# 1 X.509-Zertifikate mit XCA erstellen

Dokument-ID: 108396_de_00
Dokument-Bezeichnung: AH DE X.509 CERT XCA


Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der Adresse phoenixcontact.net/products zum Download bereit.

**Inhalt dieses Dokuments**

In diesem Dokument wird die Erstellung von X.509-Zertifikaten mit dem Tool *XCA* beschrieben.

*XCA* hat viel mehr Funktionalität zu bieten, als in diesem Dokument beschrieben wird. Weiterführende Informationen sind in der *XCA*-Dokumentation zu finden (http://xca.sourceforge.net/xca.html – 15.09.2017). Sie können das Tool *XCA* hier herunterladen: http://xca.sourceforge.net. Die Screenshots und Beschreibungen in diesem Kapitel beziehen sich auf *XCA* v1.3.2.



## 1.1 Einleitung

Die Registrierung von Zertifikaten erfordert eine Zertifizierungsstelle (Certification Authority; CA), die für einen bestimmten Zeitraum Public-Key-Zertifikate ausstellt. Eine CA kann eine private (interne) CA sein, die von Ihrer eigenen Organisation geführt wird, oder eine öffentliche CA. Eine öffentliche CA wird durch einen Drittanbieter geführt, dem Sie die Validierung der Identität der einzelnen Clients und Server, denen er ein Zertifikat ausstellt, anvertrauen.

Es stehen mehrere Tools zur Erstellung und Verwaltung von Zertifikaten zur Verfügung, wie z. B. *Microsoft Certification Authority (CA) Server*, *OpenSSL* und *XCA*.

Dieser Anwenderhinweis erläutert die Vorgehensweise zur Erstellung von X.509-Zertifikaten mit den Tools **OpenSSL** und **XCA**, um eine VPN-Verbindung mit den X.509-Zertifikaten als Authentifizierungsmethode einzurichten.

Dieses Dokument ist aufgrund des Umfangs nicht als vollständiges Benutzerhandbuch für die beschriebenen Tools geeignet. Dieses Dokument soll Ihnen helfen, mit den Tools vertraut zu werden und die benötigten Zertifikate in einem kurzen Zeitraum zu erstellen.

### 1.1.1 XCA - X Certificate and key management

*XCA* ist für die Erstellung und Verwaltung von X.509-Zertifikaten, Zertifikatsanforderungen (*Requests*), RSA-, DSA- und EC-Privatschlüsseln, Smartcards und CRLs vorgesehen. Alles, was für eine CA benötigt wird, ist implementiert. Alle CAs können Sub-CAs rekursiv signieren.

Für eine unternehmensweite Nutzung stehen Vorlagen (*Templates*) zur Verfügung, die für die Generierung von Zertifikaten oder Anfragen genutzt und angepasst werden können. Alle verschlüsselten Daten werden in einem portierbaren Dateiformat gespeichert.

## 1.2 XCA-Datenbank erstellen

Zum Erstellen von X.509-Zertifikaten und Schlüsseln unter Anwendung von *XCA* müssen Sie zuerst eine Datenbank erstellen. Gehen Sie wie folgt vor:

1. Klicken Sie auf **File >> New DataBase**.
2. Legen Sie Dateiname und Speicherort der Datenbank fest.
3. Klicken Sie auf **Save**.
4. Geben Sie ein Passwort ein, das die Datenbank vor unbefugter Nutzung schützt. Das Passwort wird jedes Mal abgefragt werden, wenn Sie die *XCA*-Datenbank öffnen.

### 1.2.1 XCA-Datenbank öffnen

Bei einem Neustart von *XCA* müssen Sie zuerst wieder eine Verbindung zur Datenbank herstellen. Um eine bereits erstellte Datenbank zu öffnen, gehen Sie wie folgt vor:

1. Klicken Sie auf **File >> Open DataBase**.
2. Wählen Sie die gewünschte Datenbank (Datei *.xdb) aus.
3. Klicken Sie auf **Open**.

### 1.2.2 Standard-Prüfsummen-Algorithmus festlegen

**ACHTUNG:** Phoenix Contact empfiehlt die Verwendung von sicheren und aktuellen Verschlüsselungen und Prüfsummen-Algorithmen gemäß den Angaben im mGuard Software-Referenzhandbuch, erhältlich unter phoenixcontact.net/products (Suchen Sie nach "UM EN MGUARD", wählen Sie ein Produkt und anschließend das Handbuch im Downloadbereich aus).

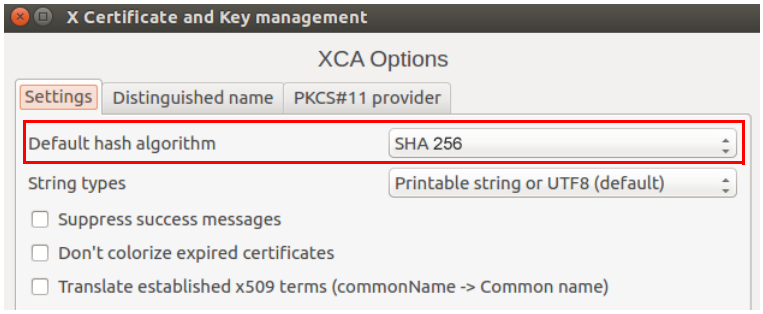
Bevor Sie mit dem Erstellen von Zertifikaten beginnen, müssen Sie den standardmäßigen Prüfsummen-Algorithmus auf **SHA 256** einstellen. Wenn Sie den Standard-Prüfsummen-Algorithmus nicht auf SHA 256 einstellen, müssen Sie diese Einstellung jedes Mal vornehmen, wenn Sie ein neues Zertifikat erstellen.

**ACHTUNG: Nicht alle Geräte unterstützen die Funktionalität der SHA 2-Familie**

Sollten Sie nicht sicher sein, ob alle Ihre Geräte die Funktionalität der SHA 2-Familie unterstützen, könnte stattdessen der nicht so sichere SHA 1-Algorithmus verwendet werden (wird von PHOENIX CONTACT nicht empfohlen und erfüllt nicht die Anforderungen der ANSSI-CSPN-2016-09).

