mit einem kleinen Aufrufbefehl z.B. in einer BAT-Datei kann der Nutzer die Verbindung zum Server nur bei Bedarf starten. Nutzen Sie den Befehl:

"\programme\openvpn\bin\openvpn-gui.exe --connect XXX.ovpn" Dabei ist XXX der Name des Config-Scriptes des Clints.

Wollen Sie die Performance des Servers schonen und Verbindungen ohne Traffic automatisch beenden, können Sie das Config-Script des jeweiligen Clints um die Zeile "inactive 300" bereichern.

Wenn Sie ein Passwort vergeben wollen:



### Einbinden in OpenVPN

Nachdem Sie nun die Zertifikate erstellt haben, kopieren für jeden Rechner seines in ein eigenes Verzeichnis. Ich darf Ihnen empfehlen, ein neues dazu anzulegen: C:\Programme\OpenVPN\cert wohin Sie die jeweilige Datei z.B. OpenVPN\_Client1.p12 hin kopieren.

Nun binden Sie dieses noch in die Konfigurations-Skriptes ein. Dazu gehen Sie in die jeweilige Datei mit der Endung .ovpn. (Im Verzeichnis C:\Programme\OpenVPN\config ) und tragen unter dem Punkt:

```
# SSL/TLS parms.  
# See the server config file for more  
# description. It's best to use  
# a separate .crt/.key file pair  
# for each client. A single ca  
# file can be used for all clients.
```

Dieses hier ein:

```
pkcs12 "C:\\Programme\\OpenVPN\\cert\\OpenVPN_Client1.p12"
```

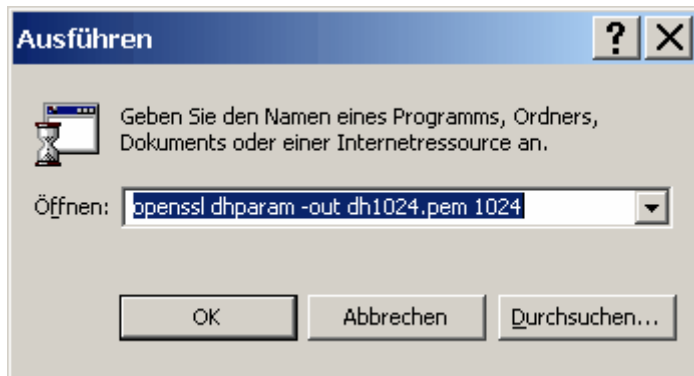
Hinweise auf andere Dateiformate für Zertifikate dürfen Sie inzwischen ignorieren: seitdem die wunderschön bequemen p12-Dateien möglich sind, gilt alles andere als nicht mehr zeitgemäß.

### was man noch so braucht:

Aus Sicherheitsgründen sollten Sie sich eine eigene DH-Datei erstellen.

Das geht sehr simpel mit der Eingabeaufforderung oder "ausführen als" und dem Befehl:

```
openssl dhparam -out dh1024.pem 1024
```



Die so erstellte Datei schliesst einige Sicherheitsprobleme und gehört auf den Server.

#### **Downloads für Sie:**

Damit Sie schnell an das Testen kommen habe ich Ihnen hier ein paar Zertifikate bereits vorproduziert. Bedenken Sie aber bitte, dass Sie um die Prozedur der eigenen Erstellung trotzdem nicht herum kommen: durch die Veröffentlichung an dieser Stelle ist die Sicherheit dieser Zertifikate nichts mehr wert.

Schauen Sie einmal hier:

<http://www.Optik-Berndt.de/xca-openvpn.html>

#### **Anmerkungen von Nutzern dieses Dokumentes:**

"...Hier gibt es ein gravierendes Problem: beim Export muss das Format "PKCS #12 with Certificate Chain" ausgewählt werden, sonst funktioniert der Tunnel nachher nicht!

Grüsse aus Coburg/BAY

Walter Laub"

#### **Zum guten Schluß:**

Der immense Funktionsumfang von openVPN und xca wird Ihnen noch viel Nutzen bringen: Sie werden sehen, das es nach einigen ersten Vorbereitungen gut und schnell von der Hand geht.

Ich darf Ihnen damit viel Spaß wünschen !

Ihr Christian Berndt



PS: Ich würde mich darüber freuen, wenn Sie meiner Webseite [www.Optik-Berndt.de](http://www.Optik-Berndt.de) und den dortigen Schwimmbrillen mit Glaswerten ein wenig Aufmerksamkeit schenken könnten.

copyright: dieses Dokument darf nach belieben frei verwendet werden. Über Ihre Anmerkungen und Notizen freue ich mich ! [info@Optik-Berndt.de](mailto:info@Optik-Berndt.de)