Hier wird beschrieben, wie man SSL-Zertifikate erstellt
 Grundsätzlich geht man wie folgt vor.

- Man erstellt ein Certificate Signing Request (CSR)
- Diesen Request gibt man an eine Zertifizierungsstelle weiter. Diese prüft die Daten und beglaubigt die Daten.
- Man bekommt ein signiertes Zertifikat und und kann es verwenden.

Der Haken an der Sache ist, dass man eine Zertifizierungsstelle (CA) (z. B. VeriSign, …) braucht, um die Zertifikate zu signieren. Das Kostet aber. Deshalb erstellen wir einfach unsere eigene CA.

Installation

```
sudo apt-get install openssl
```

Zertifikaterstellung

CA erstellen

Alle Schritte werden als normaler User gemacht. Es ist nicht notwendig, root zu sein.

Zu aller erst sollte man sich seine Umgebung erstellen, dazu im Home-Verzeichnis folgende Struktur erstellen:

```
mkdir testCA
cd testCA
mkdir certs private newcert

chmod 700 certs private
echo 01 >serial
touch index.txt
```

Die Dateien serial und index.txt dienen der Zertifikatsverwaltung

Als nächstes müssen wir die Konfigurations-Datei für ssl kopieren und anpassen

```
cp /etc/ssl/openssl.cnf .
```

In der Datei kann man verschiedene Punkte anpassen

Die Standard-Schlüssellänge wird unter

```
[ req ]
default_bits            = 1024
```

angepasst. In folgendem Abschnitt werden Namen und Angaben per default vorgegeben

```
[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
countryName_default             = DE
countryName_min                 = 2
countryName_max                 = 2

stateOrProvinceName             = State or Province Name (full name)
stateOrProvinceName_default     = Bayern

localityName                    = Locality Name (eg, city)
localityName_default            = Ort

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

# we can do this but it is not needed normally :-)
#1.organizationName             = Second Organization Name (eg, company)
#1.organizationName_default     = World Wide Web Pty Ltd

organizationalUnitName          = Organizational Unit Name (eg, section)
organizationalUnitName_default  = Abteilung

commonName                      = Common Name (eg, YOUR name)
commonName_default              = Name
commonName_max                  = 64

emailAddress                    = Email Address
emailAddress_default            = Email Adresse
emailAddress_max                = 64
```

Alle Variablen, die ein *_default* am Ende haben, können angepasst werden. Diese Werte werden als default-Werte für die erstellung der CA verwendet

Jetzt muss man openSSL.cnf noch exportieren, damit openssl später default-Einstellungen hat

```
export OPENSSL_CONF=/home/patrick/testCA/openssl.cnf
```

Jetzt kann man die CA erstellen. Dazu muss folgender Befehl eingegeben werden:

```
openssl req -x509 -days 1825 -newkey rsa:2048 -out private/cacert.pem
```

Hier wird nach einem Passwort gefragt. Dies sollte sehr sicher sein, da mit diesem Zertifikat neue Zertifikate erstellt und zurückgenommen werden können.

Hier werden einige Daten abgefragt. Einzig wichtig ist, dass der Common-Name richtig ist

Anschauen kann man sich das Zertifikat mit

```
openssl x509 -in private/cacert.pem -text -noout
```

Und damit haben wir uns unsere eingene Zertifizierungsstelle (CA) aufgebaut.

CSR erzeugen

Mit folgende Befehl wird ein CSR erzeugt.

```
openssl req -newkey rsa:1024 -keyout server.key -out server.csr
```

Nachdem man diesen Befehl eingegeben hat, wird man verschiedene Dinge gefragt. Alle Angaben sollten die gemacht werden sind eigentlich völlig egal. Es muss der Zertifizierungsstelle glaubwürdig vorkommen. Nur bei **common name** muss bis aufs i-Tüpfelchen alles richtig sein

Das eingegeben Passwort ist erst einmal ohne Bedeutung

Anzeigen kann man diese Anfrage mit

```
openssl req -in server.csr -text -noout
```

Dieses CSR müssen wir jetzt der Zertifizierungsstelle schicken. Da wir aber unsere eigene CA haben, fahren wir mit der zertifizierung fort

Zertifikat signieren

Man sollte darauf achten, dass die Variable OPENSSL_CONF noch mit dem Wert /home/patrick/testCA/openssl.cnf belegt ist, ansonsten einfach noch mal exportieren

```
export OPENSSL_CONF=/home/patrick/testCA/openssl.cnf
```

Zum zertifizieren folgende Zeile eingeben

```
openssl ca -in server.csr
```

Als erstes müssen wir das Passwort der CA eingeben. Dann sollte man die gemachten Angaben überprüfen und dann bei der Frage **Sign the certificate? [y/n]:** mit y bestätigen

Hiermit ist das Zertifikat offiziell beglaubigt.

Jetzt muss das Zertifikate noch an den CSR (in diesem Fall uns selbst) geschickt werden. Dazu eine Kopie des Zertifikats verschicken

```
cp certs/01.pem ~/server.crt
```

Verwendung

Jetzt kann man das Zertifikat, dass man bekommen hat, verwenden.