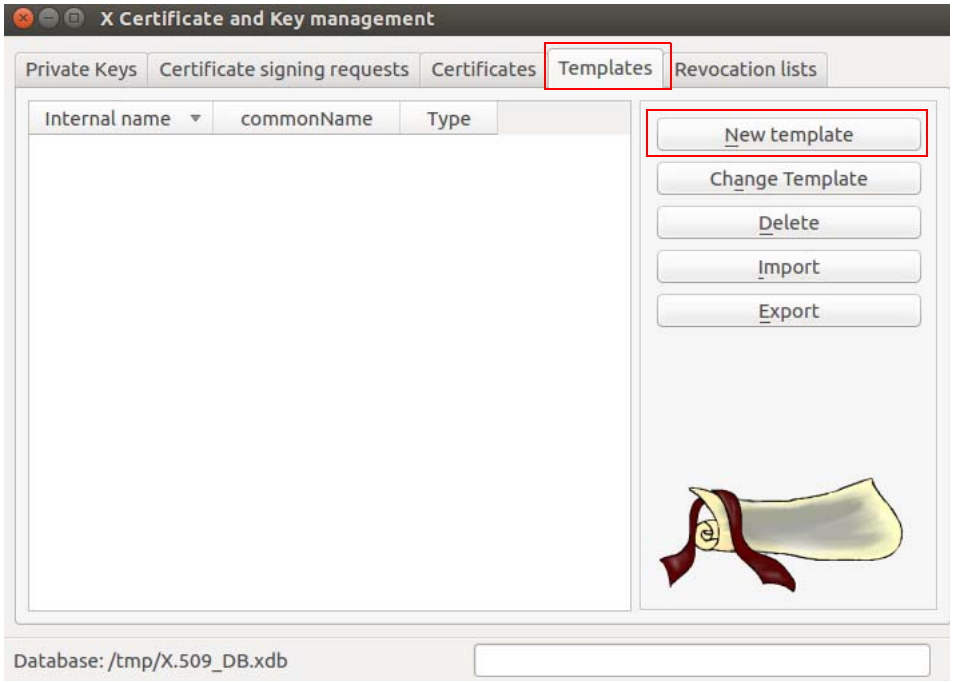
Gehen Sie wie folgt vor:

- Klicken Sie auf **File >> Options**, und setzen Sie den Standard-Prüfsummen-Algorithmus auf SHA 256 (oder den entsprechenden Algorithmus, den Sie bei Ihrer Einrichtung verwenden).



## 1.3 Zertifikatvorlage erstellen

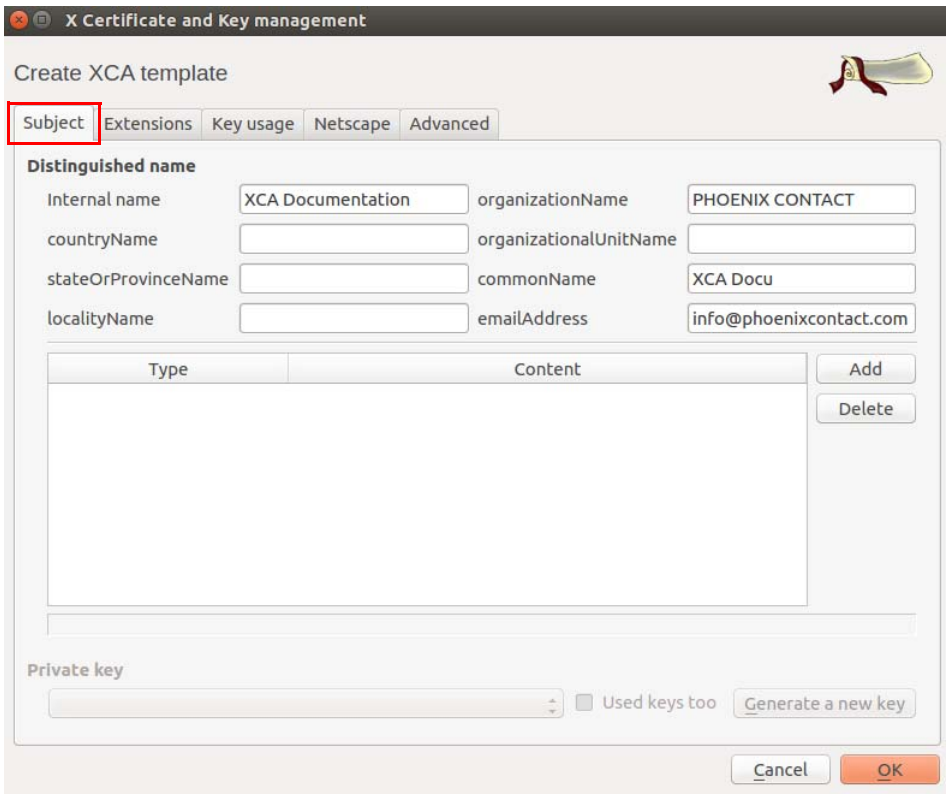
Falls Sie mehrere Zertifikate erstellen müssen, ist es hilfreich, aus Gründen der Konsistenz und für weniger Tastatureingaben eine Vorlage (Template) zu definieren. Diese Vorlage kann anschließend beim Erstellen der Zertifikate verwendet werden.




Gehen Sie wie folgt vor:

1. Wählen Sie die Registerkarte **Templates**.
2. Klicken Sie auf **New template**.
3. Wählen Sie **Preset Template Values**, und klicken Sie auf **OK**.

### 1.3.1 XCA-Vorlage erstellen >> Registerkarte: Subject

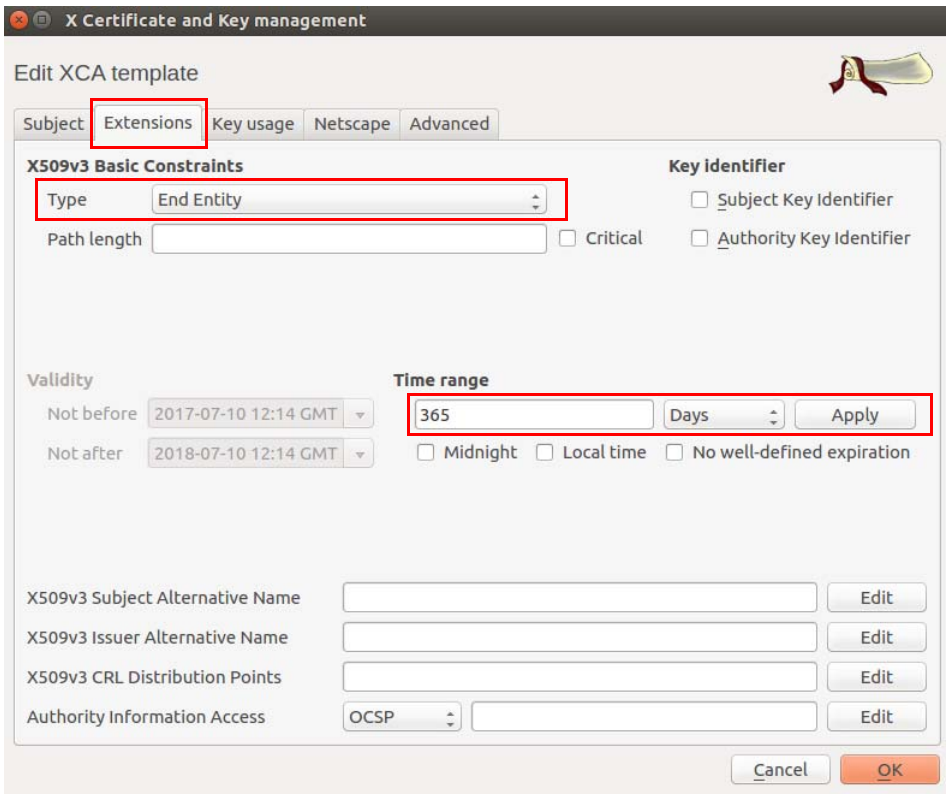



Gehen Sie wie folgt vor:

1. Wählen Sie die Registerkarte **Subject.**
2. Verwenden Sie die Eingabefelder von **Internal name** bis **emailAddress,** um die identifizierenden Parameter einzugeben, die alle Zertifikate gemeinsam haben sollen.

