Quick Guide

RMCARD 205/305

SSL-Zertifikat

1. Erstellen Sie einen Ordner "CA" und kopieren Sie openssl.cnf dorthin.

```
kevin@ubuntu:~$ mkdir CA
kevin@ubuntu:~$ cd CA
kevin@ubuntu:~/CA$ sudo cp /usr/lib/ssl/openssl.cnf ./
kevin@ubuntu:~/CA$ ls -l
total 12
-rw-r--r-- 1 root root 10845 Sep  4 17:03 openssl.cnf
kevin@ubuntu:~/CA$
```

2. Geben Sie "**openssl genrsa -des3 -out rootca.key 2048**" und das Passwort des Schlüssels ein.

```
kevin@ubuntu:~/CA$ openssl genrsa -des3 -out rootca.key 2048
Generating RSA private key, 2048 bit long modulus
..............+++
.....................................+++
e is 65537 (0x10001)
Enter pass phrase for rootca.key:
Verifying - Enter pass phrase for rootca.key:
kevin@ubuntu:~/CA$
```

3. Geben Sie "openssl req -new -key rootca.key -out rootca.req" ein und geben Sie die Informationen des RootCA-Zertifikat ein.

```
kevin@ubuntu:~/CA$ openssl req -new -key rootca.key -out rootca.req
Enter pass phrase for rootca.key:
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) [AU]:US
State or Province Name (full name) [Some-State]:Minnesota
Locality Name (eg, city) []:shakopee
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cyberpower
Organizational Unit Name (eg, section) []:firmware
Common Name (e.g. server FQDN or YOUR name) []:wr.frdistilling.com
Email Address []:test@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
kevin@ubuntu:~/CA$ _
```

4. Geben Sie "**openssl x509 -req -days 7305 -sha1 -extfile openssl.cnf -extensions v3_ca -signkey rootca.key -in rootca.req -out rootca.crt**" zur Erstellung des RootCA- Zertifikat.

```
kevin@ubuntu:~/CA$ openssl x509 -req -days 3650 -sha1 -extfile openssl.cnf -extensions v3_ca -signke
y rootca.key -in rootca.req -out rootca.crt
Signature ok
subject=/C=US/ST=Minnesota/L=shakopee/O=cyberpower/OU=firmware/CN=wr.frdistilling.com/emailAddress=t
est@gmail.com
Getting Private key
Enter pass phrase for rootca.key:
kevin@ubuntu:~/CA$ ls -l
total 24
-rw-r--r-- 1 root  root  10845 Sep  4 17:03 openssl.cnf
-rw-rw-r-- 1 kevin kevin  1456 Sep  4 17:15 rootca.crt
-rw-rw-r-- 1 kevin kevin  1743 Sep  4 17:06 rootca.key
-rw-rw-r-- 1 kevin kevin  1074 Sep  4 17:12 rootca.req
kevin@ubuntu:~/CA$ _
```

5. Geben Sie "**openssl genrsa -out server.key 2048**" ein, um den Serverschlüssel zu erstellen.

```
kevin@ubuntu:~/CA$ openssl genrsa -out server.key 2048
Generating RSA private key, 2048 bit long modulus
.........+++
............+++
e is 65537 (0x10001)
kevin@ubuntu:~/CA$ _
```

6. Geben Sie "**openssl req -new -key server.key -out server.req**" ein und geben Sie die Informationen zum Zertifikat ein.

```
kevin@ubuntu:~/CA$ openssl req -new -key server.key -out server.req
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) [AU]:US
State or Province Name (full name) [Some-State]:Minnesota
Locality Name (eg, city) []:shakopee
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cyberpower
Organizational Unit Name (eg, section) []:firmware
Common Name (e.g. server FQDN or YOUR name) []:chups01.wr.frdistilling.com
Email Address []:test@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
kevin@ubuntu:~/CA$ ls -l
total 32
-rw-r--r-- 1 root  root  10845 Sep  4 17:03 openssl.cnf
-rw-rw-r-- 1 kevin kevin  1456 Sep  4 17:15 rootca.crt
-rw-rw-r-- 1 kevin kevin  1743 Sep  4 17:06 rootca.key
-rw-rw-r-- 1 kevin kevin  1074 Sep  4 17:12 rootca.req
-rw-rw-r-- 1 kevin kevin  1679 Sep  4 17:18 server.key
-rw-rw-r-- 1 kevin kevin  1082 Sep  4 17:21 server.req
kevin@ubuntu:~/CA$
```

7. Geben Sie "**openssl x509 -req -days 3650 -sha1 -extfile openssl.cnf -extensions v3_req -CA rootca.crt -CAkey rootca.key -CAserial rootca.srl -CAcreateserial -in server.req -out server.crt**" zur Erstellung des Server Zertifikat.

