

Gutzi

“ Depending on the size of your home network, the "Create certificates" steps have to be carried out continuously, which can be annoying. Especially if you want to decide on a new domain name after some time... There are also devices, e.g. AVM routers or apps (e.g. Plex) that only accept a .pfx (PKCS#12 standard)! Hm, and we're already out of luck ☹ ...

1. all in one step, ouch ...script

For all those who have implemented the realization as recommended by me on a PI or Linux device, here is a script that is quickly adapted and then takes your domain as a parameter and automatically creates all the necessary files.

8-tung! The root certificate must exist / have already been created! and be located in the same directory as the script.

```
#!/bin/bash

#Required
domain=$1
commonname=$domain

#Change to your company details
country=<>
state=<>
locality=<>
organization=<>
organizationalunit=<>
email=<>

if [ -z "$domain" ]
then
    echo "Argument not present."
    echo "Usage $0 [common name]"

    exit 99
fi
```

```
echo "1. generating .key for $domain"
#generate a .key
openssl genrsa -out $domain.key 2048
echo "successful!"
echo ""

echo "2. generating .csr for $domain"
#generate a .csr
openssl req -new -key $domain.key -out $domain.csr \
    -subj
"/C=$country/ST=$state/L=$locality/O=$organization/OU=$organizationalunit/CN=$commonname/email
Address=$email"
echo "successful!"
echo ""

echo "3. generating .ext for $domain"
cat > $domain.ext <<EOF
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = $domain

EOF
echo "successful!"
echo ""

echo "4. creating .csr for $domain"
openssl x509 -req -in $domain.csr -CA <SLD>.pem -CAkey <SLD>.key -CAcreateserial -out
$domain.crt -days 3650 -sha256 -extfile $domain.ext
echo "successful!"
echo ""


echo "5. creating .pem for $domain"
cat $domain.crt $domain.key > $domain.pem
echo "successful!"
```

```
echo ""

echo "6. creating .pfx for $domain"
openssl pkcs12 -export -in $domain.pem -out $domain.pfx
echo "successful!"
echo ""
echo "-----"
echo "----- All Set! -----"
echo "-----"
echo
```

- You can download the script here: [genCert.zip](#)
- and adapt it to your needs (search for <> and <SLD>. Then save it.
- make the script executable with the command: "sudo chmod +x <scriptname>.sh"

DONE!

Execute with command: "./<sriptname>.sh <subDomäne.SLD.TLD>" 

Revision #2

Created 18 June 2025 08:54:10 by tomek

Updated 18 June 2025 10:00:39 by tomek