

Erstellen eines Zertifikats

Vorbereitende Maßnahmen

Installieren Sie folgende Software auf dem PC, den Sie zum Erstellen der Zertifikate nutzen wollen:

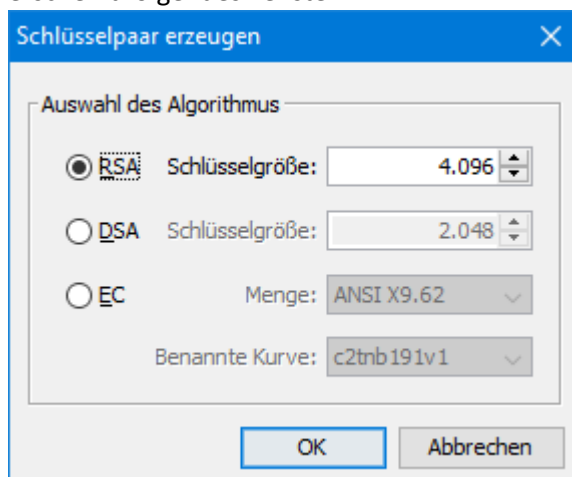
- Java von <https://www.java.com>
- KeyStore Explorer von <http://keystore-explorer.org/>

Starten Sie den KeyStore Explorer

Erstellen des Zertifikats

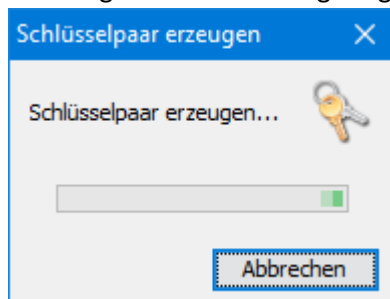
Nachträgliche Änderungen an den Zertifikaten sind nicht mehr möglich. Prüfen Sie daher bei jedem Schritt genau, ob Ihre Einstellungen richtig sind!

1. Erstellen Sie einen neuen Schlüsselspeicher (Strg+N) oder *Datei* → *Neu* vom Typ JCEKS. Wenn Sie bereits einen Schlüsselspeicher angelegt haben, können sie auch gerne diesen öffnen.
2. Erstellen Sie ein neues Schlüsselpaar (Strg+G) oder *Werkzeuge* → *Schlüsselpaar erzeugen*. Es erscheint folgendes Fenster:



Wählen Sie hier den RSA-Algorithmus mit einer beliebigen Schlüssellänge aus. Wir empfehlen einen mindestens 1024-bit RSA-Schlüssel zu verwenden.

3. Die Software erzeugt nun einen entsprechenden Schlüssel. Während der Schlüsselerzeugung wird folgendes Fenster angezeigt:



4. Nach Abschluss der Schlüsselerzeugung müssen Sie die Eigenschaften des neuen Schlüssels festlegen. Dies geschieht in folgendem Fenster:

Zertifikat für Schlüsselpaar erstellen

Version: Version 1 Version 3

Signaturalgorithmus: SHA-256 mit RSA

Gültigkeitsbeginn: 17.12.2017 21:16:05 MEZ

Gültigkeitsdauer: 1 Jahr(e) Anwenden

Gültigkeitsende: 17.12.2018 21:16:05 MEZ

Seriennummer: 1513541765

Name:

Erweiterung hinzufügen

OK Abbrechen

Wählen Sie hier Version 3 und mit einem Signaturalgorithmus „SHA-256 mit RSA“ oder besser aus. Legen Sie als nächstes die Laufzeit des Zertifikats fest. Zum Schluss müssen Sie noch den Namen des Zertifikats anpassen. Drücken Sie dazu auf den Knopf mit dem Buch. Es erscheint folgendes Fenster:

Name

Allgemeiner Name (CN): + -

Organisationseinheit (OU): + -

Organisationsname (O): + -

Ortsbezeichnung (L): + -

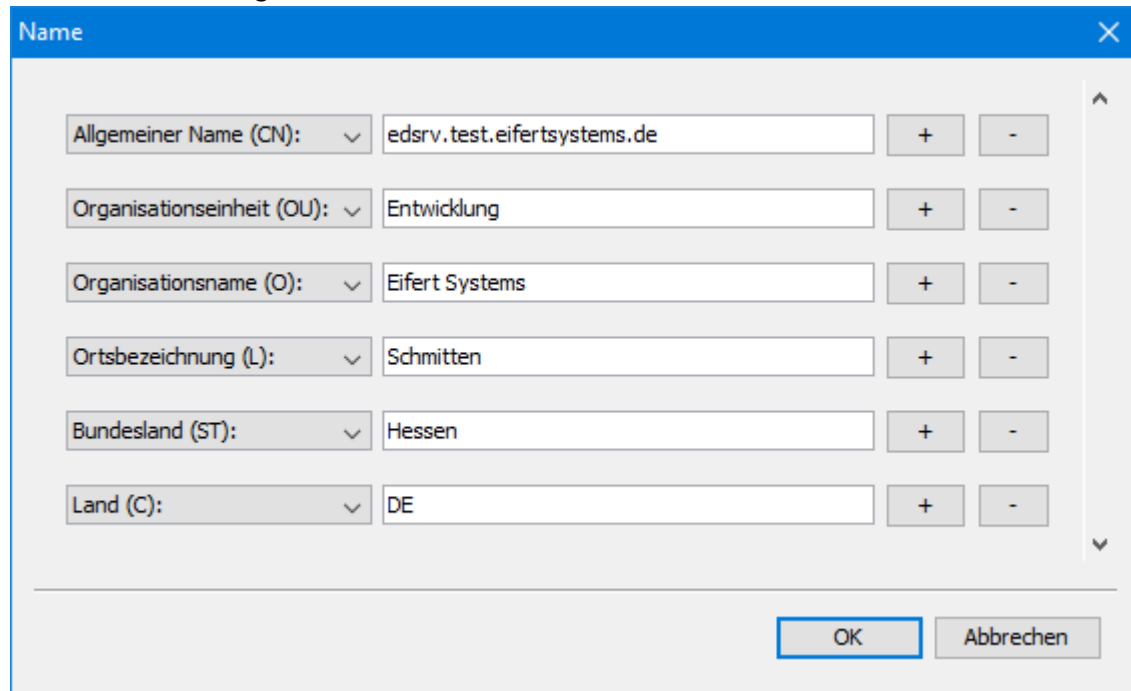
Bundesland (ST): + -

Land (C): + -

OK Abbrechen

füllen Sie hierin alle erforderlichen Daten aus, wobei der Allgemeine Name (CN) der DNS-Name des Servers ist, unter dem die Clients den Server erreichen können. Die Daten könnten

anschließend wie folgt aussehen:

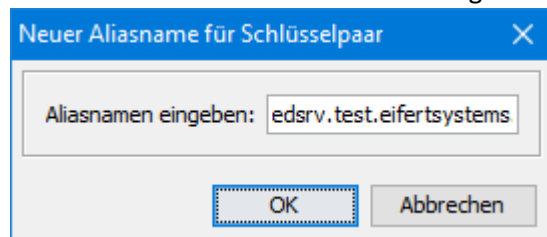


The 'Name' dialog box contains the following fields:

Field	Value
Allgemeiner Name (CN):	edsrv.test.eifertsystems.de
Organisationseinheit (OU):	Entwicklung
Organisationsname (O):	Eifert Systems
Ortsbezeichnung (L):	Schmitten
Bundesland (ST):	Hessen
Land (C):	DE

Buttons: OK, Abbrechen

- Speichern Sie den Namen des Zertifikats durch Drücken auf OK
- Speichern Sie das Zertifikat durch Drücken auf OK
- Anschließend können Sie einen beliebigen Aliasnamen vergeben

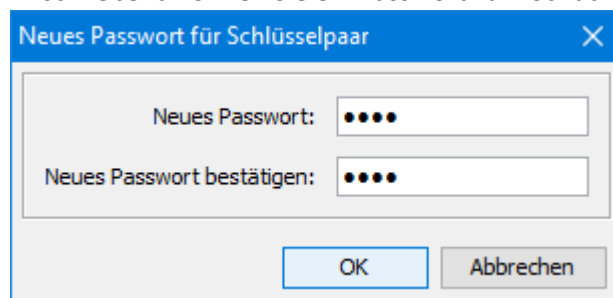


The 'Neuer Aliasname für Schlüsselpaar' dialog box contains the following field:

Field	Value
Aliasnamen eingeben:	edsrv.test.eifertsystems

Buttons: OK, Abbrechen

- Anschließend können Sie ein Passwort zum Schutz des Zertifikats vergeben

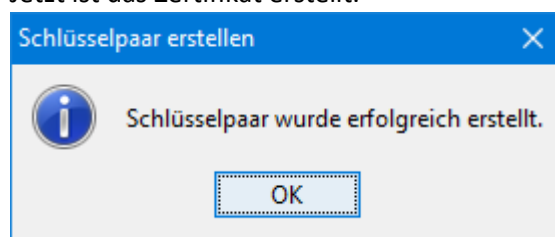


The 'Neues Passwort für Schlüsselpaar' dialog box contains the following fields:

Field	Value
Neues Passwort:	••••
Neues Passwort bestätigen:	••••

Buttons: OK, Abbrechen

- Jetzt ist das Zertifikat erstellt.

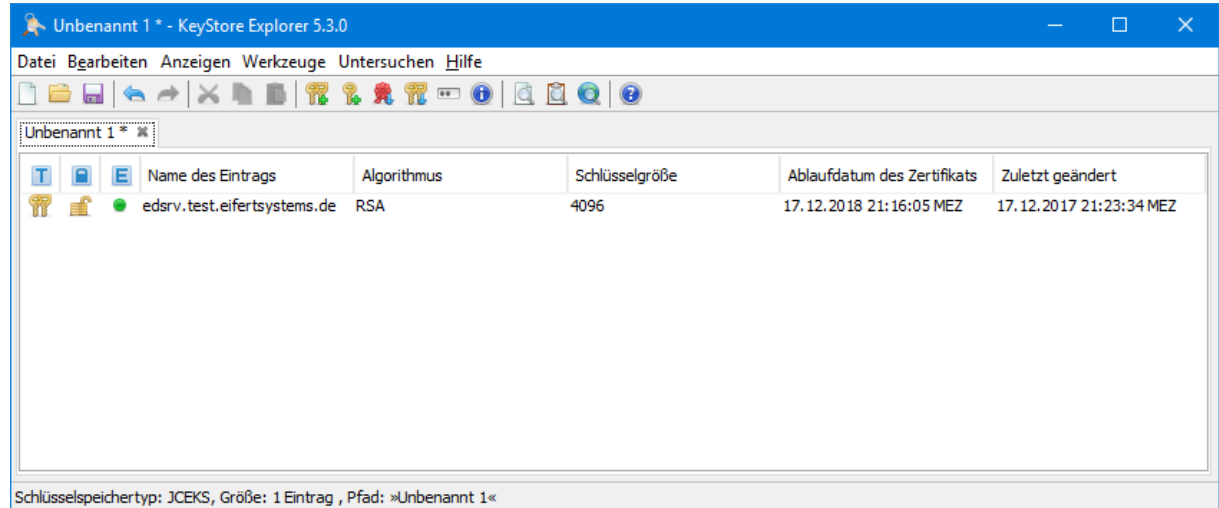


The 'Schlüsselpaar erstellen' dialog box contains the following message:

i Schlüsselpaar wurde erfolgreich erstellt.

Buttons: OK

10. Anschließend können Sie das neu erstellte Zertifikat im Speicher sehen:

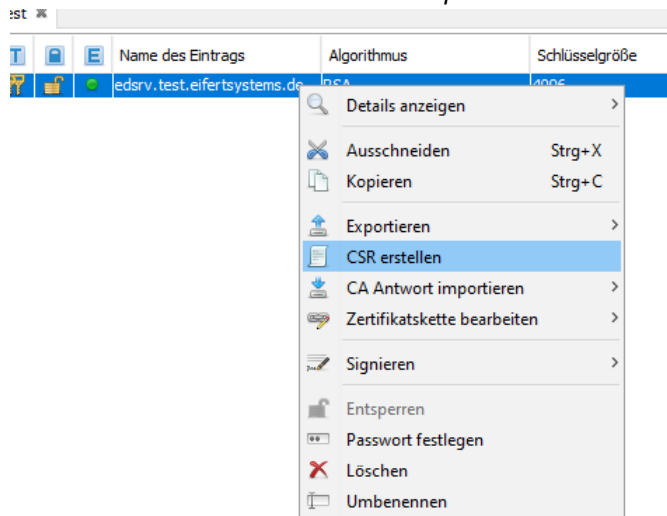


11. Speichern Sie den Zertifikatsspeicher ab (Strg+S) oder *Datei* → *Speichern*.

Zertifikat durch externe Zertifizierung signieren lassen

Wenn Sie Ihr Zertifikat nicht signieren lassen möchten, können Sie diesen Schritt überspringen.

