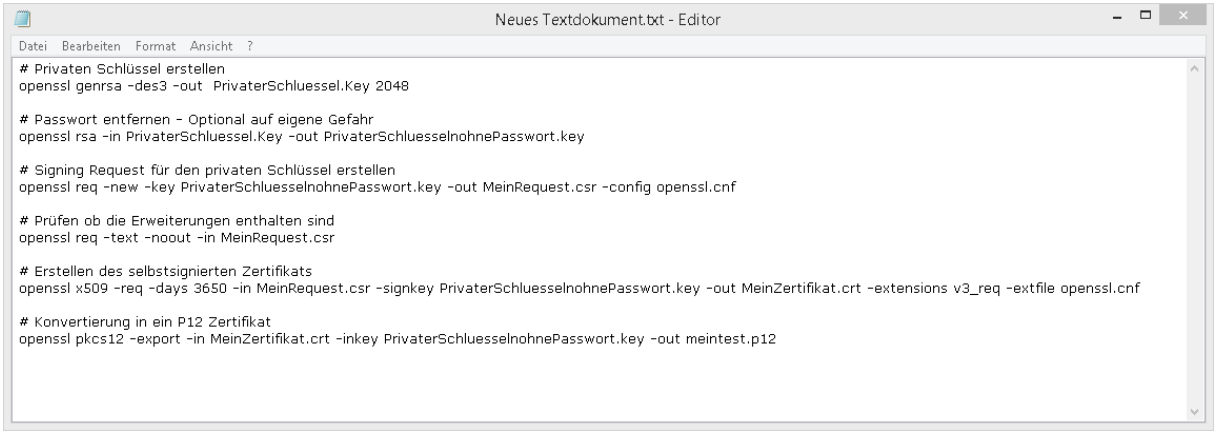
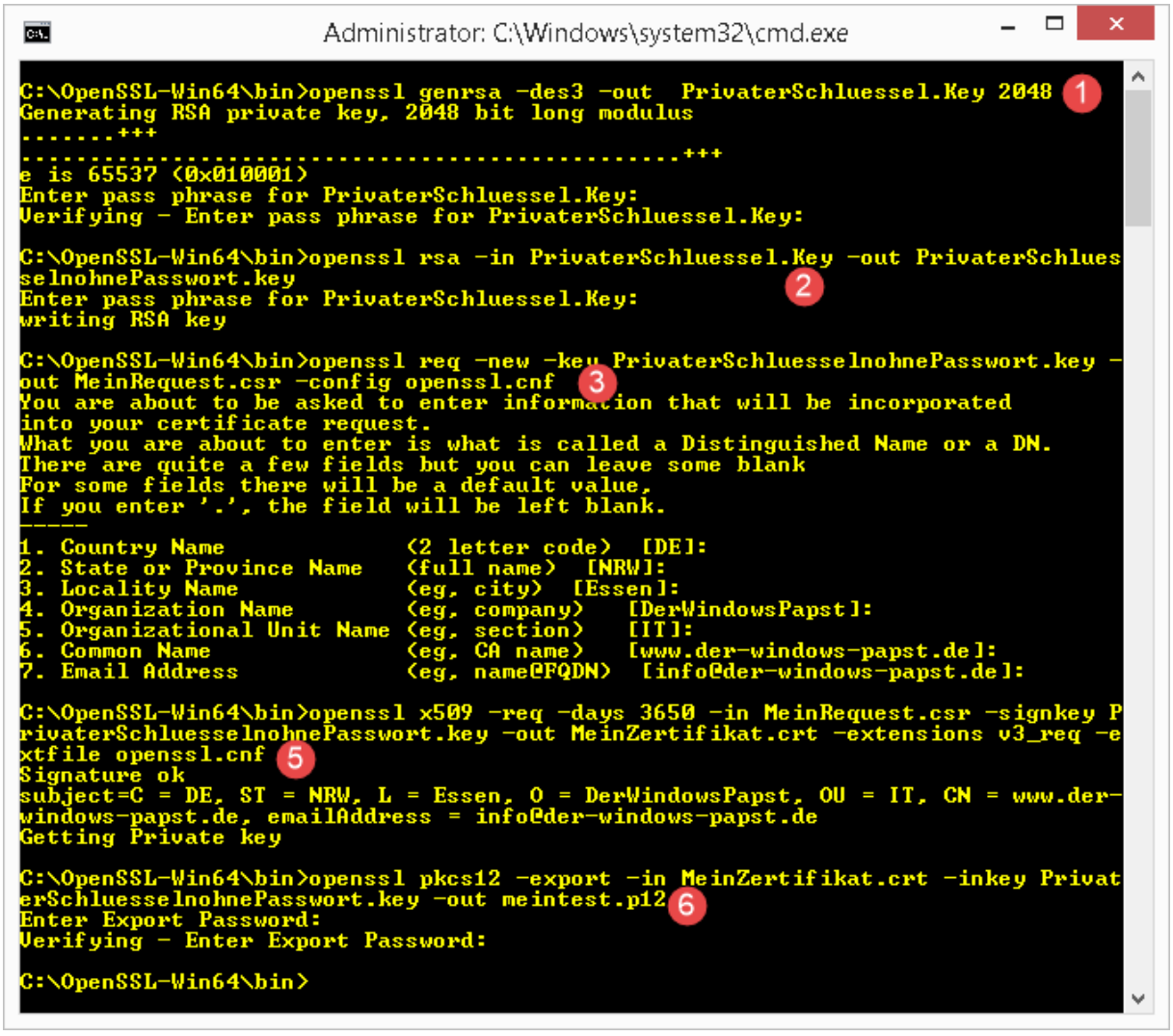
Weitere Zertifikate auf Basis eines privaten Schlüssels erstellen

