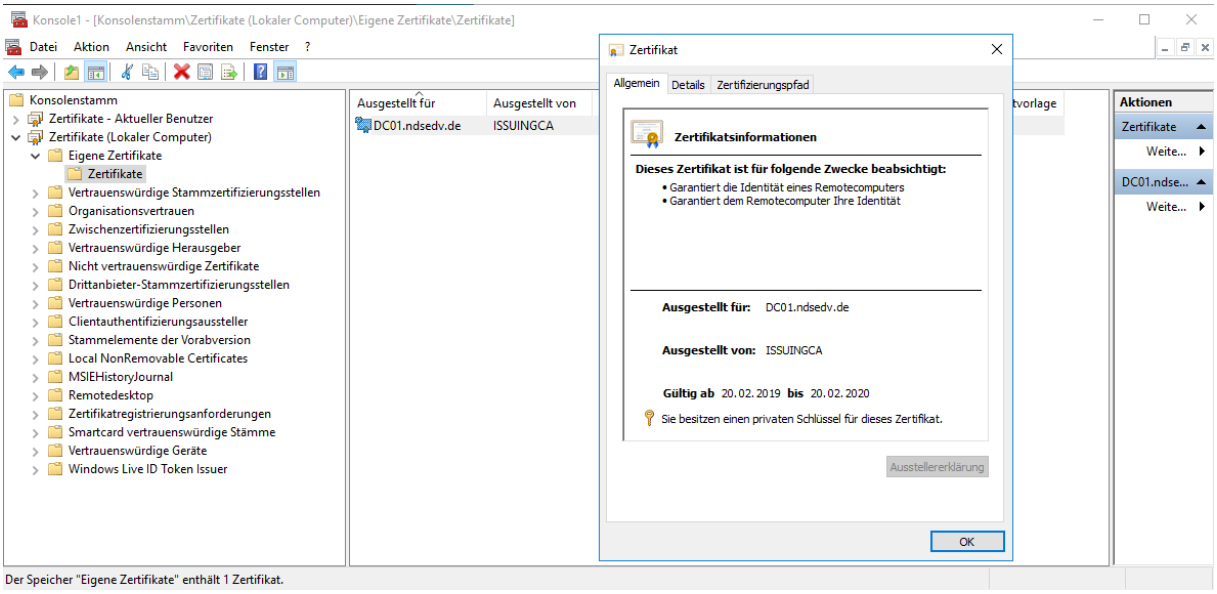
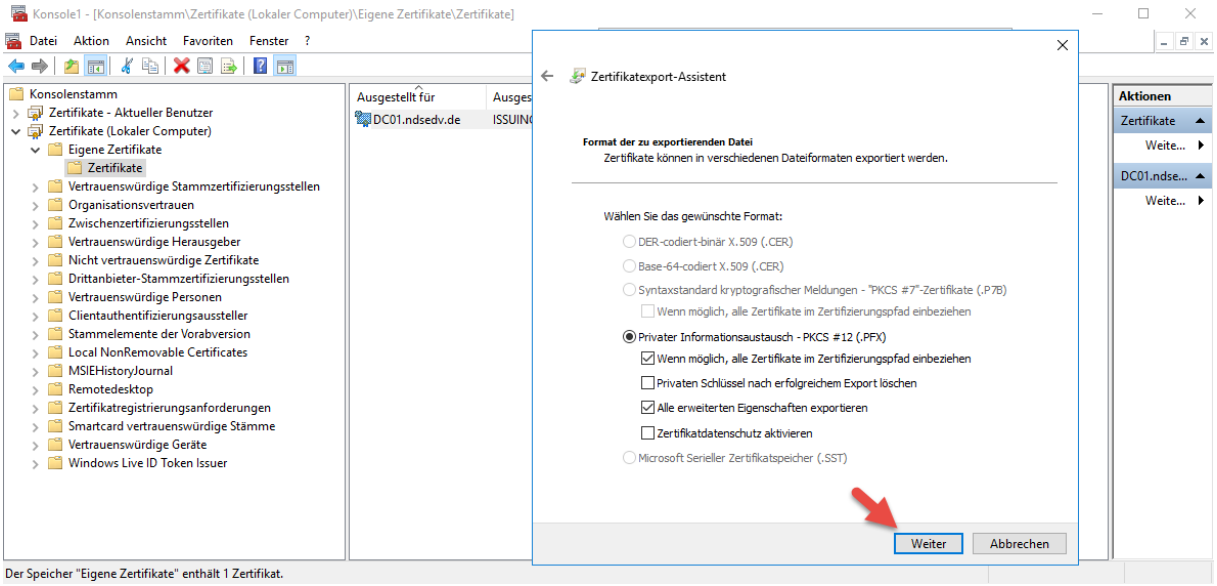
Konvertieren eines .pfx Zertifikat in .pem

Das Ziel ist die Erstellung eines Zertifikats im PEM Format. Als Basis dient ein exportiertes Privates Zertifikat von einem Windows Server.