1. Exportieren Sie den Certificate Signing Request (CSR) durch Rechtsklick auf das zu signierende Zertifikat und Auswählen von *CSR exportieren*.



- Speichern Sie die Anfrage auf der Festplatte in einem mit Ihrer Zertifizierungsstelle abgestimmten Format, z.B.

Anfrage für Zertifikatsignierung erstellen

Format: PKCS #10 SPKAC

Signaturalgorithmus: SHA-256 mit RSA

Sicherheitsabfrage:

Optionaler Firmenname:

Zertifikatserweiterung zur Anfrage hinzufügen

CSR-Datei: r:\Maune\Desktop\edsrv.test.eifertsystems.de.csr Navigieren

OK Abbrechen

- Senden Sie die exportierte Datei an Ihre Zertifizierungsstelle
- Warten Sie auf die Antwort Ihrer Zertifizierungsstelle
- Importieren Sie die Antwort Ihrer Zertifizierungsstelle durch Rechtsklick auf das Zertifikat und Auswählen von *CA Antwort importieren*.

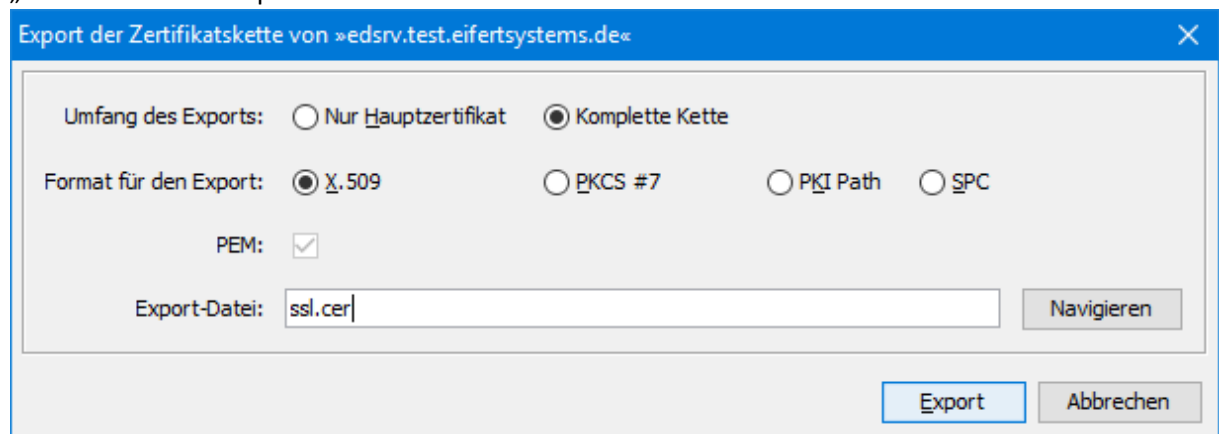
Algorithmus	Schlüsselgröße	Ablaufdatum des Zertifikats	Zuletzt geändert
RSA	4096	17.12.2018 21:16:05 MEZ	17.12.2017 2

Zertifikat für EDPweb exportieren

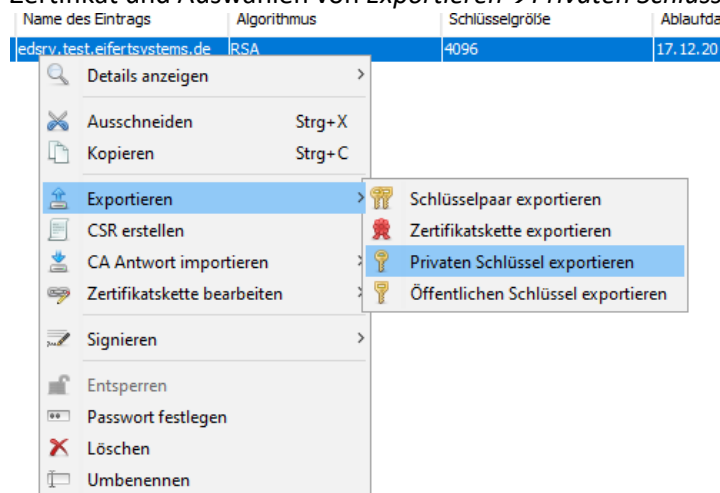
- Exportieren Sie den öffentlichen Teil des Zertifikats durch Rechtsklick auf das zu exportierende Zertifikat und Auswählen von *Exportieren* → *Zertifikatskette exportieren*.