Mit OpenSSL erstellen wir zuerst einen Private-Key (KEY), basierend auf den Private-Key ein Certificate Signing Request (CSR). Als nächstes signieren wir den CSR mit dem Hash des Private-Keys, das Resultat daraus ist ein (Public) Zertifikat (CRT). Zum Abschluss bringen wir die 2 Zertifikate (Privat- und Public-Key) zusammen und kreieren ein p12 Zertifikat.

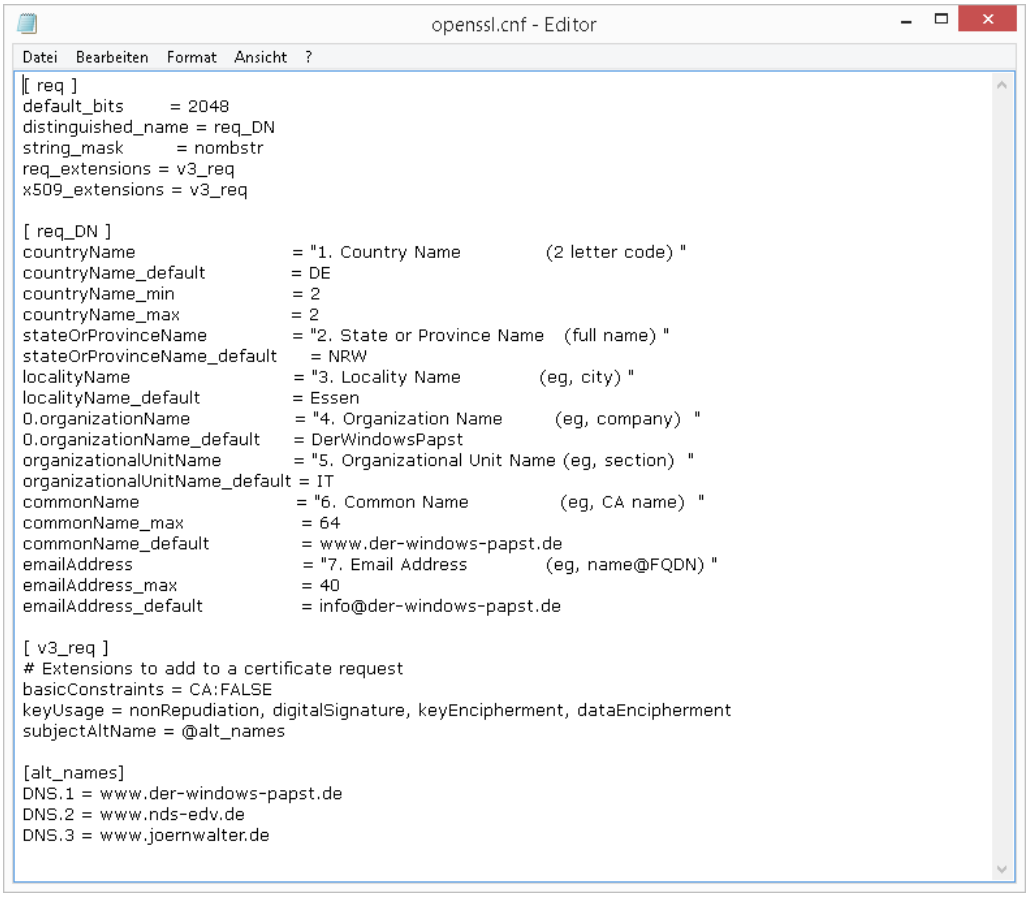
Der Befehl 2 ist optional und der Befehl 4 (in der CMD nicht ausgeführt) würde uns den Inhalt des CSR anzeigen.





