



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 -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=test@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 rootca.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/emailAddress=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.

```

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxYYxuo2FVyaayVx1jC/RnVWLxACUUExyQC2+YkB4bSp6Buvz
<gzNGShpgc8ErJ5cmHIqIfC9So9ALi1TrLamvLGRHPBUu2/DmcFva5iR62W3JhaG
AdTgUebm6Zy5nD46bqSo+KIB19ppqvJg291dpAeHK6Iwi8KXHXcCIacSRXrxKMj
JZTKCBPeT1IwC93kuxvW/za+GwKX9Yw1csvovbJod423cRv3zrB2cT26hrhXTdr
zWazJPQ7DopuxgdtQ8n0CmJ9Fjr/xk5r/CgqTSX53Yc3qs8NneJtPL8FJ92tvxV
iSsIsfS0zr1j1dNYr91ubCH10YN15xfj2ryTQIDAQAABAQIBAQC1KqZKXQ9GCR5cN
95xkvb9IsazSc62Sp4WntvJ44EeNuTQar5iXqs6h19IJSqL0+0Lze0tB4D1YqFqA
IODtrJnU1SKD5U8ZAMbtvFs+XHDAABUJSu60ow0nmco49e0VJ1htw43rvggSVBxWe
D0Bddgp8DmPpJb5bqdwfI+RPMvINnyd0Djx81uteCevmcTK+Hfrx4byPdyXJUfhT
0rYi43IOcNSymUwL+6uxXsIsFKUNxnaweGDaerB0xkAq+7nd0W7/wRyR7102Y4C
EBUElSXCNs80xa7PcYm0+asJhHqV9TE7i5Wp2Ba+k7sq7jVkpA8WmgmdQIHC+nIe
jXNhxQAdAoGBA01SyodaJE/bWCY3ygg1vDs/uvfEd+C2rU4xj26uY7rKbUv0108c
yIkE4jVDSdtThN5sk2Kv4pH6cTjTfTf4wpBshKGrG1/rpyYb4z2/wiH42GGRJSV/
YIRP94Zxe6dL18iSAbBii1bpbq2aA2DCGGnxPhKGiPPav5fexXUKGskPAoGBANUR
19QZFy+su6JLK0ZPcTheJ3x22/HaDVXU1s5t10u6ob1W8+Ygk6APkr2dhbgxm77+
3JN/P13UF9w098JImeVogVJFwGvaLiikSN42mR0EC9a2hVf3WipcWjEVJChT1Taub
7EFBw3S241lgJQ08XpFok9nz/WHtqSSUuKEp9bJAoGAbewB+K1M01wJ0RhwDnm3
PklWuH13V9y128xfKofvcb4EhGaGImtn32GM4jzkKXbLuf1SSSBNubgohxhw0or6
+/04TrNq0SssAkYsrNseh0j0KpzEChOmXV9F+MJBjChTYut696/uqQ7u6uP/zJ6w
DGr/uc7uMhyoz1wUkOxUBwsCgYaf/N8tcYlgnm6KgZIQ0xvMqiYBAQRQBBGdYi2
Px1HfjNvbtV5FvKkH1zL01ksKQ530zBtBgpjCdzQbAcMfXNa7QX7N+89EKdeyCR
z2+mDqhAdJmBr1m1k/2QkWE2MKMz3bdqTDD3YhTP6KM2I3F+JQ51WtA0xS6g9K7
tqy3/wkBgQCFF80QwZGfTv/SdVaQMV5jJuoC12Ek2mqqa3YEXuMC5xmvawIpd66XX+
KQAYGDBecHgD108VCIvuuK3puS6aCq9rG7YerKNbnJHRz2z9Dbkx8n9fneFKi+
LLcov7Lv1kryfK177WkBR52Jfw24v9ATcsULx5c5nrSJR4t5DdV4Aw==
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIIDTCCAsGgAwIBAgIJA0ErT026wwenMAOGCSqGSIb3DQEBAQUAMIG2MQswCQYD
VQQGEwVUzESMBAGA1UECAwJTWlubmVzb3RhbmRwDyVQQHDAhzaGFrb3B1Z2E0
MBEGA1UECgwKvY31i2XJub3d1c1JERMA8GA1UECwwiZm1yb3dhdhcnUxHDAaBgNVBAMM