Algorithmus	Schlüsselgröße	Ablaufdatum des Zertifikats	Zuletzt geändert
ms.de RSA	4096	17.12.2018 21:16:05 MEZ	17.12.2017 21:23:34

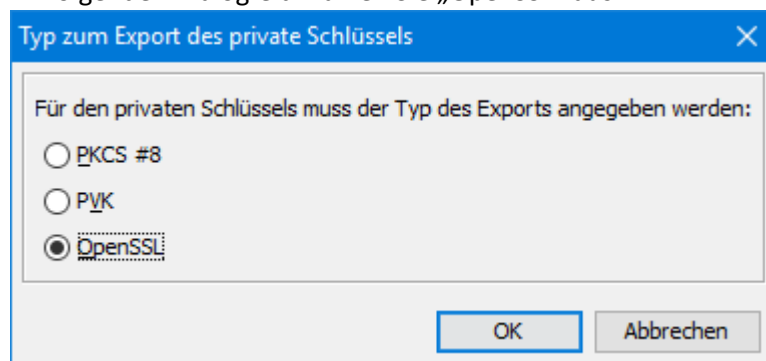
- Im folgenden Dialog verwenden Sie folgende Einstellungen und speichern das Zertifikat unter „ssl.cer“ auf der Festplatte ab.



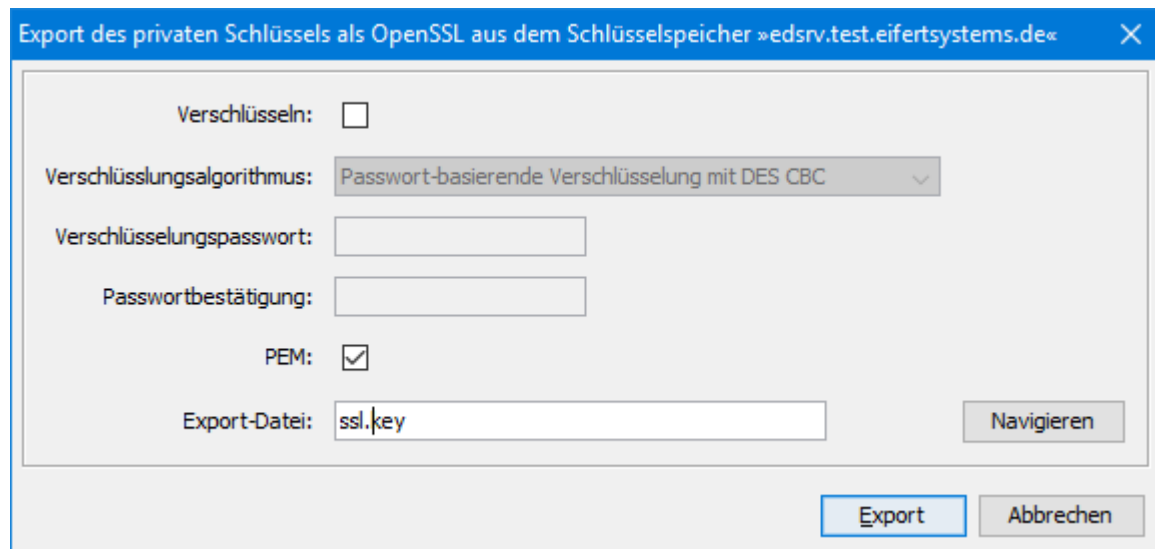
- Exportieren Sie den privaten Schlüssel des Zertifikats durch Rechtsklick auf das zu exportierende Zertifikat und Auswählen von *Exportieren* → *Privaten Schlüssel exportieren*.



