Zertifikatserstellung für Webservice-Kommunikation

Alle Teilnehmer am AAV müssen jeweils ein Client- und ggf. Serverzertifikat bei der BNetzA beantragen. Dies soll ab sofort mittels Signaturrequests in Form von sog. **CSR-Dateien** geschehen. Diese werden bei der BNetzA signiert und zurück zum Antragsteller geschickt. Berechtigte Behörden brauchen **nur ein** Clientzertifikat zu beantragen, verpflichtete Unternehmen **zusätzlich** ein Serverzertifikat.

Die Vorgaben der BNetzA für die CSR-Dateien lauten wie folgt: Es soll eine Base64-codierte CMD- oder besser PKCS#10-Datei verwendet werden. Folgende Eingaben sind mindestens erforderlich:

„Organization“ (O) = Offizieller Firmen- oder Behördenname

„Land/Country“ (C) = immer DE

„Common Name“ (CN) = IPv4-Adresse des lokalen Webservice-Servers/-Clients

“Public Key” = RSA 2048 bits

“Signature Algorithm” = SHA256, RSA

Die Erzeugung eines Client-/Server-Zertifikatssignaturrequest zur Teilnahme am Webservice-basierten AAV wird hier exemplarisch mittels des **Open Source Tools „KeyStore Explorer“** (hier V5.4) beschrieben; andere Methoden sind natürlich möglich. Dieses Programm ist für die meisten Betriebssysteme kostenfrei erhältlich.

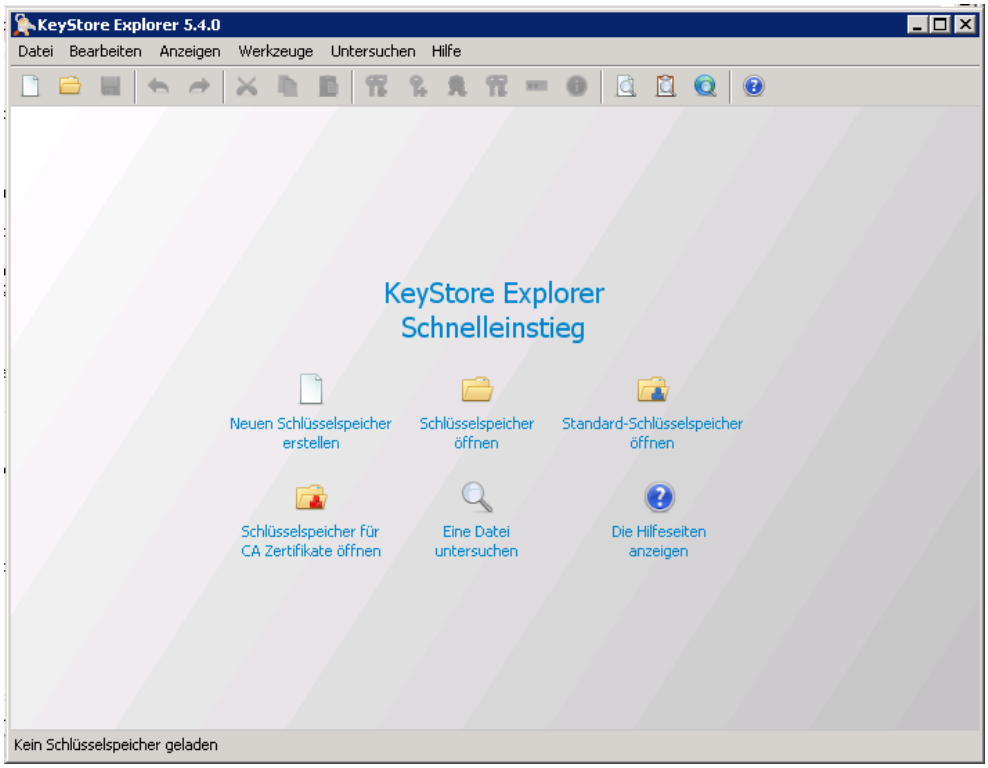
Grundsätzlicher Ablauf:

1. Erstellen eines Schlüsselspeichers u. Schlüsselpaares (geheimer + öff. Schlüssel)
2. Einsenden von CSR (Certificate Signing Request) an die BNetzA
3. Verknüpfen des signierten Request mit dem Schlüsselpaar.

