



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:

The screenshot shows the Windows Certificate Management Console (MMC) interface. The left pane displays the 'Eigene Zertifikate' (My Certificates) folder. The right pane shows a certificate issued to 'DC01.ndsedv.de' by 'ISSUINGCA'. A dialog box titled 'Zertifikat' is open, displaying the following information:

- Zertifikatsinformationen:** Dieses Zertifikat ist für folgende Zwecke beabsichtigt:
 - Garantiert die Identität eines Remotecomputers
 - Garantiert dem Remotecomputer Ihre Identität
- Ausgestellt für:** DC01.ndsedv.de
- Ausgestellt von:** ISSUINGCA
- Gültig ab:** 20.02.2019 bis 20.02.2020
- Information: Sie besitzen einen privaten Schlüssel für dieses Zertifikat.

The 'OK' button is visible at the bottom of the dialog box.

Exportieren das Zertifikat...

The screenshot shows the Windows Certificate Management Console (MMC) interface. The left pane displays the 'Eigene Zertifikate' (My Certificates) folder. The right pane shows a certificate issued to 'DC01.ndsedv.de' by 'ISSUINGCA'. A dialog box titled 'Zertifikatexport-Assistent' is open, displaying the following information:

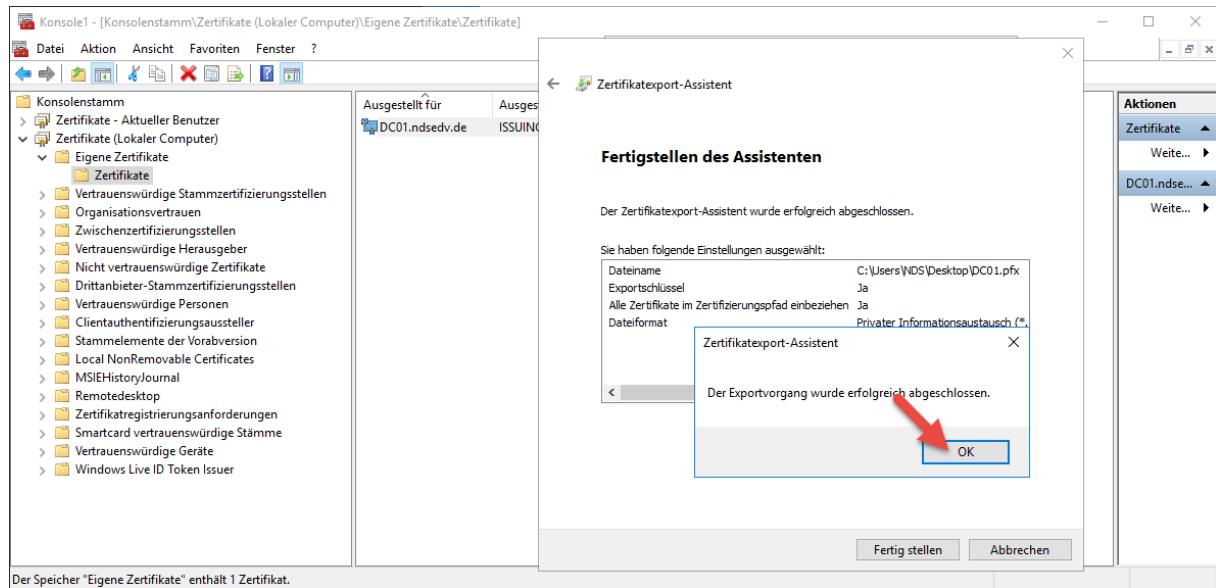
- Format der zu exportierenden Datei:** Zertifikate können in verschiedenen Dateiformaten exportiert werden.
- Wählen Sie das gewünschte Format:**
 - DER-codiert-binär X.509 (.CER)
 - Base-64-codiert X.509 (.CER)
 - Syntaxstandard kryptografischer Meldungen - PKCS #7-Zertifikate (.P7B)
 - Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
 - Privater Informationsaustausch - PKCS #12 (.PFX)
 - Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
 - Privaten Schlüssel nach erfolgreichem Export löschen
 - Alle erweiterten Eigenschaften exportieren
 - Zertifikatdatenschutz aktivieren
 - Microsoft Serieller Zertifikatspeicher (.SST)

The 'Weiter' (Next) button is highlighted with a red arrow.



