Konfigurations-Handbuch

INSYS icom

Industrielle Datenkommunikation

VPN mit INSYS-Routern

X509.v3-Zertifikate für VPNs mit XCA erzeugen

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 verschienen Teilnehmer in den jeweiligen VPN-Netzwerken. Ein Diffie-Hellman-Parametersatz ist bereits werksseitig auf dem INSYS-Router geladen, kann aber auch manuell ersetzt werden.

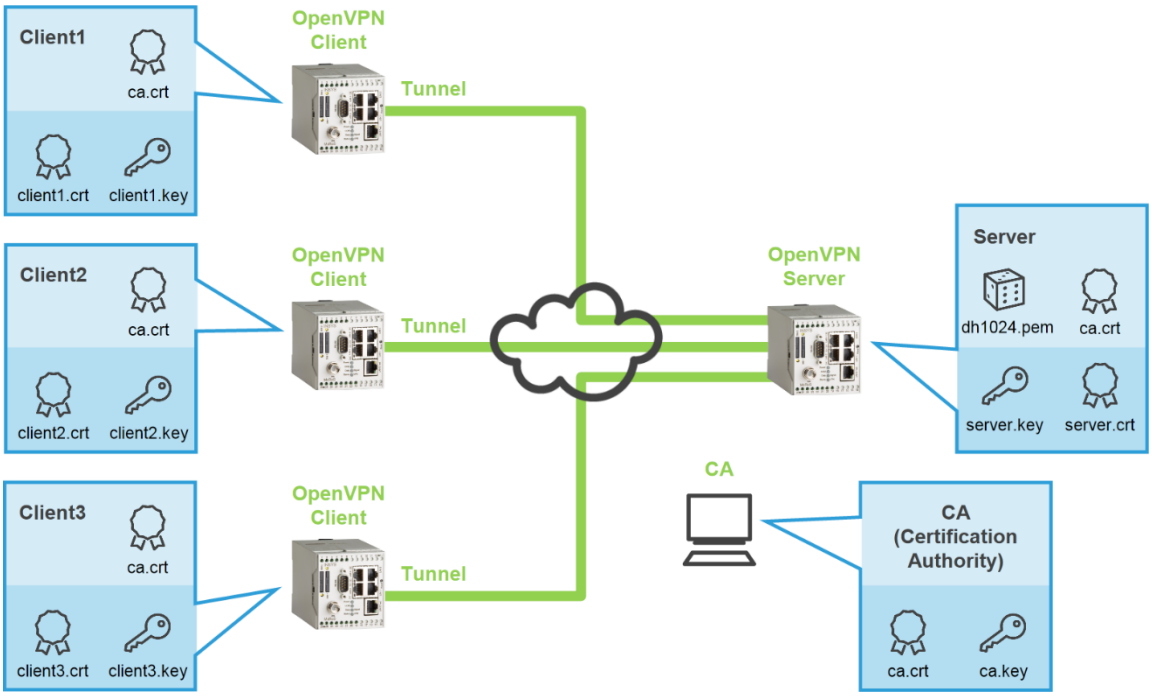


Abbildung 1: CA-Zertifikatsstruktur für OpenVPN-Server und -Client mit zertifikatsbasierter Authentifizierung, hier MoRoS als Server und als Clients

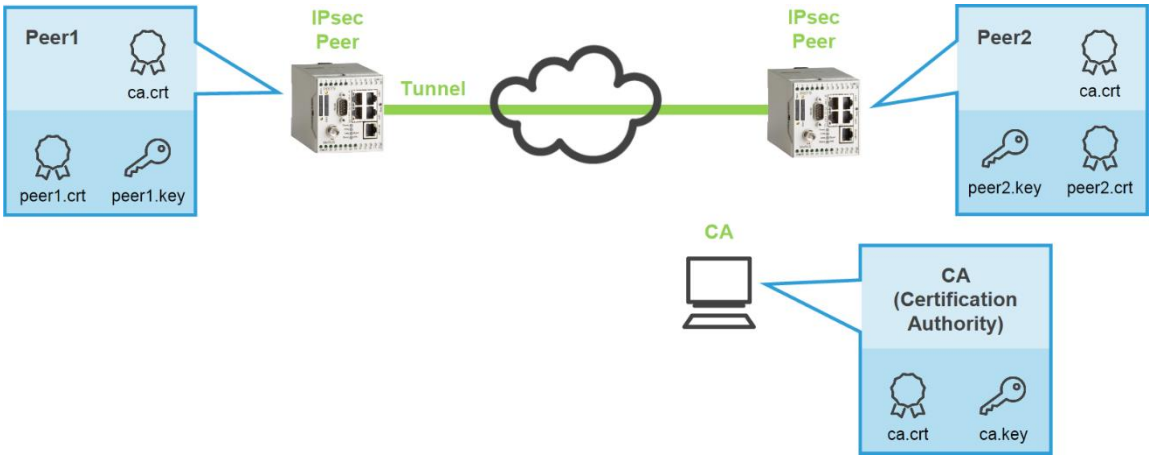


Abbildung 2: CA-Zertifikatsstruktur für IPsec-Teilnehmer mit zertifikatsbasierter Authentifizierung, hier MoRoS als Teilnehmer

2 Konfiguration

2.1 Vorbereitungen und Voreinstellungen

Vorbereitungen

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

- **XCA herunterladen**
- **XCA auf Windows-PC installieren**

- **XCA herunterladen**

  So laden Sie die Software XCA herunter.

→ PC mit ca. 30 MB freien Speicherplatz
→ Web-Browser
→ Internetverbindung

1. Öffnen Sie zum Download der Software http://sourceforge.net/projects/xca/
2. Klicken Sie auf Download.

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

3. Speichern Sie die Datei auf Ihrem PC.

✓ Damit haben Sie die Software XCA herunter geladen.

- **XCA auf Windows-PC installieren**

  So installieren Sie die Software XCA zum Erstellen der Zertifikate und Schlüssel erfolgreich auf Ihrem PC.

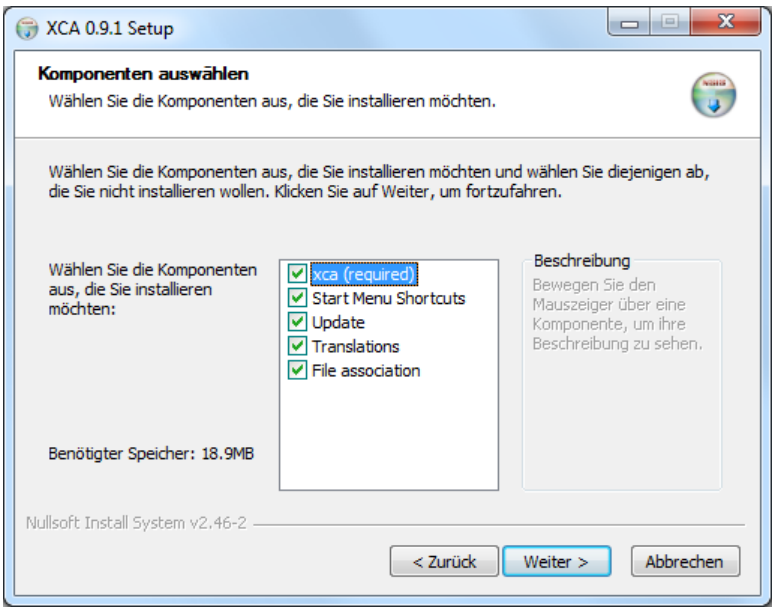
→ Sie haben die XCA-Setup-Datei (Version 0.9.1 oder höher) heruntergeladen.

1. Führen Sie die Installationsdatei aus (z.B.“setup_xca-0.9.1.exe“)

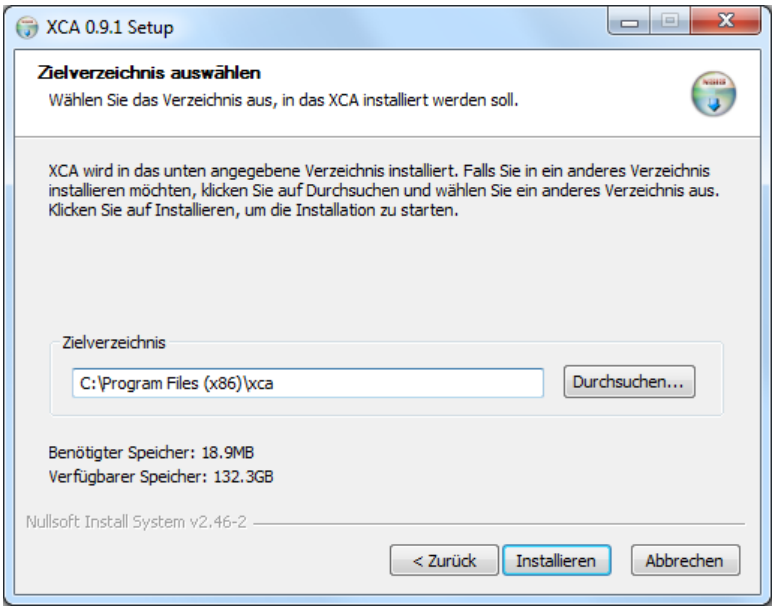
ⓘ *Führen Sie die Installationsdatei unter Windows 7 aus, indem Sie das Kontextmenü mit einem Rechtsklick öffnen und „Als Administrator ausführen“ wählen.*

✓ Falls eine Sicherheitswarnung angezeigt wird, quittieren Sie diese.

2. Wählen Sie als Installationssprache „Deutsch“ und klicken Sie auf OK.
3. Akzeptieren Sie das Lizenzabkommen mit Annehmen.
   ✓ Das Fenster zur Auswahl der Komponenten erscheint:



4. Übernehmen Sie die Auswahl aller Komponenten und klicken Sie auf Weiter.
   ✓ Das Fenster zum Festlegen des Zielverzeichnisses erscheint:



5. Legen Sie das Zielverzeichnis fest und klicken Sie auf Installieren.
6. Schließen Sie die Installation mit Fertig stellen ab.
   ✓ Damit haben Sie die Software XCA erfolgreich auf Ihrem PC installiert und die Vorbereitungen abgeschlossen.

