

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) []:ur.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$

```

- 8. 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
kgZNSHpgc8ER75cmIq1fYc9So9AL IITrL amVL GRHPBUU2/DmcFva51R62N3ThaG
adTgUlebmGzY5n046bqSo+KIB19pgoV jg291dpAeHK6Iwi8KXHXCCtAcSRXrXKM1
JZTKDBPeT1IwCg93kuxvH/za+GwKX9YulcsvoybJod423cRv9ZrB2cT26hrhXTdr
sWazJFQ7DopuxgdTQ8n0cmj9FJr/xk5r/CqgTSXS53Yc3qs8NneJtPL6FJ921vxv
lSsISf5s0zr1j1dNyr9lucbCH10YNI5XfJ2rYtQIDAQAABAIQAQCkQXQ9GcR5CN
R5xkvb9IsazS62Sp4NntvJ44EeNuTQar5LQs6h191TsqLO+Lze0tB4D1YqFqA
I00trJnU1SK0sU8ZAmBtvfs+XHDABuJSu60ou0nmco49eQVJ1htu043rggSVBxKe
J0Bddgpb0mufJb5gqdufI+rPmV1Nnyd00Jx8LuteCevmcTK+Hfrx4byPdyXJUFhT
0rYl43lDcNSymUu1+6uxUsIsFKUNxawebDaer80dkAq+7nd0T7/uRyr7102Y4C
EBUeLsCXNS80xa7PcVmo+asJHHQV9TE715np2Ba+K7sq7JVKpABMmmdQ1HC+n1e
jKXhXcndag0B91SuydaJE/bMCI3ugQ1V0s4uVf0d+PZrU4XJ26u17rK0uV108e
y1KE4JVD8dtTh55kZKv4Pm6GtJ1FTT4upBshKGrB1/rpyYb422uW1H426Gr3sY/
YIRP94zveedL18JSAH8b111b0g2aa20G68nxPhK61PPav5fexXUKGSKPa0GBANUR
19Q2Fy+su6JLk02PcTruU3x22/HaOVXU1S5t10u6ob1N8+Yqk6APkR2Dhbzxm77+
9JN/P13UF9u098JlmeVogVJFqGva1JykSN4zmR0EC9a2NvF3W1TpcHEVJchT1Taub
7EFBwG24X1gJqJ0BXPfok9nz/WHTqSSUuKEp9bJaoGABeub+K1M0u10Rhw0nm3
9K1uW1H3Vy128xfk06vcb4EhGaGimt n32gM4JzkdXbLUF1SS8Bmubgohxhw0or6
40/4TrHQssakYsrNseh0J0kqzEChomXV9F+NUJ8JChTvt696/uaq7U6uP/zJ6xv
Dgr/UC7uMhyoz1uJk0x0JubScgYaf/N8tcYLgnmkGzIq0XvMq1VBAQnQBBGdY12
Px1kFJNvbtV5fAVK12L0IkSK530zBT86ppJcd2QbACmFNa7QX7N+89EKedyCR
c2+mQohAdJm8r1m1k/2DkWE2MkMH23bddTdd3YhTP6K42I3F+JQ51WTA0x69K7
tqy3/wkGQCF8QWzGfTv/SdVaQMVSJJu0C12EK2mq3XUeM5CxmvaupId66XX+
K0ABedecRg0108Vc1UuUkC3pu6aC0q9G7VerKbnJHRJ2zz5DKbxn6UfneFK1+
ILc0v7L1KmpfJ177MKR6RZJfu24V9ATcULX5c5nrSJR4t5Dv4Auu=
