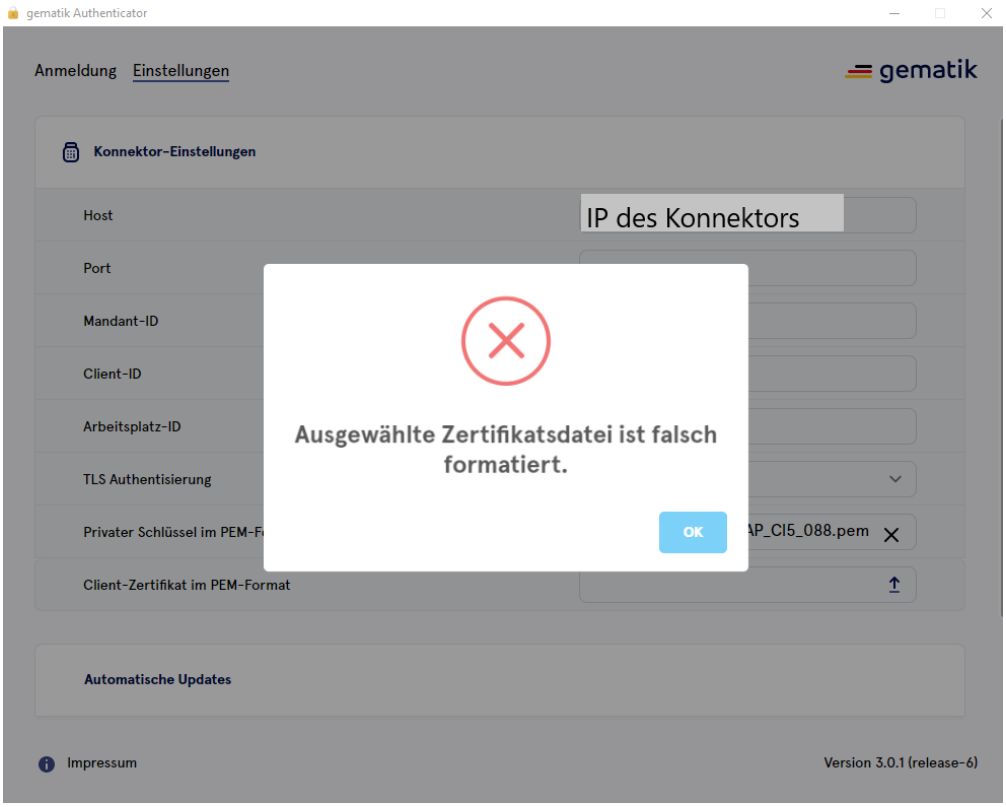
Umwandlung einer p12-Datei in PEM-Format

Grundsätzlich empfehlen wir bei einer zertifikatsbasierten Authentifizierung eine P12-Datei zu verwenden!

Wird in den Einstellungen des Authenticators die TLS-Authentisierung **Zertifikat PEM-Format** gewählt, muss der Private-Key sowie der Client-Key im PEM-Format vorliegen, da es ansonsten zu einer Fehlermeldung führt:

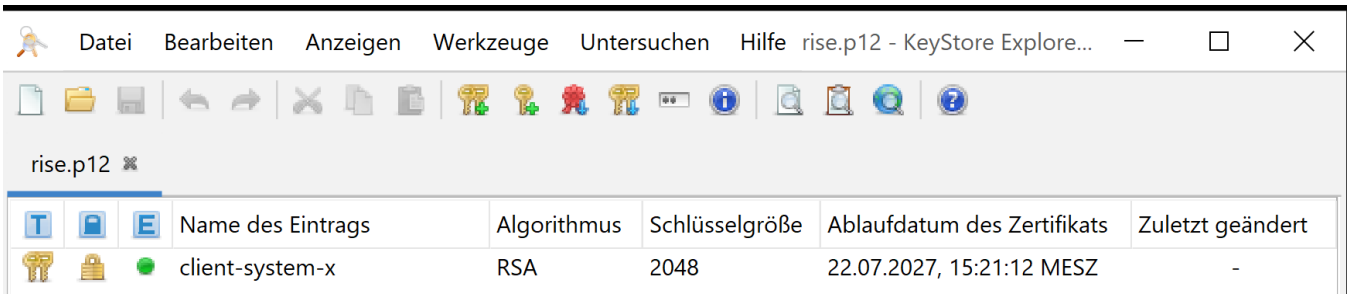


Step-by-Step: Umwandlung der p12-Datei

Die p12-Datei ist durch ein Passwort geschützt und enthält zwei Schlüsselpaare (Private-Key und Client-Key). Die p12-Datei kann mit dem Programm Key Store Explorer geöffnet werden, sodass der Private-Key und der Client-Key im PEM-Format aus dem RSA-Schlüsselpaar exportiert werden können. Sollten Sie beispielsweise auch ein EC-Schlüsselpaar erhalten haben, wird dieses hierfür nicht benötigt.

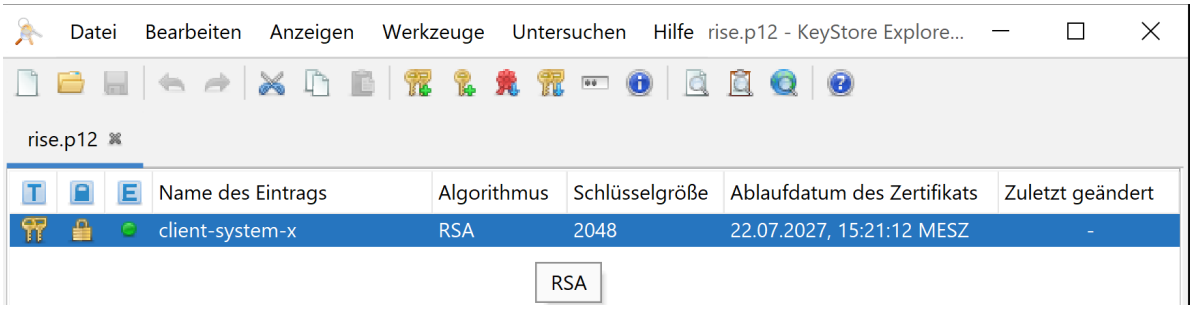
1 Öffnen der p12-Datei im KeyStore Explorer

- Öffnen Sie den KeyStore Explorer (dieser kann hier heruntergeladen werden: KeyStore Explorer)
- Die p12-Datei kann nun einfach per Drag and Drop in den KeyStore Explorer hineingezogen werden, sodass Sie nach einem Passwort gefragt werden
- Geben Sie das benötigte Passwort ein
- Es sollte nun ungefähr so bei Ihnen aussehen:

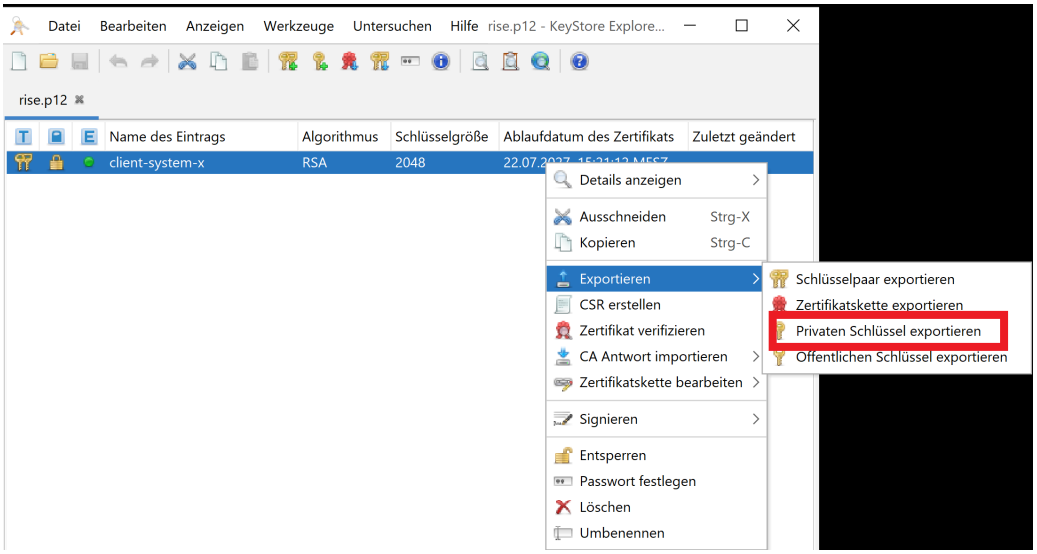


2 Exportieren des Private Keys

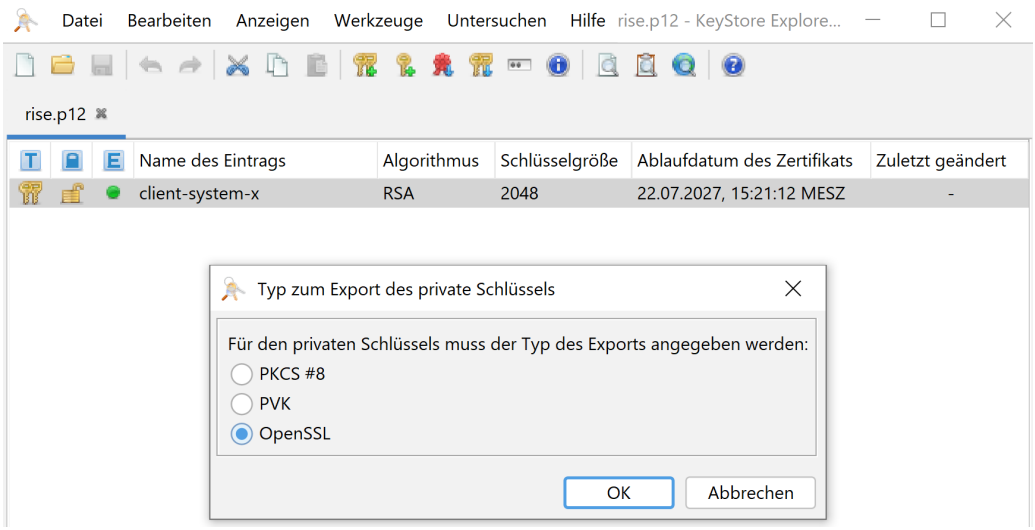
- Wählen Sie das RSA-Schlüsselpaar:



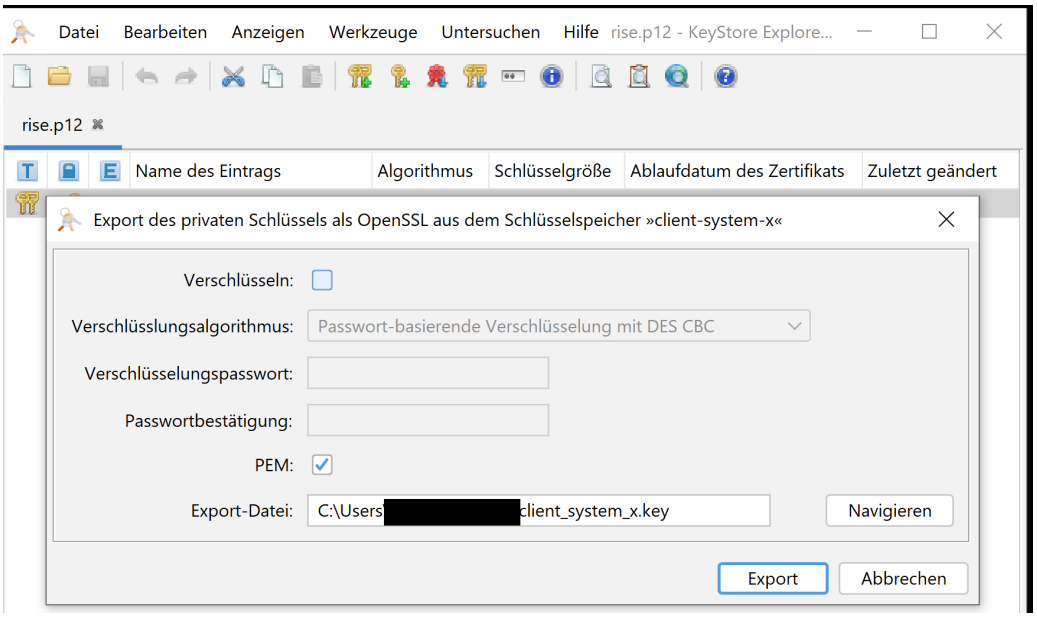
- Nutzen Sie den Rechtsklick, um das Menü aufzurufen
- Klicken Sie auf den Menüpunkt **Exportieren** und anschließend auf **Privaten Schlüssel exportieren**:



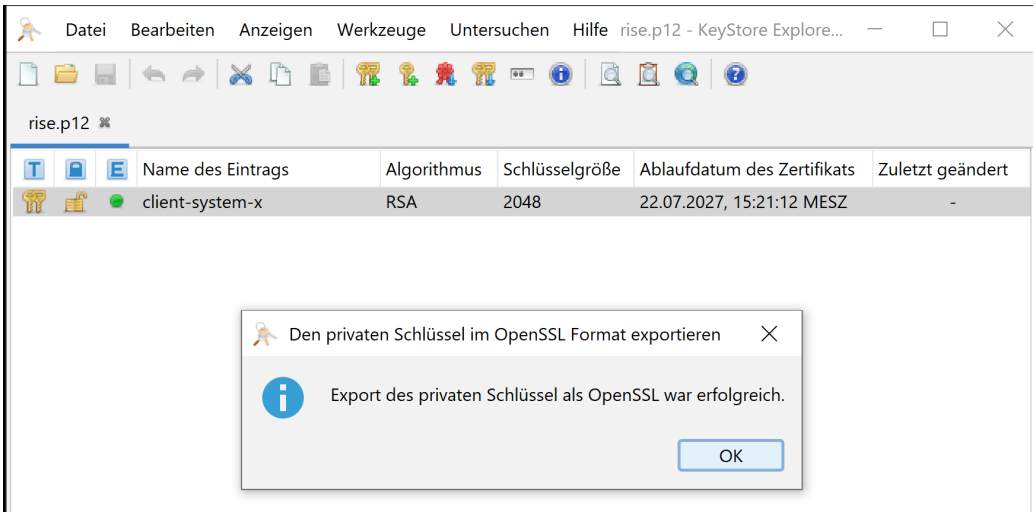
- ***Hinweis:*** *Es kann sein, dass eine erneute Passwort-Abfrage erscheint - Geben Sie das gleiche Passwort, wie zuvor ein*
- Es öffnet sich ein Dialogfenster, klicken Sie auf **OpenSSL** und anschließend auf **OK**



- Ein neues Dialogfenster öffnet sich, übernehmen Sie die Einstellungen wie nachfolgend dargestellt
- Klicken Sie anschließend auf **Export**

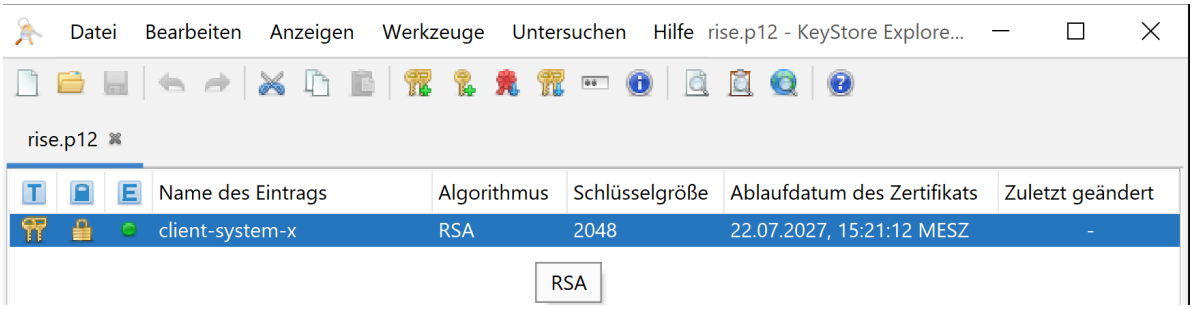


- Es erscheint ein neues Dialogfenster, welches den erfolgreichen Export bestätigt
- Klicken Sie auf **OK**