- Im folgenden Dialogfeld wählen Sie „OpenSSL“ aus:



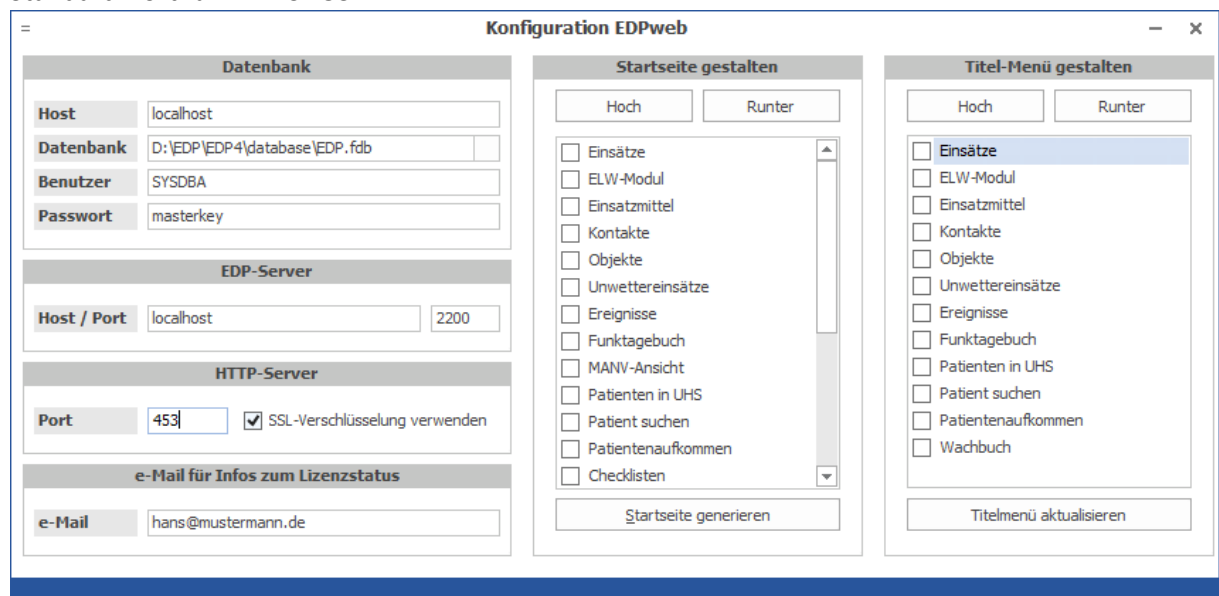
- Im folgenden Dialogfeld, deaktivieren Sie die Verschlüsselung des privaten Schlüssels und speichern ihn als „ssl.key“ auf der Festplatte ab.



Hinweis: Wenn Sie den privaten Schlüssel verschlüsseln, ist ein Start des EDPweb-Servers nicht möglich.

SSL in EDPweb aktivieren

1. Kopieren Sie beide Daten „ssl.key“ und „ssl.cer“ in den Installationsordner von EDPweb.
2. Aktivieren Sie die SSL-Option in der EDPweb-Konfiguration. Am besten verwenden Sie den Standard-Port für HTTPS 453.



3. Starten Sie den EDPweb-Server neu.
4. Prüfen Sie das LogFile „EDPweb.log“ auf mögliche Fehlermeldungen.

Allgemeine Hinweise

- Das Zertifikat zusammen mit dem privaten Schlüssel ist der Ausweis des EDPweb-Servers. Sorgen Sie in allen Umständen dafür, dass der private Schlüssel geheim bleibt und den Server nicht verlässt.
- Wählen Sie eine möglichst kurze Laufzeit des Schlüssels, um im Falle einer Kompromittierung des Zertifikats die Zeitspanne eines möglichen Angriffs so kurz wie möglich zu halten. Im Bereich des

Internet sind heutzutage Zertifikate mit Gültigkeitsdauern kleiner 3 Monate bei sensiblen Domains (z.B. google.de) vorgesehen.

- Wenn Sie die Browser-Warnung für ein selbst-signiertes Zertifikat umgehen wollen, müssen Sie sich Ihr Zertifikat von einer autorisierten Stelle signieren lassen. Je nach Anbieter ist diese Signatur kostenpflichtig. In vielen Netzwerkimplementierungen betreiben die Administratoren eine lokale Zertifizierungsstelle, die Zertifikate für den lokalen Einsatz ebenfalls signieren können.
- Signierte Zertifikaten können im Gegensatz zu selbst-signierten für ungültig erklärt werden.
- Wenn der EDPweb-Server unter verschiedenen DNS-Namen oder nur mit der IP-Adresse erreicht werden kann, können Sie dies unter Zertifikatserweiterungen berücksichtigen. Bitte beachten Sie, dass dies bereits beim Erstellen des Zertifikats geschehen muss.