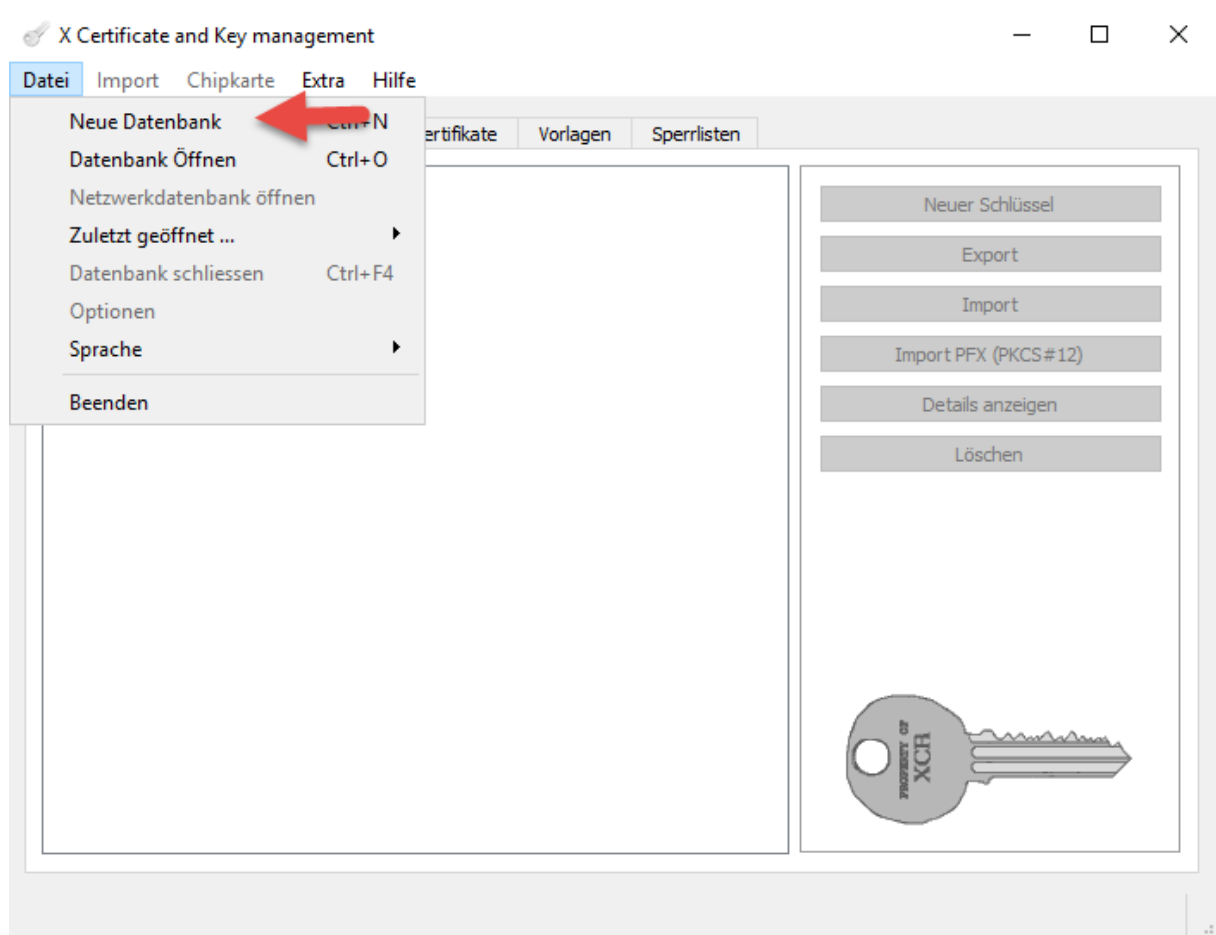
Konvertieren eines .pfx Zertifikat in .pem

...und vergeben ein Passwort:



Starten das Tool XCA und erstellen als erstes eine neue Datenbank:

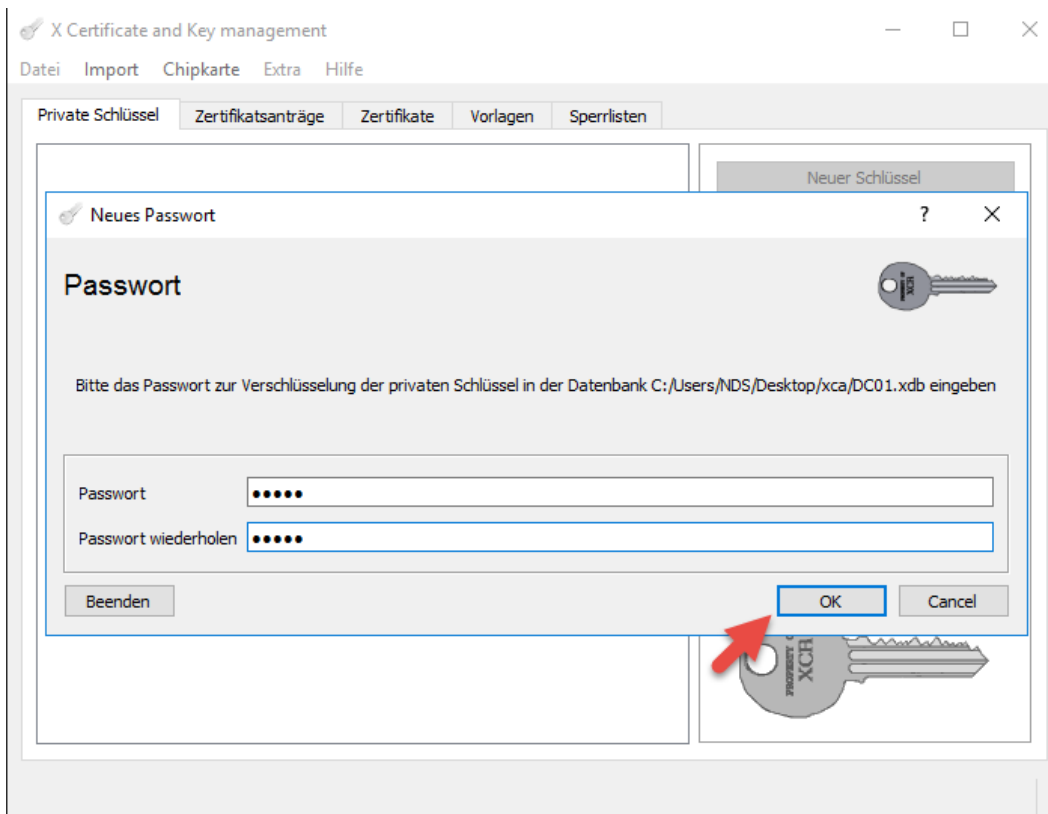
<https://hohnstaedt.de/xca/>



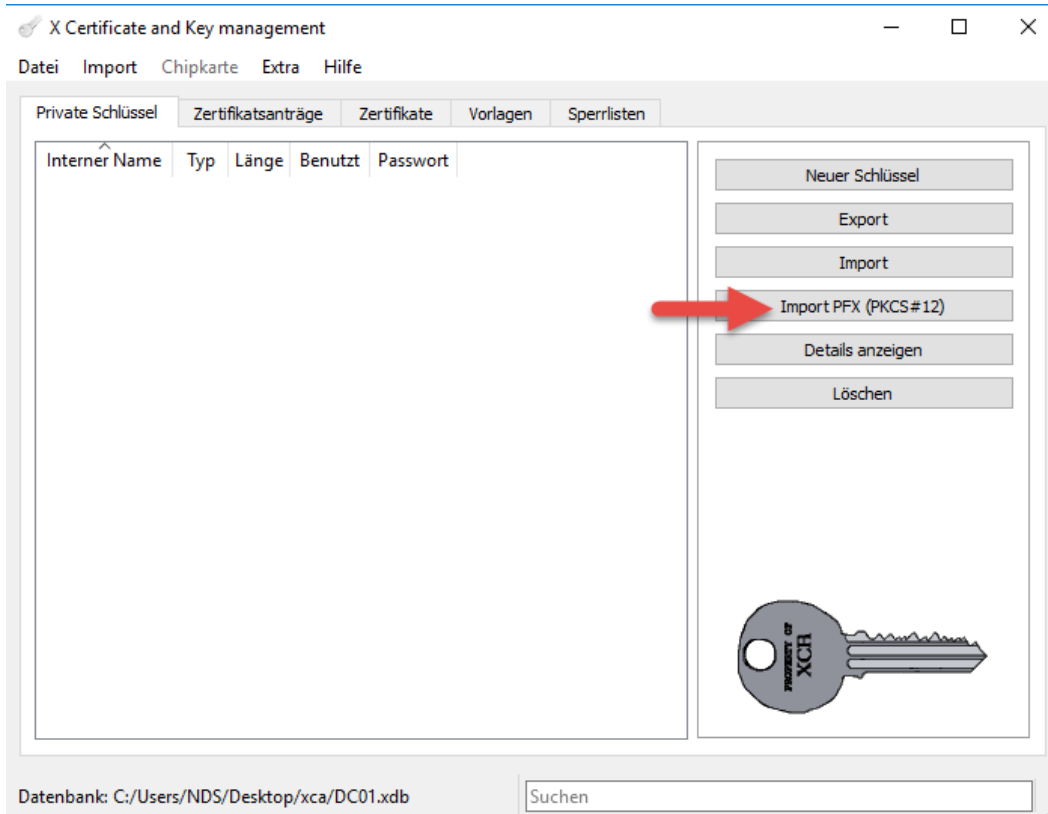


Konvertieren eines .pfx Zertifikat in .pem

Vergeben ein Passwort für die Datenbank:



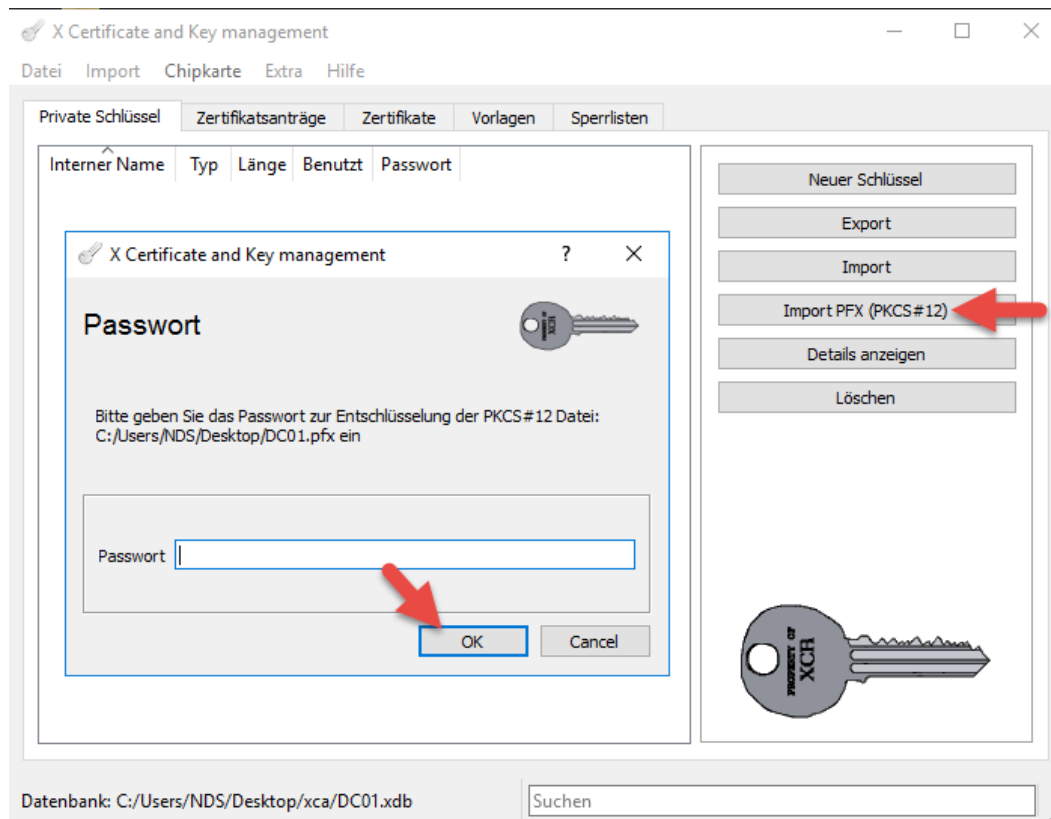
Importieren das gerade exportierte Private Zertifikat:



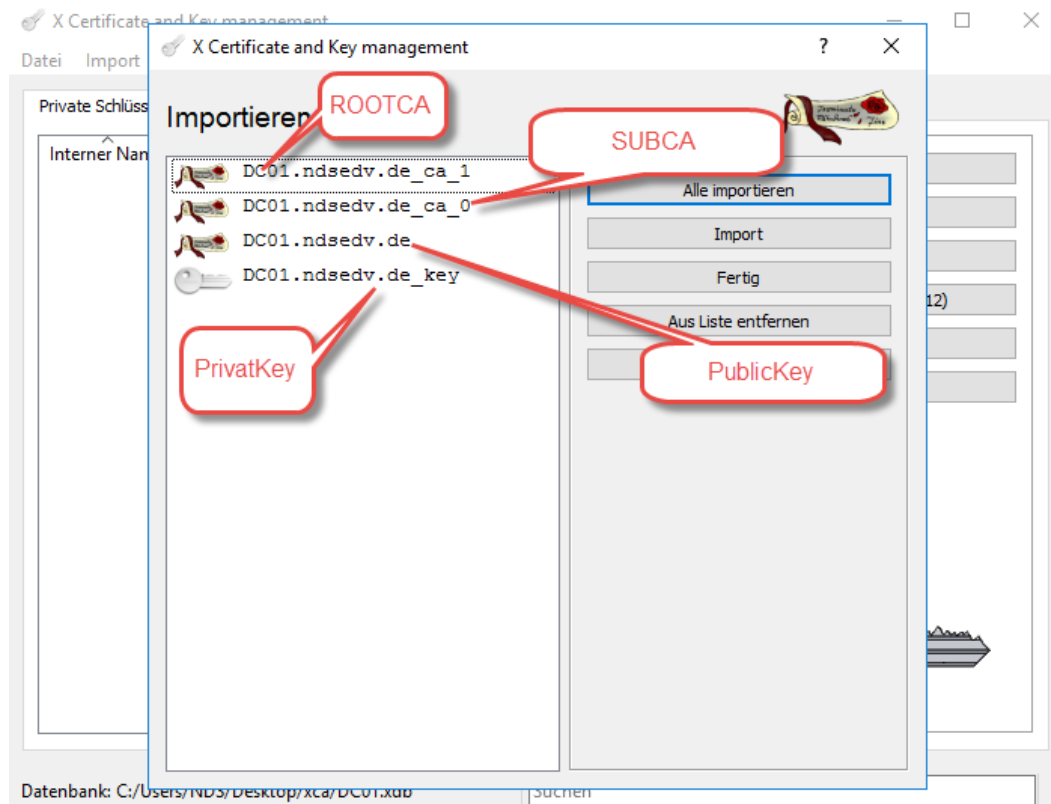


Konvertieren eines .pfx Zertifikat in .pem

Geben das Passwort ein welches wir beim Export vergeben haben:



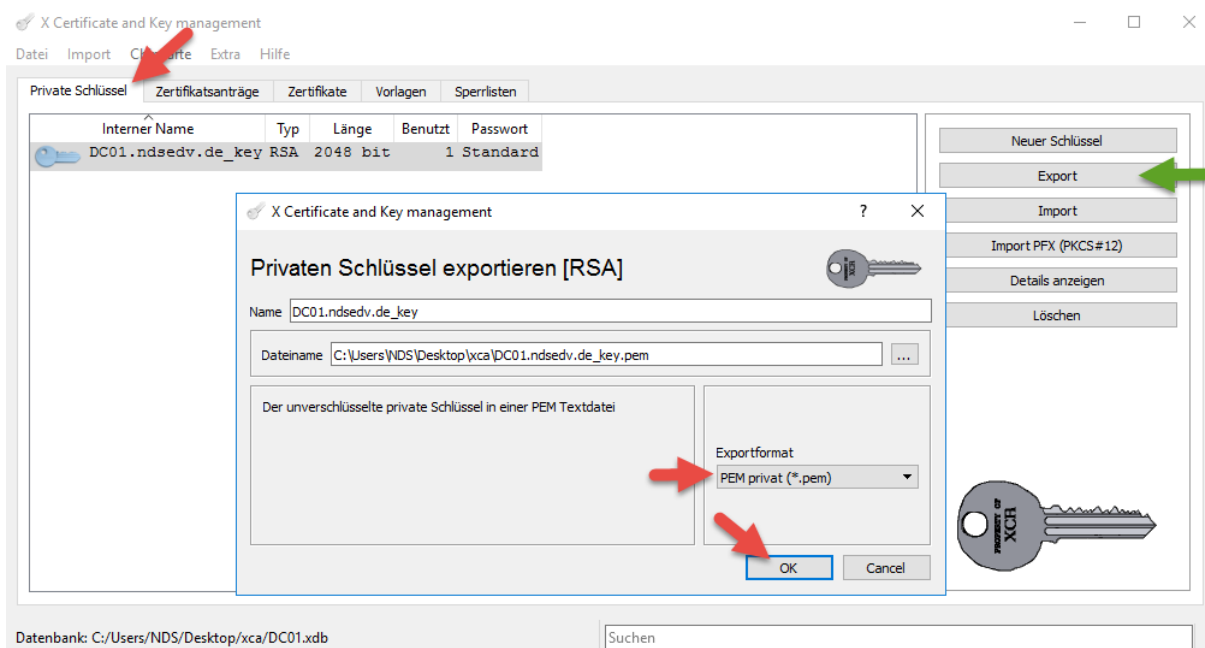
Erklärung zum Aufbau der Zertifikatskette. Die oberen 3 sind jeweils öffentliche Schlüssel.