Voreinstellungen in XCA

Bevor Sie mit XCA eine Zertifikatsstruktur erstellen können, müssen Sie eine Projektdatenbank erstellen. In dieser Datenbank werden alle Schlüssel und Zertifikate dieses CA-Projekts abgelegt.

Zum schnellen und fehlerfreien Erzeugen der Schlüssel- und Zertifikatsdateien ist es hilfreich, Vorlagen für CA-, Server- und Client-Zertifikate zu erstellen.

Führen Sie dazu folgende Voreinstellungen durch:

- XCA starten und Datenbank erstellen
- Eine CA-Vorlage erstellen
- Eine Server-Vorlage erstellen
- Eine Client-Vorlage erstellen

XCA starten und Datenbank erstellen

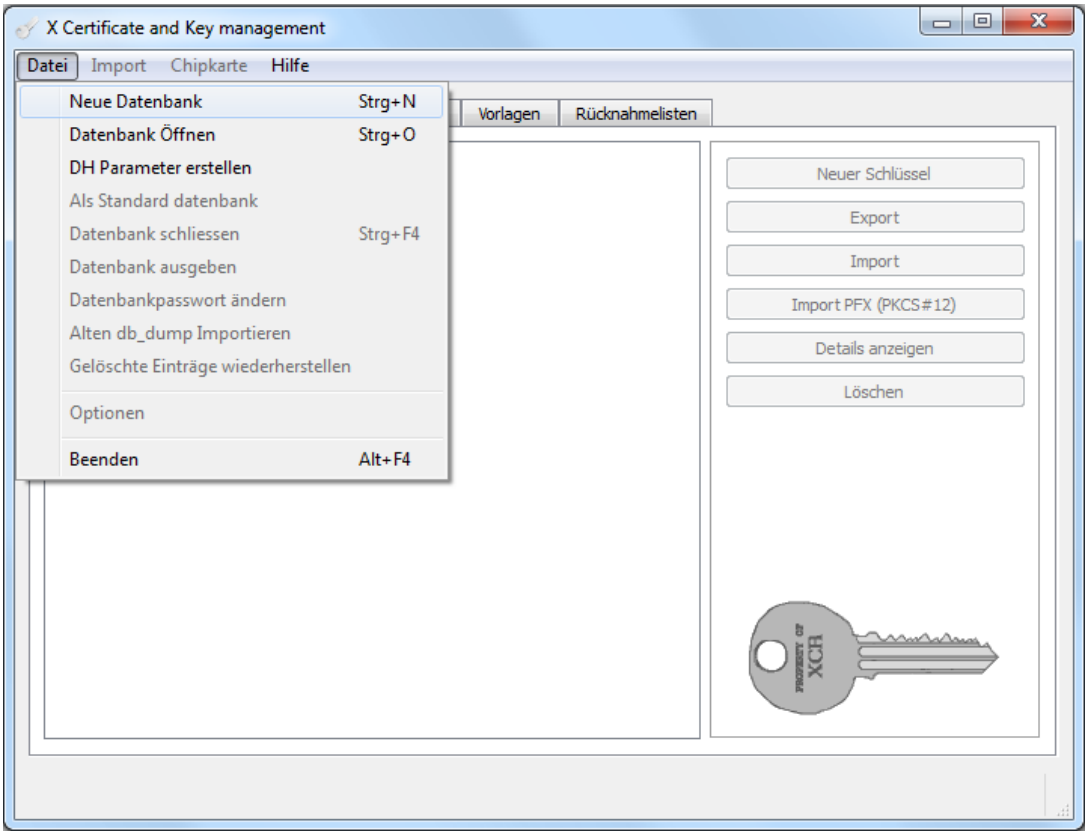
So starten Sie die Software XCA und erstellen eine neue Datenbank für das CA-Projekt.

→ Sie haben die Software XCA erfolgreich auf Ihrem PC installiert.

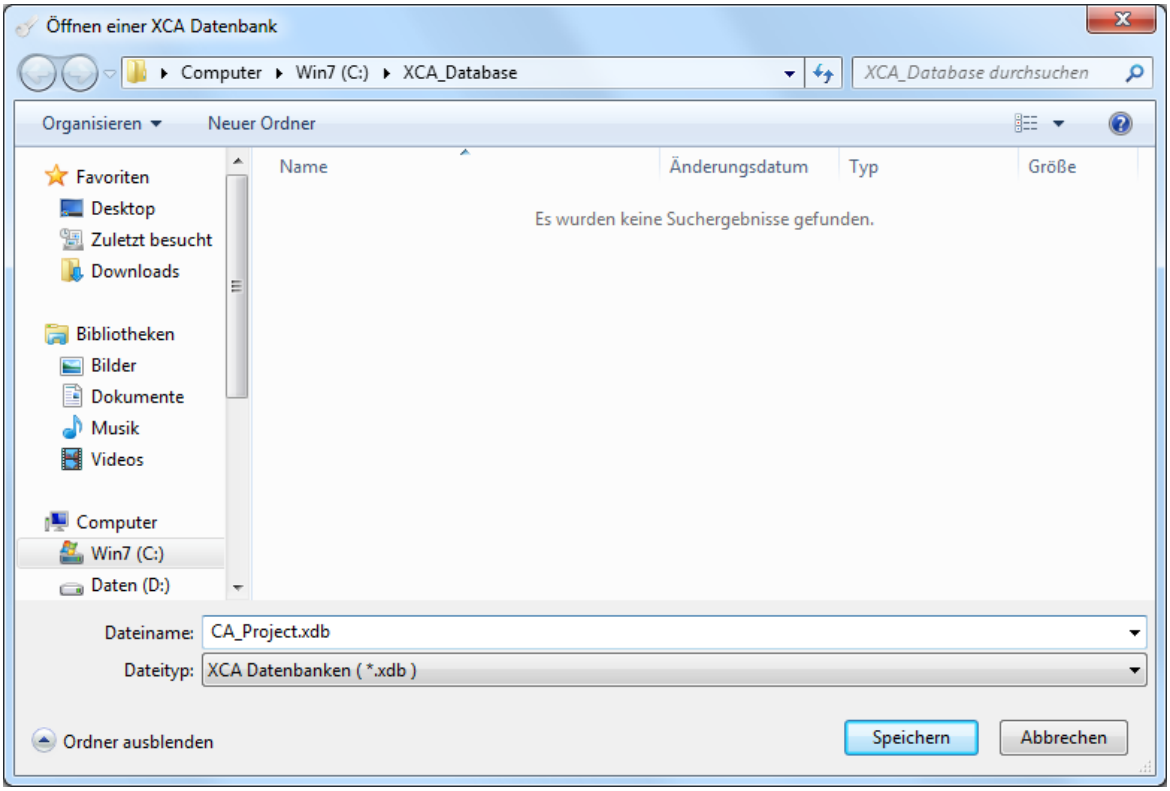
1. Wählen Sie im Start-Menü Programme → xca → xca

   ⓘ *Führen Sie das Programm unter Windows 7 aus, indem Sie das Kontextmenü mit einem Rechtsklick auf „xca“ öffnen und „Als Administrator ausführen“ wählen.*

   ✓ Das XCA-Programmfenster erscheint:



2. Wählen Sie im Menü „Datei“ die Option „Neue Datenbank“.
   ✓ Das Dialogfenster zur Auswahl der Datenbank erscheint:



3. Legen Sie Pfad und Dateinamen fest und klicken Sie auf Speichern.
   ✓ Das Dialogfenster zur Vergabe des Passworts erscheint:

4. Legen Sie ein Passwort fest und klicken Sie auf OK.

   ⓘ *Legen Sie unbedingt ein Passwort fest und merken Sie sich dieses gut, da Sie es jedes Mal benötigen, wenn Sie die Datenbank dieses CA-Projekts öffnen wollen.*

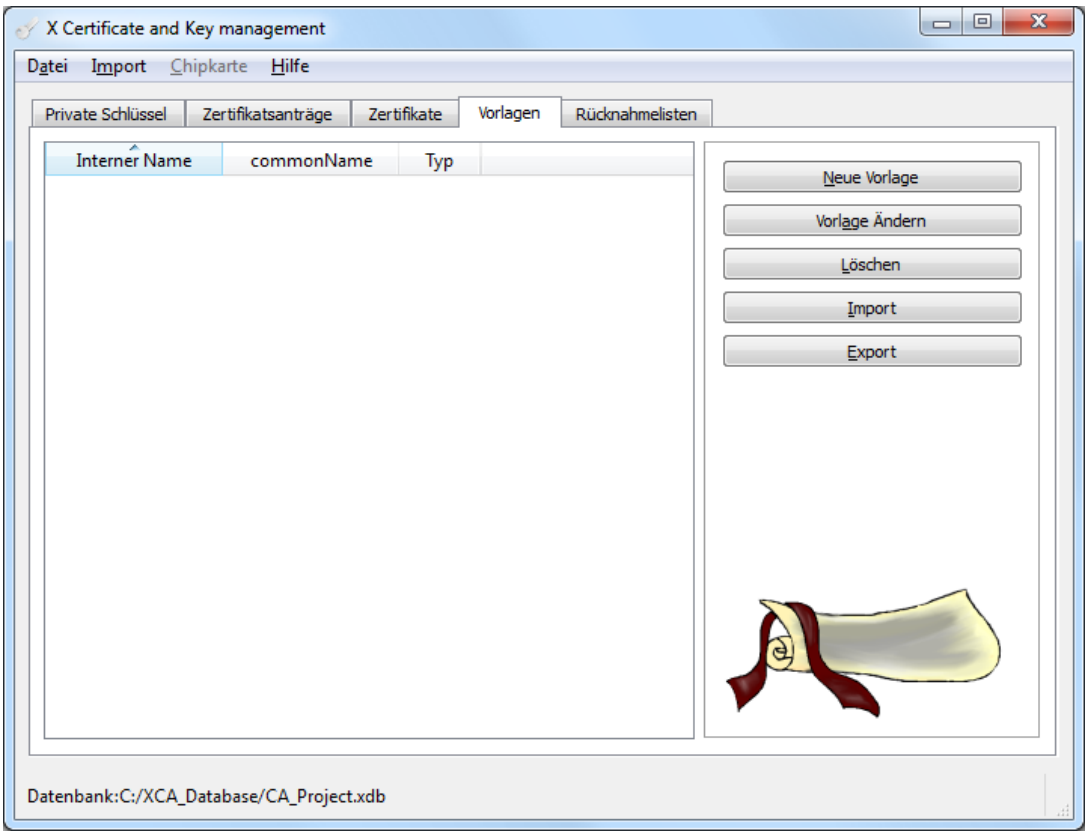
   ✓ Damit haben Sie eine neue Datenbank für das CA-Projekt erstellt.