   Die Vorlage wird in *XCA* unter **Internal name** gespeichert.
3. Wählen Sie die Registerkarte **Extensions**.

### 1.3.2 XCA-Vorlage erstellen >> Registerkarte: Extensions

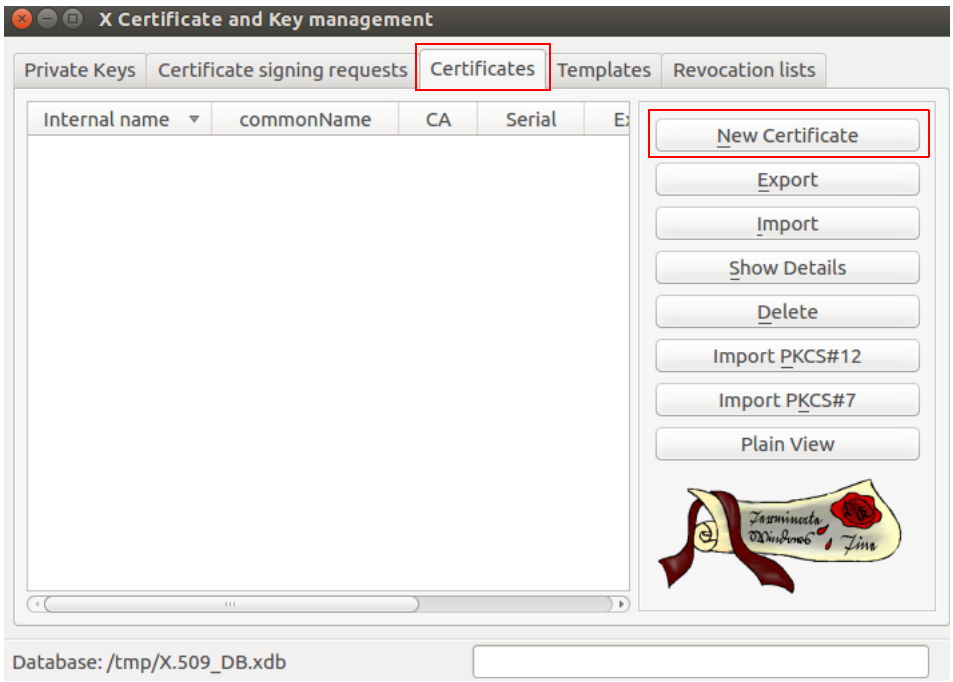



Gehen Sie wie folgt vor:

1. In Abschnitt **X509v3 Basic Constraints**:
   - Setzen Sie **Type** auf *End Entity*, wenn Sie die Vorlage zum Erstellen von Client-Zertifikaten verwenden möchten.
   - Setzen Sie **Type** auf *Certification Authority*, wenn die Vorlage zum Erstellen von CA-Zertifikaten verwendet werden soll.
2. Im Abschnitt **Time Range**:
   - Stellen Sie die Standard-Lebensdauer der Zertifikate ein, und klicken Sie auf **Apply**.
3. Klicken Sie zum Erstellen der Vorlage auf **OK**.

## 1.4 CA-Zertifikat erstellen

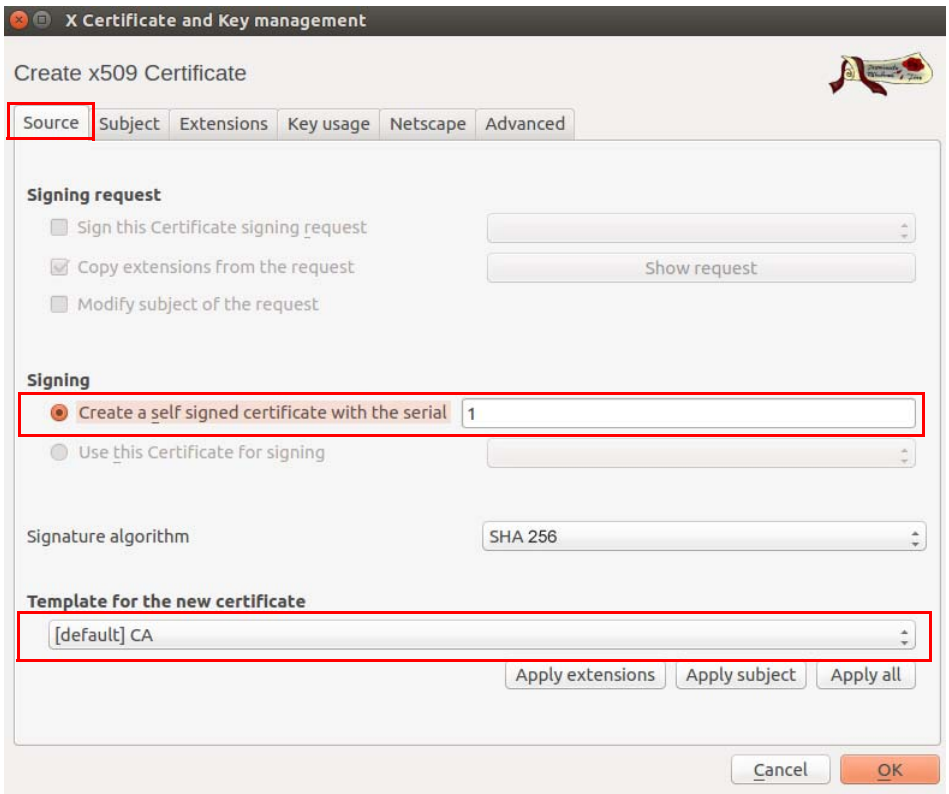
Falls Sie keine selbstsignierten Client-Zertifikate verwenden, muss ein Client-Zertifikat durch das CA-Zertifikat signiert werden, um zu einem gültigen Zertifikat zu werden. Aus diesem Grund müssen Sie zuerst das CA-Zertifikat erstellen, bevor Sie die Client-Zertifikate erstellen. Das CA-Zertifikat ist ein selbstsigniertes Zertifikat.




Gehen Sie wie folgt vor:

1. Wählen Sie die Registerkarte **Certificates**.
2. Klicken Sie auf **New Certificate**.

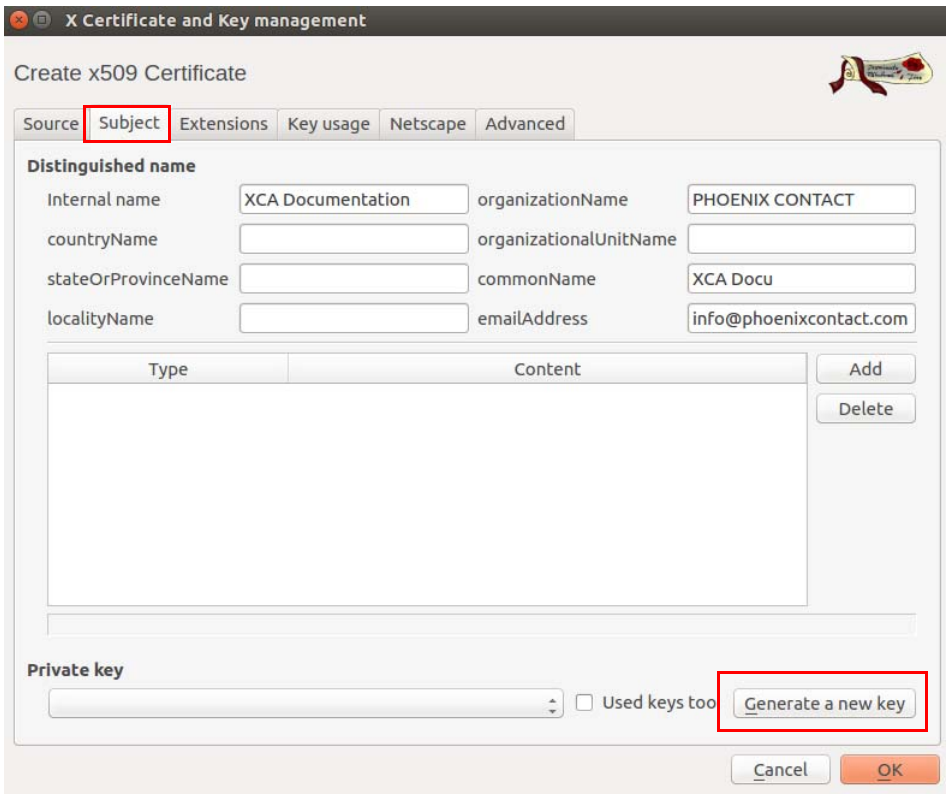
### 1.4.1 x509- (CA-) Zertifikat erstellen >> Registerkarte: Source




Gehen Sie wie folgt vor:

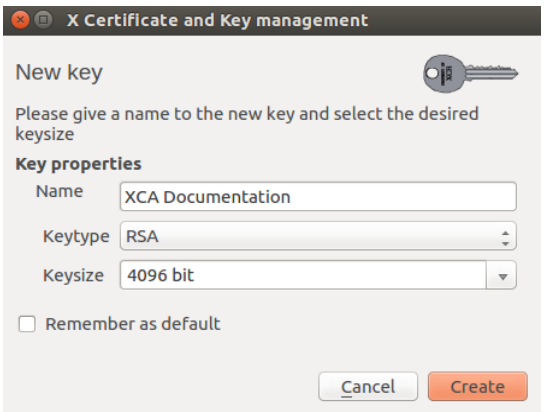
1. Wählen Sie die Registerkarte **Source**.
2. Im Abschnitt **Signing**: Stellen Sie sicher, dass **Create a self signed certificate with the serial** ausgewählt ist.
3. Sie können eine Seriennummer für das Zertifikat eingeben oder den Standardwert beibehalten.
4. Im Abschnitt **Template for the new certificate**: Wenn Sie eine Vorlage zum Erstellen von CA-Zertifikaten erstellt haben, können Sie diese nun auswählen und auf **Apply** klicken.
5. Wählen Sie die Registerkarte **Subject**.

### 1.4.2 x509- (CA-) Zertifikat erstellen >> Registerkarte: Subject



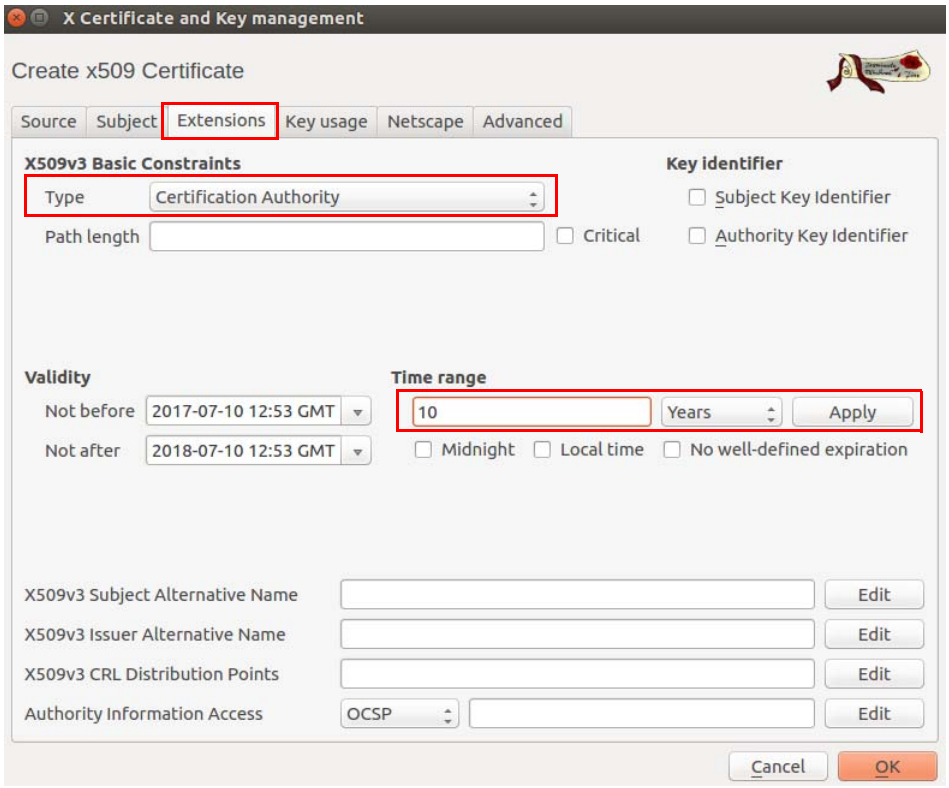

Gehen Sie wie folgt vor:

1. Im Abschnitt **Distinguished name**: Verwenden Sie die Eingabefelder von **Internal name** bis **emailAddress**, um die identifizierenden Parameter des CA-Zertifikats einzugeben.
2. Im Abschnitt **Private key**: Klicken Sie auf **Generate a new key**, um den privaten RSA-Schlüssel für das CA-Zertifikat zu erstellen.




3. Geben Sie einen **Namen** für den Schlüssel ein, legen Sie die gewünschten Werte für **Keytype** und **Keysize** fest, und klicken Sie auf **Create**.
4. Wählen Sie die Registerkarte **Extensions**.

