

CyberPower®

Quick Guide

RMCARD

SSL-Zertifikat erstellen

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 dann geben Sie die Informationen des RootCA-Zertifikats 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- Zertifikats.

```
kevin@ubuntu:~/CA$ openssl x509 -req -days 3650 -sha1 -extfile openssl.cnf -extensions v3_ca -signkey  
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=tes  
t@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
```

```

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$

```

zur Erstellung des Server Zertifikat. 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$

```

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

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxYyuu0ZFYyayVx1Jc/RnVVLxACUUEjyQC2+Yk84bSp6Buvz
kgzNSpgc8ER75cmIQT1fC9S09ALIIlTrLamVLGRHPBUu2/DmcFva51R62N3ThaG
adTgllebmgzY5n046bqSo+KIB19pgovJg291dpPAeHK6Iwi8KXhCCtACSRxKMI
JZTKDBPeT1IwCg93kukvH/za+GkX9YulcsvoYbJod423cRv9ZrB2cT26hrhXTdR
sWazJFQ7DopuxgdTQ8n0cmj9FJr/xk5r/CqgTSXS53Yc3qs8NneJtPL6FJ921vxV
lSsI9f5s0zr1J1dNyr91ubCH10Yn15XFJ2rYQ1DAQAABaIBAQCkQxQ9GcR5Cn
R5xkvb9Iaszc6S2p4NntvJ44EeNuTQar5LQs6h191JtsqLO+Lze0tB4D1YqFQA
100trJnU1SK0sU82AmbtVfs+XhDABuJSu600u0nmco49eQVJ1htu043rpgSVBxKe
j0B0dgpB0mufJb5gqduwI+rPmV1Nnyd00Jx8LuteCevmcTK+Hfrx4byPdyXJufhT
OrYl43l0cNSymJw1+6ux0sIsFKUNxawebDaer80dxAqu+7nd0T7/urYr7102Y4C
EBUelSXNS80xa7PcVmo+asJHHQV9TE715np2Ba+K7sq7JVkP8BnmmdQ1HC+n1e
JkMhx0adag0B915yadaJE/bMCI3ug01V0s4VfEDmCZrUkxJZ6U17rK0uV108e
y1KE4JVD8dtTh55k2Kv4pM6GtJ1fTt4up8hKGrB1/rpyYb422uW1H428gR3sV/
YIRP94zveedL18JSAHb1111b0g2aA2D0G6nXPhkG1PPav5fexXUKGSKPa0BANUR
19Q2Fu+su6JLk02PCTruU3x22/HaOVXU1s5t10u6ob1N8+Yqk6APkr2Dhbgnm77+
9JN/P13UF9u098JlmeVogVJFgVa1JykSN4zmR0EC9a2nVf3W1tPcKEVJchT1Taub
7EFBwQSZ4X1gJqJ0BxPpK9nz/WHtqSSUuKEp9bJAOGAbew8-K1M0u10RHu0nm3
9k1uW1H3Vv128xfk0eVcb4EhGaGimt932gM4JzkdxBLUf1SS8Bnuhgohxhu0or6
40/4TrHQssasAKYsrNseh0Jk0zEChomXV9F+NUJ8JChTvt696/uaq7U6uP/zJ6xv
Dgr/UC7uMhyoz1uJk0x0JbusCgYaf/N8tcYLgnmkGzIqOXvMq1VBAQnQBBGdY12
Px1kFJNvbtV5FAVKH12L0IkSkQ530zBT86ppJcd2QbACmFXNa7QX7N+89EKedycR
c2+m0qAdJmBrImk/2DkWE2MkMhZ3bddTdd3YhTP6K42I3F+JQ51WTA0x69k7
tqg3/wkGQCF8QWzGfTv/SdVaQWV5JJu0C12EK2mq3XUeM5CxmvaUpd66XX+
K0ABeDecRg0108Vc1VuuKc9p6aC0q967VerKbnJHRJ2zz5DKbxn6UfneFK1+
lLc0v7LkKmfJ177MkR6RZJfu24V9ATcULx5c5nrSJR4t5Dv4Au==
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIDDTCCAqSgAwIBAgIJAdeRTO26wuenMA0GCSqGSIb3QQEJBQUAMIG2M0suCQYD
VQQGEwVUZEEMBAAGIUECAwUJTMubmVzY3RmRREuYWV0QHQ0AHzaaGFnb3B1ZTET
MBEGA1UECgwKY311ZkUub3d1cJERMABGA1UECmZmlubXh0cmJkXHM0AAgVNBAMM