■ CA-Vorlage erstellen

So erstellen Sie eine Vorlage für CA-Zertifikate.

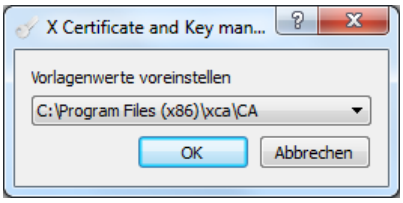
→ Die Software XCA ist gestartet und die Projektdatenbank geöffnet.

1. Wechseln Sie zum Reiter „Vorlagen“.



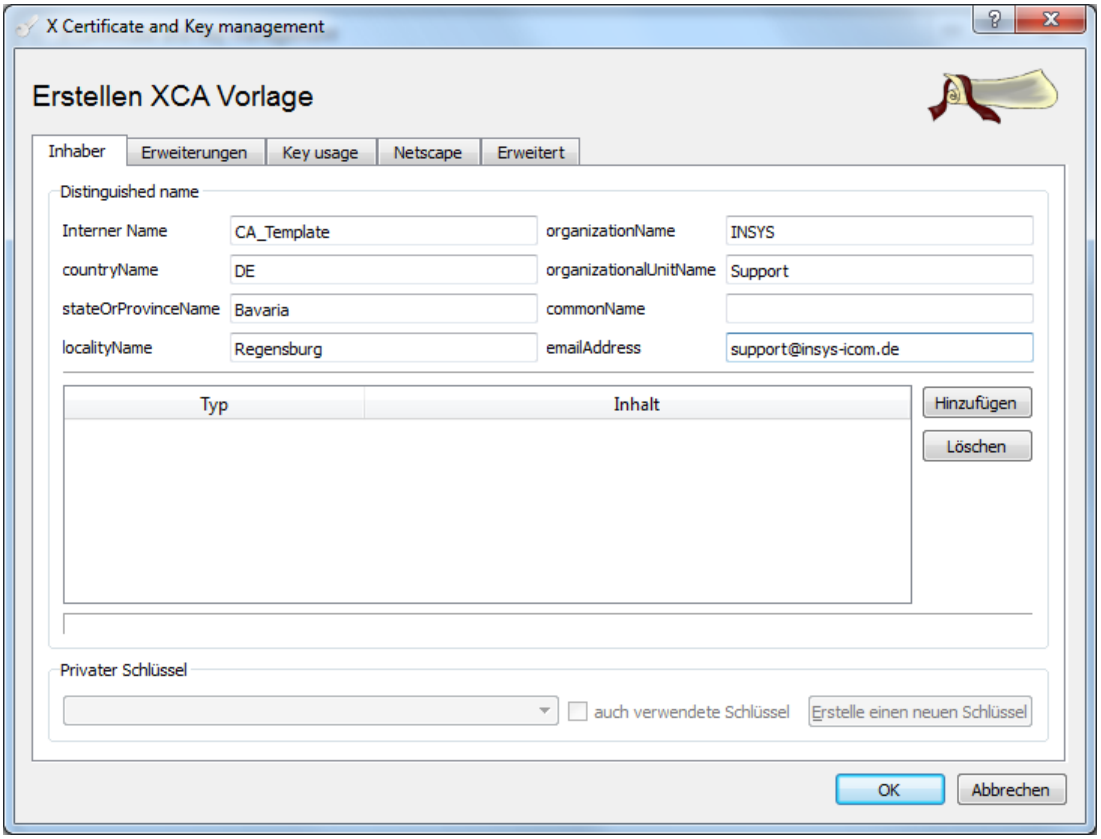
2. Wählen Sie Neue Vorlage.

✓ Das Dialogfenster zur Auswahl der Vorlagenwerte erscheint:

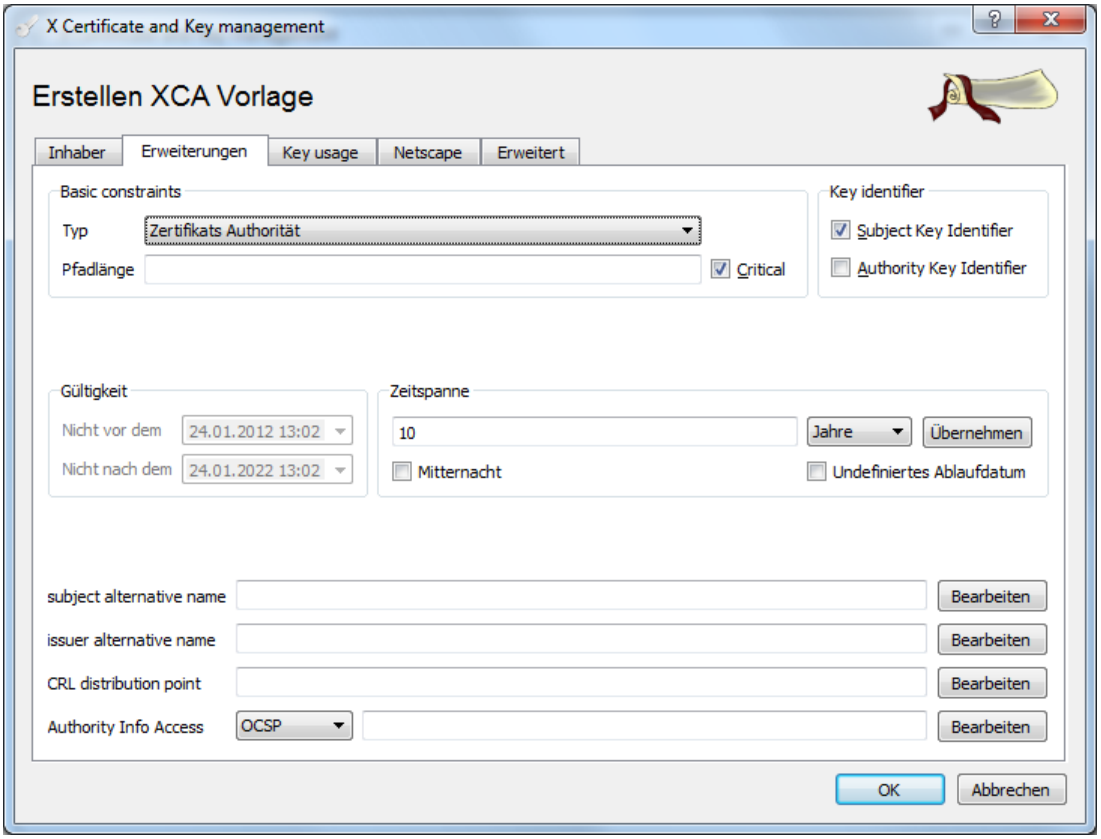


3. Wählen Sie „CA“ und klicken Sie auf OK.

✓ Das Dialogfenster zum Erstellen der Vorlage erscheint:



4. Legen Sie Ihre Vorgabewerte fest ohne einen „Common Name“ (Üblicher Name) zu vergeben.
5. Wechseln Sie zum Reiter „Erweiterungen“.



6. Passen Sie ggf. die Zeitspanne für die Gültigkeit des Zertifikats an und klicken Sie dann auf OK.

   ⓘ *Wählen Sie einen für Ihren Zweck angemessenen und sinnvollen Zeitraum. Die Vorgabewerte sind eine gute Richtlinie. Zu lange Zeitspannen können Sicherheits- oder Kompatibilitätsprobleme verursachen.*

7. Bestätigen Sie die Erstellung der Vorlage mit OK.

   ✓ Damit haben Sie eine Vorlage für ein CA-Zertifikat angelegt. Beim Erstellen eines CA-Zertifikats unter Verwendung dieser Vorlage werden die entsprechenden Felder mit den hier eingegebenen Werten vorbelegt.

■ Server-Vorlage erstellen

Gehen Sie beim Erstellen der Vorlage für Server-Zertifikate genauso vor, wie für die CA-Vorlage, wählen Sie jedoch bei der Auswahl der Vorlagenwerte „HTTPS_server“.

■ Client-Vorlage erstellen

Gehen Sie beim Erstellen der Vorlage für Client-Zertifikate genauso vor, wie für die CA- oder Server-Vorlage, wählen Sie jedoch bei der Auswahl der Vorlagenwerte „HTTPS_client“.

2.2 Zertifikate erzeugen

Zertifikatsstruktur mit XCA erzeugen

Eine Public-Key-Infrastruktur (PKI) umfasst Dienste 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 jeweiligen Geräte hochgeladen.

