**openSSL:**SEC/SEC-SSL/01-openSSL-zertifikate.odt / UE Zertifikate(.tgz)

1) sudo apt-get install openssl

->openssl installieren

2) openssl genrsa -out www-name-org.key -des3 2048

->Schlüsselerzeugung

2.1) (optional) openssl rsa -in www-name-org.key > www-name-org-unencrypted.key

->Entfernen der Triple-DES Verschlüsselung

2.2) (optional) openssl rsa -in www-name-org.key -text -noout

->Inhalt der Schlüsseldatei ansehen

4) openssl req -new -key www-name-org.key -out www-name-org.csr

->Certification Signing Request (CSR) erzeugen

4.1) (optional) openssl req -in www-name-org.csr -text -noout

->CSR anzeigen

6) openssl req -x509 -newkey rsa:512 -keyout CA.key -out CA.crt

->eigene (private) Certification Authority (CA) erzeugen

7) openssl x509 -req -in www-name-org.csr -CA CA.crt -CAkey CA.key -CAcreateserial -out www-name-org.crt -days 365

->Signieren eines CSR

7.1) (optional) openssl x509 -in www-name-org.crt -text -noout

->Ausgabe Zertifikat

**SHORT**:

1) openssl req -new -keyout www-name-org.key -out www-name-org.csr -newkey rsa:2048 -nodes

->KEY & CSR erzeugen

2) openssl req -x509 -newkey rsa:512 -keyout CA.key -out CA.crt

->CA-Stamm-Zertifikat erzeugen

3) openssl x509 -req -in www-name-org.csr -CA CA.crt -CAkey CA.key -CAcreateserial -out www-name-org.crt -days 365

->CSR signieren

**TESTEN**:

1) sudo nano /etc/hosts -> 127.0.0.1 www.name.org

->“localhost“ mit DNS des Servers austauschen

2) openssl s\_server -WWW -accept 8000 -key www-name-org.key -cert www-name-org.crt

->Server starten

3\_1) https://www.name.org:8000/CA.config

->Testen mit Browser

3\_2) openssl s\_client -connect WWW.NAME.ORG:8000 -key www-name-org.key -cert www-name-org.crt

->Testen in Konsole