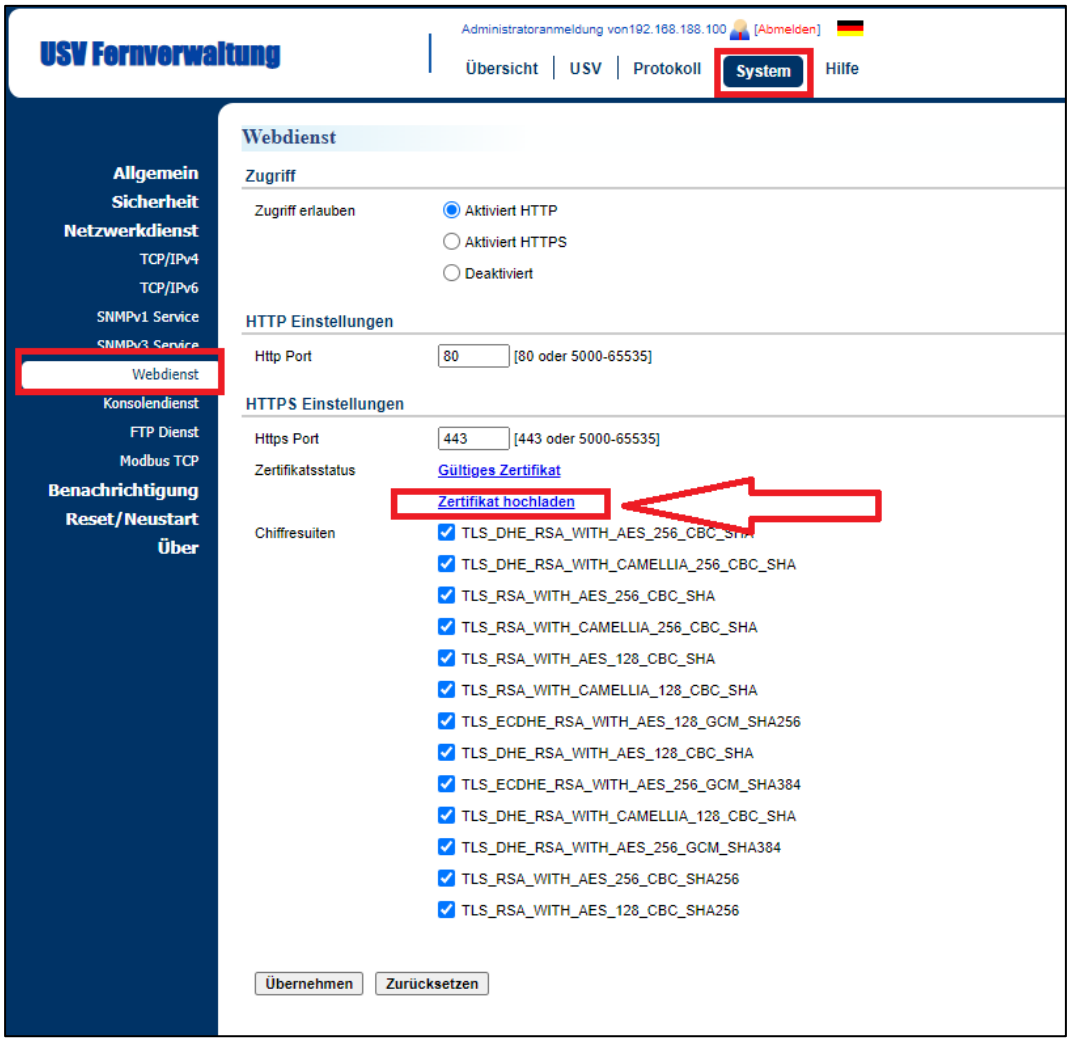
```
kevin@ubuntu:~/CA$ openssl x509 -req -days 3650 -sha1 -extfile openssl.cnf -extensions v3_req -CA ro
otca.crt -CAkey rootca.key -CAserial rootca.srl -CAcreateserial -in server.req -out server.crt
Signature ok
subject=/C=US/ST=Minnesota/L=shakopee/O=cyberpower/OU=firmware/CN=chups01.wr.frdistilling.com/emailA
ddress=test@gmail.com
Getting CA Private Key
Enter pass phrase for rootca.key:
kevin@ubuntu:~/CA$
```