E3adyLnzG1zd61sbq1u2y5Jb20xHTAb8kghk1G9w0BCQEHOdr1c3RA221haWuu
Y291tB4XDTE4MDkuNDAsM1YyMfOXTD14NDkuMTA5M1YyMfOwEaCzA1BjBNVBAyT
A1VTRluEAY0VQ0IDA1Nak5U2XNvdGEtEAFBGNVBAcMCHNOYhtvcGV1MRMueQYD
VQQKDApJekJlcnBvd2VUMREuYWV0QHQ0AHmaXJtd2FyZTEKMGIA1UEAuu1Y2h1
CHMuMS53c15mcmRoc3RpbGxpbnmuY291tR0uGaUJKoZlInvcNAQBFg5O2XNOQGdt
Yw1S1mNvbTCCAS1uQ0Jk0ZlInvcNAQEBBQADgEPADCCAQoQggEABGMAGMCKRvWG
hsc1sdY3P021V18QA1FhscAtvmJP0G0qgbr85IMzRkoA9HPKyeXJ11k1HuwUqP
QdYJ6y2pzykRzuVLTvwsnBb2yKekt1tyR2hgHU4Fhm5hs20Zw+0m6kqP1A2fa
agL44NvZxaTuHhyu1M1vC1x8QgIAHEKv685J1IGUyggT3k5SFf1P95Lsb1v82vh1
qF7AMJkLLGMiyhEd8Ebu2auinE2eoa4V03a01msjT00w6kbsYhdUP79aoo/Rsa
f820u/wkkx010ud24t6PP231btY/Bsfdrb8VYkDcE+hDss9YXTK/dmum56g
pYUv349b8k0CAuFAAAaM8BwQ0YvROTBA1uADALBgNw08EBwMCEAu0DyJKozI
nvcNAQEFBQADgEBAcU1I28ML0k1NhnRgh+Yv53bPUGcvuc+44CJT0NNVNoFJkZ
doAch44ebR12h01sPLg9RmEVQcR5xhFPJCNm4fPc0VYTxuIn5pGHFP2cM0m7kK
JR1a++9oISmx03JAuA0oomLM33240TJfFMCAX6y7T+E1AcYdL/2Sph4uPXNvy
u0QB1R/SJ0j+7Ar01gonoVX7atg/FK/gBT24722xahHeknp2SscadJ/eogA1S1U
JIC64+Sx7S8ApungLa0VXh9ubrdaznDe6KEsRiY5AH7XVYUhusP240SutI+3Q
lpJ1kxMH45250abbkQpGdRTKmbvPeW5urJ1g8g=
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIEBzCCAu+gAwIBAgIJAkudu4N8IBzRMA0GCSqGSIb3QQEJBQUAMIG2M0suCQYD
VQQGEwVUZEEMBAAGIUECAwUJTMubmVzY3RmRREuYWV0QHQ0AHzaaGFnb3B1ZTET
MBEGA1UECgwKY311ZkUub3d1cJERMABGA1UECmZmlubXh0cmJkXHM0AAgVNBAMM
E3adyLnzG1zd61sbq1u2y5Jb20xHTAb8kghk1G9w0BCQEHOdr1c3RA221haWuu
Y291tB4XDTE4MDkuNDAsM1YyMfOXTD14NDkuMTA5M1YyMfOwEaCzA1BjBNVBAyT
A1VTRluEAY0VQ0IDA1Nak5U2XNvdGEtEAFBGNVBAcMCHNOYhtvcGV1MRMueQYD
VQQKDApJekJlcnBvd2VUMREuYWV0QHQ0AHmaXJtd2FyZTEKMGIA1UEAuu1Y2h1
CHMuMS53c15mcmRoc3RpbGxpbnmuY291tR0uGaUJKoZlInvcNAQBFg5O2XNOQGdt
Yw1S1mNvbTCCAS1uQ0Jk0ZlInvcNAQEBBQADgEPADCCAQoQggEABGMAGMCKRvWG
hsc1sdY3P021V18QA1FhscAtvmJP0G0qgbr85IMzRkoA9HPKyeXJ11k1HuwUqP
QdYJ6y2pzykRzuVLTvwsnBb2yKekt1tyR2hgHU4Fhm5hs20Zw+0m6kqP1A2fa
agL44NvZxaTuHhyu1M1vC1x8QgIAHEKv685J1IGUyggT3k5SFf1P95Lsb1v82vh1
qF7AMJkLLGMiyhEd8Ebu2auinE2eoa4V03a01msjT00w6kbsYhdUP79aoo/Rsa
f820u/wkkx010ud24t6PP231btY/Bsfdrb8VYkDcE+hDss9YXTK/dmum56g
pYUv349b8k0CAuFAAAaM8BwQ0YvROTBA1uADALBgNw08EBwMCEAu0DyJKozI
nvcNAQEFBQADgEBAcU1I28ML0k1NhnRgh+Yv53bPUGcvuc+44CJT0NNVNoFJkZ
doAch44ebR12h01sPLg9RmEVQcR5xhFPJCNm4fPc0VYTxuIn5pGHFP2cM0m7kK
JR1a++9oISmx03JAuA0oomLM33240TJfFMCAX6y7T+E1AcYdL/2Sph4uPXNvy
u0QB1R/SJ0j+7Ar01gonoVX7atg/FK/gBT24722xahHeknp2SscadJ/eogA1S1U
JIC64+Sx7S8ApungLa0VXh9ubrdaznDe6KEsRiY5AH7XVYUhusP240SutI+3Q
lpJ1kxMH45250abbkQpGdRTKmbvPeW5urJ1g8g=
-----END CERTIFICATE-----

"rootca.crt" 24L, 1456C written
kevin@ubuntu:~/CA$ _
```