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIDTCCASG8wIBAgIUAQErT026uuenMA0GCSqGSIb3DQEBAQUAIGZMQsuCQYD
VQQGEwVUJESMBAGA1UECwwJTH1ubmVzbnRmREUwYVQ0HQDhzaGFnbnB1Z2TET
MBEGA1UECgwKYS11Z3Uub3JlcjERMARGA1UECwwJZm1ubXhkbXNjXHMARGA1UEAAM
E30dyLnzG1zd61sbG1u2y5Jb20xHTAb8Kqghk1G9u0BCQEHR1c3RAZ21haWuu
Y291tB4XDTE4MDkuNDAsM1YumfOXDTI4NDkuMTA5M1YumfOwgaEzA2A3BGNVBA
YTA1VTRlUeAYDQIDA1NAk5U2XNvdGExEAPBGNVBAcMCHNOYhtvcGV1MRMUEQYD
VQQKDApJekJlcnBvd2VUMREUwYVQ0LDAHMAJ1d2FyZTEKMGIA1UEAuuY2h1
CHMuMS53c15mcmRoc3RpbGxpbnmcuY291tR0uGwJKoZlhcNAQBFg5O2XNOQGdt
YV1SLmNvbTCCASUwQ0Jk0ZlhcNAQEBBQAGGEPADCCAAQCGEBAAGMCKRVRWG
hsc1sdY3P021V18QA1FhscAtvnmJPOG0qgbr85IMzRkoAYHPKyeXJ11K1HuwUqP
QdYJ6y2pzykRzuvLTw5nBb2uYkett1tr2hgHU4Fhm5hs20Zw+0m6kqP1A2fa
9qL44NvZxaTuHhyu1M1Vc18Q6IAHEK1688J1IGUyggT3k5SFf1P9SLsb1v82vh1
qF7AMJXLLGMjyHed8E8u2auuE2eoa4V03a0Im5jT00w6KbsYHdUP79Apo/RSa
f820u/wkK010ud2A16PP231btY/Bsfdrb8VYKpCEn+hdss9Y5XWK/dmum506
DYUv34908K0CAuFAAaM8BwCQYVROTBAUwDALBgNwH08EBwMCEAu0DyJKozI
nvcNAQEFBQADggEBACU1128ML0k1NhnRgh+YV53bPUgcvuc+44CJT0NNVnoFJkZ
hoAch44ebR12h0jSPLg9RmEVQcR5xfHPJ0Nm4fPc0VYTxuIn5pGHfP2cM0M7Kk
JR1a++9oISmX03JAUa0oomLGM33240TjFFMCAx6y7T+E1AcYdL/25Mph4UPXNY
uQB1R/SJ0j+7Ar01gonoVX7atg/FK/gBT4722xahHehKnp2SscadJ/eogA1S0
JIC604+Sx7S8ApungLaOVXh9ubrdaznDeB6KESrIy5AH7XVYUhuwP240SutI+3Q
lpJ1k5H45250abbkQpGdRTKmbvPeW5urJ1g8g=
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIEBzCCAu+gAuIBAgIJAkudu4N8IBzRMA0GCSqGSIb3DQEBAQUAIGZMQsuCQYD
VQQGEwVUJESMBAGA1UECwwJTH1ubmVzbnRmREUwYVQ0HQDhzaGFnbnB1Z2TET
MBEGA1UECgwKYS11Z3Uub3JlcjERMARGA1UECwwJZm1ubXhkbXNjXHMARGA1UEAAM
E30dyLnzG1zd61sbG1u2y5Jb20xHTAb8Kqghk1G9u0BCQEHR1c3RAZ21haWuu
Y291tB4XDTE4MDkuNDAsM1YumfOXDTI4NDkuMTA5M1YumfOwgaEzA2A3BGNVBA
YTA1VTRlUeAYDQIDA1NAk5U2XNvdGExEAPBGNVBAcMCHNOYhtvcGV1MRMUEQYD
