

Inhaltsverzeichnis

Neues CA Zertifikat erzeugen

neues Server Zertifikat erstellen

sub-CA Zertifikat erstellen

.p12 Datei erzeugen

.....

.....

.....

.....

3

3

3

4

Zertifiats Authority



**CERTIFICATE
AUTHORITY**

Neues CA Zertifikat erzeugen

- <https://help.univention.com/t/how-to-extend-the-end-date-of-the-ucs-ca-root-certificate/9740>
- <https://help.univention.com/t/renewing-the-ssl-certificates/37>
- <https://help.univention.com/t/add-subject-alternative-names-to-existing-certificate/7433>
- <https://help.univention.com/t/cool-solution-creation-and-management-of-user-and-windows-certificates/11782>

neues Server Zertifikat erstellen

```
. /usr/share/univention-ssl/make-certificates.sh
declare -x ServerName=FQHN
univention-certificate new -name "${ServerName}" -days 1825
cd /etc/univention/ssl/${ServerName}
nano openssl.cnf
```

Ändern oder Anpassen der SAN auf ca Zeile 103. Die Zeile enthält bereits `subjectAltName = DNS:${ServerName}`, ... den FQDN und den einfachen Hostnamen. Es können kommagetrennt weitere SAN angegeben werden, wie z.B. `IP:1.2.3.4` oder `DNS:ein.anderer.hostname.domain`. Dann die Datei `openssl.cnf` speichern.

```
openssl req -new -key private.key -config openssl.cnf -out req.pem
openssl req -in req.pem -noout -text | grep -E "(Subject Alternative Name|DNS)"
univention-certificate renew -name ${ServerName} -days 1825
```

sub-CA Zertifikat erstellen

```
. /usr/share/univention-ssl/make-certificates.sh
declare -x ServerName=FQHN
```

```
univention-certificate new -name "${ServerName}" -days 1825
cd /etc/univention/ssl/${ServerName}
nano openssl.cnf
```

Ändern der [v3_req] Sektion, um Zeile 100:

```
[ v3_req ]
basicConstraints          = critical, CA:TRUE
keyUsage                  = cRLSign, keyCertSign
nsCertType                = sslCA, emailCA, objCA
subjectAltName            = email:copy
#issuerAltName            = issuer:copy
nsComment                 = This is a Fake Root CA Certificate
```

Bevor der Request unterschrieben werden kann muss das /etc/univention/ssl/openssl.cnf File angepasst werden. Diese Änderung unbedingt wieder rückgängig machen nach dem signieren des Requests! Ungefähr Zeile 100 ebenfalls in der [v3_req] Sektion

```
[ v3_req ]

basicConstraints = critica, CA:TRUE
keyUsage          = cRLSign, keyCertSign
#basicConstraints = critical, CA:FALSE
#keyUsage = nonRepudiation, digitalSignature, keyEncipherment
```

Danach den Zertifikatsrequest mit `openssl req -new -config openssl.cnf -key private.key -out req.pem` erstellen und dann von der CA unterschreiben lassen: `univention-certificate renew -name ${ServerName} -days 1825`

.p12 Datei erzeugen

```
export ServerName=my.domain.name
openssl pkcs12 -export -out /root/${ServerName}.p12 -in
/etc/univention/ssl/${ServerName}/cert.pem -inkey
/etc/univention/ssl/${ServerName}/private.key -passout
pass:xZtGhgBBt635mTapXzK
```

[Quelle](#)

From:

<https://aha-it.ch/wiki/> - **AHa-IT**

Permanent link:

<https://aha-it.ch/wiki/lx/ucs/ca?rev=1667835029>

Last update: **07.11.2022 15:30**