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

Für den OpenVPN-Server:

- das CA-Zertifikat (z.B. ca.crt)
- das Server-Zertifikat (z.B. server.crt)
- den Server-Schlüssel (z.B. server.key)
- einen Diffie-Hellman-Parametersatz (z.B. dh1024.pem)

ⓘ *Die Erzeugung eines Diffie-Hellman-Parametersatzes mit XCA (Menü Datei – DH Parameter erstellen) ist hier nicht beschrieben, da auf jedem INSYS-Router im Auslieferungszustand ein solcher geladen ist. Der Diffie-Hellman-Parametersatz kann im Web-Interface des INSYS-Routers auf der Seite „OpenVPN-Server" im Abschnitt „Authentifizierung mit Zertifikaten" heruntergeladen werden.*

Für jeden OpenVPN-Client (1-n):

- das CA-Zertifikat (z.B. ca.crt)
- ein Client-Zertifikat (z.B. client1.crt)
- einen Client-Schlüssel (z.B. client1.key)

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

ⓘ *Das CA-Zertifikat ist für jeden Client (und auch den Server) dasselbe.*

ⓘ *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. Er muss von der CA streng gesichert werden und darf niemals exportiert werden.*

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

Für jeden der beiden IPsec-Teilnehmer:

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

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

ein Teilnehmer-Schlüssel (z.B. peer1.key)

ⓘ *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:

- CA-Zertifikat und -Schlüssel erzeugen
- Zertifikat und Schlüssel für einen Server erzeugen
- Zertifikat und Schlüssel für einen Client erzeugen

■ CA-Zertifikat und -Schlüssel erzeugen

So erzeugen Sie mit XCA Ihre eigenen Zertifizierungsstelle (CA, Certificate Authority). Die CA-Zertifikatsstruktur besteht aus dem geheimen Schlüssel und dem öffentlichen Zertifikat.

ⓘ *Die Geheimhaltung des Schlüssels ist essentiell für die Sicherheit des gesamten Netzwerks.*

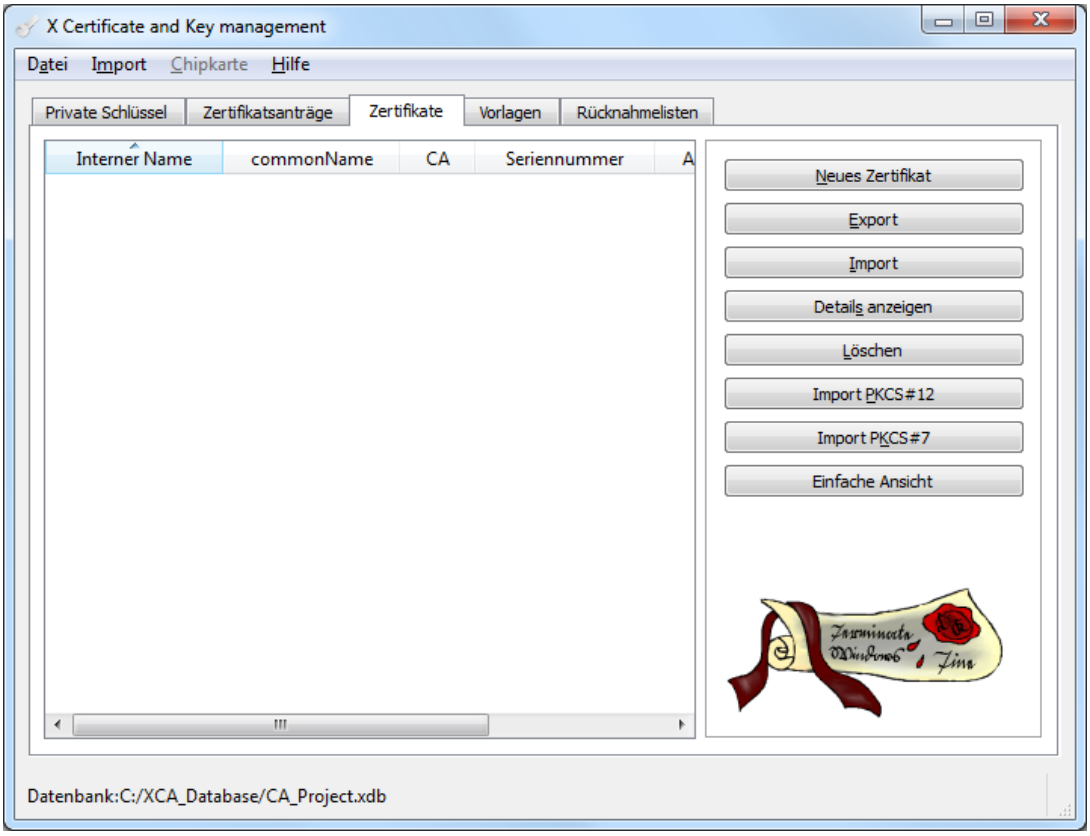
→ Die Software XCA ist gestartet und die Projektdatenbank geöffnet.

→ Eine CA-Vorlage wurde erstellt.

→ Uhrzeit und Datum im PC sind korrekt.

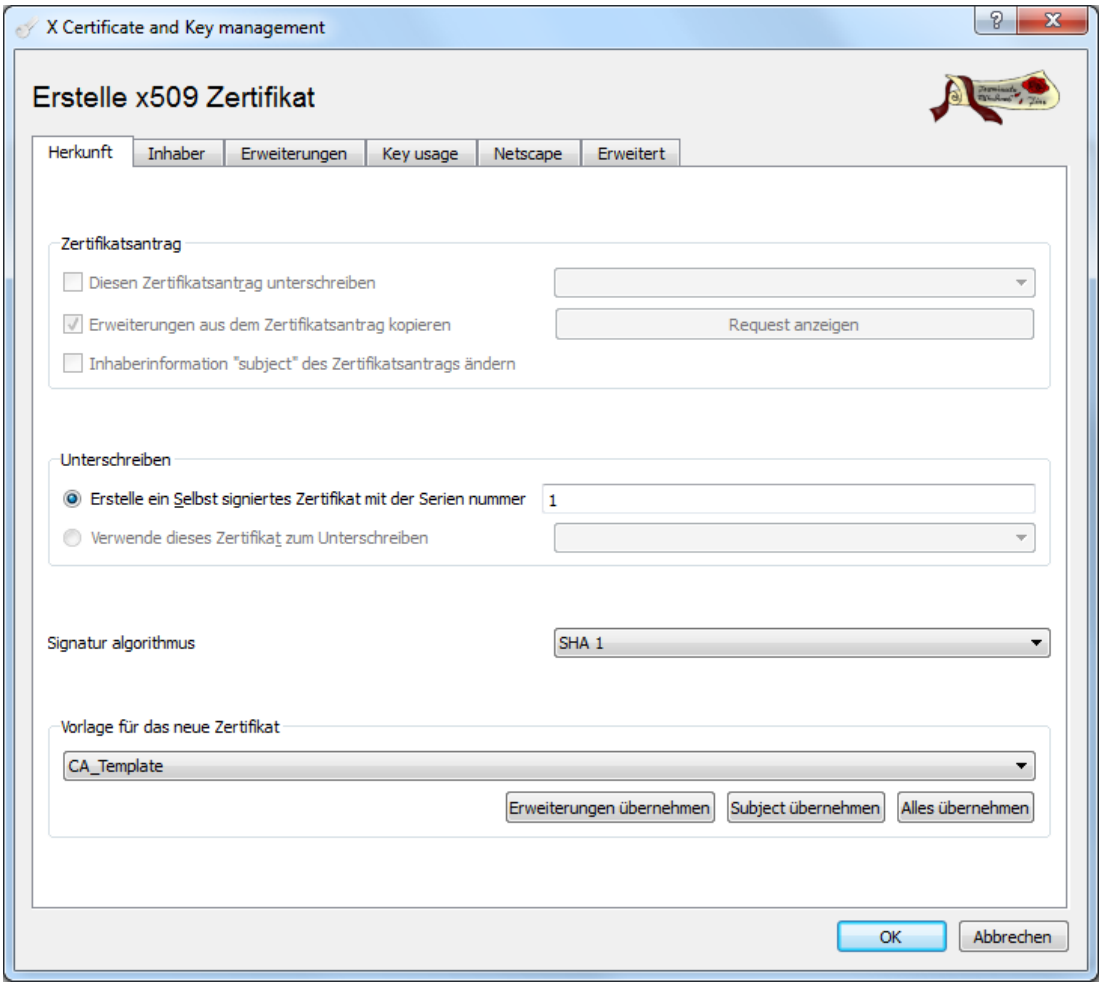
ⓘ *Zertifikate haben ein Gültigkeitsdatum. Eine falsche Systemzeit (Uhrzeit und Datum) sind häufige Fehlerquellen. Achten Sie deshalb auf die korrekte Systemzeit sowohl im PC bei der Erstellung als auch im INSYS-Router bei der Inbetriebnahme des Servers oder Clients.*

