

SSL/TLS Certificates - Self-signed certificate

This guide generates a self-signed certificate for the haproxy service.

OpenSSL Configuration

Edit the file `/etc/pki/tls/openssl.cnf` and make various modifications (read the comments carefully!)

`/etc/pki/tls/openssl.cnf`

```
#
# Insert at the end:
#

[ alternate_names ]
DNS.1      = acd-lb.domain.de
DNS.2      = acd-lb.domain.local
DNS.3      = acd-lb

#
# Insert in this section:
#

[ v3_ca ]
subjectAltName      = @alternate_names

#
# Insert or modify in this section:
#

[ v3_ca ]
keyUsage = digitalSignature, keyEncipherment

#
# Change or comment in this section:
#

[ CA_default ]
copy_extensions = copy
```

Generate Keys

First, create a directory for the keys, and then generate the keys.

ATTENTION: The following section also includes outputs from the system.

Generate Keys

```
mkdir /etc/ssl/newkey
openssl genrsa -out /etc/ssl/newkey/cert.key 3072
openssl req -new -x509 -key /etc/ssl/newkey/cert.key -sha256 -out /etc/ssl/newkey/cert.pem -days 730

#
# Answer the questions as follows (for example):
#

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:DE
State or Province Name (full name) []:Bavaria
Locality Name (eg, city) [Default City]:Munich
Organization Name (eg, company) [Default Company Ltd]:jtel GmbH
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:acd-lb.domain.de
Email Address []:lewis.graham@jtel.de
```

Check the generated certificate

Check whether the alternative names have been entered:

Check

```
openssl x509 -in /etc/ssl/newkey/cert.pem -text -noout

# Check if all DNS names are listed with this entry:
# X509v3 Subject Alternative Name:
```

Create and copy combined .pem

Combined PEM

```
cat /etc/ssl/newkey/cert.key > /etc/ssl/newkey/comb.pem
cat /etc/ssl/newkey/cert.pem >> /etc/ssl/newkey/comb.pem
cp /etc/ssl/newkey/comb.pem /etc/haproxy/haproxy.pem
chmod 400 /etc/haproxy/haproxy.pem
```

enter certificate in haproxy.cfg and adjust frontend configuration to redirect

Combined PEM

```
#
# Frontend http redirects to https
#
frontend acdportal_http
    mode            http
    bind            :80
    redirect        scheme https if !{ ssl_fc }

#
# Frontend for https with certificate
#
frontend acdportal_https
    mode            http
    bind            :443 ssl crt /etc/haproxy/haproxy.pem #verify optional
...

```