Weitere Zertifikate auf Basis eines privaten Schlüssels erstellen

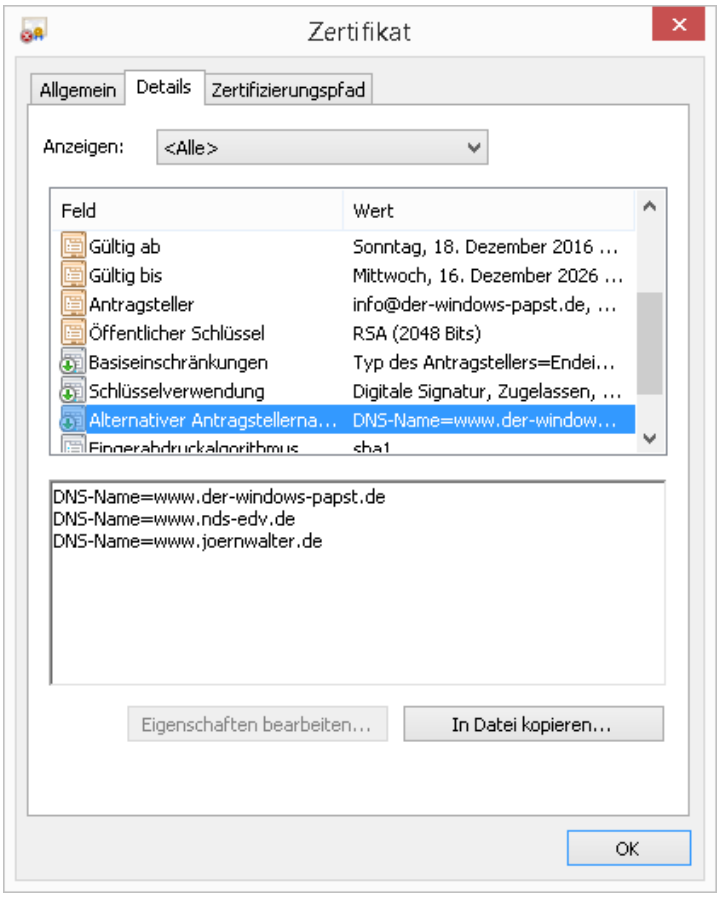
Den CSR erstellen wir aus der Vorlage openssl.cnf. Der Parameter commonName_default ist der Name des Servers oder Clients für den wir ein Zertifikat erstellen wollen.