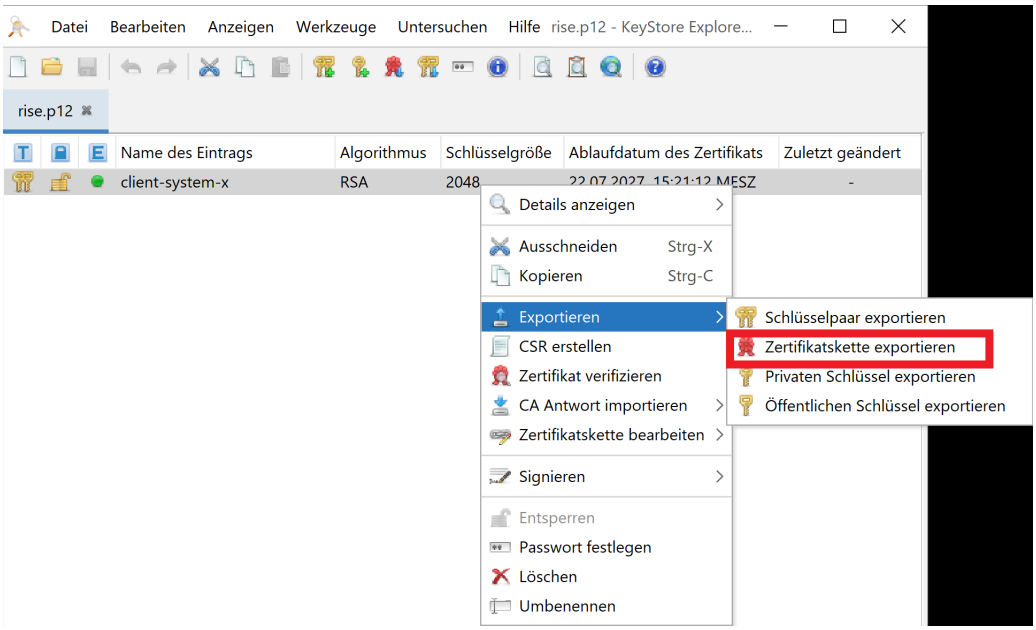


3 Exportieren des Client Zertifikats

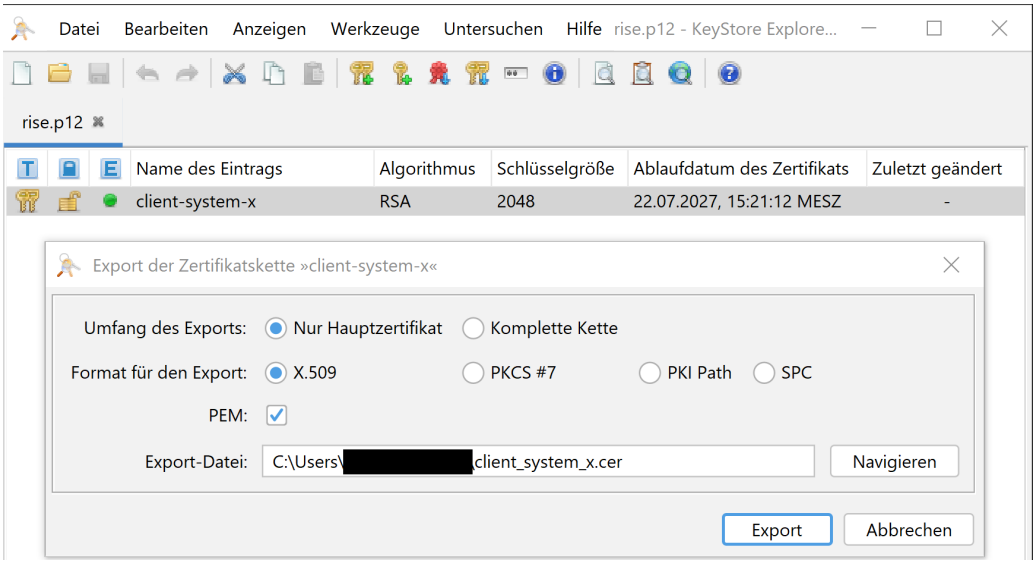
- Wählen Sie das RSA-Schlüsselpaar:



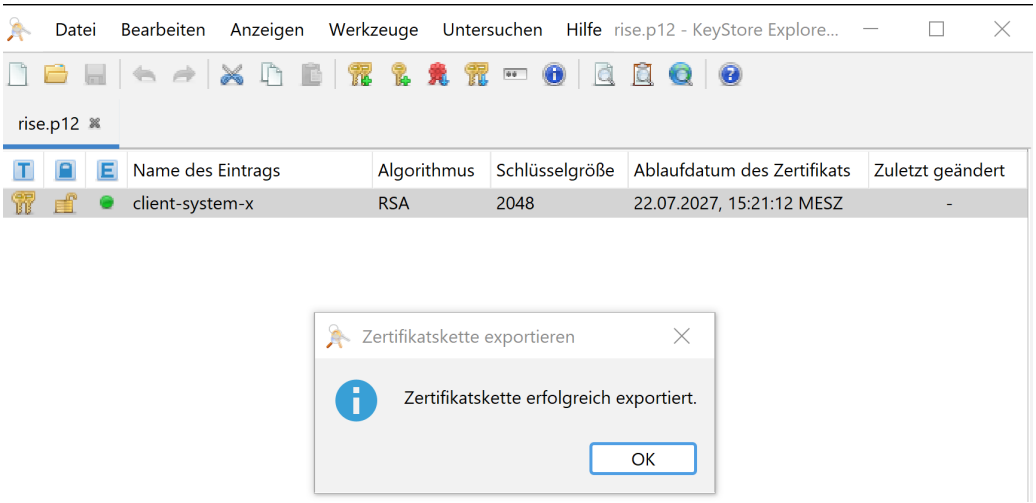
- Nutzen Sie den Rechtsklick, um das Menü aufzurufen
- Klicken Sie auf den Menüpunkt **Exportieren** und anschließend auf **Zertifikatskette exportieren**:



- Es erscheint ein Dialogfenster, übernehmen Sie die Eingaben wie folgt und klicken Sie anschließend auf **Export**



- Es erscheint ein neues Dialogfenster, welches den erfolgreichen Export bestätigt
- Klicken Sie auf **OK**

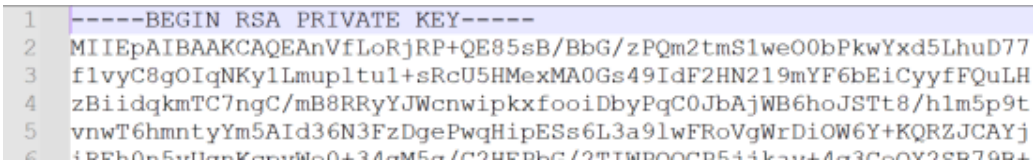


4 Überprüfung der exportierten Zertifikate im PEM-Format

- Die exportierten Dateien finden Sie in dem im vorherigen Dialogfenster unter **Export-Datei** von Ihnen hinterlegtem Ablagepfad
- Navigieren Sie dorthin und öffnen Sie die beiden PEM-Dateien jeweils in einem Texteditor
- Die Datei sollte für das **Client-Zertifikat** folgendes Format aufweisen:

```
1 -----BEGIN CERTIFICATE-----
2 MIIDHjCCAgagAwIBAgIGAYImEboAMA0GCSqGSIb3DQEBCwUAMCIxIDAeBgNVBAM
3 F2tvbm5la3Rvci1jbGllbnQua29ubGFuMB4XDTIyMDcyMjEzMjExMloXDTI3MDc
4 MjEzMjExMlowIjEgMB4GA1UEAwwXa29ubmVrdG9yLWNsaWVudC5rb25sYW4wggE
5 MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCdV8uhGNE/5ATzmwH8Fsb/M9C
6 a2ZLXB47Rs+TBjF3kuG4Pvt/W/ILyA4io0rLUua6mW27X6xFxTkcx7EwDQazj0h
```

- Für den **Private Key** sollte die Datei folgendes Format haben:



```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAnVfLoRjRP+QE85sB/BbG/zPQm2tmS1weO0bPkwYxd5LhuD77
flvyC8gOIqNKylLmupltu1+sRcU5HMexMA0Gs49IdF2HN219mYF6bEiCyyfFQuLH
zBiidqkmTC7ngC/mB8RRyYJWcnwipkxfooiDbyPqC0JbAjWB6hoJSTt8/hlm5p9t
vnwT6hmntyYm5AId36N3FzDgePwqHipESs6L3a9lwFRoVgWrDiOW6Y+KQRZJCAYj
```

Der Private-Key und das Client-Zertifikat sind nun im PEM-Format und können unter Einstellungen im Authenticator geladen werden.