### 1.4.3 x509- (CA-) Zertifikat erstellen >> Registerkarte: Extensions



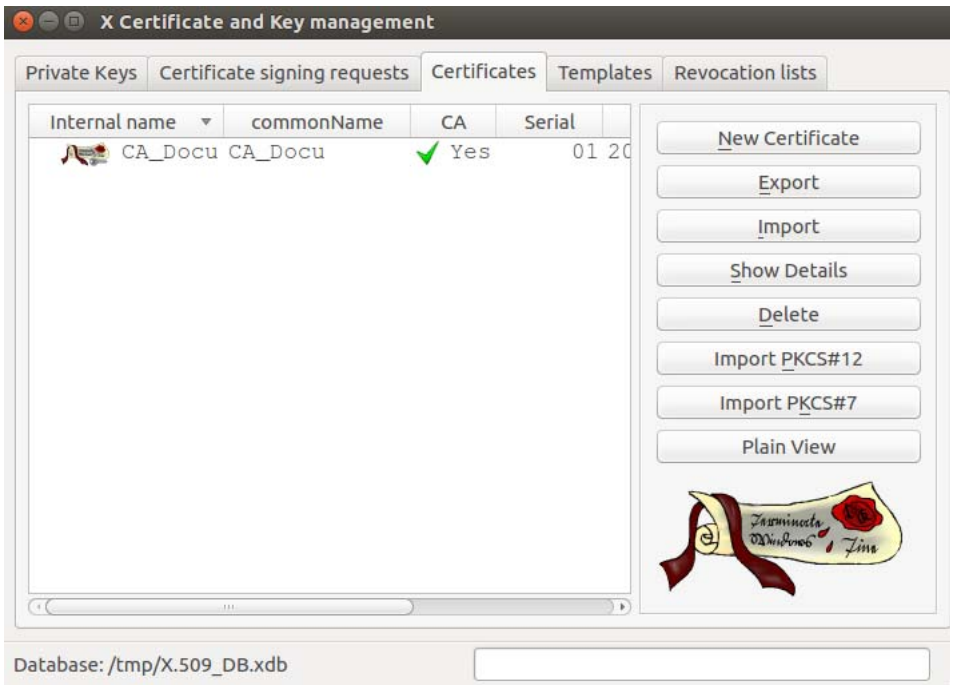

Gehen Sie wie folgt vor:

5. Im Abschnitt **X509v3 Basic Constraints**: Stellen Sie **Type** auf *Certification Authority* ein.
6. Im Abschnitt **Time Range**: Stellen Sie die Standard-Lebensdauer der Zertifikate ein, und klicken Sie auf **Apply**.
   Für ein CA-Zertifikat wünschen Sie sich unter Umständen eine längere Gültigkeit als für die Client-Zertifikate, sodass Sie die Zertifikate nicht so häufig erneut ausstellen müssen. Eine Lebensdauer von 10 Jahren ist im Allgemeinen ein guter Wert.
7. Klicken Sie auf **Apply**.
8. Klicken Sie zum Erstellen des Zertifikats auf **OK**.
   Das CA-Zertifikat wird auf der Registerkarte **Certificates** angezeigt.

## 1.5 Client-Zertifikat erstellen

Wenn Sie Client-Zertifikate erstellen möchten, müssen Sie zuerst ein CA-Zertifikat erstellen oder importieren, das anschließend zum Signieren des Client-Zertifikats verwendet wird. Das Client-Zertifikat erhält durch die Signatur des CA-Zertifikats seine Gültigkeit.

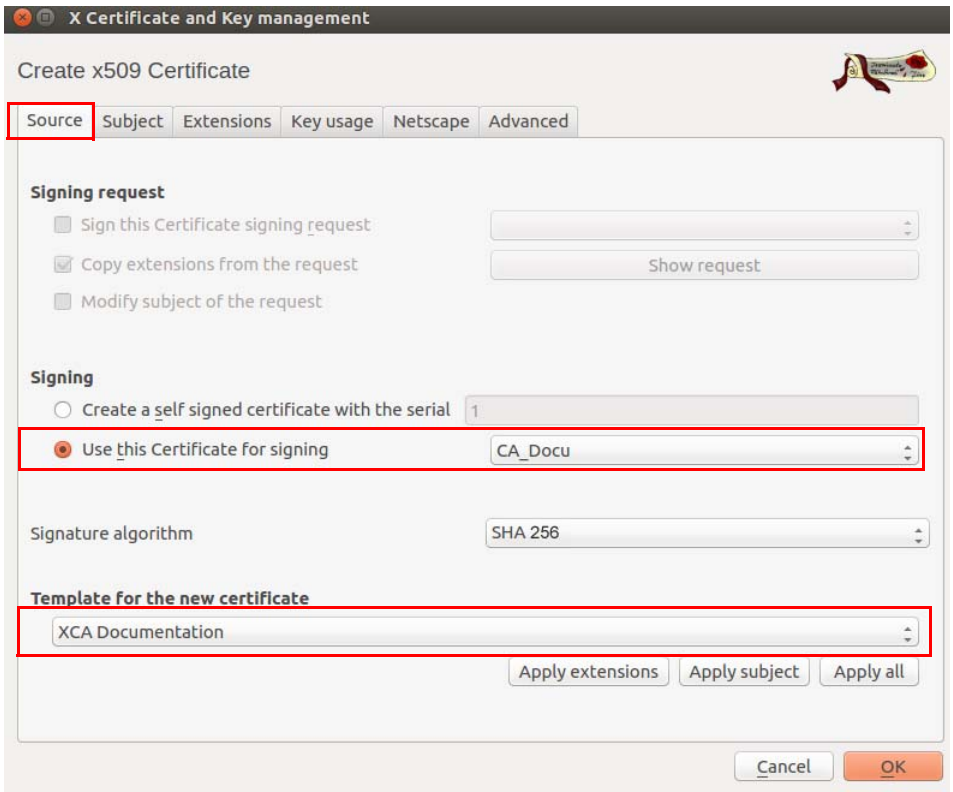
In der *XCA*-Datenbank muss ein CA-Zertifikat zum Signieren des Client-Zertifikats verfügbar sein. Sollte das CA-Zertifikat nicht verfügbar sein, muss es zuerst erstellt werden (siehe „CA-Zertifikat erstellen“ auf Seite 8).




Gehen Sie wie folgt vor:

1. Wählen Sie die Registerkarte **Certificates**.
2. Klicken Sie auf **New Certificate**.

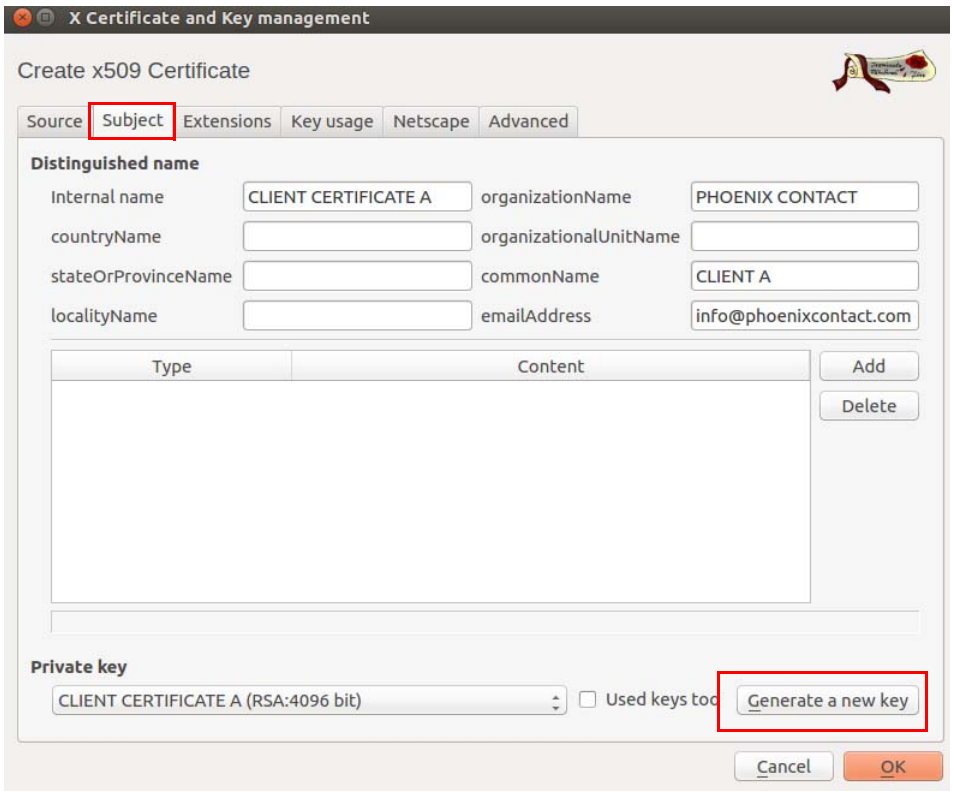
### 1.5.1 x509- (Client-) Zertifikat erstellen >> Registerkarte: Source