1. Wechseln Sie zum Reiter „Zertifikate“.

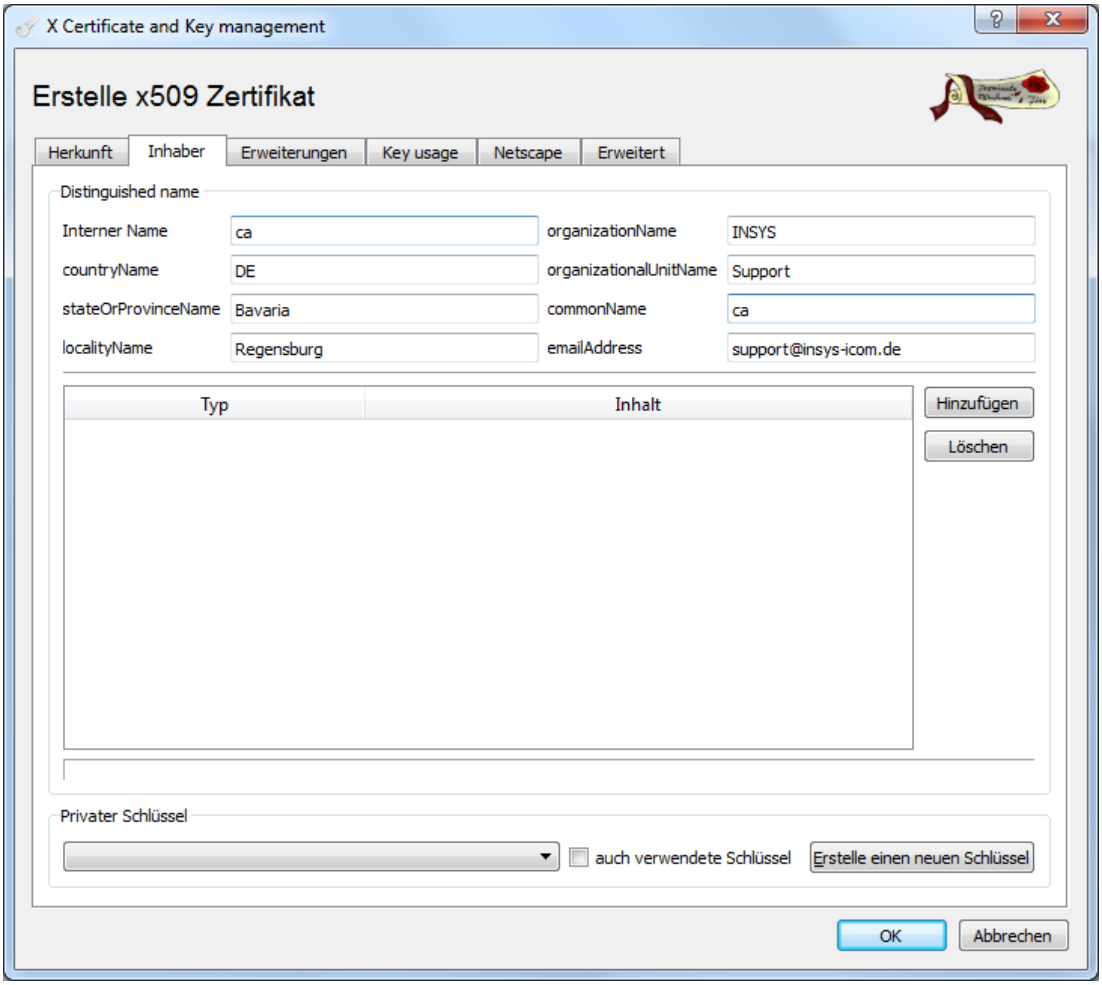


2. Wählen Sie Neues Zertifikat.

✓ Das Dialogfenster zur Erstellung eines Zertifikats erscheint:

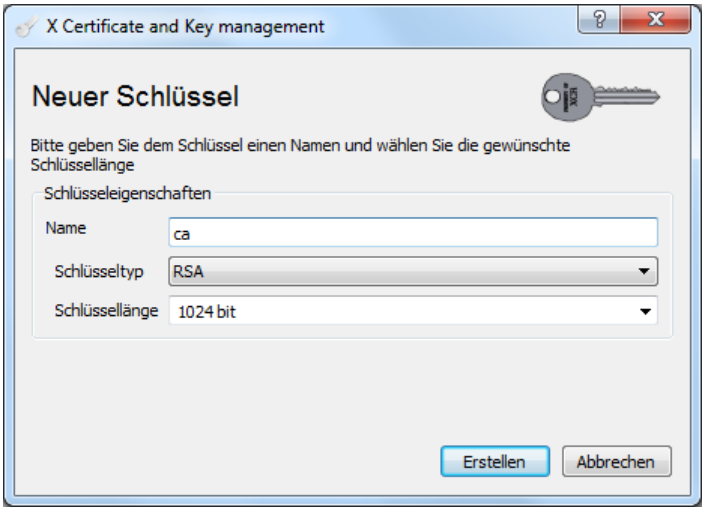


3. Wählen Sie als Vorlage die vorher erstellte CA-Vorlage.
4. Klicken Sie auf Alles übernehmen.
5. Wechseln Sie zum Reiter „Inhaber“.



6. Legen Sie den „Common Name“ (Üblicher Name) fest und vergeben Sie diesen auch als internen Namen (z.B. „ca“).
7. Klicken Sie auf Erstelle einen neuen Schlüssel.

   ✓ Das Dialogfenster zur Erstellung eines neuen Schlüssels erscheint:



8. Vergeben Sie vorzugsweise denselben Namen wie den „Common Name“.
9. Klicken Sie auf Erstellen.
10. Bestätigen Sie die Erstellung des Schlüssels mit OK.
11. Klicken Sie auf OK.

12. Bestätigen Sie die Erstellung des Zertifikats mit OK.
    ✓ Damit ist die Erzeugung der CA abgeschlossen.

■ Zertifikat und Schlüssel für einen Server erzeugen

So erzeugen Sie mit XCA den privaten Schlüssel und das öffentliche Zertifikat für einen Server.

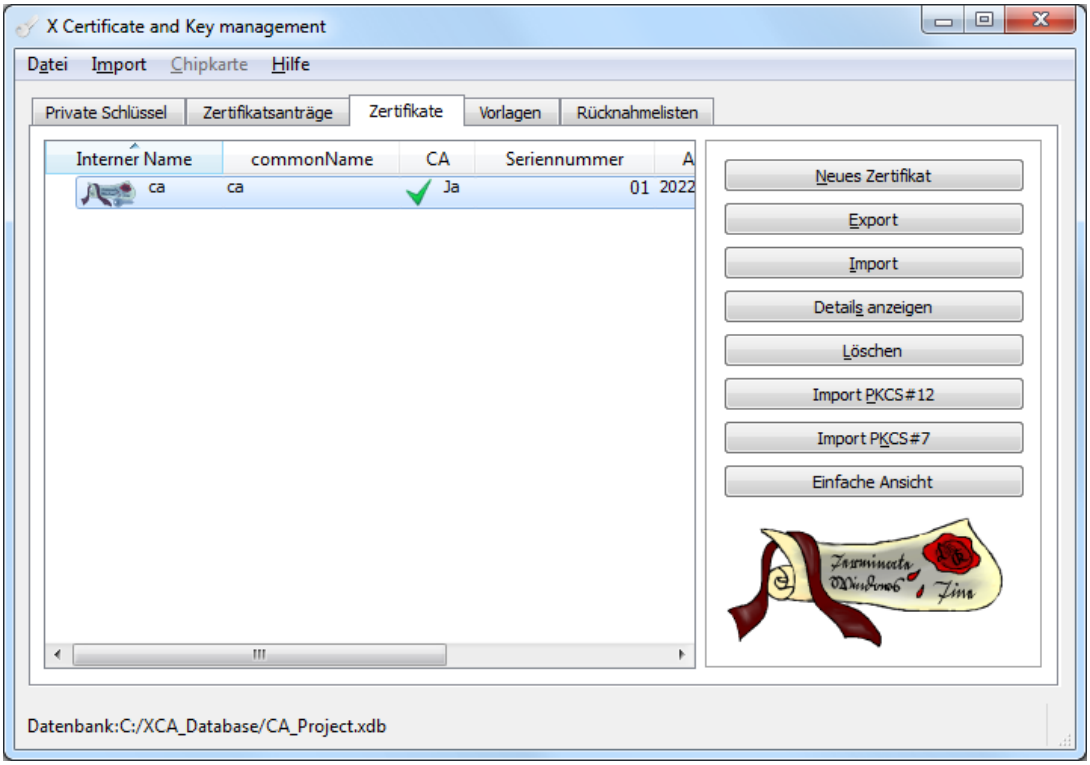
Für die Erzeugung benötigen Sie einen „Common Name“ für den Server. Der „Common Name“ ist der einzigartige Mitgliedsname eines Teilnehmers im gesicherten Netzwerk und wird z. B. zum Routing in die Clientnetze verwendet. Der „Common Name“ darf nur für einen Teilnehmer verwendet werden und ist nach der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

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

→ Die Software XCA ist gestartet und die Projektdatenbank geöffnet.
→ Eine Server-Vorlage wurde erstellt.
→ Ein CA-Zertifikat wurde erstellt.
→ Uhrzeit und Datum im PC sind korrekt.

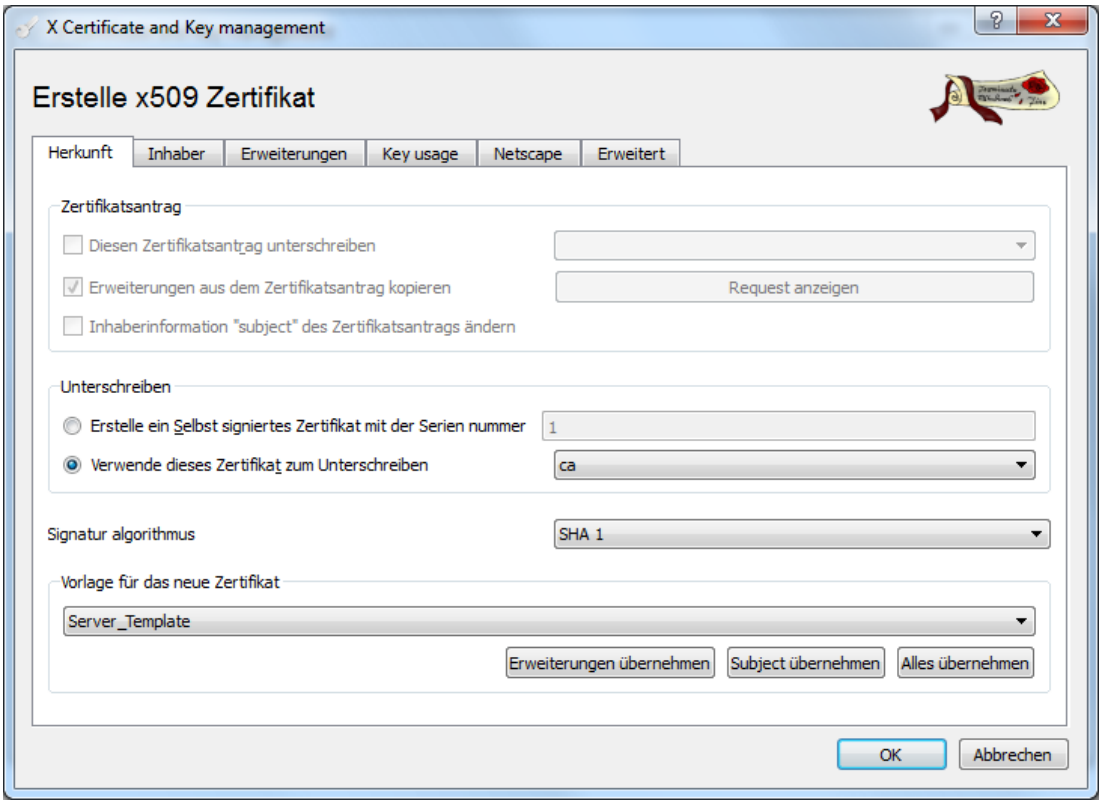
ⓘ *Zertifikate haben ein Gültigkeitsdatum. Eine falsche Systemzeit (Uhrzeit und Datum) sind häufige Fehlerquellen. Achten Sie deshalb auf die korrekte Systemzeit sowohl im PC bei der Erstellung als auch im INSYS-Router bei der Inbetriebnahme des Servers oder Clients.*

