

Gutzi

“Je nach Größe eures Heimnetzwerkes müssen die Schritte "[Zertifikate erstellen](#)" dauernd abgearbeitet werden, was nervig werden kann. Vor allen Dingen wenn man sich mal nach einiger Zeit für einen neuen Domänen Namen entscheiden will... Es gibt auch Geräte, z.B. AVM Router oder Apps (z.B. Plex) die akzeptieren nur eine .pfx (PKCS#12-Standard)! Hm, und schon wären wir gekniffen ☹ ...

1. alles in einem Schritt, ouch ...Script

Für alle die, die die Realisierung wie von mir empfohlen auf einem PI oder Linux Gerät implementiert haben, kommt hier ein Script, das schnell angepasst ist und dann eure Domäne als Parameter nimmt und alle erforderlichen Dateien automatisch erstellt.

8-tung! Das Stammzertifikat muss vorhanden / bereits erstellt sein! und sich im gleichen Verzeichnis befinden wie das 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
```

- Hier könnt ihr das Script herunterladen: [genCert.zip](#)
- entpacken und auf eure Bedürfnisse anpassen (sucht nach <> und nach <SLD>. Dann abspeichern.
- mit dem Kommando: "sudo chmod +x <scriptname>.sh" ausführbar machen

fertig!

ausführen mit Kommando: "./<sriptname>.sh <subDomäne.SLD.TLD>" 

Revision #7

Created 17 June 2025 12:10:57 by tomek

Updated 17 June 2025 12:50:37 by tomek