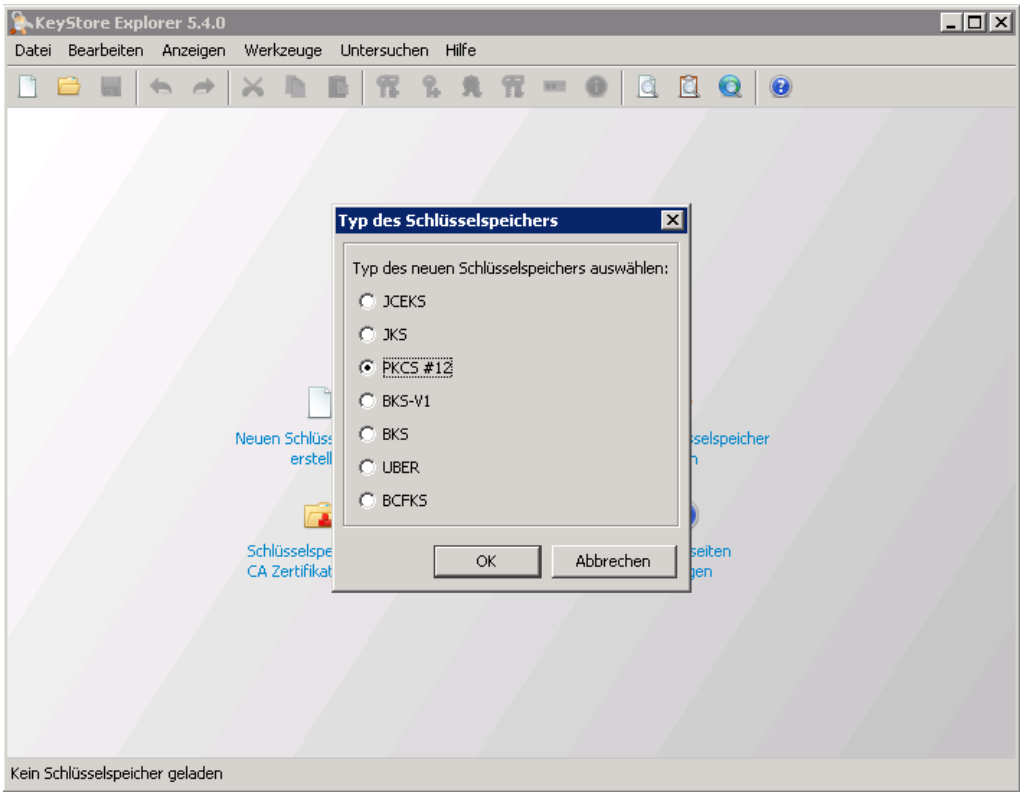
Diese Anleitung erhebt keinen Anspruch auf Vollständigkeit und kann jederzeit geändert werden.

Die Gültigkeitsdauer des erzeugten Zertifikates ist vom Teilnehmer selbst zu überwachen (siehe auch die TR-AAV in der jeweils gültigen Fassung).