2. Wechseln Sie zum Reiter „Zertifikate“.

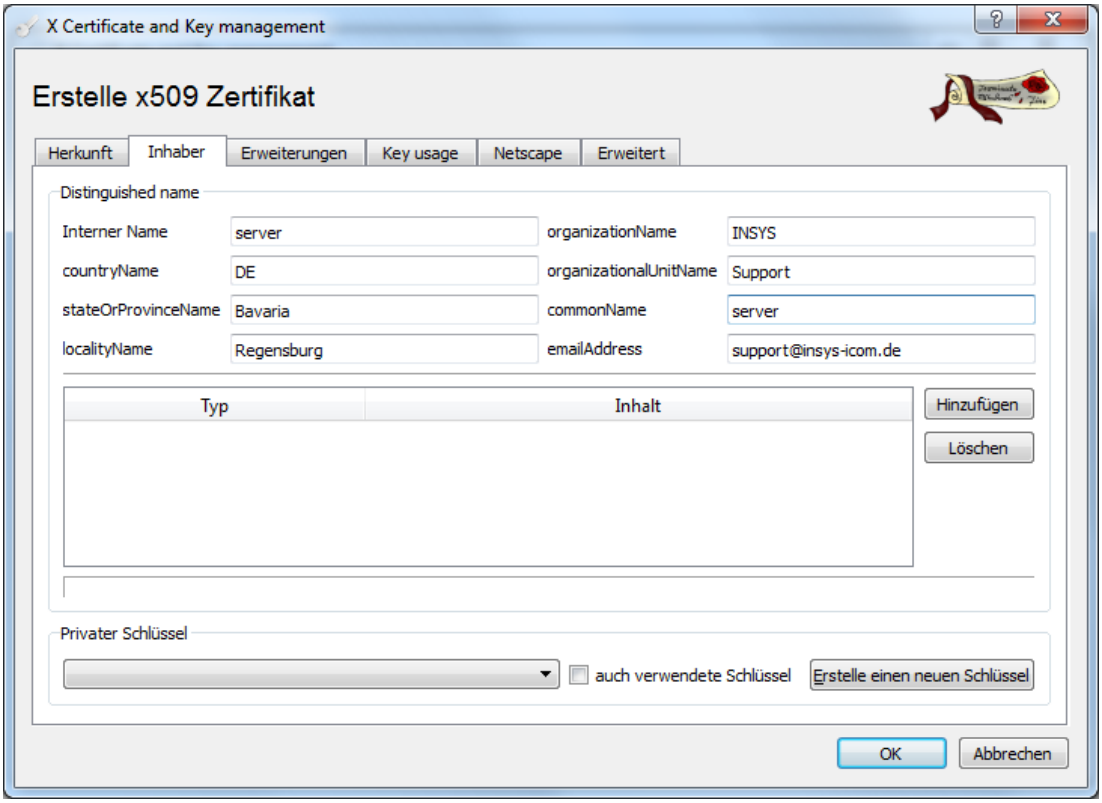


3. Markieren Sie das CA-Zertifikat und wählen Sie Neues Zertifikat.

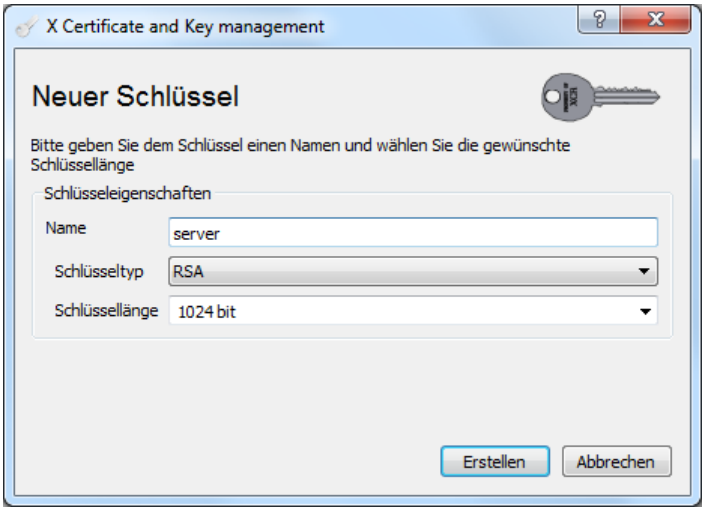
   ✓ Das Dialogfenster zur Erstellung eines Zertifikats erscheint:



4. Wählen Sie im Abschnitt „Unterschreiben“ das vorher erstellte CA-Zertifikat.
5. Wählen Sie im Abschnitt „Vorlage für das neue Zertifikat“ die vorher erstellte Server-Vorlage.
6. Klicken Sie auf Alles übernehmen.
7. Wechseln Sie zum Reiter „Inhaber“.



8. Legen Sie den „Common Name“ (Üblicher Name) fest und vergeben Sie diesen auch als internen Namen (z.B. server).
9. Klicken Sie auf Erstelle einen neuen Schlüssel.
   ✓ Das Dialogfenster zur Erstellung eines neuen Schlüssels erscheint:



10. Vergeben Sie vorzugsweise denselben Namen wie den „Common Name“.
11. Klicken Sie auf Erstellen.
12. Bestätigen Sie die Erstellung des Schlüssels mit OK.
13. Klicken Sie auf OK.
14. Bestätigen Sie die Erstellung des Zertifikats mit OK.
    ✓ Damit ist die Erzeugung von Server-Zertifikat und -Schlüssel abgeschlossen.

- **Zertifikat und Schlüssel für einen Client erzeugen**

  Gehen Sie beim Erstellen von Zertifikat und Schlüssel für einen Client genauso vor, wie für den Server, wählen Sie jedoch bei der Auswahl der Vorlage die Vorlage für den Client.

  Erzeugen Sie ggf. weitere Client-Zertifikate.

2.3 Zertifikate exportieren

Zertifikate und Schlüssel aus XCA exportieren

Die mit XCA erzeugten Zertifikate und Schlüssel werden in der entsprechenden XCA-Datenbank aufbewahrt. Um die Zertifikate und Schlüssel auf die jeweiligen INSYS-Router hochladen zu können, müssen diese exportiert werden.

XCA bietet für den Export verschiedene Dateiformate an. In diesem Konfigurations-Handbuch beschreiben wir den Export in das Dateiformat PKCS#12, da dieses für alle INSYS-Router außer den MoRoS PRO der Version 1.x geeignet ist. PKCS#12 ermöglicht zudem den Export von kompletten Schlüsselpaaren in einen Container, wodurch der Hochladeaufwand reduziert wird. Da auch die Zertifikatskette mit exportiert werden kann, muss das CA-Zertifikat nicht separat exportiert werden. Ein Passwortschutz kann dabei ab der Firmware 2.3.0 angewendet werden.

> ⓘ *Exportieren Sie niemals den CA-Schlüssel, da dieser essentiell für die Sicherheit des VPN-Netzwerks ist.*

Exportieren Sie die Zertifikate und Schlüssel in der Reihenfolge dieser Abschnitte:

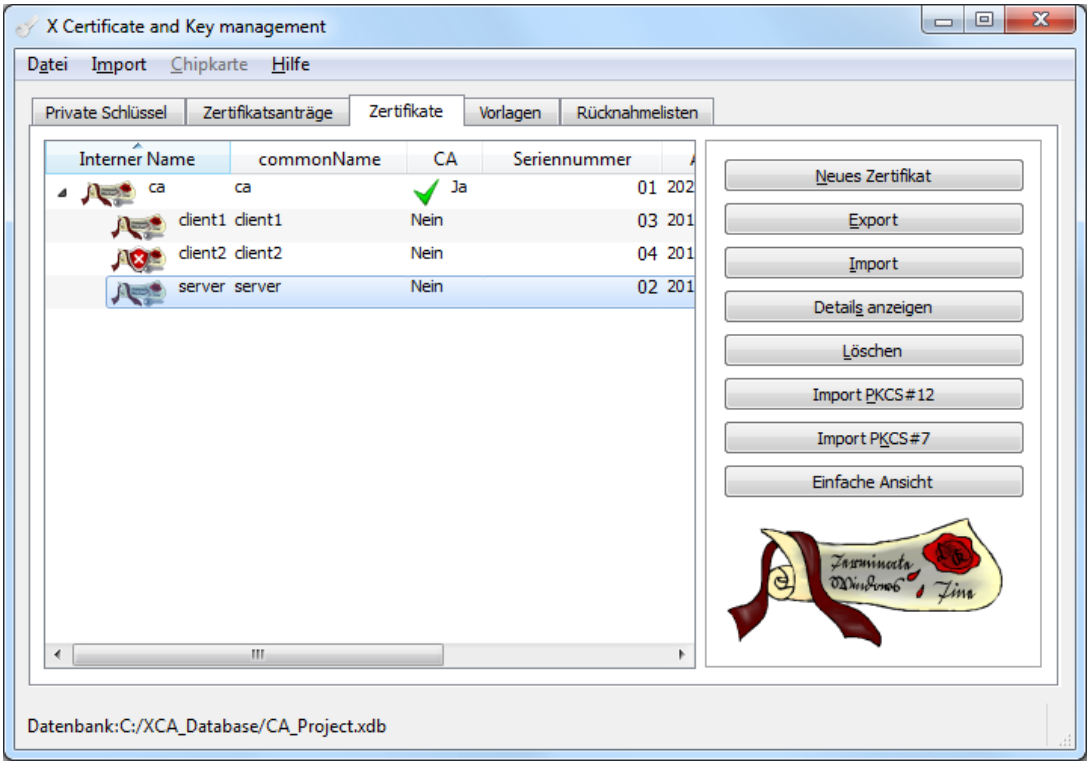
- Server-Zertifikats-Container exportieren
- Client-Zertifikats-Container exportieren

■ Server-Zertifikats-Container exportieren

So exportieren Sie das erzeugte Server-Schlüsselpaar aus der XCA-Datenbank in einen PKCS#12-Container. Der Container enthält das Server-Zertifikat und den zugehörigen öffentlichen Schlüssel. Wenn die Zertifikatskette mit exportiert wird, wird auch noch das CA-Zertifikat in den Container gepackt.