Gehen Sie wie folgt vor:

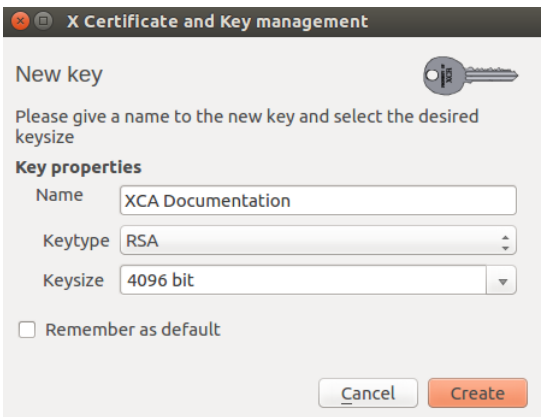
1. Wählen Sie die Registerkarte **Source**.
2. Im Abschnitt **Signing**: Stellen Sie sicher, dass das korrekte CA im Feld **Use this certificate for signing** ausgewählt ist.
3. Im Abschnitt **Template for the new certificate**: Wenn Sie eine Vorlage zum Erstellen von Client-Zertifikaten erstellt haben, können Sie diese nun auswählen und auf **Apply** klicken.
4. Wählen Sie die Registerkarte **Subject**.

### 1.5.2 x509- (Client-) Zertifikat erstellen >> Registerkarte: Subject



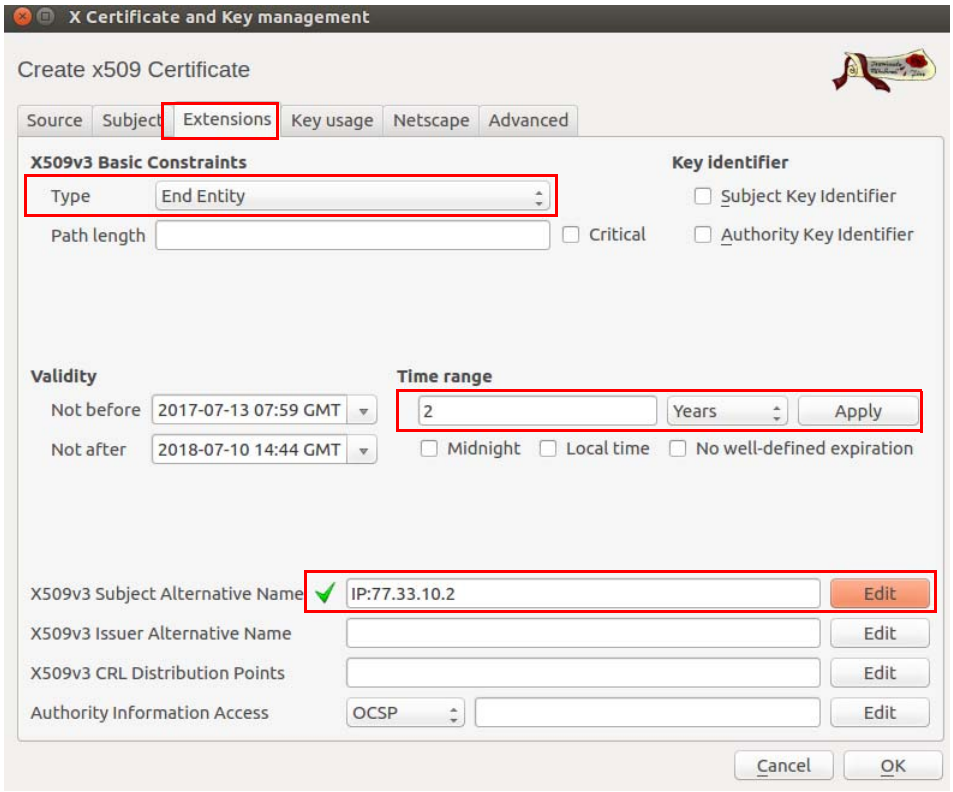

Gehen Sie wie folgt vor:

1. Im Abschnitt **Distinguished name**: Verwenden Sie die Eingabefelder von **Internal name** bis **emailAddress**, um die identifizierenden Parameter des Client-Zertifikats einzugeben.
2. Im Abschnitt **Private key**: Klicken Sie auf **Generate a new key**, um den privaten RSA-Schlüssel für das Zertifikat zu erstellen.




3. Geben Sie einen **Namen** für den Schlüssel ein, legen Sie die gewünschten Werte für **Keytype** und **Keysize** fest, und klicken Sie auf **Create**.
4. Wählen Sie die Registerkarte **Extensions**.

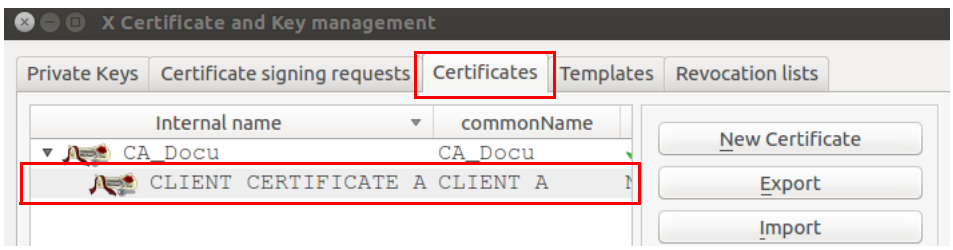
### 1.5.3 x509- (Client-) Zertifikat erstellen >> Registerkarte: Extensions




1. Im Abschnitt **X509v3 Basic Constraints**: Stellen Sie **Type** auf *End Entity* ein.
2. Im Abschnitt **Time Range**: Stellen Sie die Standard-Lebensdauer der Zertifikate ein, und klicken Sie auf **Apply**.
3. Der mGuard verwendet als standardmäßige VPN-Benennung den Subjektnamen des Zertifikats. Wenn Sie eine abweichende VPN-Benennung verwenden möchten (z. B. E-Mail-Adresse, Hostname oder IP-Adresse), muss diese Benennung als **subject alternative name** im Zertifikat vorhanden sein.

   Um eine weitere Benennung hinzuzufügen, klicken Sie in der Zeile **X509v3 Subject Alternative Name** auf **Edit**, wählen den Benennungstyp (E-Mail, DNS oder IP) aus, geben den Wert ein, klicken auf **Add** und anschließend auf **Apply**.
4. Klicken Sie zum Erstellen des Zertifikats auf **OK**.