Öffnen die MMC:

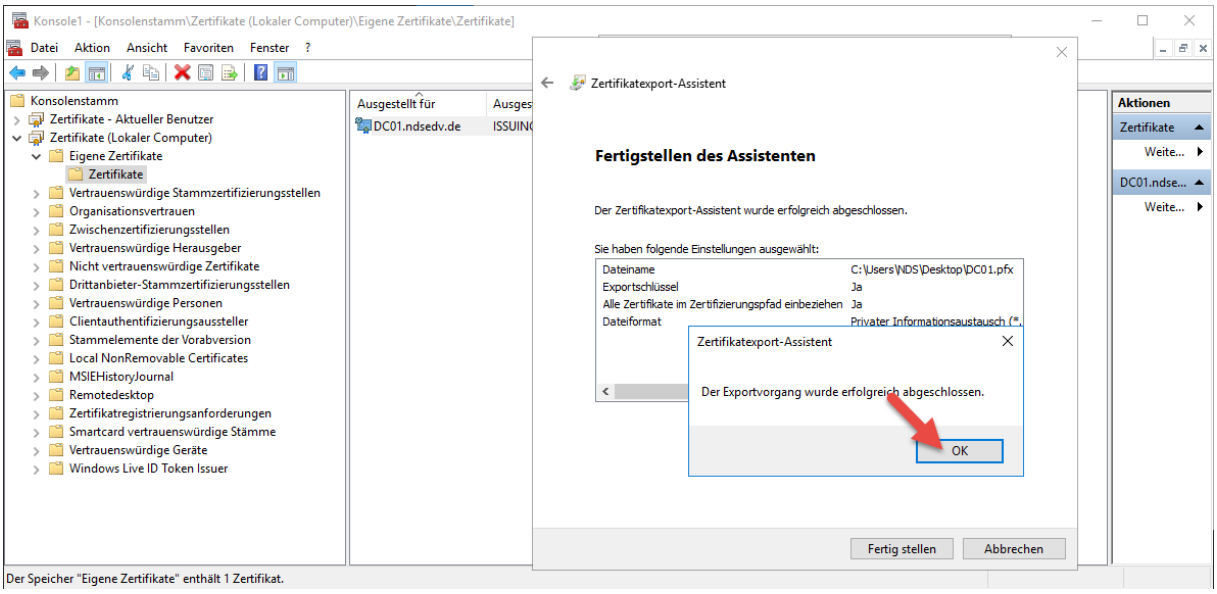


Exportieren das Zertifikat…

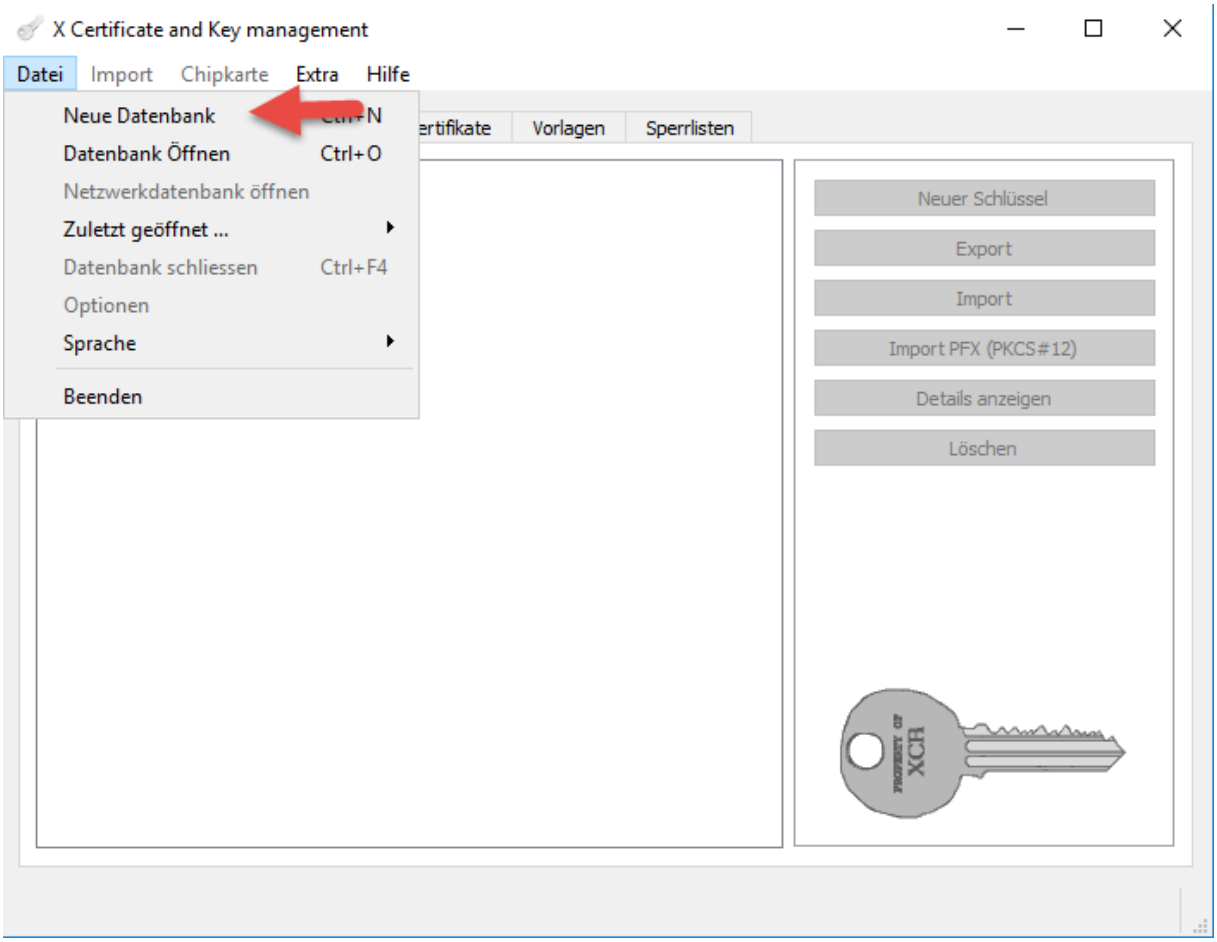


Konvertieren eines .pfx Zertifikat in .pem