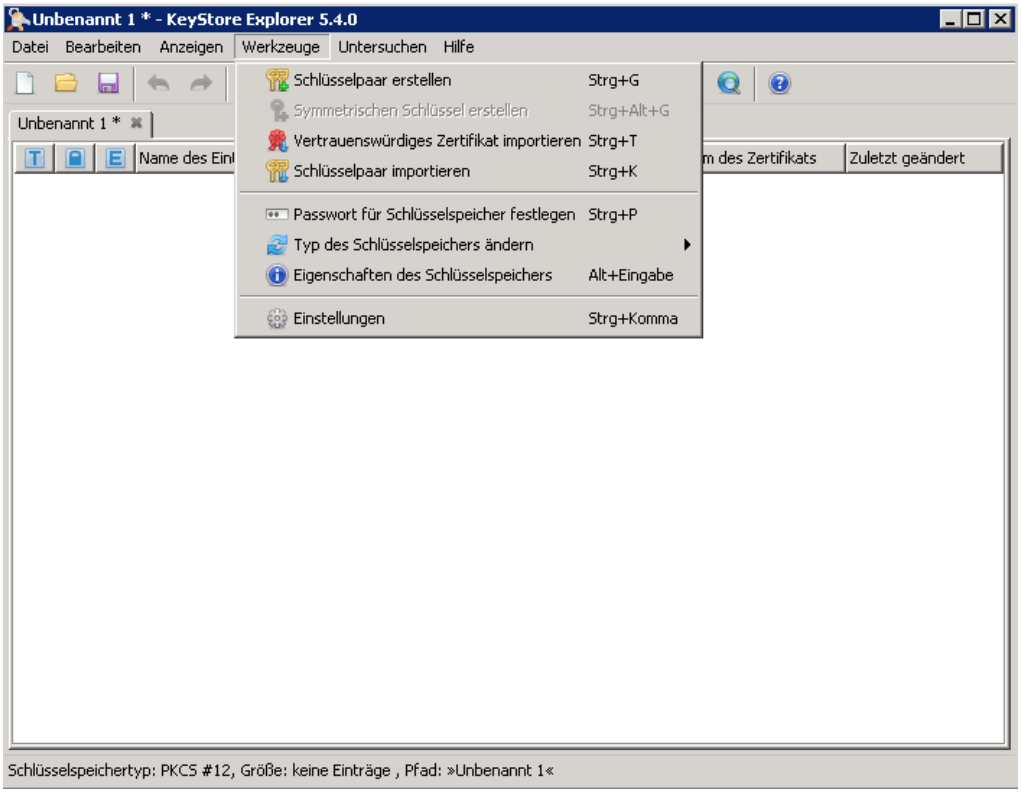
1. Im KeyStore Explorer einen neuen Schlüsselspeicher anlegen:



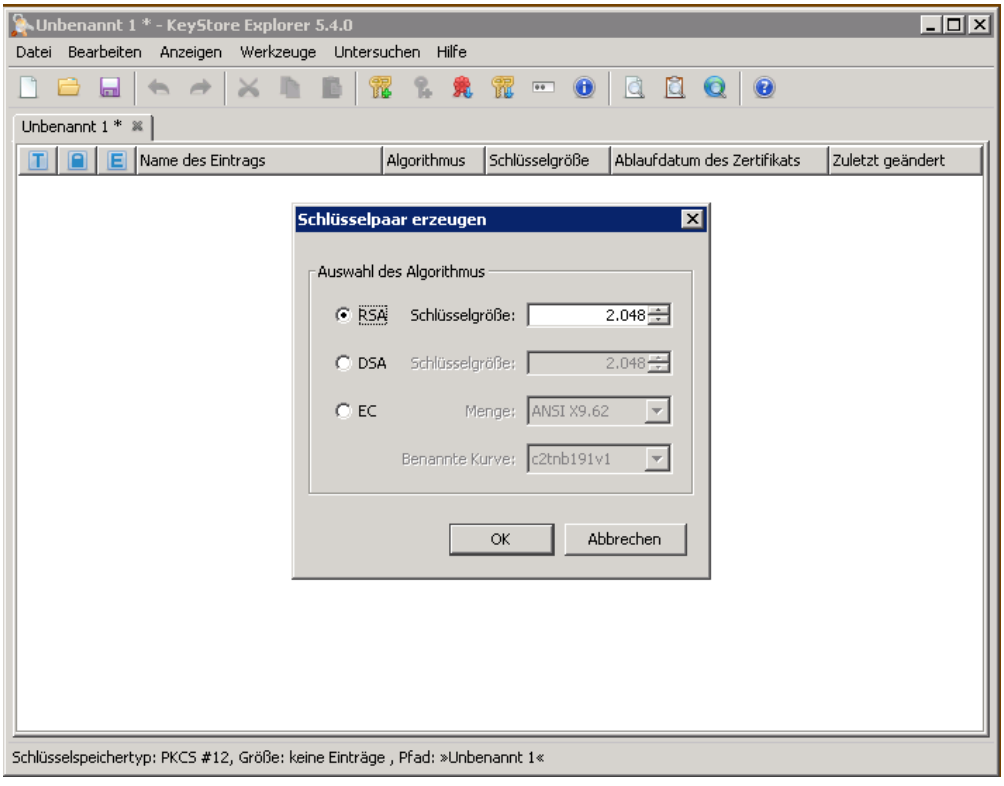
1.1 Typ des Schlüsselspeichers auswählen:



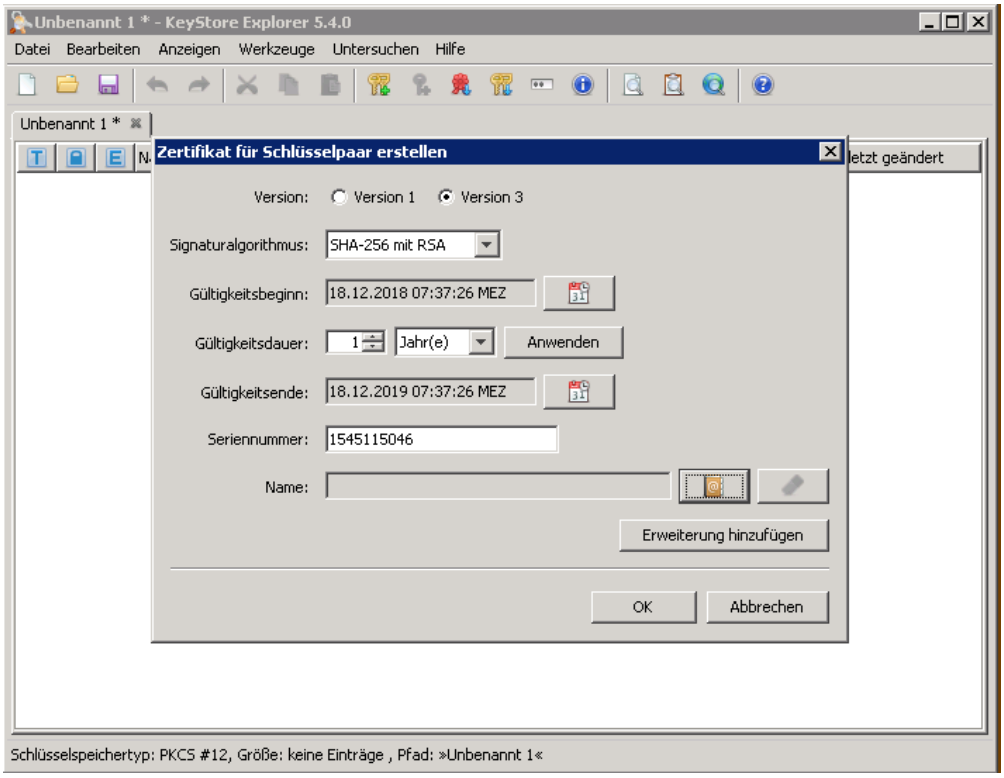
1.2 Auf „Werkzeuge“ gehen und auf „Schlüsselpaar erstellen“ klicken:



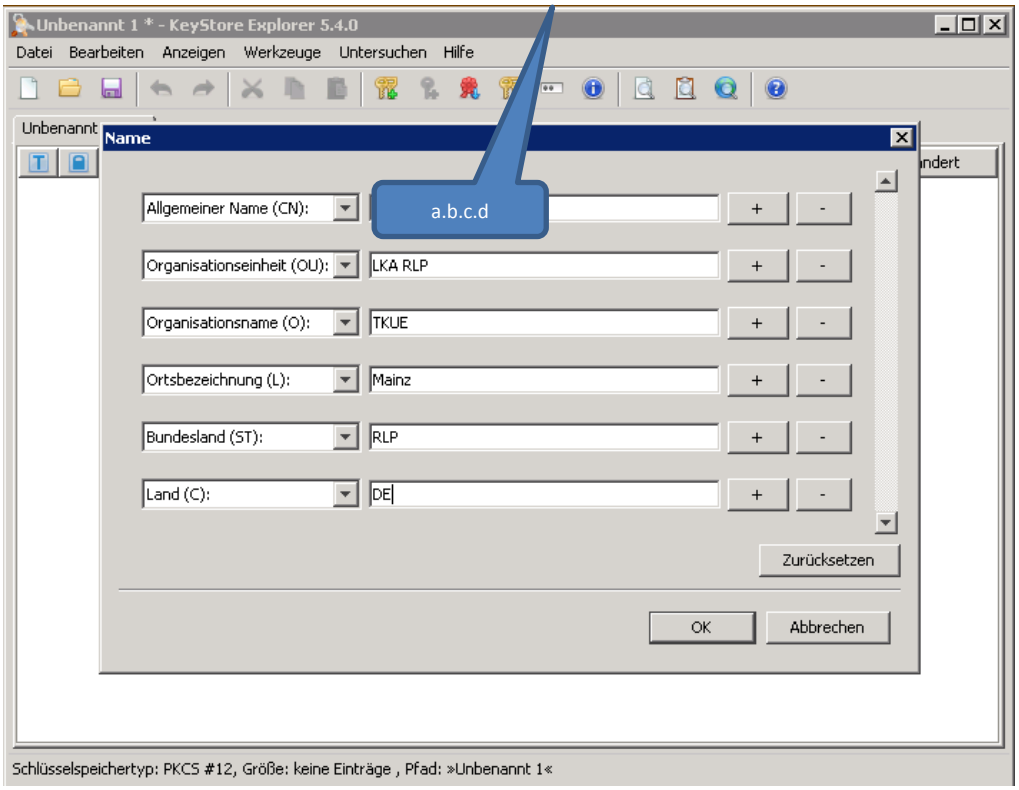
1.3 Schlüsselgröße wählen:



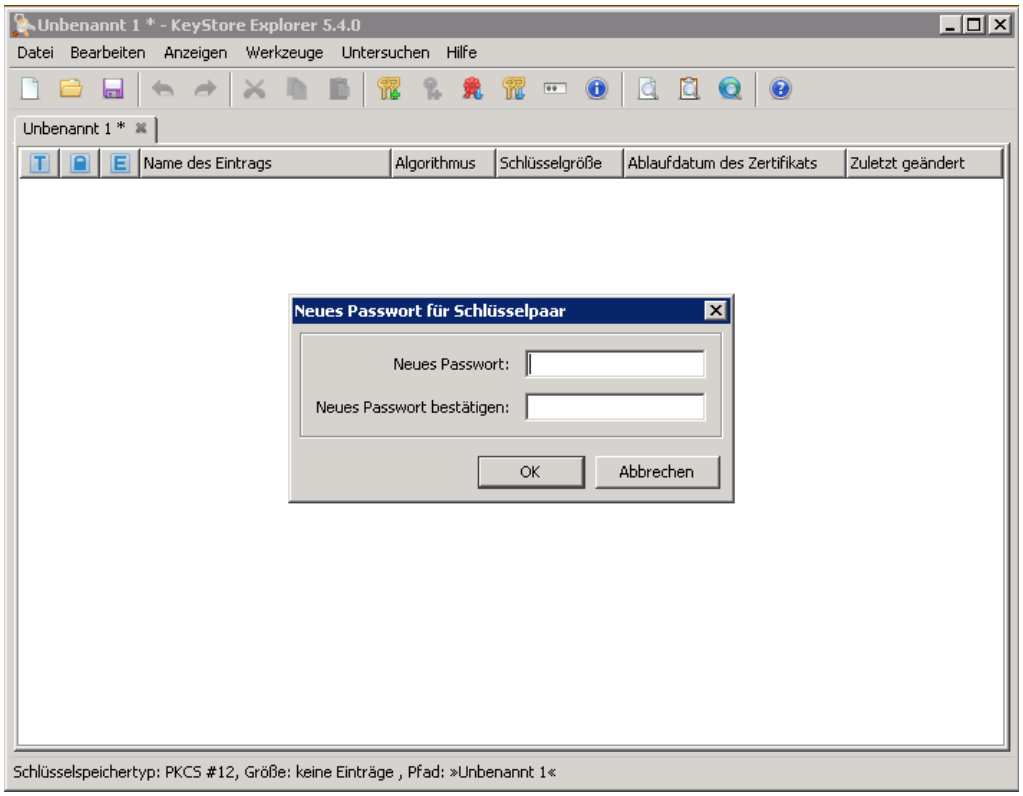
1.4 Namen eingeben (auf das Zeichen mit dem @ klicken) und die Gültigkeitsdauer auf **sechs Jahre** einstellen (auf „Anwenden“ klicken):