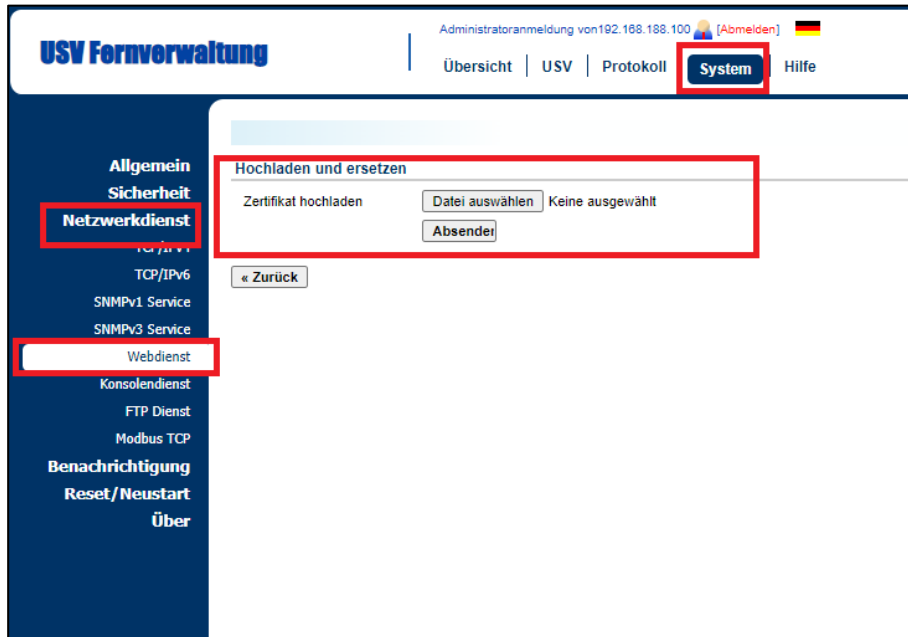
9. Die Weboberfläche der RMCARD öffnen unter System >> Netzwerkservice >> Webservice >> „Zertifikat hochladen“

The screenshot shows the 'USV Fernverwaltung' web interface. The top navigation bar includes 'System' and 'Hilfe'. The left sidebar lists various services, with 'Webdienst' highlighted in a red box. The main content area is titled 'Webdienst' and contains the following sections:

- Zugriff:** Radio buttons for 'Aktiviert HTTP' (selected), 'Aktiviert HTTPS', and 'Deaktiviert'.
- HTTP Einstellungen:** 'Http Port' set to 80.
- HTTPS Einstellungen:** 'Https Port' set to 443.
- Zertifikatsstatus:** A link for 'Gültiges Zertifikat' and a link for 'Zertifikat hochladen' (highlighted with a red box and arrow).
- Chiffresuiten:** A list of 15 TLS cipher suites, all of which are checked.

At the bottom of the configuration area, there are buttons for 'Übernehmen' and 'Zurücksetzen'.

10. Laden Sie die Datei **RMC.crt** hoch.



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





CyberPower

CyberPower | USV Systeme, PDU, Überspannungsschutz |
Professionelle Stromversorgung Lösungen

CyberPower Systems GmbH
Edisonstr. 16,
85716 Unterschleissheim
Germany

T: +49-89-1 222 166 -0 F: +49-89-1 222 166 -29

E-mail: service@cyberpower.de

Web: www.cyberpower.de

CyberPower Wiki: [Home](#) | [CyberPower Wiki \(cyberpowersystems.de\)](#)

CyberPower und das CyberPower-Logo sind Marken von Cyber Power Systems, Inc. und/oder verbundenen Unternehmen, die in vielen Ländern und Regionen registriert. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.