…und vergeben ein Passwort:



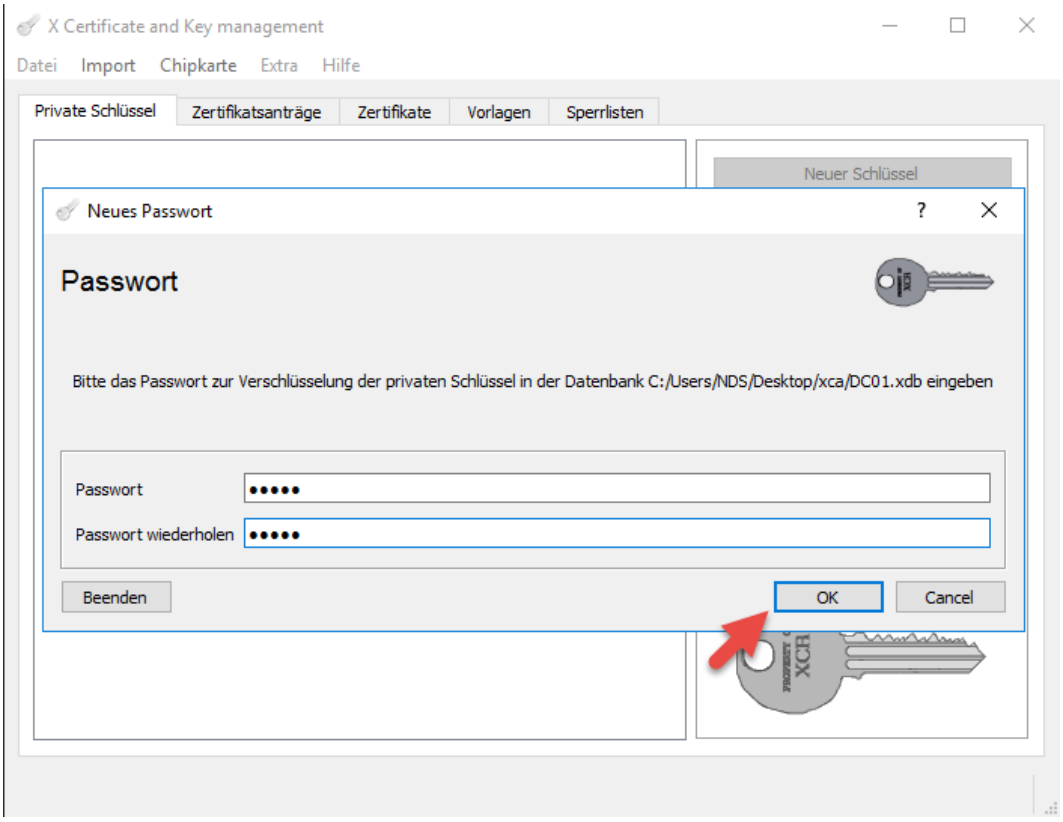
Starten das Tool XCA und erstellen als erstes eine neue Datenbank:
https://hohnstaedt.de/xca/