VQQKDApJekJlcnBvd2VUMREUwYVQ0LDAHMAJ1d2FyZTEKMGIA1UEAuuY2h1
CHMuMS53c15mcmRoc3RpbGxpbnmcuY291tR0uGwJKoZlhcNAQBFg5O2XNOQGdt
YV1SLmNvbTCCASUwQ0Jk0ZlhcNAQEBBQAGGEPADCCAAQCGEBAAGMCKRVRWG
hsc1sdY3P021V18QA1FhscAtvnmJPOG0qgbr85IMzRkoAYHPKyeXJ11K1HuwUqP
QdYJ6y2pzykRzuvLTw5nBb2uYkett1tr2hgHU4Fhm5hs20Zw+0m6kqP1A2fa
9qL44NvZxaTuHhyu1M1Vc18Q6IAHEK1688J1IGUyggT3k5SFf1P9SLsb1v82vh1
qF7AMJXLLGMjyHed8E8u2auuE2eoa4V03a0Im5jT00w6KbsYHdUP79Apo/RSa
f820u/wkK010ud2A16PP231btY/Bsfdrb8VYKpCEn+hdss9Y5XWK/dmum506
DYUv34908K0CAuFAAaM8BwCQYVROTBAUwDALBgNwH08EBwMCEAu0DyJKozI
nvcNAQEFBQADggEBACU1128ML0k1NhnRgh+YV53bPUgcvuc+44CJT0NNVnoFJkZ
hoAch44ebR12h0jSPLg9RmEVQcR5xfHPJ0Nm4fPc0VYTxuIn5pGHfP2cM0M7Kk
JR1a++9oISmX03JAUa0oomLGM33240TjFFMCAx6y7T+E1AcYdL/25Mph4UPXNY
uQB1R/SJ0j+7Ar01gonoVX7atg/FK/gBT4722xahHehKnp2SscadJ/eogA1S0
JIC604+Sx7S8ApungLaOVXh9ubrdaznDeB6KESrIy5AH7XVYUhuwP240SutI+3Q
lpJ1k5H45250abbkQpGdRTKmbvPeW5urJ1g8g=
-----END CERTIFICATE-----

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

server.key

server.crt

rootca.crt

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

USV Fernverwaltung | Administratoranmeldung von 192.188.188.100 [Abmelden] | Übersicht | USV | Protokoll | **System** | Hilfe

Webdienst

Zugriff

Zugriff erlauben Aktiviert HTTP
 Aktiviert HTTPS
 Deaktiviert

HTTP Einstellungen

Http Port [80 oder 5000-65535]

HTTPS Einstellungen

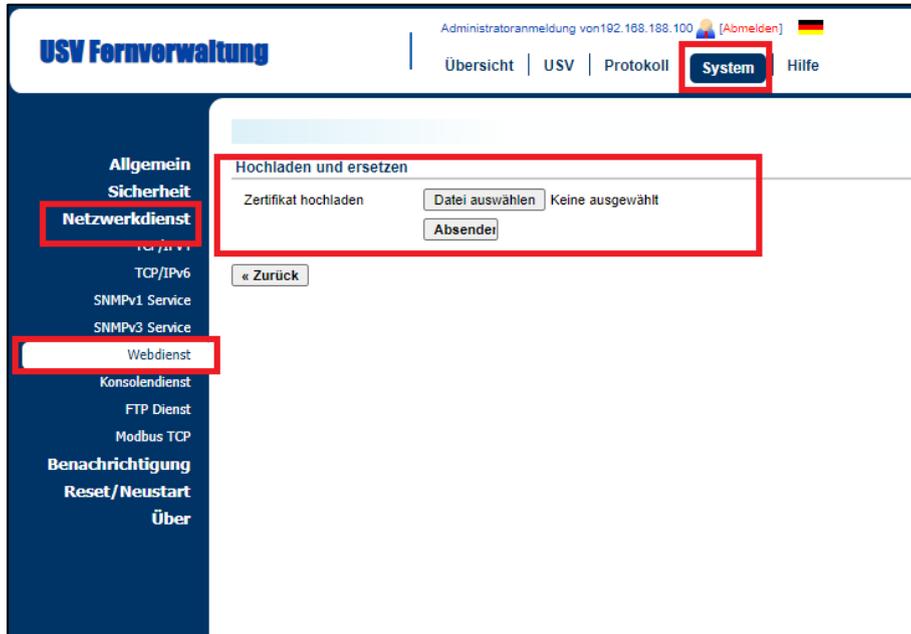
Https Port [443 oder 5000-65535]

Zertifikatsstatus [Gültiges Zertifikat](#)
[Zertifikat hochladen](#)

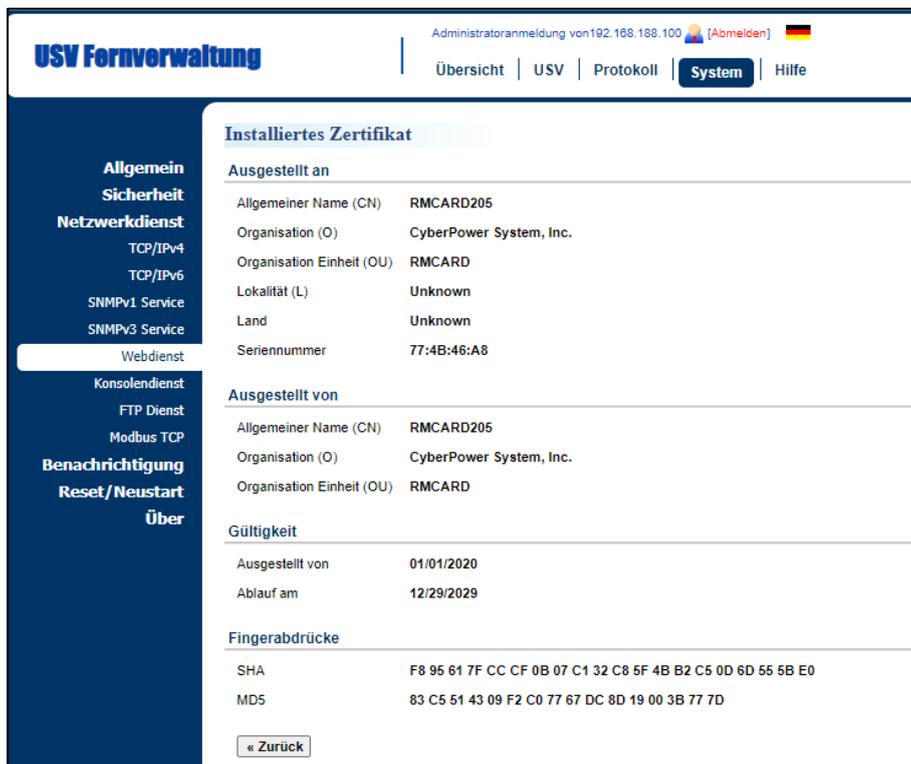
Chiffresuiten

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

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 \(cyberpowersystems.de\)](http://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.