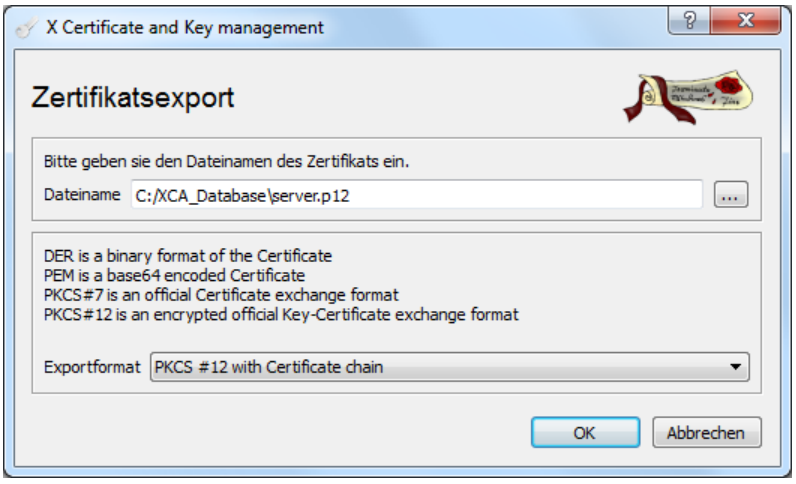
→ Die Software XCA ist gestartet und die Projektdatenbank geöffnet.
→ Ein Server-Zertifikat wurde erstellt.

1. Wechseln Sie zum Reiter „Zertifikate“.



2. Markieren Sie das Server-Zertifikat und wählen Sie Export

   ✓ Das Dialogfenster für den Zertifikatexport erscheint:

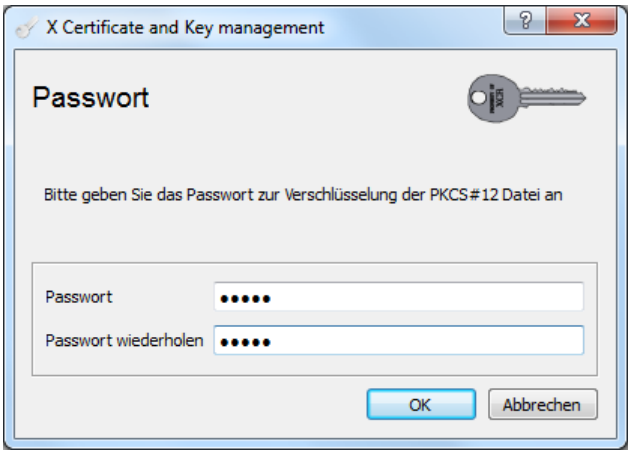


3. Legen Sie einen Pfad und Dateinamen fest.

   ⓘ *Wir empfehlen zur Verbesserung der Übersichtlichkeit, den Dateinamen gleich dem „Common Name" zu wählen, sofern dies keinen Sicherheitsbedenken widerspricht.*

4. Wählen Sie das Exportformat „PKCS#12 with Certificate chain".
5. Klicken Sie auf OK

✓ Das Dialogfenster zur Vergabe des Passworts erscheint:



6. Vergeben Sie ein Passwort, wenn Sie die Sicherheit der Übertragung der Zertifikatsdateien erhöhen wollen und klicken Sie auf OK

✓ Hiermit haben Sie den Server-Zertifikats-Container exportiert.

■ Client-Zertifikats-Container exportieren

Gehen Sie beim Export der Zertifikats-Container für die einzelnen Clients genauso vor, wie beim Export des Containers für das Server-Zertifikat.

2.4 Zertifikate zurückrufen

Zertifikate zurückrufen

Für OpenVPN ist es möglich, eine Certificate Revocation List (CRL, Zertifikatssperrliste oder Rücknahmeliste) 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.

Rufen Sie Zertifikate zurück, indem Sie in der Reihenfolge dieser Abschnitte vorgehen:

- **Zertifikat zurückrufen**
- **Certificate Revocation List erzeugen**
- **Certificate Revocation List exportieren**

- **Zertifikat zurückrufen**

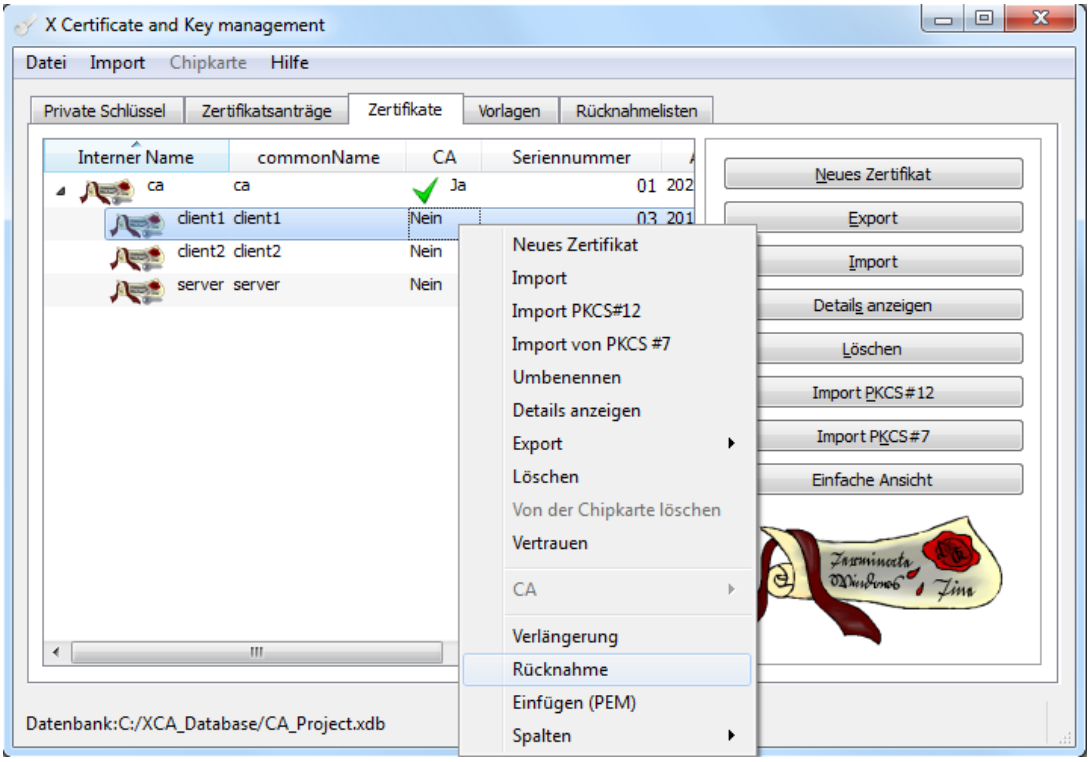
  So rufen Sie ein Zertifikat vor seinem Ablaufdatum zurück (beispielsweise wegen missbräuchlicher Verwendung), um es der Certificate Revocation List hinzuzufügen.

  ⓘ *Eine Certificate Revocation List ist zum Aufbau eines OpenVPN-Netzwerks mit zertifikatsbasierter Authentifizierung nicht zwingend notwendig.*

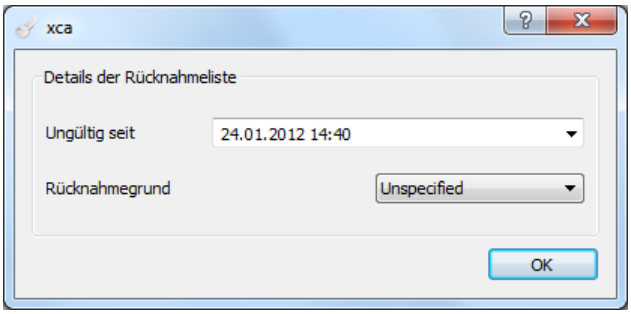
→ Die Software XCA ist gestartet und die Projektdatenbank geöffnet.

→ Client- bzw. Server-Zertifikate wurden bereits erzeugt.

1. Wechseln Sie zum Reiter „Zertifikate“.



2. Wählen Sie das Zertifikat, das Sie zurückrufen wollen, an und wählen Sie im Kontextmenü (Rechtsklick) „Rücknahme“.



3. Wählen Sie ggf. einen Rücknahmegrund und klicken Sie auf OK.

   ✓ Damit haben Sie das Zertifikat für eine Rücknahme vorgesehen.