   Das Client-Zertifikat wird in der Registerkarte **Certificates** unterhalb des CA-Zertifikats angezeigt.



## 1.6 Zertifikat exportieren

Zum Exportieren eines Zertifikats, das mit *XCA* erstellt wurde, gehen Sie wie folgt vor:

1. Wählen Sie die Registerkarte **Certificates**.
2. Markieren Sie das Zertifikat, das exportiert werden soll.
3. Klicken Sie auf **Export**.


4. Wählen Sie das **Export Format** (PEM oder PKCS#12 – siehe Infobox unten).
5. Geben Sie den gewünschten **Filename** (Dateinamen) und den Ort an, an dem die Exportdatei gespeichert werden soll.
6. Klicken Sie auf **OK**.
7. Wenn Sie das Zertifikat als PKCS#12 exportieren, erscheint eine Eingabeaufforderung, in der Sie ein Passwort eingeben müssen, durch das der Export vor unbefugter Nutzung geschützt wird. Geben Sie das Passwort ein, und klicken Sie auf **OK**.

**PKCS (Public Key Cryptography Standards)**

PKCS #12: Personal Information Exchange Syntax v1.1 (Personaldaten-Austauschsyntax; definiert in **RFC 7292**)

PKCS #12 v1.1 beschreibt eine Übertragungssyntax für personenbezogene Identitätsinformationen, einschließlich der privaten Schlüssel, Zertifikate, verschiedener Geheimdaten und Erweiterungen. Maschinen, Applikationen, Browser, Internet-Kiosks usw., die diesen Standard unterstützen, ermöglichen einem Anwender den Import, Export und die Ausführung eines einzelnen Satzes aus personenbezogenen Identitätsinformationen. Dieser Standard unterstützt die direkte Übertragung personenbezogener Daten unter mehreren Privatsphäre- und Integritätsmodalitäten (RFC 7292).

**PEM (Privacy-Enhanced Mail)** (definiert in RFC 1421 bis 1424)

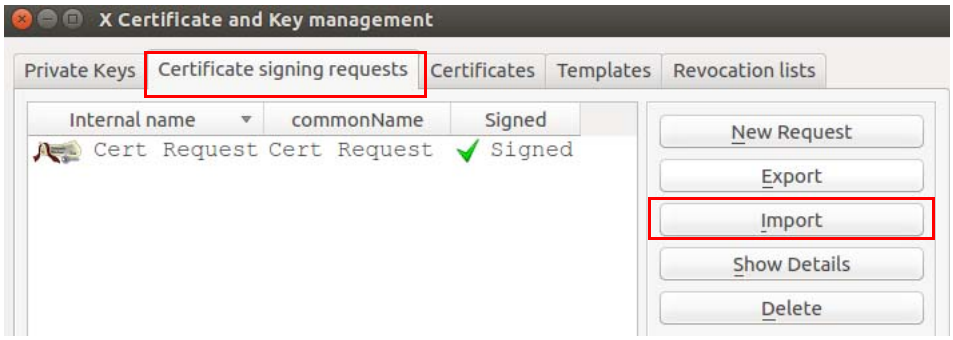
Ein PEM-Container kann nur das öffentliche Zertifikat oder eine gesamte Zertifikatskette enthalten (einschließlich des öffentlichen Schlüssels, privaten Schlüssels und der Root-Zertifikate).

PEM-Daten werden gewöhnlich in Dateien mit einem Suffix "**.pem**" oder "**.cer**" oder einem Suffix "**.crt**" (bei Zertifikaten) oder einem Suffix "**.key**" (bei öffentlichen oder privaten Schlüsseln) gespeichert.

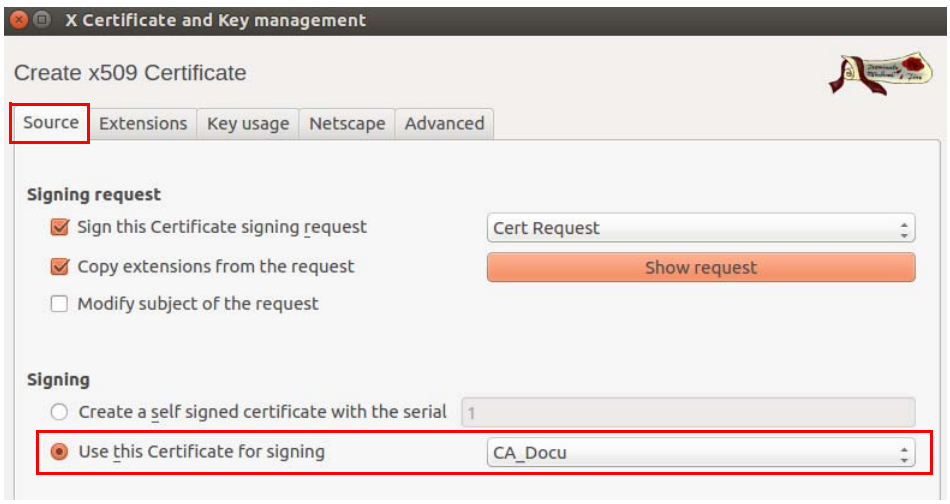
## 1.7 Zertifikatanfrage mit dem CA signieren

Gehen Sie zum Signieren eines Zertifikats wie folgt vor:

1. Wählen Sie die Registerkarte **Certificate signing requests**.
2. Klicken Sie auf **Import**.
3. Wählen Sie eine Zertifikatanfrage aus (PKCS#10-Datei), die durch die CA signiert werden soll, und klicken Sie auf **Open**.
4. Die importierte Zertifikatanfrage wird auf der Registerkarte **Certificate signing requests** angezeigt.