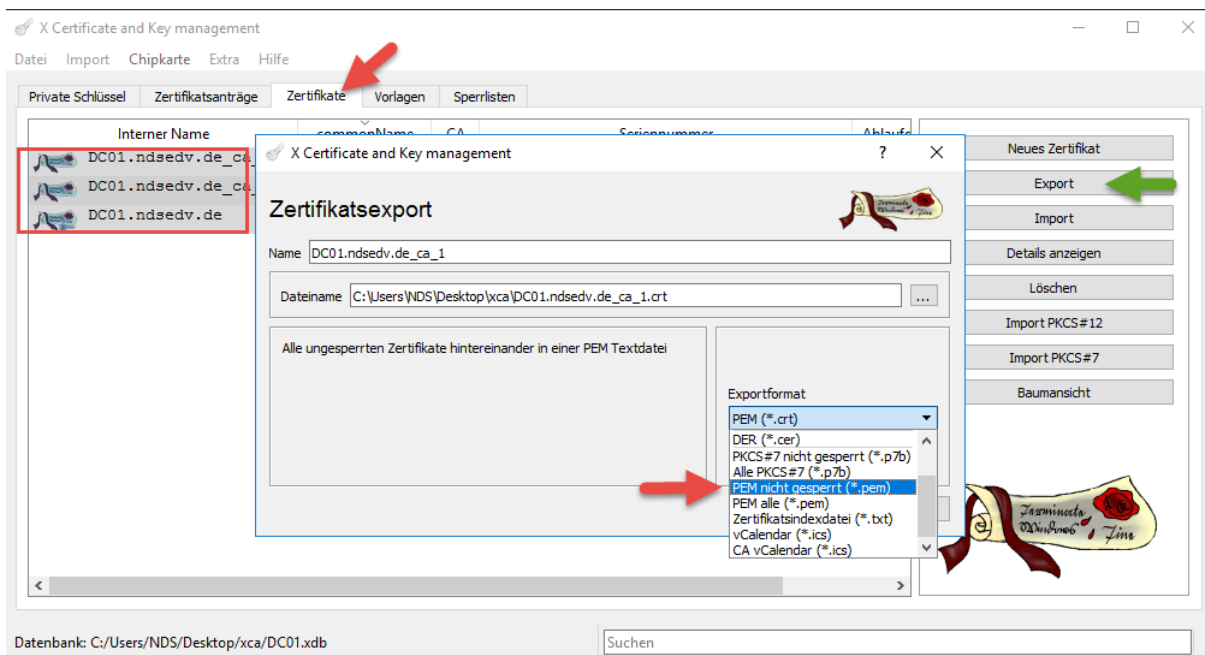


Konvertieren eines .pfx Zertifikat in .pem

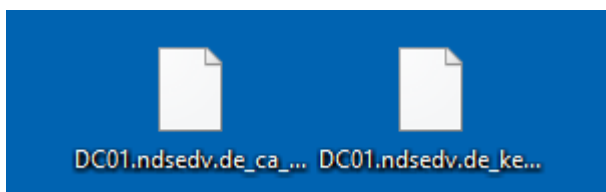
Nach dem Import des Zertifikats fangen wir an, dieses in zwei Teile zu exportieren. Zuerst exportieren wir nur den Privaten Schlüssel (unverschlüsselt).



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...

```
C:\Users\joern\Desktop\DC01.ndsdev.de_key.pem - Notepad++
Datei Bearbeiten Suchen Ansicht Kodierung Sprachen Einstellungen Werkzeuge Makro Ausführen Erweiterungen Fenster ?
DC01.ndsdev.de_ca_1.pem DC01.ndsdev.de_key.pem
1 -----BEGIN RSA PRIVATE KEY-----
2 MIIEowIBAAKCAQEApJnBV5FLVdajdnZ25WZ910cjuqH808dI7RHhYQctXV/091x
3 6UUYkrYgktbVXEentqwr00G1jzyz5kc3mg14cT1vF9tJ13rInkEFbg6J9+tu4+hD
4 NdmxPe+nPqkqXx5e2P1gAJ6626706q1RTgGP9SX21sRAh082c0GpeuyzgwKdppX
5 3uxFcmkLwFxsNSu0g/S4W8m1p031h/O6VqbcXUhyY0ZUoYeE+75CgPb1QCe65Nn
6 q1BgU1yHte/Flxk10gsI2NpFx+vUNUyWxKEHGs5vY0L1ym3ZpiusAd52g4QEWLJ
7 IEfvG82NfHsYJ+/HHMQar92YQ91WFo43Ic3wIDAQABAoIBAEzdpQyIS8BO01Hq
8 EeRkAy9S68tbtSMCgNgHq7j2p09/Nhr+GSK/cOedQLUHjzG4WFIqYgs71Uxz5gB
9 zec2wcbbs8USPqg41bgj1LRS+rkqWxgq8Cp1VB7X8Lks63EzLa98jN1nm9Mhcmq
10 BOFmVY/O9o3r4V51o68Tog1wtqTH0E4S4taHCfapRgJJO+Xx8r0TsF01h/auIE
11 jfrQmxb0or3usRBPmcVLb53dkhG51yqgYm+5afVg41zPFRM7wFggj7yk8/IG23
12 ZpEkf9CIR12W11JDFH50f22XQB2/2K/hLQr1noYIELC71mE9yf3S0wFbT29+Xya
13 M+g61iECgYEA0r6xIx1H11P4Rmc9AFkTqD+o3vSmeCIY016LP6P5iJibZyTAMApS
14 8vDdSoGHQxHYE1A8XF13w8YBuYZKXn6FXzUn11xX9m0b25c5rPKSV8mr8gRvC
15 3xW6h704T4yBuAw60211e8S/K3POQA90KNOgKryfhyEh+Bzn7DYXv8CgYEAJTPY
16 Kgo9U9FqkT/sf160TdzsdYFSLPYsgqC4Et1hNmAPDwN3FoSgwjT56u+DkpJ5WF
17 QBfxD7YrXSSyPoEfqI7NFVgcoX0yS0xSyTeDegFsvfmdUKAL5A5o+Flpjjy7jgpc
18 ecXIUbCmxx7VASRBjClmfGV2apos+rz+epUQ1iECgYBGs+kz0FB041wCKrKngKEB
19 ClJfm56Z5Q5b1g/5KucVt7UzVoaAs0ZneP1c+LXLf5oRaLLHf1gD1ETIU7wPjBph
20 7SwT+GHnk1eJeHBVKjprB/iyeg5/H1VZLH0wzHlpmUcV79wH0S2IAMo0S6ymwR
21 aumzKybtv12MRHYmFluR0wK8gQCWhmj kH7Ih1coYIU0Y90Uf/DxTnMf5MT+9BPE
22 p3kpPV4Eujyc3gVNOICj0G3Kw1fSgFkKATS41DS4cxS9zpd9yYmV9T7dEA0zn
23 x3S0ZCUI55Ct1jbnOSk+w2aAheajnnycyHEzXegV+CUZBmN7fswjryzGWA3qkFY6
24 Dya8wQKbgE1CKn1Uhu00m1HeeDRCo/pl2tg5wmR7EH3NLQr2c015x61SEL57iNY
25 /OzenBumqTvg+QvTz9Y5wCd2NwzKvUeVW9VW9ZRO7rCrSZJFWPGoU9fEHLR
26 57L90NECgIfHs6xkSqdDVU5+JAU091SUz5oS0oTbda1I3Xb1Cx8
27 -----END RSA PRIVATE KEY-----
28
```

