OpenSSL

Certificate mit SANs

request.conf

```
[req]
distinguished_name = dn
prompt             = no
req_extensions     = req_ext

[dn]
C="DE"
ST="Germany"
L="."
O="ORG"
OU="ORG UNIT"
emailAddress="MAIL"
CN="COMMON NAME"

[req_ext]
subjectAltName = @alt_names

[alt_names]
DNS.1 = [Domain 1]
DNS.2 = [Domain 2]
DNS.3 = [Domain 3]
```

```
# create csr
openssl req -new -key private_key.key -out csr.csr -config request.conf
# check csr
openssl req -text -verify -in csr.csr
# alt.: self-sign
openssl req -new -key private_key.key -x509 -out cert.pem -config request.conf
```

pkcs12/pfx

```
# create
openssl pkcs12 -export -out OUT.pfx -inkey KEY.key -in CERT.cer -in INTERMEDIATE.cer -in
ROOT.cer
# export
openssl pkcs12 -in file.pfx -out file.withkey.pem -nodes
```

keys

```
# rsa
openssl genrsa -out [KEY].key [encryption] [BITS]
# encryption can be omitted for unencrypted key or:
# -aes128, -aes192, -aes256, -aria128, -aria192, -aria256, -camellia128, -camellia192, -
camellia256

# elliptic curve
# list available curves
openssl ecparam -list_curves
# secp384r1 or secp521r1 is a good curve
openssl ecparam -name [CURVE] -genkey -out [KEY].key
```

get cert/key content

```
# cert
openssl x509 -in [CERT].crt -text
# key
openssl rsa -in [RSA-KEY] -text
openssl ec -in [EC-KEY] -text
# csr
openssl req -in [REQUEST] -text
# optionally add -check (keys) or -verify (csr) to check for consistency

# check match key and cert
```

```
openssl x509 -noout -modulus -in server.crt | openssl md5
openssl rsa -noout -modulus -in server.key | openssl md5
```

self sign crt

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -nodes -days 365
```

connection testing

https/smtps

```
openssl s_client -quiet -connect example.com:443
openssl s_client -quiet -connect mail.yourserver.tld:485
```

smtp/imap starttls

```
openssl s_client -quiet -starttls smtp -connect mail.yourserver.tld:25
openssl s_client -quiet -starttls imap -connect mail.yourserver.tld:143
```

Created 2022-03-08 19:22:37 UTC by Krumel
Updated 2022-12-13 10:21:47 UTC by Krumel