In einigen Fällen wird ein SSL-Zertifikat benötigt. Die Erstellung, samt zugehöriger CA, wird nachfolgend beschrieben.

1 - CA

Schritt 1: Erstellen des privaten Schlüssels „ca.key“ für die CA:

```
~# openssl genrsa -out ca.key 4096
```

Schritt 2: Erstellen des CA-Zertifikats „ca.crt“:

```
~# openssl req -x509 -new -nodes -sha512 -days 3650 -subj
"/C=DE/ST=Niedersachsen/L=Hannover/O=looper/OU=Personal/CN=Personal Root CA"
-key ca.key -out ca.crt
```

2 - Server-Zertifikat

Am Beispiel des Harbor kann jetzt ein Server-Zertifikat erstellt werden.

Schritt 1: Erstellen des privaten Schlüssels „slxharbor.fritz.box.key“ für den Server:

```
~# openssl genrsa -out slxharbor.fritz.box.key 4096
```

Schritt 2: Generieren einer Zertifikatsanforderung (CSR):

```
~# openssl req -sha512 -new -subj
"/C=DE/ST=Niedersachsen/L=Hannover/O=looper/OU=Personal/CN=slxharbor.fritz.b
ox" -key slxharbor.fritz.box.key -out slxharbor.fritz.box.csr
```

Schritt 3: Erstellen der X509-Erweiterungsdatei „v3.ext“:

```
~# cat> v3.ext <<-EOF
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment,
dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names

[alt_names]
```

```
DNS.1=slxharbor.fritz.box
DNS.2=slxharbor.fritz
DNS.3=slxharbor
DNS.4=harbor.fritz.box
DNS.5=harbor
EOF
~#
```

Schritt 4: Erstellen des Zertifikats „`slxharbor.fritz.box.crt`“: <code>~# openssl x509 -req -sha512 -days 3650 -extfile v3.ext -CA ca.crt -CAkey ca.key -CAcreateserial -in slxharbor.fritz.box.csr -out slxharbor.fritz.box.crt Certificate request self-signature ok subject=C=DE, ST=Niedersachsen, L=Hannover, O=looper, OU=Personal, CN=slxharbor.fritz.box ~#

</file>

.Ende des Dokuments