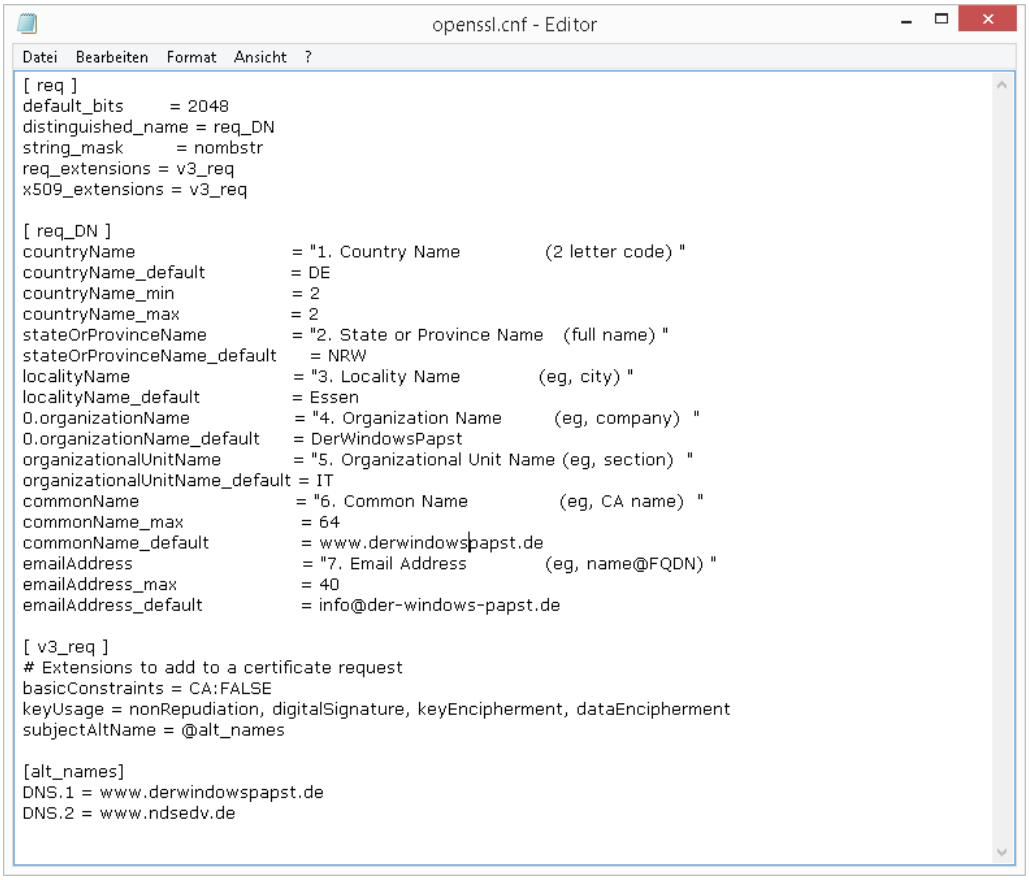
In diesem Fall www.der-windows-papst.de mit den alternativen DNS Namen

- www.der-windows-papst.de
- www.nds-edv.de
- www.joernwalter.de

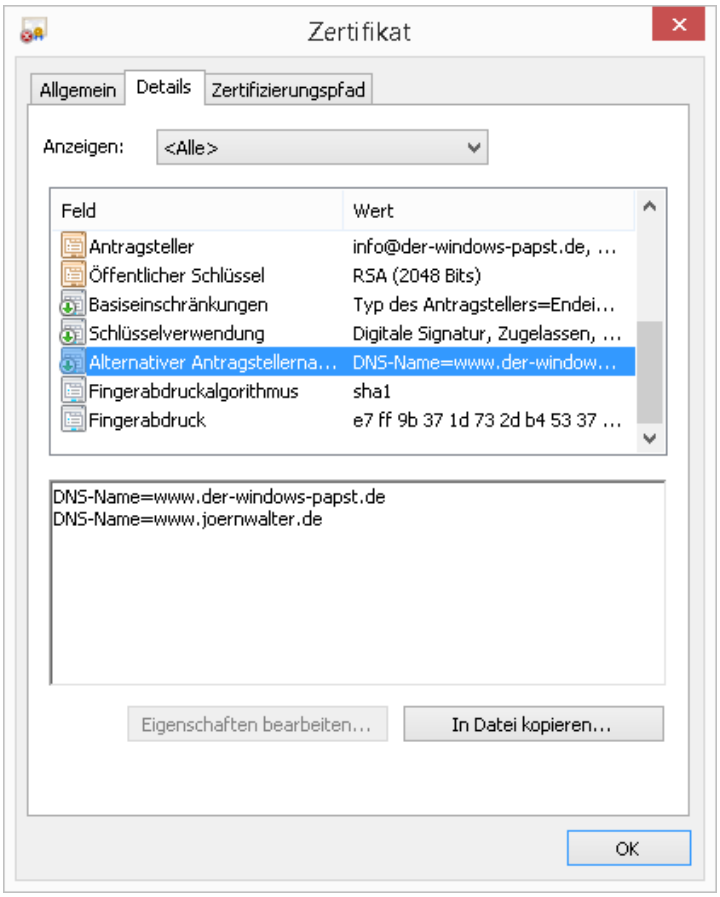
Weitere Zertifikate auf Basis eines privaten Schlüssels erstellen



Vorlage verändert und die Bindestriche in den alternativen DNS Namen entfernt. Ein weiteren Request erstellt und wieder mit dem Hash des Private-Keys signiert.



Weitere Zertifikate auf Basis eines privaten Schlüssels erstellen



Beide Zertifikate nebeneinander gelegt und finden den gleichen öffentlichen Schlüssel des Private-Keys wieder.