# ANLEITUNG: ZERTIFIKATSERSTELLUNG WINDOWS AD

# SCHRITT FÜR SCHRITT ANLEITUNG

## Ziel:

Erstellung und Signatur eines Zertifikats in einer Windows-AD-Umgebung für einen Webserver.

## Schritt 1

Zunächst kann, wenn die Zertifizierungsstelle nicht bekannt ist, die Applikation **„Zertifizierungsstelle“** gestartet werden:

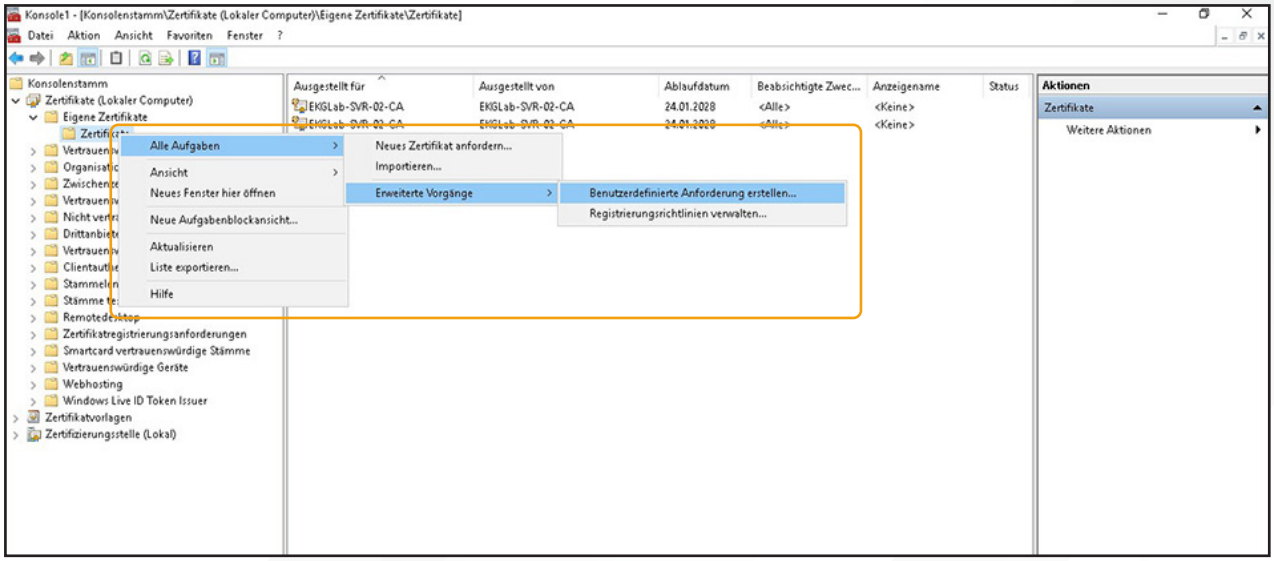

## Schritt 2

Anschließend ist die Zertifizierungsstelle zu sehen, hier EKGLab-SVR-02-CA:

# SCHRITT FÜR SCHRITT ANLEITUNG

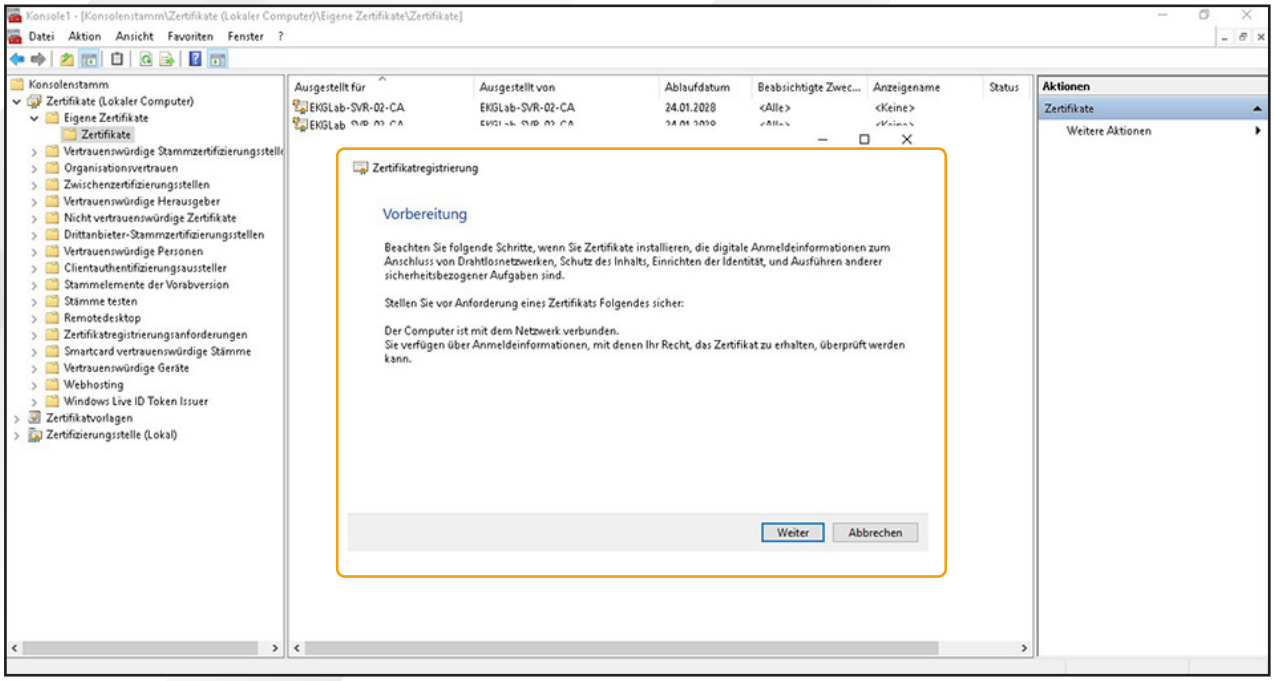
## Schritt 3

Dann muss das Konsolen-Snap-In **„Zertifikate“** in der Microsoft Management Console ausgewählt werden und dort unter **„Eigene Zertifikate → Zertifikate → Alle Aufgaben → Erweiterte Vorgänge → Benutzerdefinierte Anforderung erstellen...“** gewählt werden:




## Schritt 4

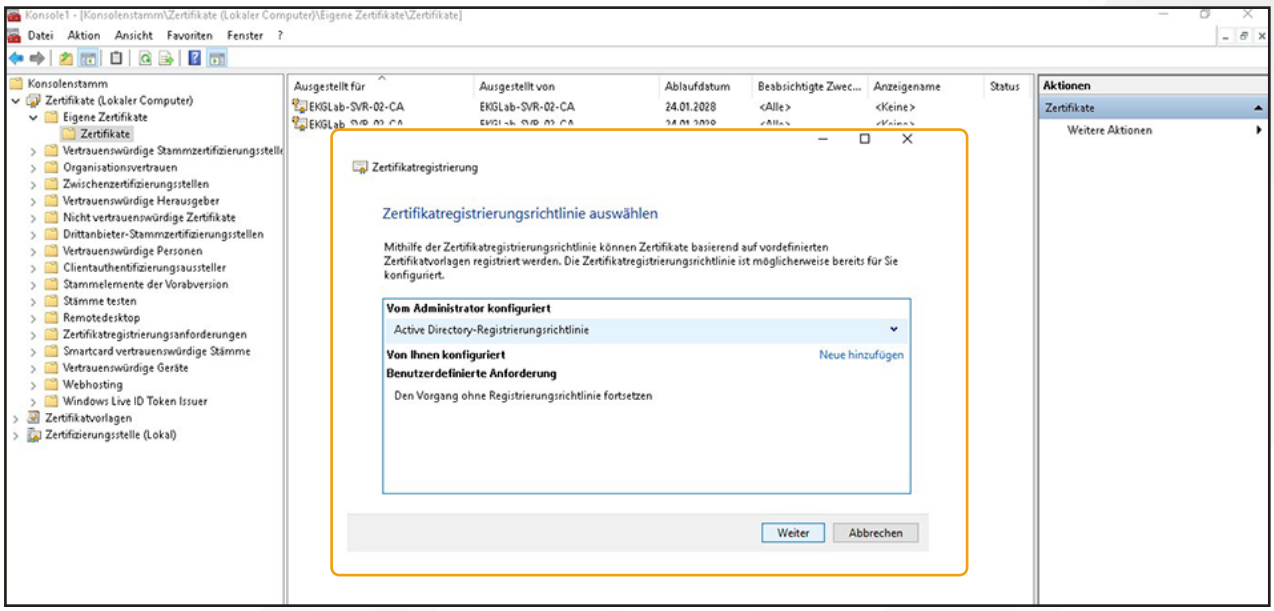
Anschließend muss dem Assistenten gefolgt werden:



# SCHRITT FÜR SCHRITT ANLEITUNG

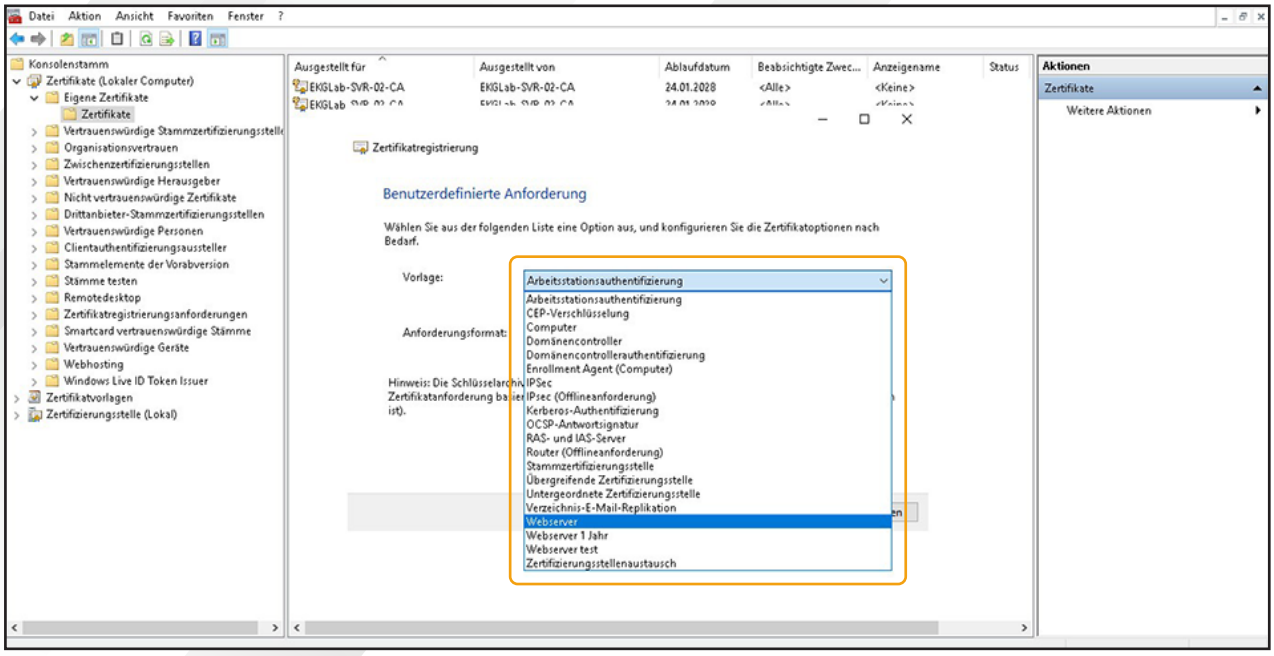
## Schritt 5

Im nächsten Schritt sollte **„Active-Directory-Registrierungsrichtlinie“** gewählt werden, wenn vorhanden, sonst **„Den Vorgang ohne Registrierungsrichtlinie fortsetzen“**:




## Schritt 6

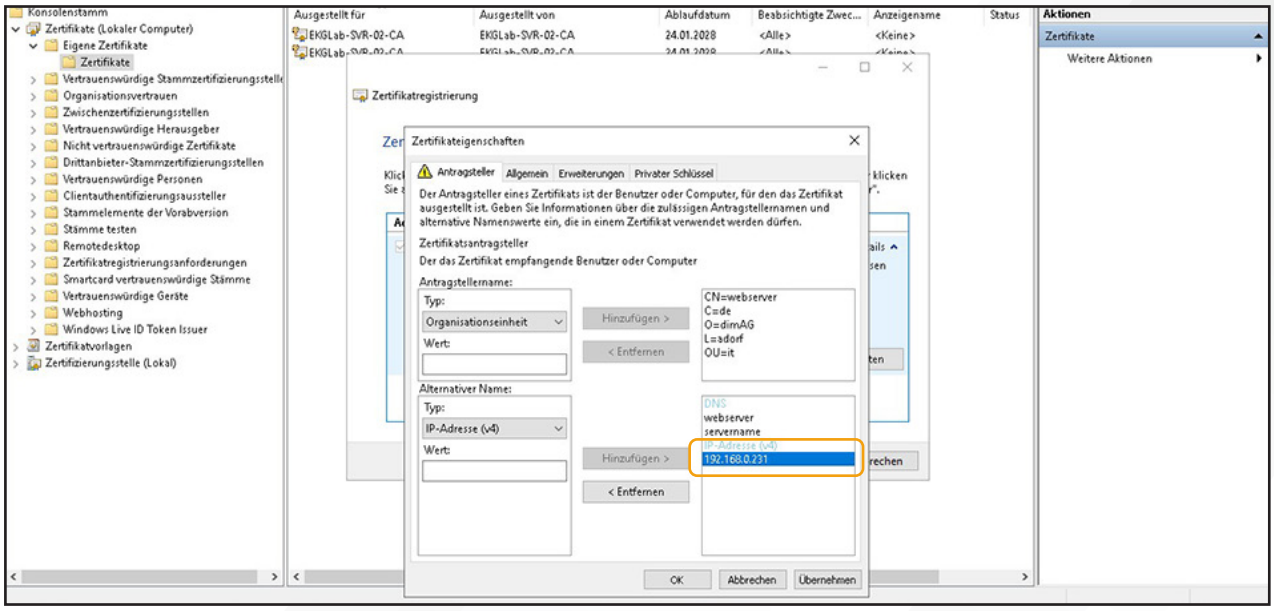
Im nächsten Schritt wird die Standard-Vorlage **„Webserver“** ausgewählt:



# SCHRITT FÜR SCHRITT ANLEITUNG

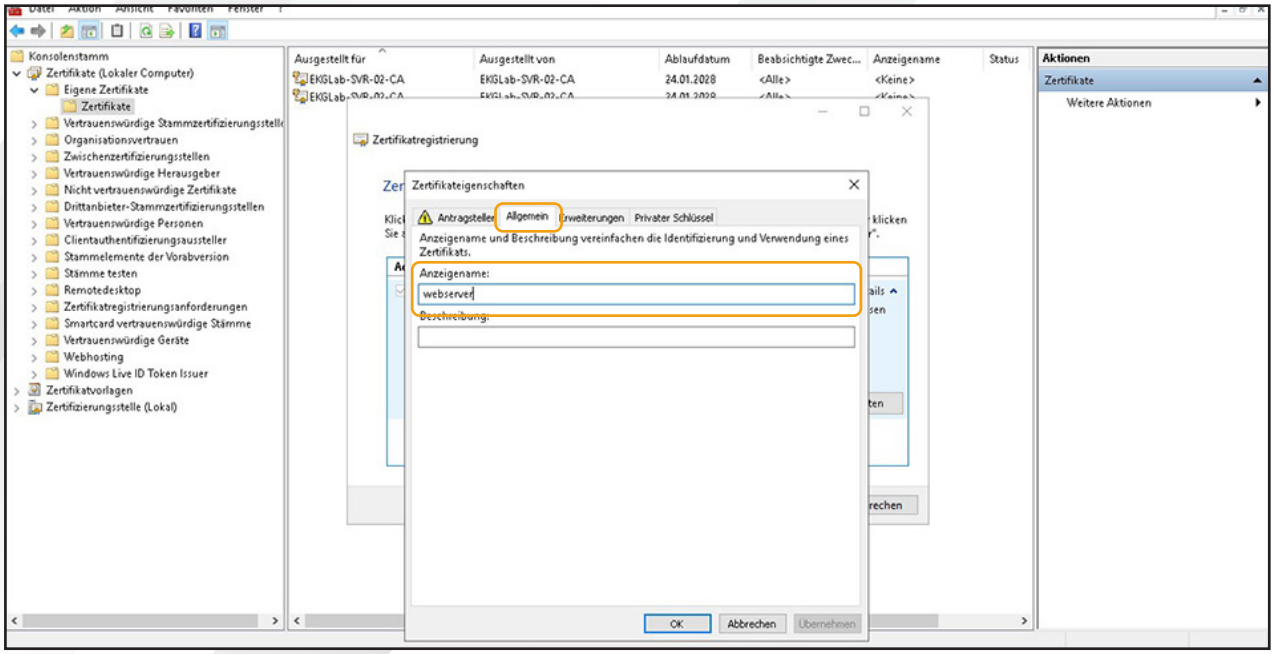
## Schritt 7

Daraufhin muss unter **„Alternativer Name“** der DNS-Name des Servers bzw. die IP-Adresse angegeben werden:




## Schritt 8

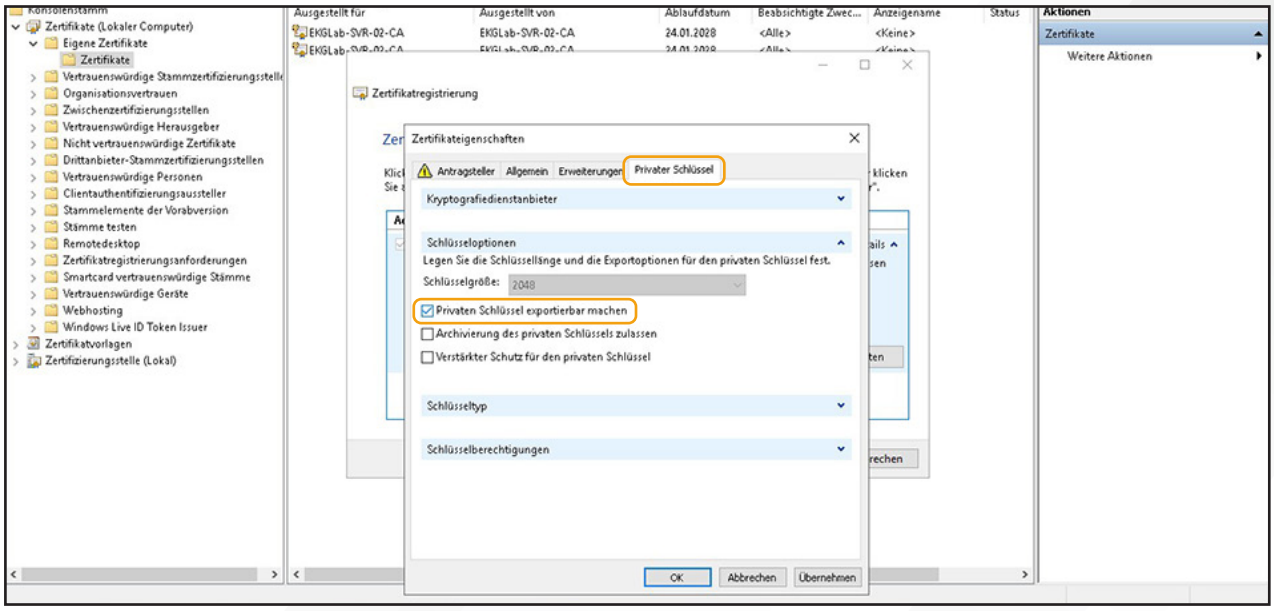
Im nächsten Schritt wird die Standard-Vorlage **„Webserver“** ausgewählt:



# SCHRITT FÜR SCHRITT ANLEITUNG

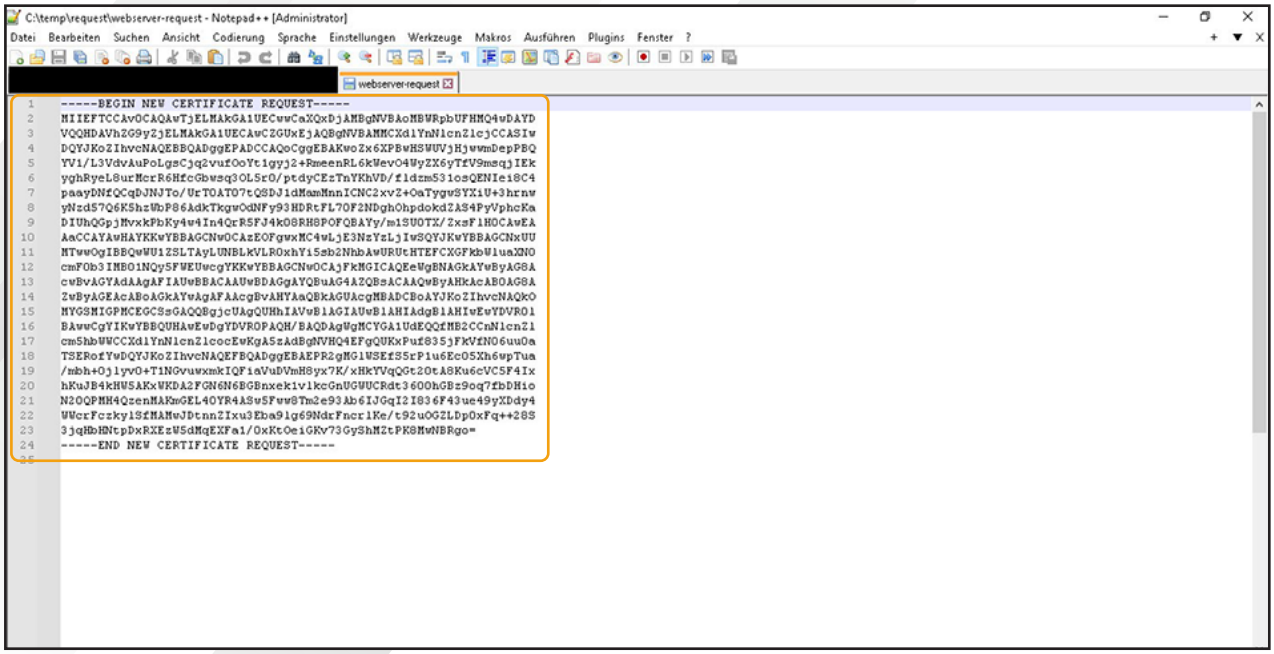
## Schritt 9

Unter **„Privater Schlüssel“** muss die Option **„Privaten Schlüssel exportierbar machen“** gewählt werden:




## Schritt 10

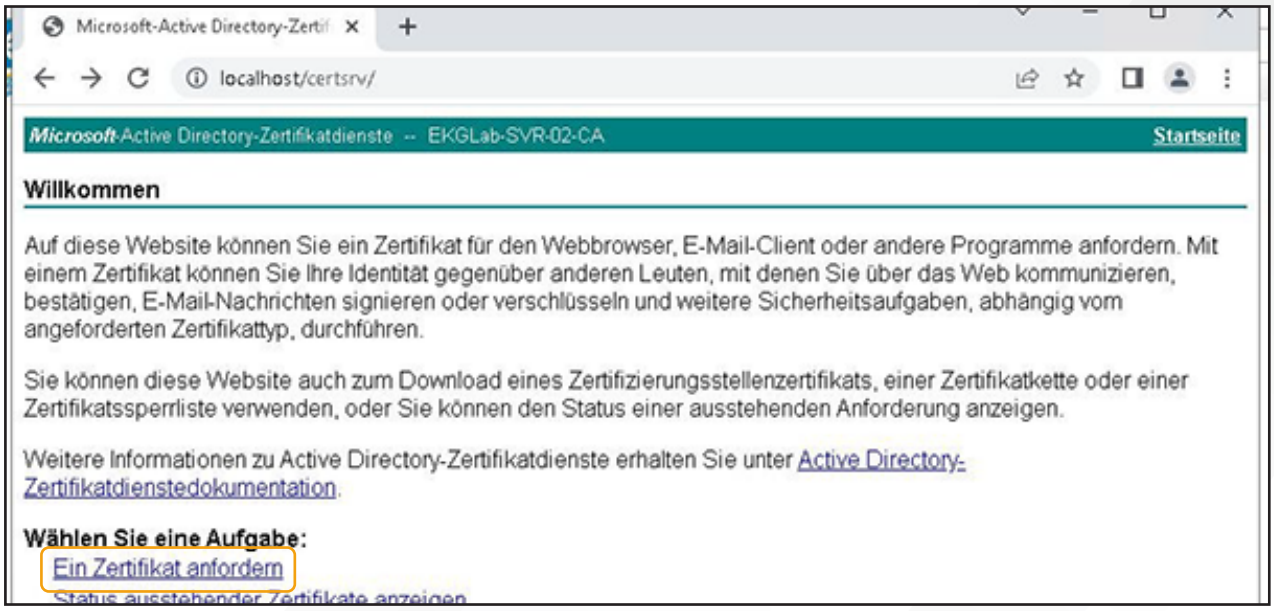
Daraus wird eine Datei ausgegeben, diese muss in einem Editor geöffnet und der Inhalt kopiert werden:



# SCHRITT FÜR SCHRITT ANLEITUNG

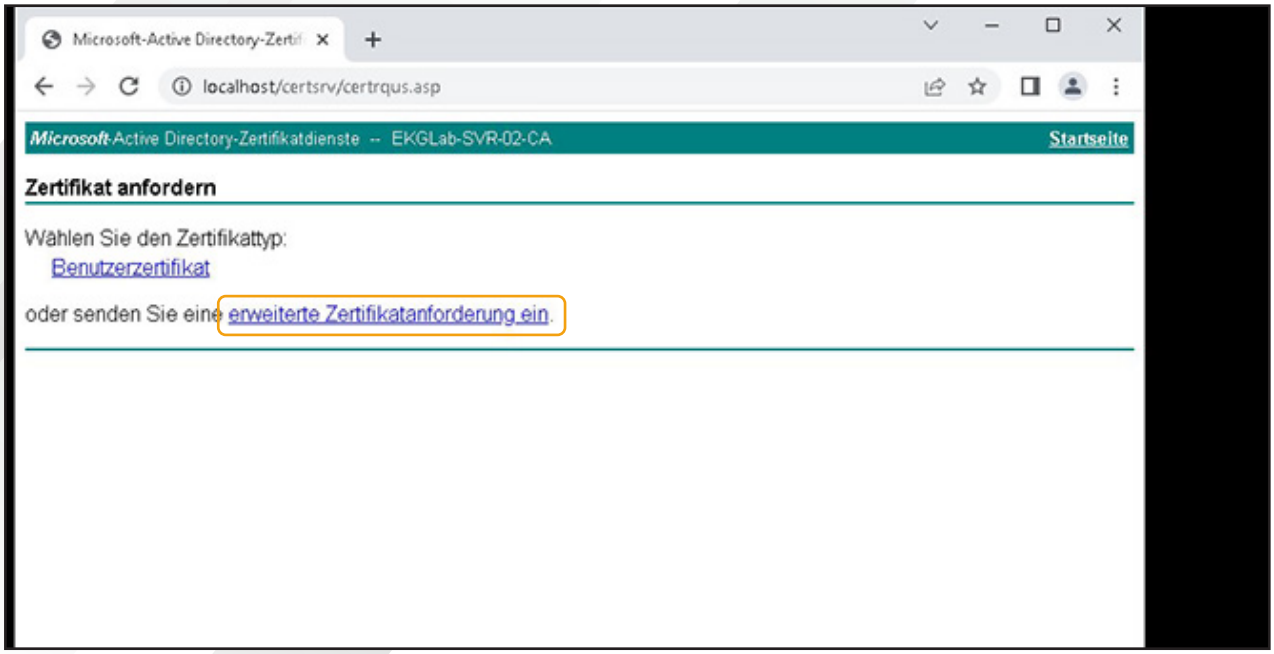
## Schritt 11

Anschließend müssen die **Active-Directory-Zertifikatsdienste** im Browser geöffnet werden:




## Schritt 12

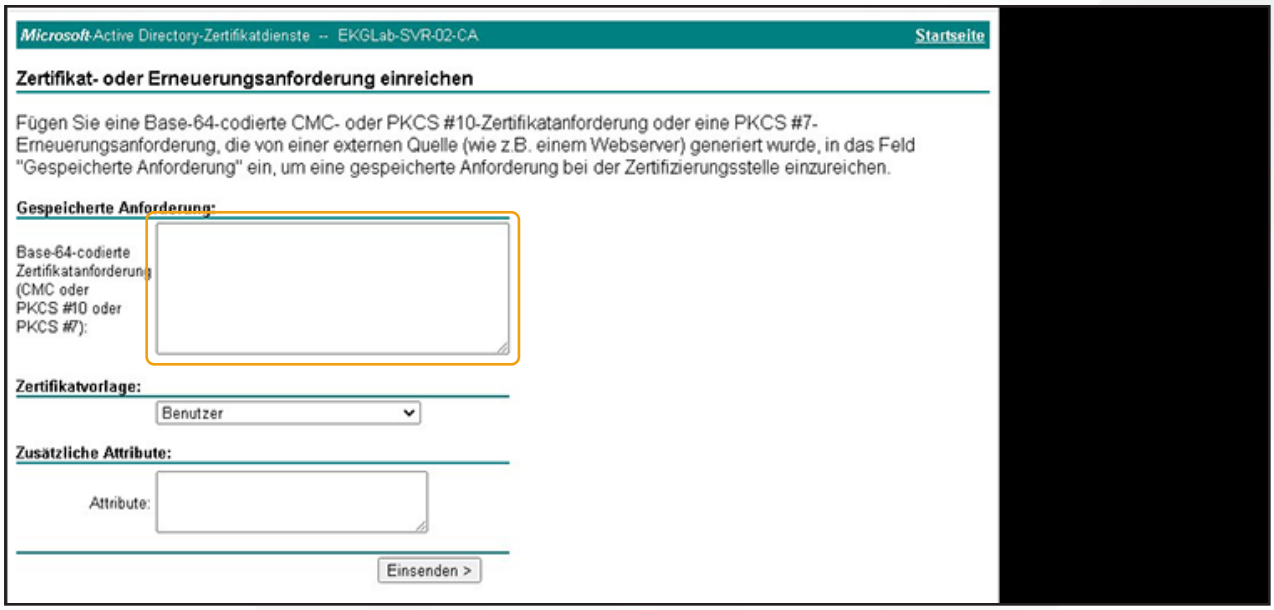
Dort muss **„Ein Zertifikat anfordern“** und dort **„Erweiterte Zertifikatanforderung“** gewählt werden:



# SCHRITT FÜR SCHRITT ANLEITUNG

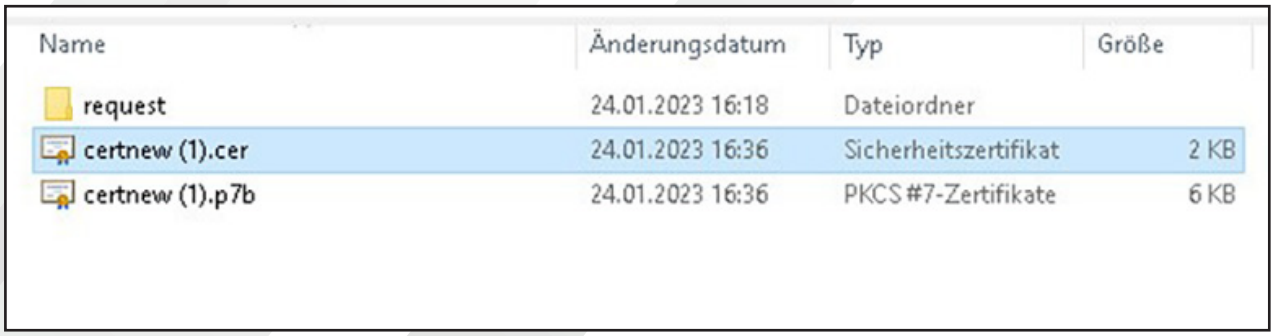
## Schritt 13

In das Feld **„Base-64-codierte Zertifikatanforderung“** muss der zuvor kopierte Inhalt eingefügt werden, die restlichen Felder können leer bleiben:




## Schritt 14

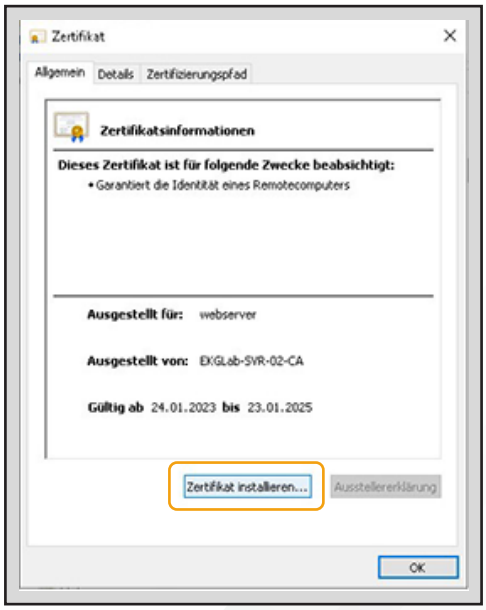
Nach einem Klick auf **„Einsenden“** kann das signierte Zertifikat heruntergeladen werden. Dieses muss dann im Explorer durch Doppelklick geöffnet werden:



# SCHRITT FÜR SCHRITT ANLEITUNG

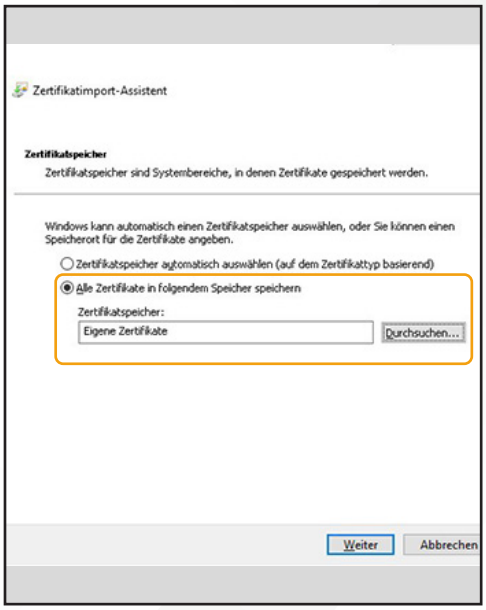
## Schritt 15

Im darauf folgenden Dialog muss **„Zertifikat installieren“** gewählt werden und dem Assistenten gefolgt:



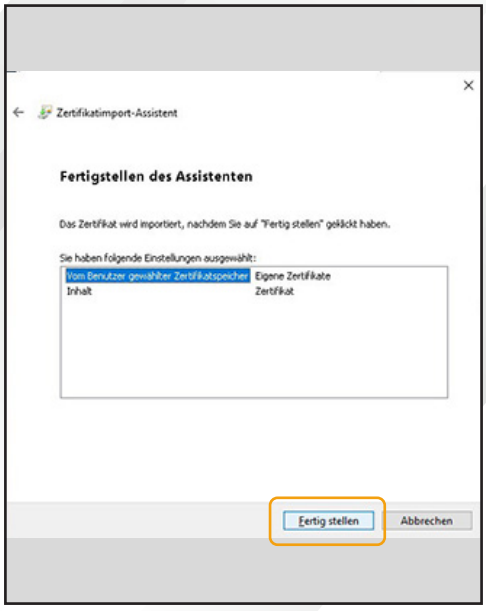

## Schritt 16

Im nächsten Schritt wird ein Zertifikatspeicher gewählt, hier sollte **„Eigene Zertifikate“** gewählt werden:



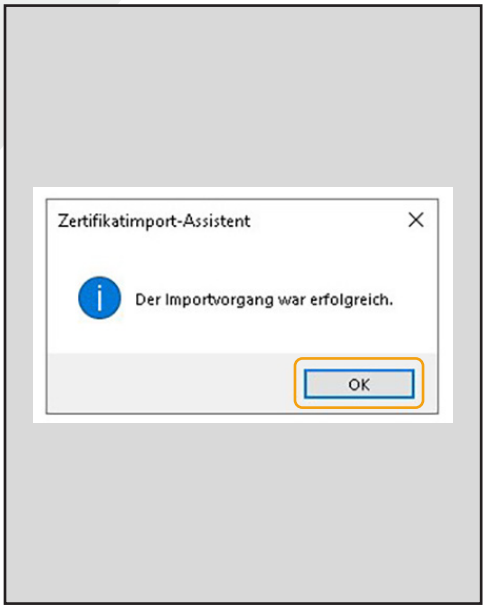

## Schritt 17

Dies muss mit einem Klick auf **„Fertig stellen“** bestätigt werden:




## Schritt 18

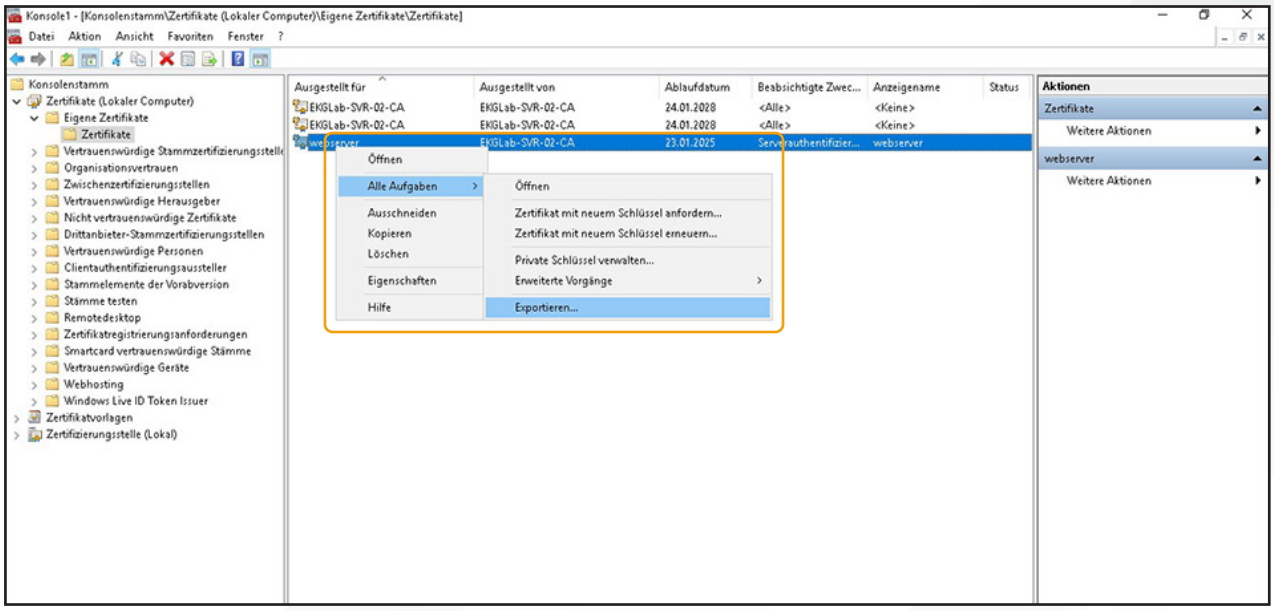
Dies wird bestätigt:



# SCHRITT FÜR SCHRITT ANLEITUNG

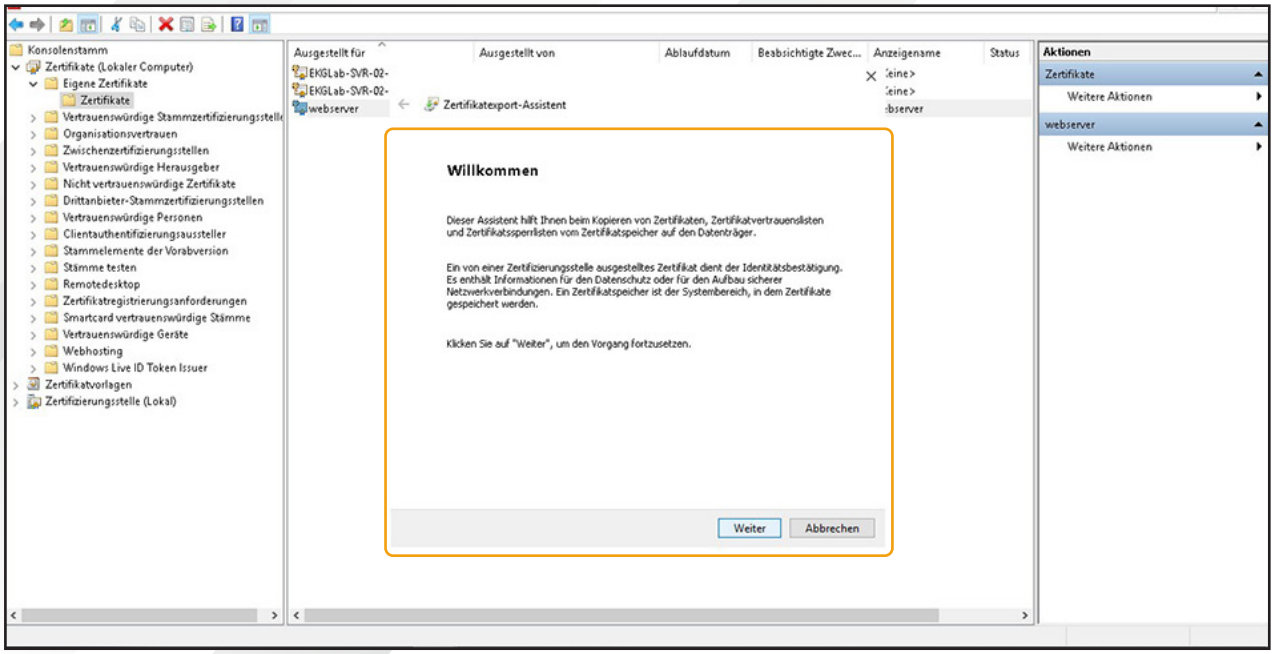
## Schritt 19

Anschließend erscheint das Zertifikat in der Liste und kann über **„Alle Aufgaben → Exportieren“** exportiert werden:




## Schritt 20

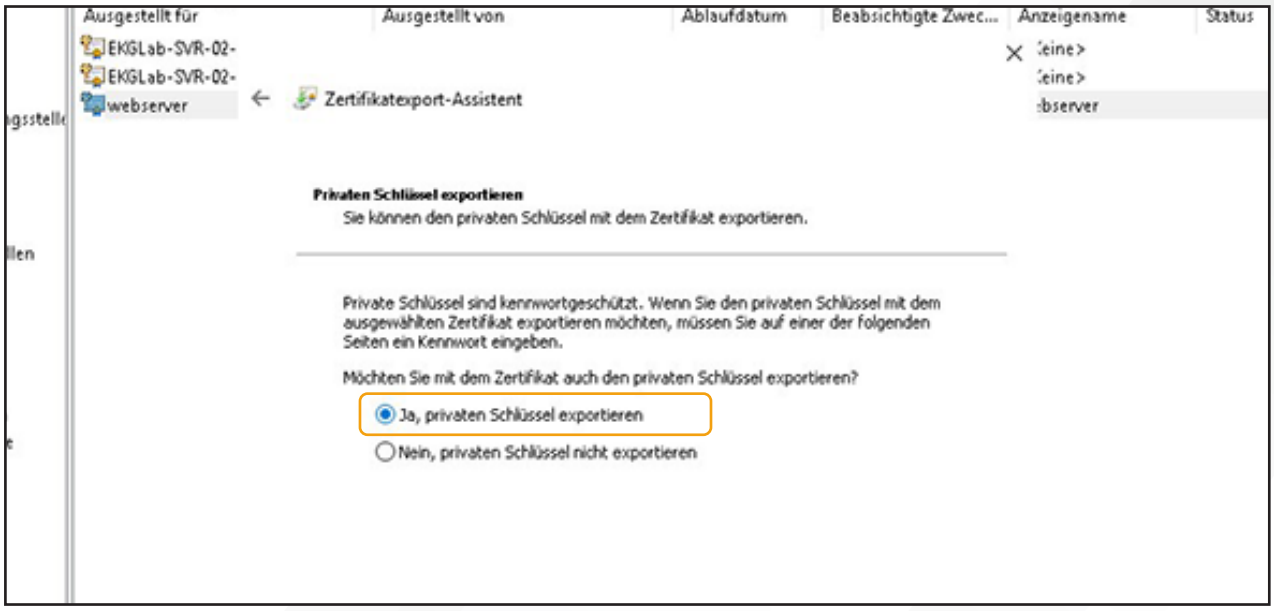
Auch hier muss wieder einem Assistenten gefolgt werden:



# SCHRITT FÜR SCHRITT ANLEITUNG

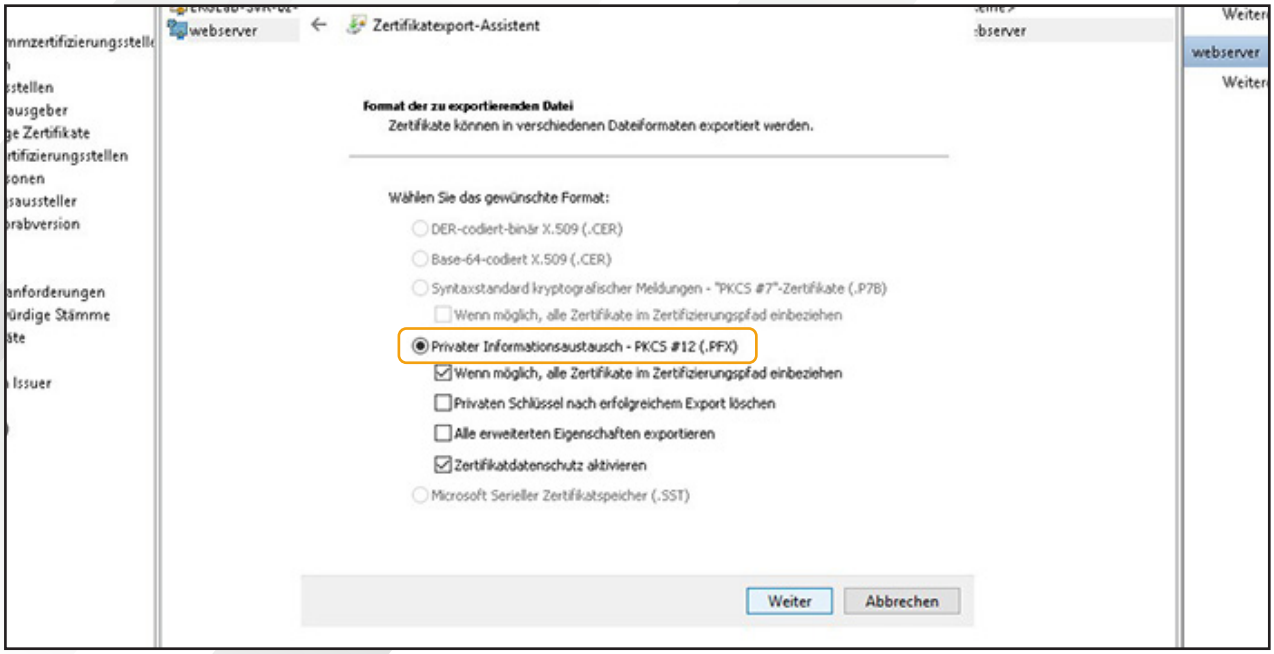
## Schritt 21

Im nächsten Schritt muss **„Ja, privaten Schlüssel exportieren“** gewählt werden:




## Schritt 22

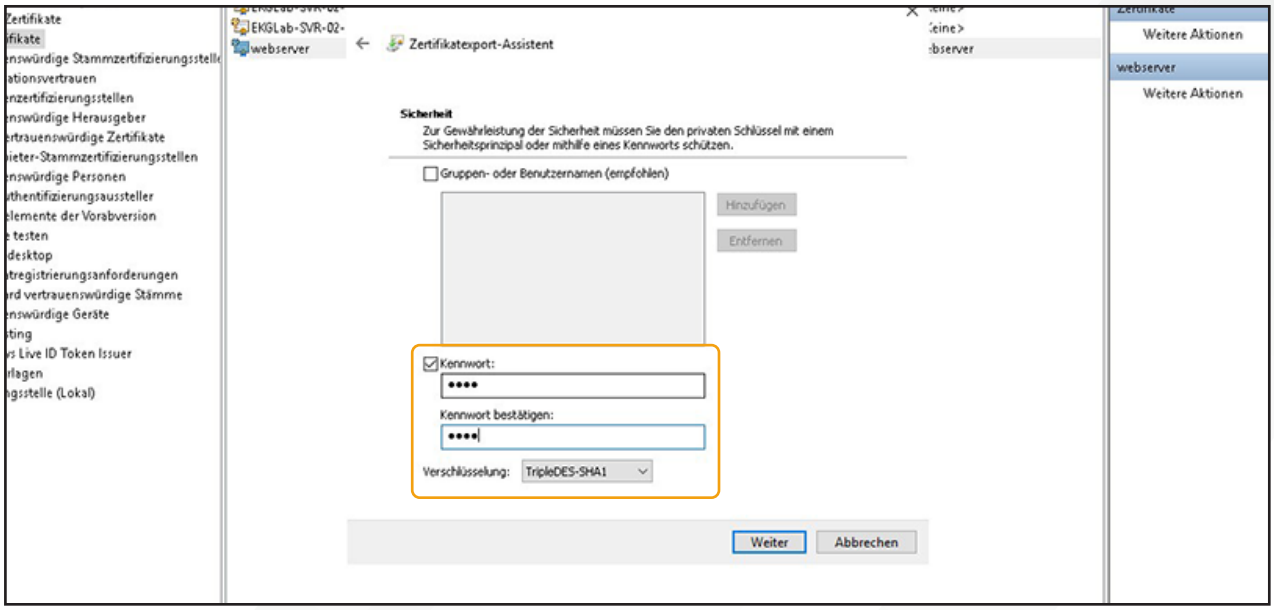
Daraufhin muss die Option **„PKCS #12“** gewählt werden:



# SCHRITT FÜR SCHRITT ANLEITUNG

## Schritt 23

Im nächsten Schritt muss das Zertifikat mit einem **Passwort** geschützt werden, hier kann ein Dummy-Passwort gewählt werden, ein leeres Passwort oder kein Passwort wird aber u.U. abgelehnt:




## Schritt 24

Die daraus resultierende **.pfx-Datei** muss nun auf den **Server** übertragen werden. Bei IIS kann diese direkt verwendet werden, zur Verwendung mit nginx oder dem Apache httpd muss eine .crt- und eine .key-Datei erzeugt werden. Dies geht mit openssl:

```
openssl pkcs12 -in beispiel.pfx -clcerts -nokeys -out beispiel.crt
```

```
openssl pkcs12 -in beispiel.pfx -nocerts -nodes -out beispiel.key
```

Wurde zuvor ein Passwort gesetzt, kann es von der .key-Datei entfernt werden:

```
openssl rsa -in beispiel.key -out beispiel-unlocked.key
```

Dazu muss einmalig das Passwort eingegeben werden.