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

```
C:\Users\joern\Desktop\DC01.ndsdev.de_ca_1.pem - Notepad++
Datei Bearbeiten Suchen Ansicht Kodierung Sprachen Einstellungen Werkzeuge Makro Ausführen Erweiterungen Fenster ?
DC01.ndsdev.de_ca_1.pem DC01.ndsdev.de_key.pem
1 -----BEGIN RSA PRIVATE KEY-----
2 MIIEowIBAAKCAQEApJnBV5FLVdajdnZ25WZ910cjuqH808dI7RHhYQctXV/091x
3 6UUYkrYgktbVXEentqwr00G1jzyz5kc3mg14cT1vF9tJ13rInkEFbg6J9+tu4+hD
4 NdmxPe+nPqkqXx5e2P1gAJ6626706q1RTgGP9SX21sRAh082c0GpeuyzgwKdppX
5 3uxFcmkLwFxsNSu0g/S4W8m1p031h/O6VqbcXUhyY0ZUoYeE+75CgPb1QCe65Nn
6 q1BgU1yHte/Flxk10gsI2NpFx+vUNUyWxKEHGs5vY0L1ym3ZpiusAd52g4QEWLJ
7 IEfvG82NfHsYJ+/HHMQar92YQ91WFo43Ic3wIDAQABAoIBAEzdpQyIS8BO01Hq
8 EeRkAy9S68tbtSMCgNgHq7j2p09/Nhr+GSK/cOedQLUHjzG4WFIqYgs71Uxz5gB
9 zec2wcbbs8USPqg41bgj1LRS+rkqWxgq8Cp1VB7X8Lks63EzLa98jN1nm9Mhcmq
10 BOFmVY/O9o3r4V51o68Tog1wtqTH0E4S4taHCfapRgJJO+Xx8r0TsF01h/auIE
11 jfrQmxb0or3usRBPmcVLb53dkhG51yqgYm+5afVg41zPFRM7wFggj7yk8/IG23
12 ZpEkf9CIR12W11JDFH50f22XQB2/2K/hLQr1noYIELC71mE9yf3S0wFbT29+Xya
13 M+g61iECgYEA0r6xIx1H11P4Rmc9AFkTqD+o3vSmeCIY016LP6P5iJibZyTAMApS
14 8vDdSoGHQxHYE1A8XF13w8YBuYZKXn6FXzUn11xX9m0b25c5rPKSV8mr8gRvC
15 3xW6h704T4yBuAw60211e8S/K3POQA90KNOgKryfhyEh+Bzn7DYXv8CgYEAJTPY
16 Kgo9U9FqkT/sf160TdzsdYFSLPYsgqC4Et1hNmAPDwN3FoSgwjT56u+DkpJ5WF
17 QBfxD7YrXSSyPoEfqI7NFVgcoX0yS0xSyTeDegFsvfmdUKAL5A5o+Flpjjy7jgpc
18 ecXIUbCmxx7VASRBjClmfGV2apos+rz+epUQ1iECgYBGs+kz0FB041wCKrKngKEB
19 ClJfm56Z5Q5b1g/5KucVt7UzVoaAs0ZneP1c+LXLf5oRaLLHf1gD1ETIU7wPjBph
20 7SwT+GHnk1eJeHBVKjprB/iyeg5/H1VZLH0wzHlpmUcV79wH0S2IAMo0S6ymwR
21 aumzKybtv12MRHYmFluR0wK8gQCWhmj kH7Ih1coYIU0Y90Uf/DxTnMf5MT+9BPE
22 p3kpPV4Eujyc3gVNOICj0G3Kw1fSgFkKATS41DS4cxS9zpd9yYmV9T7dEA0zn
23 x3S0ZCUI55Ct1jbnOSk+w2aAheajnnycyHEzXegV+CUZBmN7fswjryzGWA3qkFY6
24 Dya8wQKbgE1CKn1Uhu00m1HeeDRCo/pl2tg5wmR7EH3NLQr2c015x61SEL57iNY
25 /OzenBumqTvg+QvTz9Y5wCd2NwzKvUeVW9VW9ZRO7rCrSZJFWPGoU9fEHLR
26 57L90NECgIfHs6xkSqdDVU5+JAU091SUz5oS0oTbda1I3Xb1Cx8
27 -----END RSA PRIVATE KEY-----
28 -----BEGIN CERTIFICATE-----
29 MIIFqzCCA5OgAwIBAgIQOM5CPhwMAQJnyY5oYnpVujANBgkqhkiG9w0BAQsFADAR
30 MQ8wDQYDVQDEwZSt09UQ0EwHhcNMjYxMTEyMTE0MjYwODIyMjYwODIyMjYwODIy
31 WjARMQ8wDQYDVQDEwZSt09UQ0EwEgwgI1MAQCSqGSIb3DQEBAQUAA4IDCwAwggEIK
32 AoICAQDkq9LndArC7X08Hx1cQDKraLLVITt1PV6bLUL0cVvtjz0oy2w5Txl1+yYLI
33 lueEkkS0w+NYCDT5VHsFrCXKXx3ZnRnTcg1xKZFlq184zL0cIKzP490dV9
34 e+Jhm8ERvw3w24HQQLDvzsjFE40xUCIv9S3b5F1CpeAD7c9318Pep6mb5ACW
35 oVXKERCf3zTGTUjP/36StoNvPFBF4T9Q5YXcy38n5CPaZ2Y11f76T0U2+tw9
36 +XRQd+ZiAdb1PPDYHaARLNSInIefwUvZ;P4M5i3kCBQd1YrAClM/YIEbFXwCTS
37 h1iM5FR1kK0b1+gDeOgfFnDBT2vpsuDDnYOUNSL7rdcAqg034ByHOppqK4Wub0r
38 rPhqFw7IvzY4qo0L080eIih2Ikk89I8Lrn4Tj4L1DIdwJv+S2Qy3JyWkbtFAMEJ
39 fEPIg3XWVn/Mf39XpjpWt1LF7MCKoU2yfy5EX3CN3s32kuGjy5Up34m79BjKk7A
40 9e9oDF2FrgTqE2HdxUdeEq3kw3gn5T9/20FKIKSuccRo+/y9WjXjEompyL7jeJ
41 nAh5jyF5sArKh6XvBuzOpBSzWfueRqQcZd;KU2E9qrhJ5w4GIkA08HvVxfg42L0
42 I89zmVInACbDajP2I7vMvHovrgtAxTqCzV77ga1aus1E/ks1pQIDAQABo4+M1H7
43 MAeGalUdDQEAwIbhjASBgnVHRMBAf8ECDAGAQH/AgECCoGAlUdDgQWBQTXwv9
44 6ep0Kge5w669tUb5bh73zAQBgkrBgeEYAI3FQEEAwIBADCPgYDVR0gBIGeMIgB
45 MIGYBgqAwSLLONZBTCB1zCBIAIYKwYBBOUHAgiTfE5B6FQAAABPAAHMAIABQAEsA
46 SQAgAKAcwAgAGKABgBQAUAUabqBKAUAZAAGAGYABwByACAAQBAQAAQZQBYAg4A
```