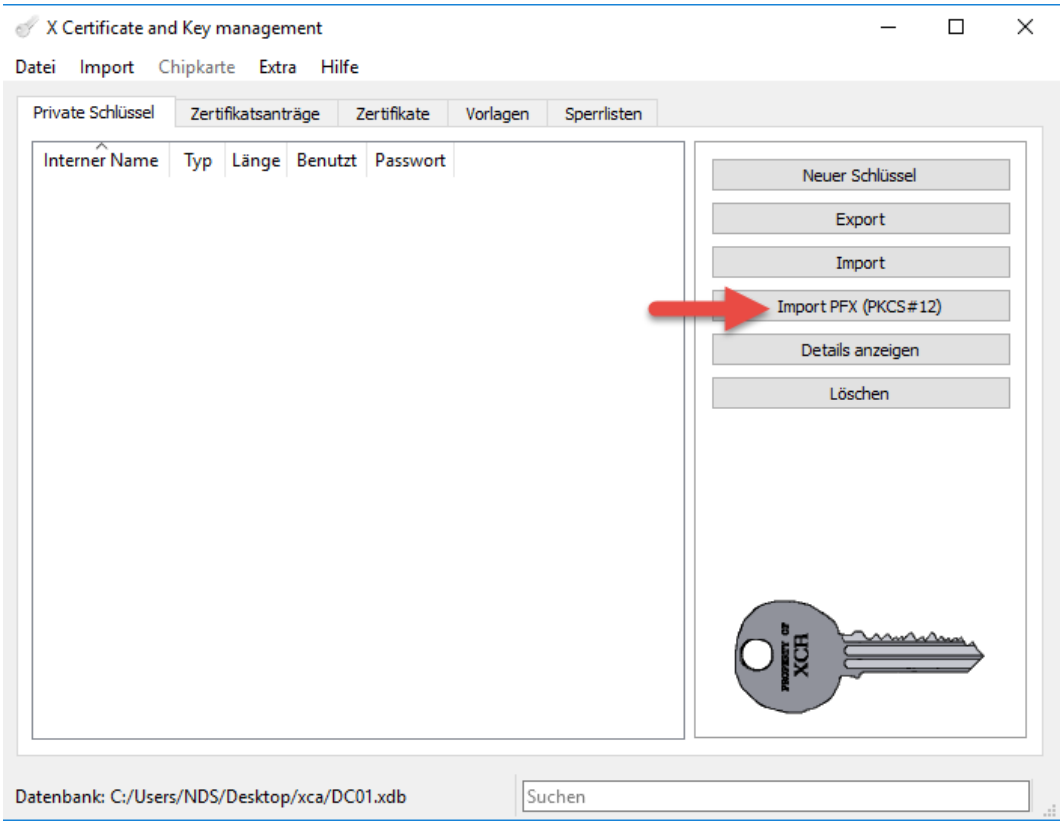
Erstellt von Jörn Walter **17.02.2019**

Konvertieren eines .pfx Zertifikat in .pem

Vergeben ein Passwort für die Datenbank:

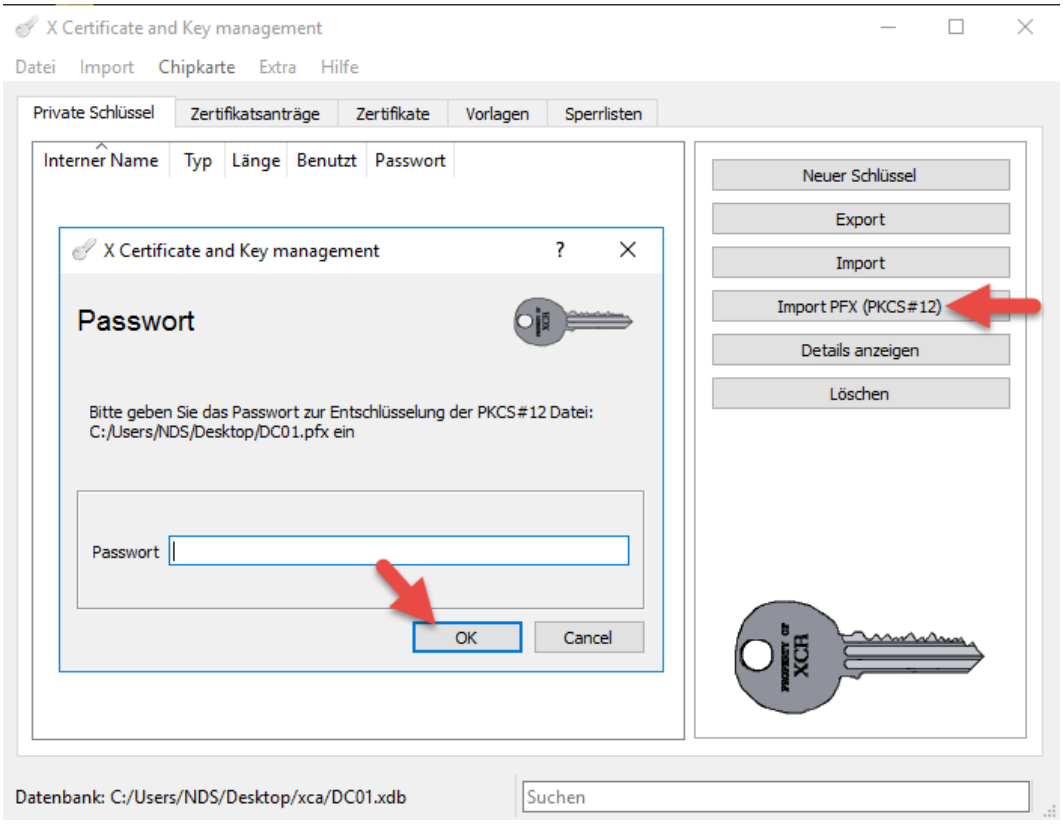


Importieren das gerade exportierte Private Zertifikat:

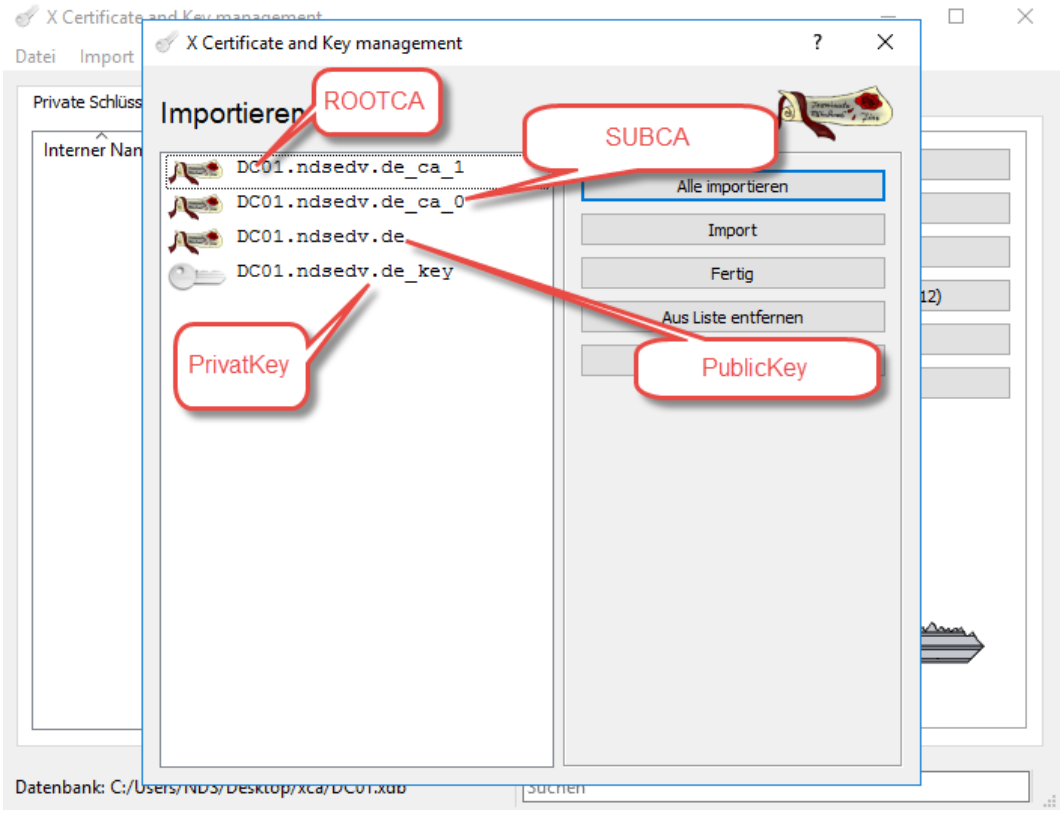


Konvertieren eines .pfx Zertifikat in .pem

Geben das Passwort ein welches wir beim Export vergeben haben:

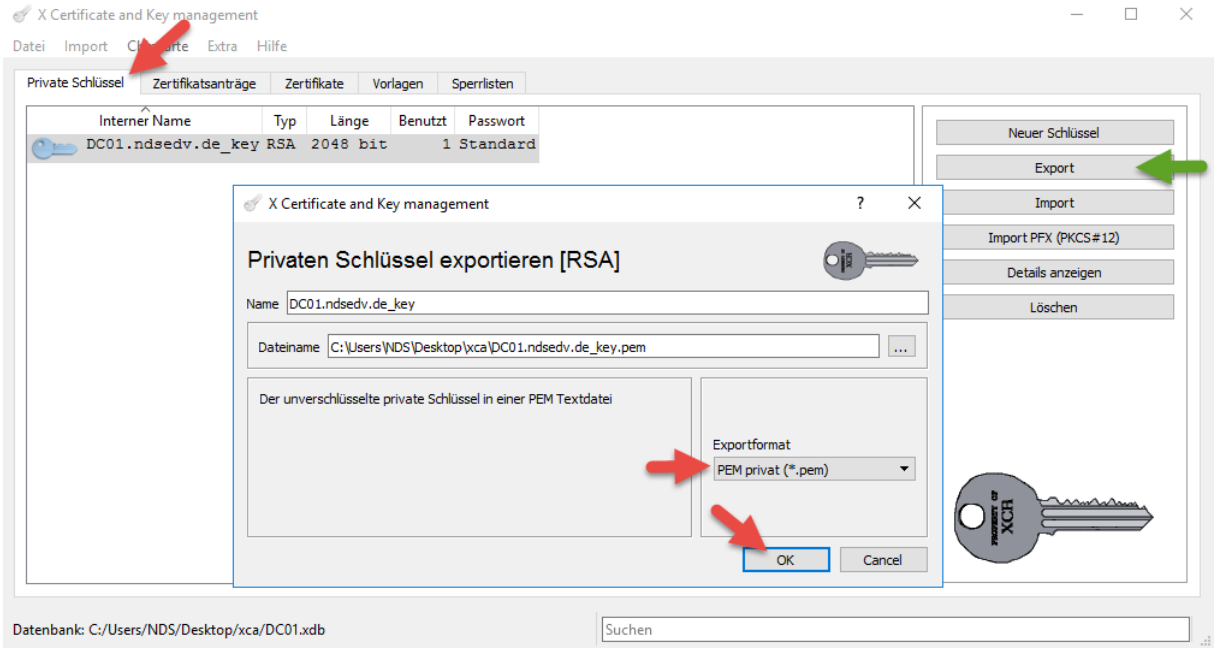


Erklärung zum Aufbau der Zertifikatskette. Die oberen 3 sind jeweils öffentliche Schlüssel.