   ⓘ *Danach muss die Certificate Revocation List neu erstellt werden.*

■ Certificate Revocation List erzeugen

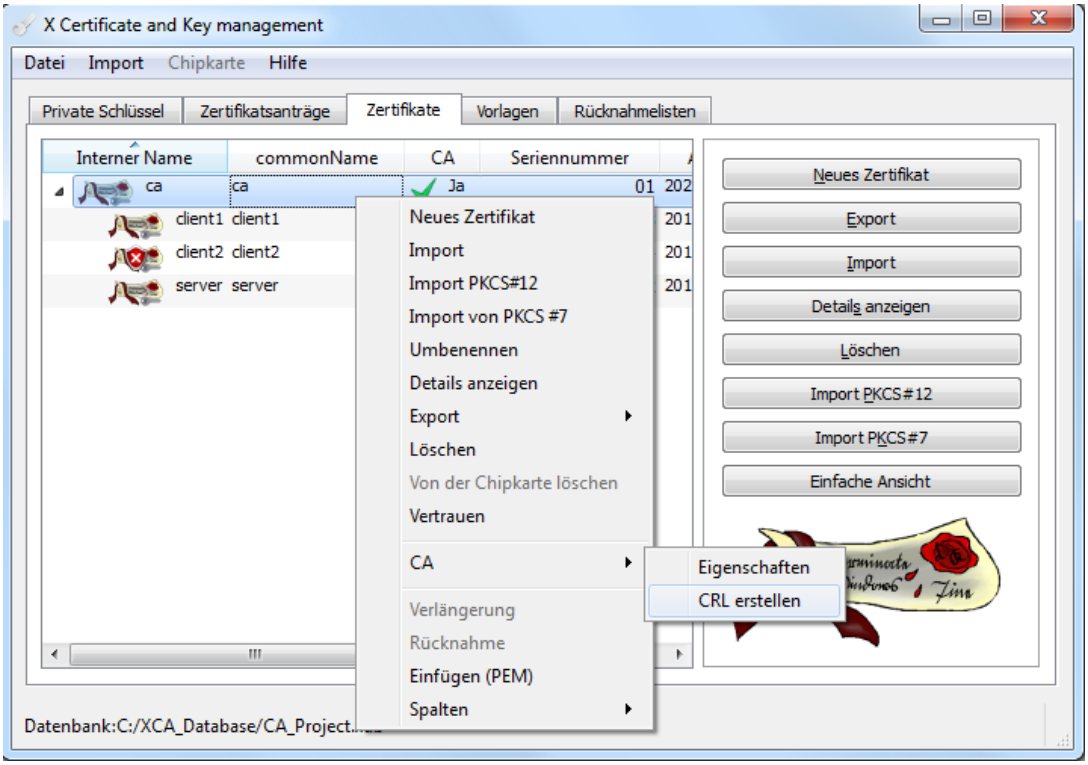
So erzeugen Sie mit XCA eine Certificate Revocation List.

ⓘ *Eine Certificate Revocation List ist zum Aufbau eines OpenVPN-Netzwerks mit zertifikatsbasierter Authentifizierung nicht zwingend notwendig.*

→ Die Software XCA ist gestartet und die Projektdatenbank geöffnet.

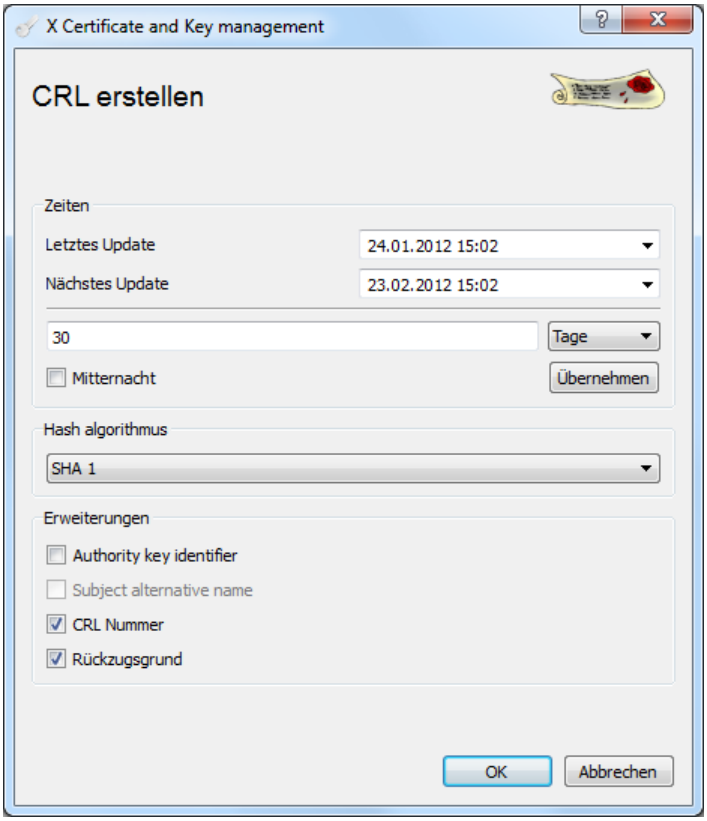
→ Mindestens ein Zertifikat wurde zurückgerufen.

1. Wechseln Sie zum Reiter „Zertifikate“.



2. Wählen Sie das CA-Zertifikat an und wählen Sie im Kontextmenü (Rechtsklick) CA → CRL erstellen.

   ✓ Das Dialogfenster zur Erstellung einer CRL erscheint:



3. Klicken Sie auf OK.
4. Bestätigen Sie die Erstellung der Certificate Revocation List mit OK.

✓ Damit haben Sie eine Certificate Revocation List erzeugt, die alle zurückgerufenen Zertifikate dieser CA enthält.

ⓘ *Wenn nach Erzeugen der Certificate Revocation List weitere Zertifikate zurückgerufen werden, muss die Certificate Revocation List neu erzeugt werden.*

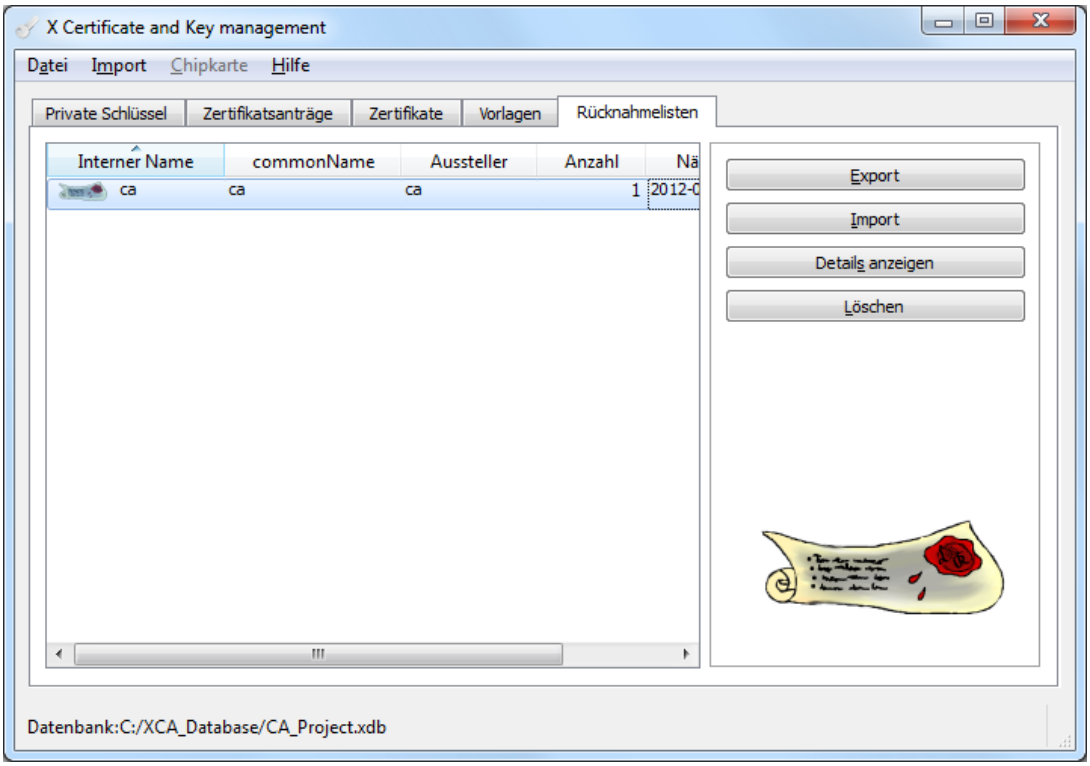
■ Certificate Revocation List exportieren

So exportieren Sie die Certificate Revocation List aus der XCA-Datenbank.

→ Die Software XCA ist gestartet und die Projektdatenbank geöffnet.

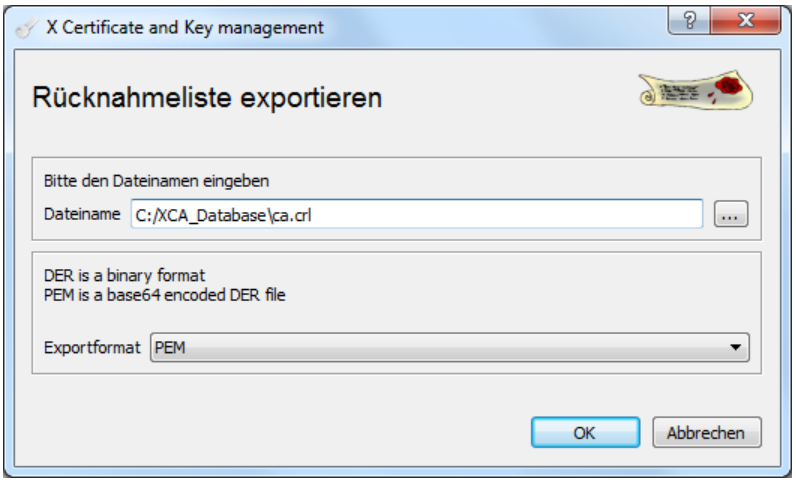
→ Eine Certificate Revocation List wurde erstellt.

1. Wechseln Sie zum Reiter „Rücknahmelisten“.



2. Markieren Sie die Certificate Revocation List und wählen Sie Export.

✓ Das Dialogfenster für den Export der Rücknahmeliste erscheint:



3. Legen Sie einen Pfad und Dateinamen fest.

   ⓘ *Wir empfehlen zur Verbesserung der Übersichtlichkeit, den Dateinamen mit der Endung „.crl“ zu versehen sowie gleich dem „Common Name“ des Zertifikats zu wählen, sofern dies keinen Sicherheitsbedenken widerspricht.*

4. Wählen Sie das Exportformat „PEM“.
5. Klicken Sie auf OK.

   ✓ Hiermit haben Sie die Certificate Revocation List exportiert. Die CRL muss nun noch auf den OpenVPN-Server hochgeladen werden, damit die enthaltenen Zertifikate zurückgerufen werden.

3 Verwendete Komponenten

Software

Bezeichnung	Hersteller	Typ	Version
XCA	Christian Hohnstädt (Freeware)	X-Zertifikat- und Schlüssel-Management	0.9.1 oder höher
Betriebssystem	Microsoft	Windows	XP, Vista, 7

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 Repulic

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