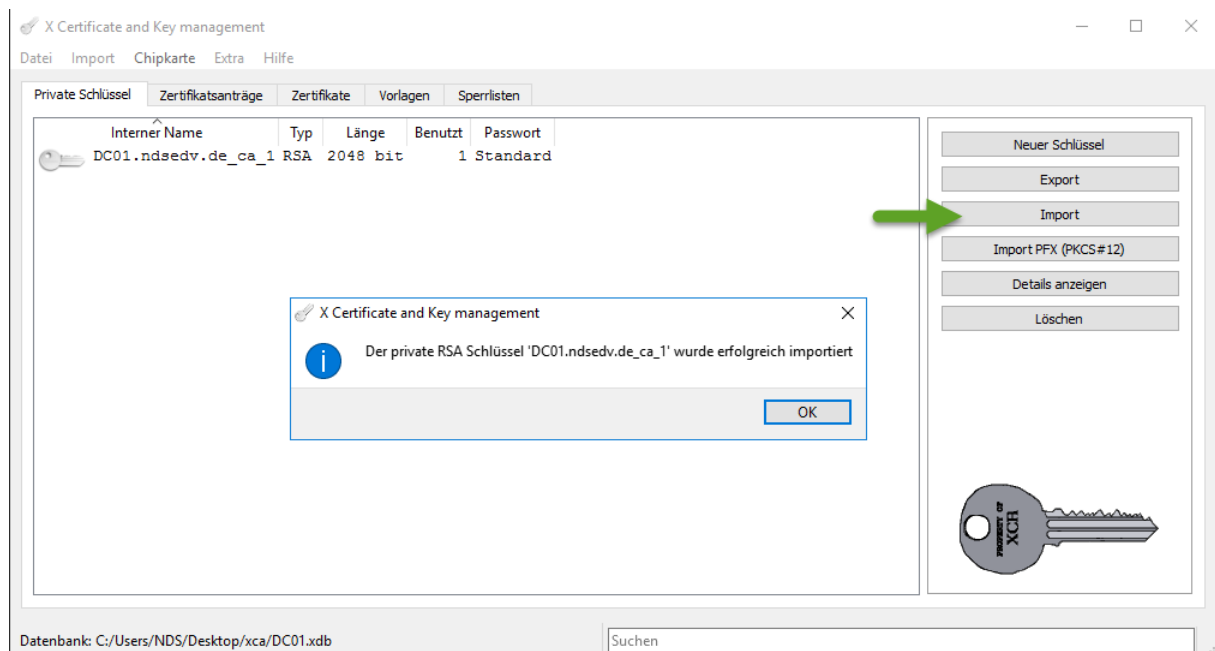


Konvertieren eines .pfx Zertifikat in .pem

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.