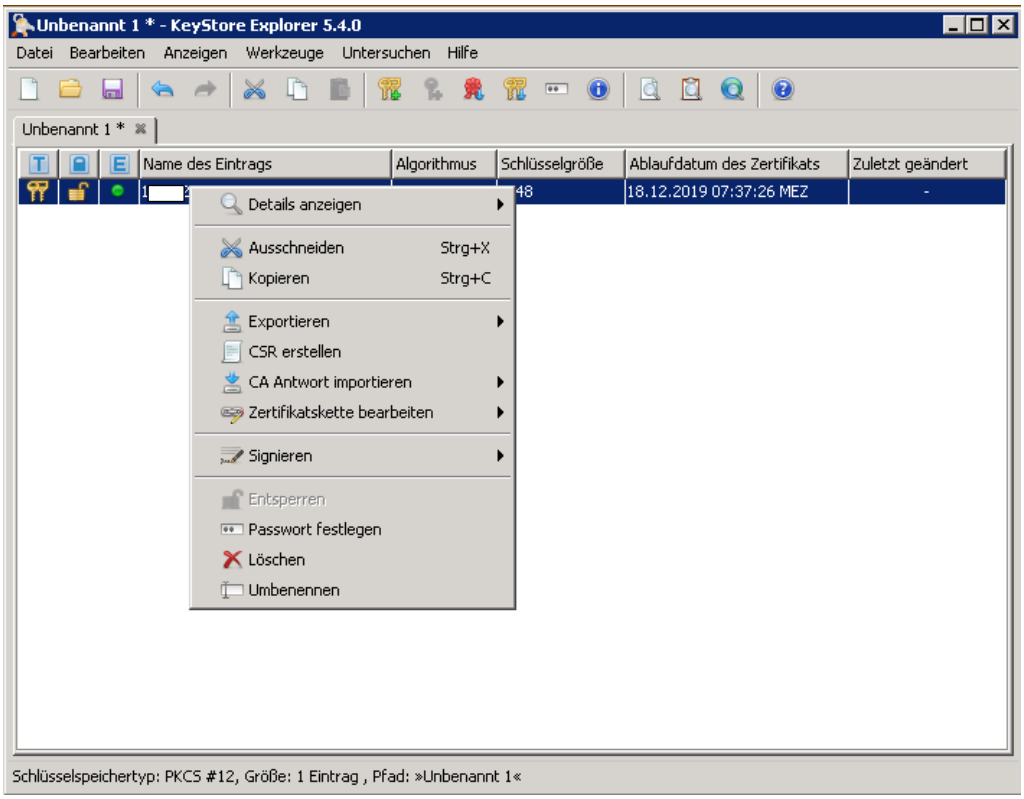
1.5 Daten eingeben (keine deutschen Umlaute; Webservice IP-Adresse von Behörden mit a.b.c.d und von Verpflichteten ist Server- **gleich** Clientadresse):