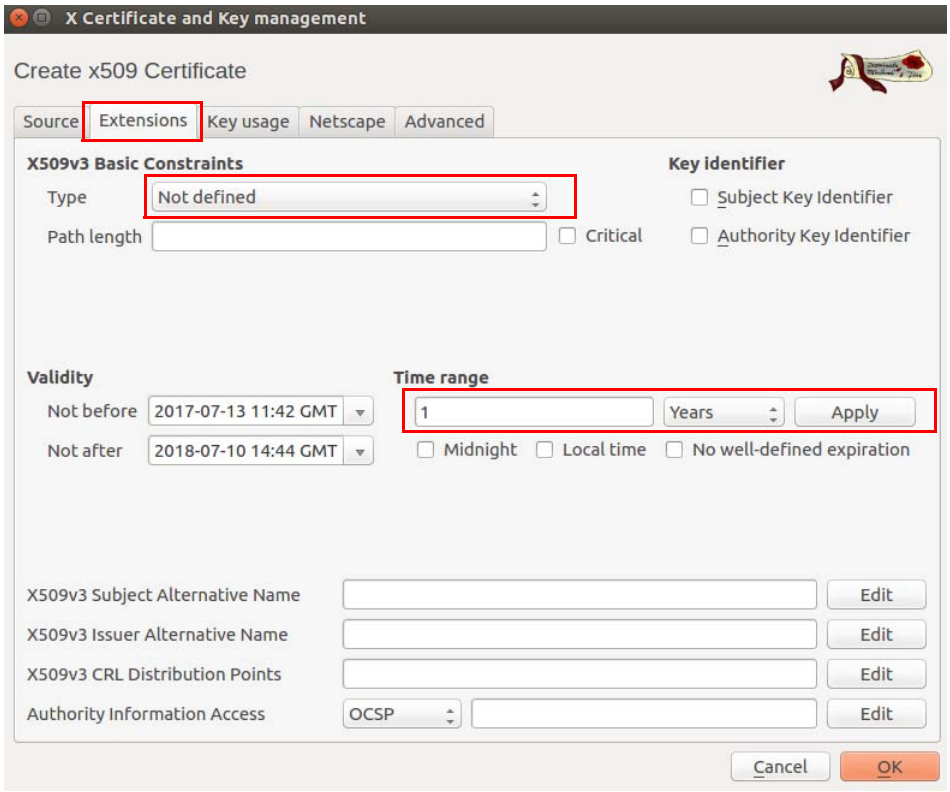

### 1.7.1 X-Zertifikat- und Schlüssel-Management >> Registerkarte: Source



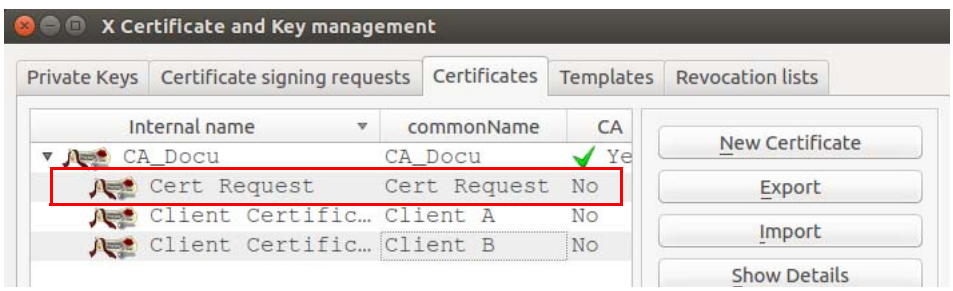

Gehen Sie zum Signieren der Zertifikatanfrage wie folgt vor:

1. Wählen Sie die Registerkarte **Certificate signing requests**.
2. Klicken Sie mit rechter Maustaste auf die Zertifikatanfrage, und wählen Sie im Kontextmenü **Sign**.
3. Im Abschnitt **Signing**: Stellen Sie sicher, dass das korrekte CA-Zertifikat im Feld **Use this certificate for signing** ausgewählt ist.
4. Wählen Sie die Registerkarte **Extensions**.

### 1.7.2 X-Zertifikat- und Schlüssel-Management >> Registerkarte: Extensions




1. Im Abschnitt **X509v3 Basic Constraints**: Lassen Sie **Type** auf *Not defined* eingestellt. Andernfalls würde *XCA* die Zertifikaterweiterungen zwei Mal in das signierte Zertifikat kopieren.
2. Im Abschnitt **Time Range**: Stellen Sie die Standard-Lebensdauer für das neue Zertifikat ein, und klicken Sie auf **Apply**.
3. Klicken Sie auf **OK**.
4. Die signierte Zertifikatanfrage wird in der Registerkarte **Certificates** unterhalb des CA-Zertifikats angezeigt.



## 1.8 Zertifikatssperrliste (Certificate Revocation List; CRL) verwenden

### 1.8.1 Zertifikat sperren

1. Wählen Sie die Registerkarte **Certificates**.
2. Klicken Sie mit rechter Maustaste auf das Client-Zertifikat, das gesperrt werden soll, und wählen Sie im Kontextmenü **Revoke**.
3. Bearbeiten Sie die Parameter, und klicken Sie auf **OK**.
4. Das gesperrte Zertifikat wird mit einem Kreuzsymbol gekennzeichnet  , und der Zustand **Trust state** ist *Not trusted*.

### 1.8.2 CRL-Erneuerungszeitraum festlegen

1. Wählen Sie die Registerkarte **Certificates**.
2. Klicken Sie mit rechter Maustaste auf die CA, und wählen Sie im Kontextmenü **CA >> Properties**.
3. Geben Sie den gewünschten Erneuerungszeitraum im Feld **Days until next CRL issuing** ein.
4. Klicken Sie auf **OK**.

### 1.8.3 CRL erstellen

1. Wählen Sie die Registerkarte **Certificates**.
2. Klicken Sie mit rechter Maustaste auf die CA, und wählen Sie im Kontextmenü **CA >> Generate CRL**.
3. Bearbeiten Sie die Parameter, und klicken Sie auf **OK**.
4. Die CRL wird auf der Registerkarte **Revocation lists** angezeigt.

### 1.8.4 Informationen über eine CRL einholen

1. Wählen Sie die Registerkarte **Revocation lists**.
2. Markieren Sie die CRL, und klicken Sie auf **Show Details**.

### 1.8.5 CRL exportieren

1. Wählen Sie die Registerkarte **Revocation lists**.
2. Markieren Sie die CRL.
3. Klicken Sie auf **Export**.
4. Legen Sie Dateiname und Speicherort der CRL fest.
5. Wählen Sie das Exportformat (DER oder PEM).
6. Klicken Sie auf **OK**.

## 1.9 Beispiel: VPN-Verbindung zwischen zwei mGuard-Geräten

Um die benötigten Zertifikate für eine VPN-Verbindung zwischen zwei mGuard-Geräten zu erstellen und zu importieren, gehen Sie wie folgt vor:

**CA-Zertifikat**

- Erstellen Sie ein CA-Zertifikat gemäß der Beschreibung in Kapitel „CA-Zertifikat erstellen“ auf Seite 8.

**Client-Zertifikat**

- Erstellen Sie ein Client-Zertifikat für mGuard **#1** und ein Client-Zertifikat für mGuard **#2** (siehe die Beschreibung in Kapitel „Client-Zertifikat erstellen“ auf Seite 12).

**Exportzertifikate**

- Exportieren Sie die Zertifikate gemäß der Beschreibung in Kapitel „Zertifikat exportieren“ auf Seite 16.

Die folgenden Exporte sind erforderlich:

– mGuard **#1** als PKCS#12: Dieser Export muss bei mGuard **#1** als *Maschinenzertifikat* importiert werden (Menü: Authentifizierung >> Zertifikate, Registerkarte *Maschinenzertifikate*).

– mGuard **#2** als PKCS#12: Dieser Export muss bei mGuard **#2** als *Maschinenzertifikat* importiert werden (Menü: Authentifizierung >> Zertifikate, Registerkarte *Maschinenzertifikate*).

– mGuard **#1** als PEM: Dieser Export muss bei mGuard **#2** als Verbindungszertifikat importiert werden (Menü: IPsec VPN >> Verbindungen >> (*Bearbeiten*), Registerkarte *Authentifizierung*).

– mGuard **#2** als PEM: Dieser Export muss bei mGuard **#1** als Verbindungszertifikat importiert werden (Menü: IPsec VPN >> Verbindungen >> (*Bearbeiten*), Registerkarte *Authentifizierung*).