

### Adobe Acrobat

Erstellung eines Requests mit OpenSSL

---

**Stand:** 12.05.2016

#### Schlüsselgenerierung

Erzeugung eines RSA 2048bit Schlüssels der mittels der Option `-des3` verschlüsselt auf dem Rechner in der Datei, die nach `-out` angegeben wird, abgelegt wird.

```
#openssl genrsa -des3 -out Key.pem 2048
```

#### Erzeugung eines Requests

Erzeugung eines Requests mit der Angabe der Datei, die den privaten Schlüssel `Key.pem` enthält. Nach der Eingabe des Befehls erwartet OpenSSL die folgenden Eingaben.

Hinweis: Soll ein Eintrag leer gelassen werden, muss ein Punkt eingegeben werden.

```
#openssl req -new -key Key.pem -out - Req.pem
```

### **Angaben im Zertifikat:**

Country Name (C ) = DE

Organization Name (O) = Hochschule Harz, Hochschule fuer angewandte Wissenschaften

Common Name (CN) = Benutzername (Vorname Nachname) / Serverhostname

Locality Name (L) = Wernigerode

State or Province Name (ST) = Sachsen-Anhalt

Emailadresse = Emailadresse

Passphrase = Passwort zum Schutz des Privaten Schlüssels

**Wichtig:** Ohne dieses Passwort kann niemand Daten entschlüsseln, wenn dieses Passwort vergessen wird, sind verschlüsselte Daten unwiderruflich verloren.

### **Fingerabdruck erstellen (optional)**

Generiert ein SHA1- Fingerabdruck vom Modulus des Schlüssels aus dem Request *Req.pem*.

```
#openssl req -noout -modulus -in Req.pem | openssl sha1 -c
```