1.6 Mit „OK“ bestätigen und Passwort vergeben (**Passwort merken!**):

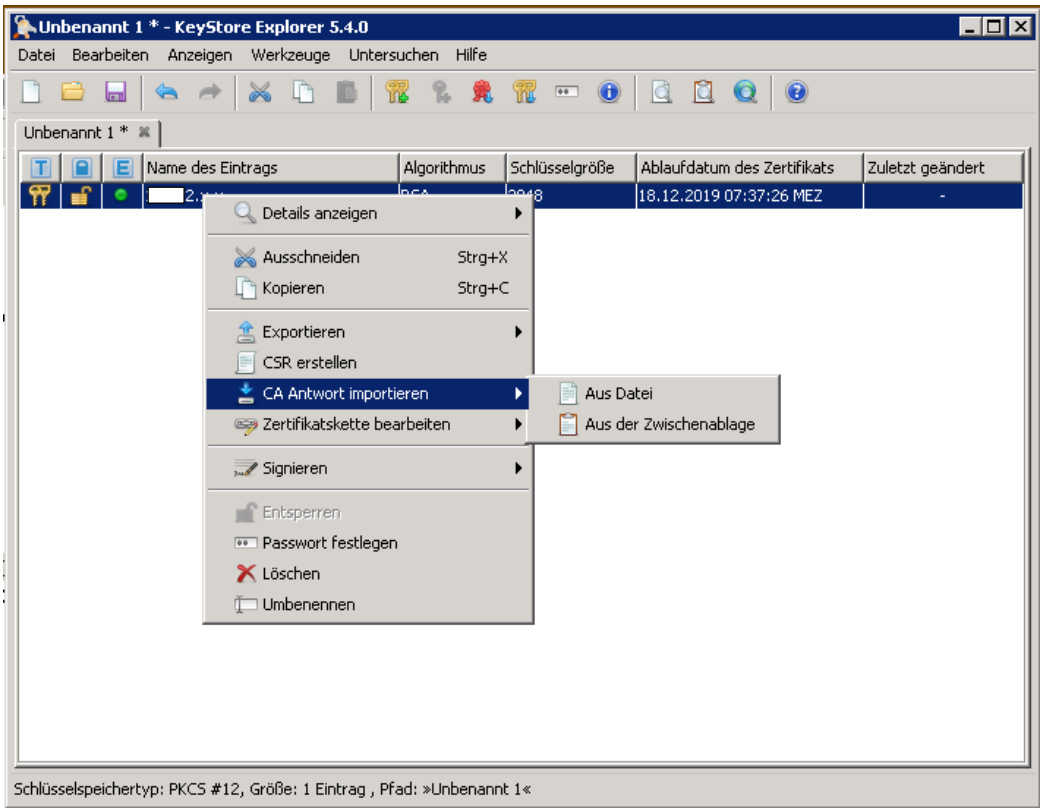


1.7 Rechtsklick auf das erstellte Schlüsselpaar und „CSR erstellen“ auswählen:

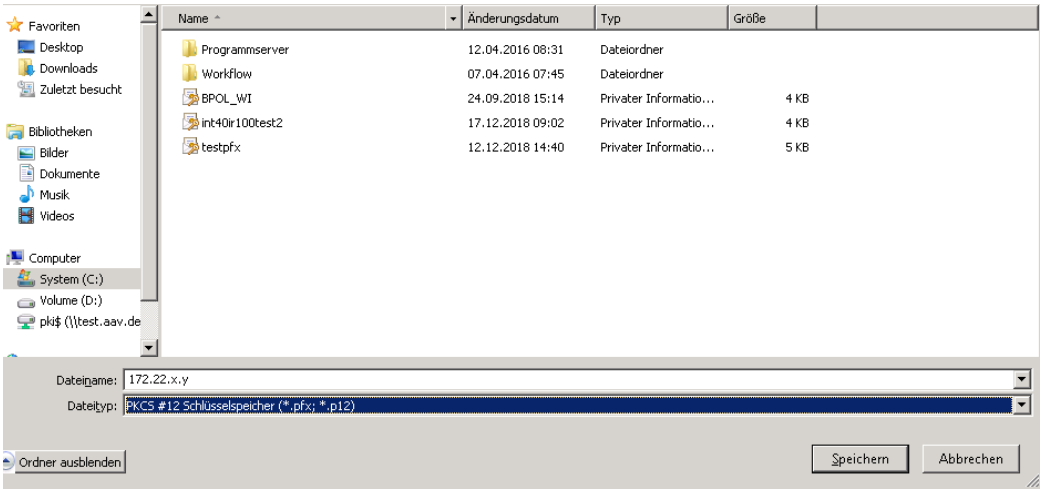


2. Die so erzeugte Datei –hier „a.b.c.d.csr“ - per E-Mail an die BNetzA senden. Bei den verpflichteten Unternehmen **sind es immer zwei Dateien** (Client- und Server-CSR), daher müssen die Schritte ab einschließlich 1.2 wiederholt werden. Wenn das Programm jetzt beendet wird: **Schlüsselpaar sicherheitshalber exportieren nicht vergessen!**

3. Wenn der **signierte Request** der BNetzA vorliegt, kann dieser wieder mit dem Schlüsselpaar verknüpft werden (Rechtsklick auf das Keypair, „CA-Antwort importieren“, „aus Datei“)



3.1 Anschließend „Datei speichern unter“ wählen; einen Namen wählen und den Dateityp passend zum Betriebssystem (z. B. **PKCS#12)** auswählen:



Der Sicherheitsvorteil dieser Lösung ist, dass der private Schlüssel beim Anwender verbleibt.