

Schlüsselerzeugung und Requesterstellung auf Linux mit OpenSSL

1. Sicherstellen, dass OpenSSL installiert ist (default)

z.B. mit: # openssl version
output z.B.: # OpenSSL 0.9.8 08 Feb 2011 => alles ok

2. Konfigurationsdatei für OpenSSL - /etc/ssl/openssl.cnf - anpassen

von <http://grid.fzk.de/ca/openssl-gridka.cnf> holen und eventuell auf openssl.cnf kopieren.
Falls keine root - Rechte vorhanden sind, kann die Konfigurationsdatei über
-config /path/to/openssl-gridka.cnf angegeben werden.

Manuelle Anpassungen im Abschnitt:

#####

[req_distinguished_name]

countryName = Country Name (2 letter code)
countryName_default = DE
countryName_min = 2
countryName_max = 2

0.organizationName = Organization Name (eg, company)
0.organizationName_default = GermanGrid

organizationalUnitName = Organizational Unit Name (eg, section
organizationalUnitName_default = **OU**

Wichtig: Als **OU** bitte das eigene Institutskürzel verwenden.
(<http://grid.fzk.de/ca/RA.html> - Liste aller Organisationen)

folgende Zeilen müssen unbedingt auskommentiert werden:

#localityName = Locality Name (eg, city)
#stateOrProvinceName = State or Province Name (full name)
#stateOrProvinceName_default = SomeState
#emailAddress = Email Address
#emailAddress_max = 64
#challengePassword = A challenge password
#challengePassword_max = 20
#challengePassword_min = 4
#unstructuredName = An optional company name

#####

3. Schlüssel und Request erzeugen:

(wird in dem Verzeichnis erstellt, in dem Sie sich befinden):

a) Für Userkeys mit Passwortschutz des private Keys (privkey.pem):

```
# openssl req -newkey rsa:2048 -sha1 [-config /path/to/openssl-gridka.cnf] -out userreq.pem  
-rand /usr/bin/
```

Erläuterung: Zunächst wird ein 2048-Bit langer RSA-Schlüssel erzeugt, für den Sie eine Passphrase angeben müssen. Diese soll mindestens 12 Zeichen lang und kein einfaches Wort sein. „-sha1“ bezeichnet den Signaturalgorithmus, „-config“ gibt an welche Konfigurationsdatei verwendet werden soll, „-out“ den Name der Ausgabedatei und „-rand“ schliesslich den Ort wo Zufallsdaten gesammelt werden sollen.

b) Für Serverkeys ohne Passwortschutz des privaten Keys zunächst den Schlüssel erzeugen:

```
# openssl genrsa -out hostkey.pem -rand /usr/bin/ 2048
```

Dann den Request File:

```
# openssl req -new -sha1 -key hostkey.pem -out hostreq.pem
```

4. Request ansehen, Angaben ueberpruefen

```
# openssl req -verify -text -in hostreq.pem
```

5. Request zur GridKa-CA hochladen

<https://gridka-ca-sec.fzk.de> → Wähle Persönliche oder Host/Servicezertifikate, wähle jeweils „PEM-request“, mit „*“ gekennzeichnete Felder im Formular ausfüllen, Datei zum Hochladen auswählen, „absenden“. Fertig.

6. Warten, Zertifikat herunterladen und an die richtige Stelle kopieren:

Userzertifikat nach ~/.globus/usercert.pem im Homeverzeichnis
(und privkey.pem -> ~/.globus/userkey.pem)

Serverzertifikat nach /etc/grid-security/hostcert.pem und /etc/grid-security/hostkey.pem

Webserver siehe apache.conf