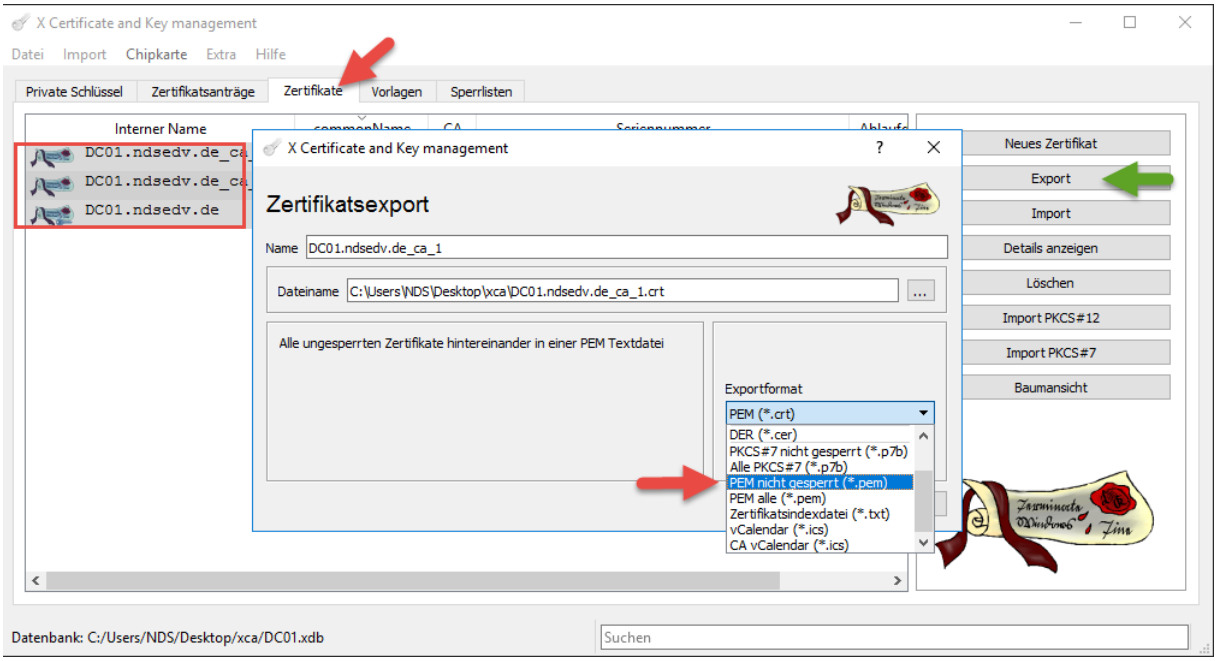


Konvertieren eines .pfx Zertifikat in .pem

Nach dem Import des Zertifikats fangen wir an, dieses in zwei Teile zu exportieren. Zuerst exportieren wir nur den Privaten Schlüssel (unverschlüsselt).



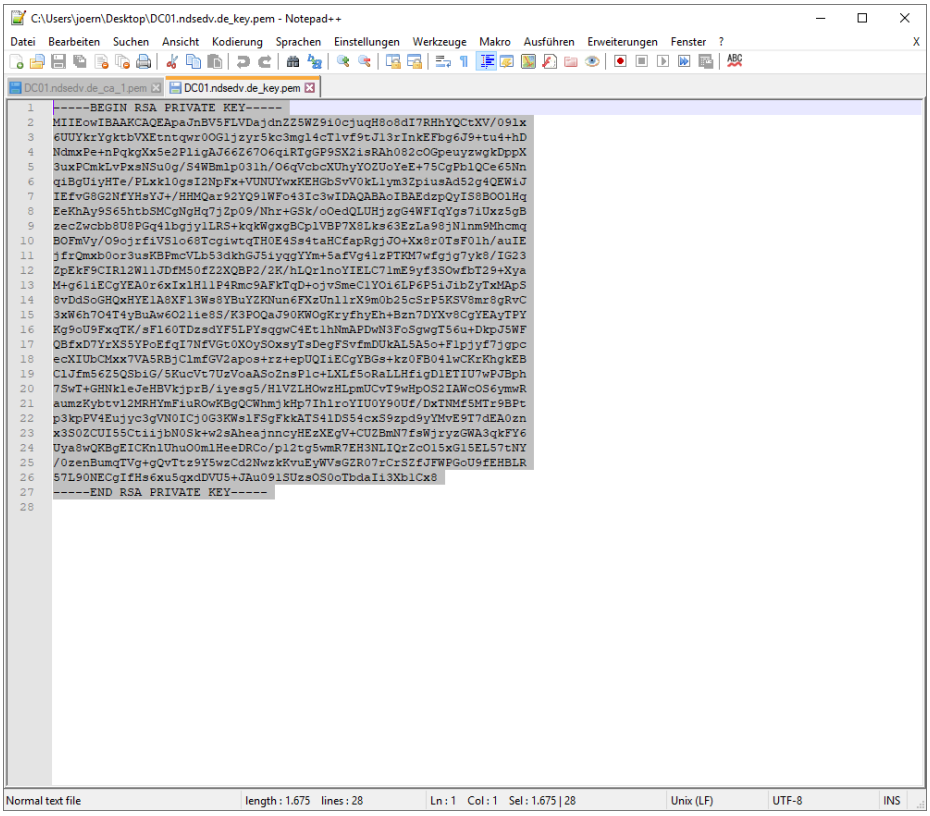
Danach exportieren wir die 3 öffentlichen Schlüssel der restlichen Zertifikatskette:



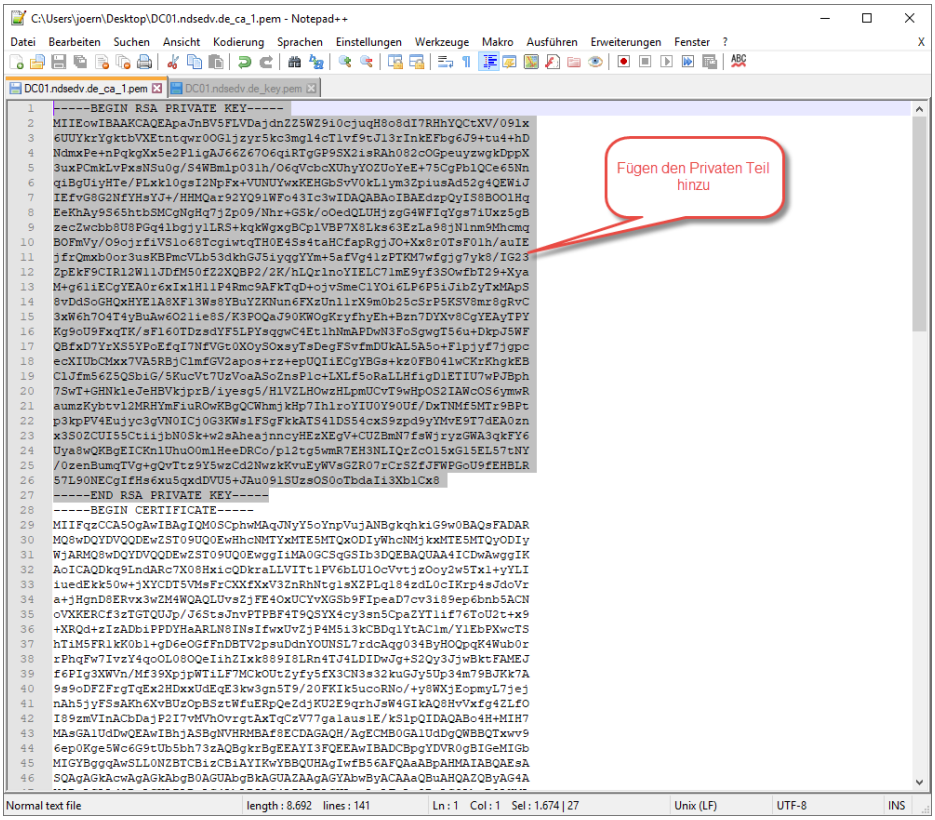
2 exportierte Teile sollten nun auf dem Desktop liegen.