8. Sie sehen dann die folgenden drei Dateien.

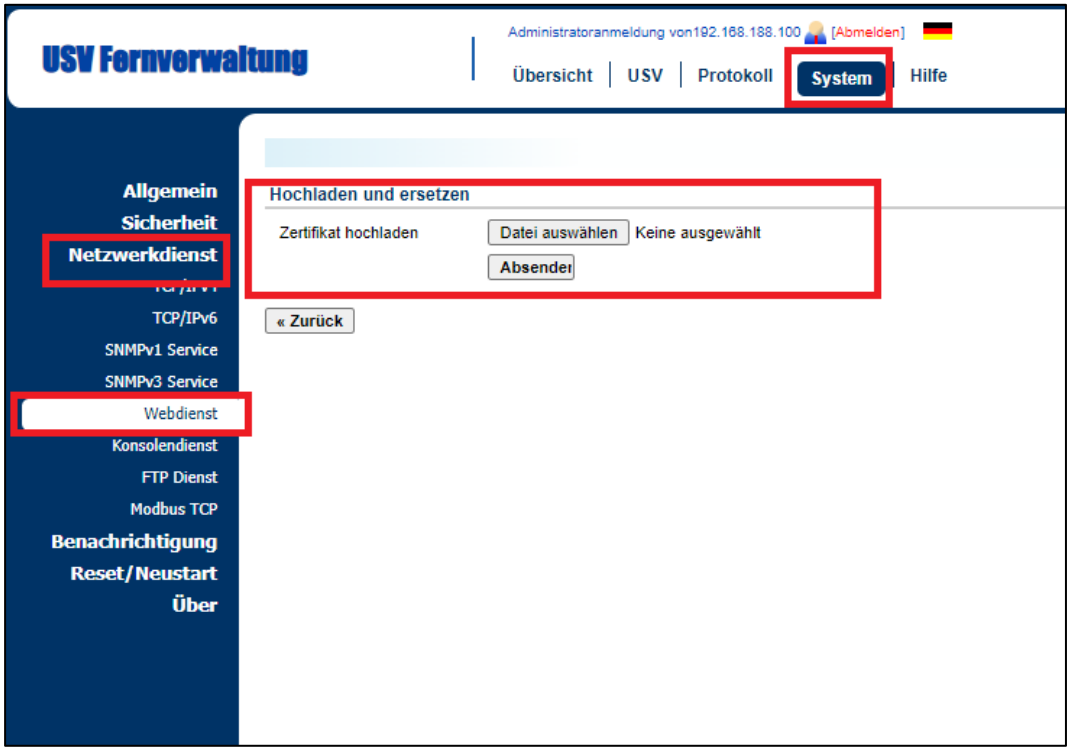
```
-rw-r--r-- 1 root  root  10845 Sep  4 17:03 openssl.cnf
-rw-rw-r-- 1 kevin kevin  1456 Sep  4 17:15 rootca.crt
-rw-rw-r-- 1 kevin kevin  1743 Sep  4 17:06 rootca.key
-rw-rw-r-- 1 kevin kevin  1074 Sep  4 17:12 rootca.req
-rw-rw-r-- 1 kevin kevin    17 Sep  4 17:26 rootca.srl
-rw-rw-r-- 1 kevin kevin  1395 Sep  4 17:26 server.crt
-rw-rw-r-- 1 kevin kevin  1679 Sep  4 17:18 server.key
-rw-rw-r-- 1 kevin kevin  1082 Sep  4 17:21 server.req
kevin@ubuntu:~/CA$
```

10. Erstellen Sie eine Datei mit dem Namen RMC.crt und fügen Sie den Inhalt der drei Dateien in diese Datei ein.

11. Die Weboberfläche der RMCARD öffnen unter
System >> Netzwerkservice >> Webservice >> „Zertifikat hochladen“



12. Laden Sie die Datei RMC.crt hoch.



13. Klicken Sie dann auf "Gültiges Zertifikat", um die Informationen über das Zertifikat anzuzeigen.