Konvertieren eines .pfx Zertifikat in .pem

Öffnen beide Teile mit einem Texteditor und führen diesen zusammen. Dazu kopieren wir den exportierten privaten Teil des Schlüssels…



…und fügen diesen in die Datei mit den 3 öffentlichen Schlüsseln ganz oben ein. Speichern!

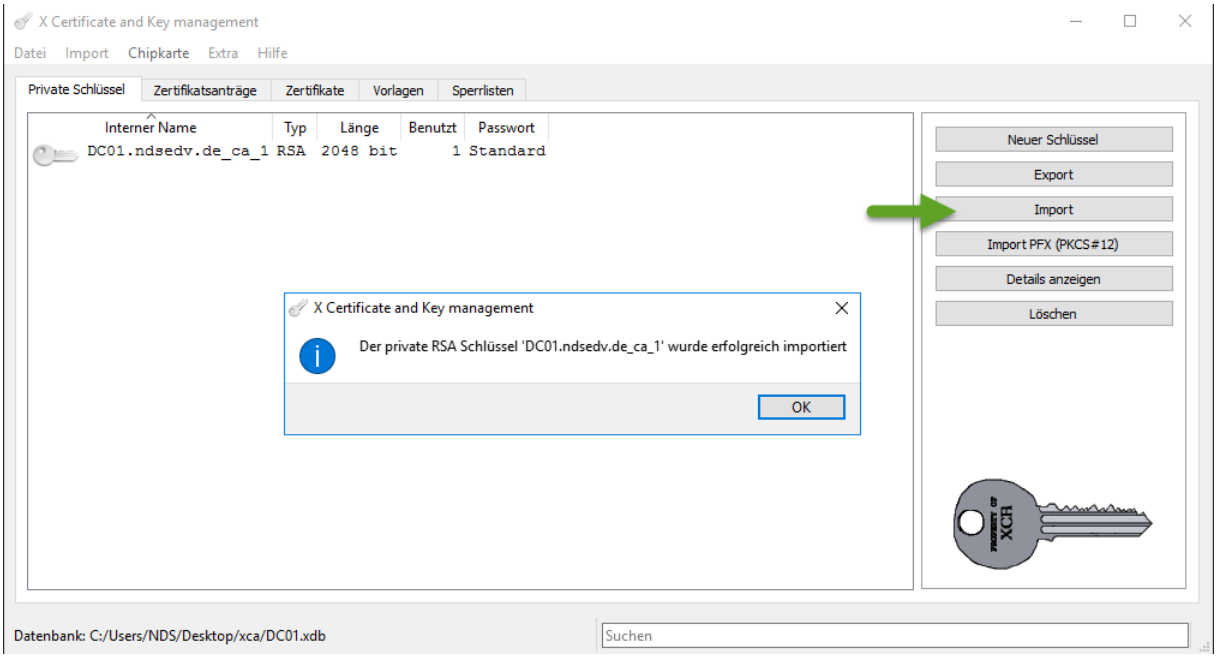


Konvertieren eines .pfx Zertifikat in .pem

Der Aufbau sieht dann wie folgt aus:

-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: TheIntermediateCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TheTrustedRoot.crt)
-----END CERTIFICATE-----

Zum Testen importieren wir nun die neue .PEM Datei. Es sollte kein Passwort abgefragt werden.



Es gibt Situationen in denen die .PEM Datei unverschlüsselt vorliegen muss.