E3dylmZy21zdg1sbG1u2y5Jb20xHTAbBgkqhkiG9w0BCQEWDnR1c3RAZ21haWw
y29tM4XDTE4MDkwNDAS5jYyMFOxDTI4MDkwMTA5MjYyMFowgaExCzAJBgNVBAYT
A1VTRMRlWEAYDVoQIDA1NAh5u2XNvdGEExTAPBgNVBACMCHNoYkYvcG9V1MRMwEQYD
VoQKDApJekJ1cnBvd2VyMREwDyVQQLDAhmaXJtd2Fy2TEkMGA1UEAwwbY2h1
cHMwS53c15mcmR3c3RpbGxpbmV29tMR0wGyVJKozThvcNAQkBFg502XNOQgdT
YW1sLmNvb2CCAsIwdQYJKozThvcNAQEBBQADgEPADCCAQoCggEBAMWGMckGRVWG
ms1cdY3P021V18QA1FHsckAtvmJPD0qdeqbr85IMzRkOaYHPBKyeXJ11HwUuqP
QcyJU6y2pryxkRzwVLtw5nBb2uYket1tYR2hgHU4FHm5hs20Zw+0m6kqP1iAZfa
3oL44Nz2XaTuWihyuiIvC18qQIAHEKv68Sj1lGUyggT3k55FNIpD5Lsb1v82vhl
oF/WHJXL6MmyaHeGd3E92awdnE2eoa4V03a81msyT00w6KbsYhbUPJ9Apo/RSa
/8Z0a/wokK010ud2AtrPD231bTy/Bsfdrb8VYkrCEn+bdS69Y5TK/dmoh5dG
DyUv349q8k0CAwEAAMaMBwCQYDVROTBAAIwADALBgNVHQEBAMCBeAwDQYJKozI
hvcNAQEFBQADgEBACUJ12BMLDk1NhNrgH+XV53bPUGcvuc+ac4JTONNVNPFjgkz
doAch44ebR12h0iSPLg9RmEVQcRsfHPjCNm4fPcOvYTYxTh5pXHGfP2cM0m7kK
JR1a++9qJ5mx03JAUAo0omLGM3z4GTjffMCAx6y7T+EiAcYyLd/2sWph4uPXWYy
+uQBIR/SJ8j+7ArdIgonovK7atg/FK/gBT247Z2xahHehKnp2SscaoDj/eogA1Su
jJc604+Sx7s8ApungLaOYCXh9yBrdaznDeB6KEsRIy5AH7XYAUhwsP24pSutI+3Q
lpJikSH4S25DabbkQPGdRTKmbbvePW5wrJ1g8g=
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIIEBzCCAu+gAwIBAgIJA0Mudu4N8IBzRMAOGCSqGSIb3DQEBAQUAMIG2MQswCQYD
VQQGEwVUzESMBAGA1UECAwJTWlubmVzb3RhbmRwDyVQQHDAhzaGFrb3B1Z2E0
MBEGA1UECgwKvY31i2XJub3d1c1JERMA8GA1UECwwiZm1yb3dhdhcnUxHDAaBgNVBAMM
E3dylmZy21zdg1sbG1u2y5Jb20xHTAbBgkqhkiG9w0BCQEWDnR1c3RAZ21haWw
y29tM4XDTE4MDkwNDAS5jYyMFOxDTI4MDkwMTA5MjYyMFowgaExCzAJBgNVBAYT
A1VTRMRlWEAYDVoQIDA1NAh5u2XNvdGEExTAPBgNVBACMCHNoYkYvcG9V1MRMwEQYD
VoQKDApJekJ1cnBvd2VyMREwDyVQQLDAhmaXJtd2Fy2TEkMGA1UEAwwbY2h1
cHMwS53c15mcmR3c3RpbGxpbmV29tMR0wGyVJKozThvcNAQkBFg502XNOQgdT
YW1sLmNvb2CCAsIwdQYJKozThvcNAQEBBQADgEPADCCAQoCggEBAMWGMckGRVWG
ggEiMAOGCSqGSIb3DQEBAQUAA4IBDwAwggEKAAoIBAQDxSRUf1PH1RFJqAq1cc411
46DFURlIx4ttduj7mBWq0Um1GpWnBH/n5ciqgPuUVc8Ijfeh1IHT4ND+FX2d27W
sY10/NGCPLEvt59A0IUG3ANJj9ptnRds0s9J19egfGTyrNmZi/DoQ/LukTjYhPR1W
+Z5j0Aym5bW25CxlqJ21CK3zUjB9Jfua0TcQXD2MHWDcoUkD11/cRu8CNXhm4Hd
bbbb1ekDCLbPgpucML25MqnIj1DzeEapaJd+v120MMKGR0vIYCGA2qMfkaDw8++
E/D14/TUbfdHD7xc16TdmZub/hgoLmIDr0E0AUGbcfb2/GPGSRXCbk5Bn3tk3Kqo9
AgMBAAGjJUDBOmB0GA1udDgQWBBTpadyM/g5tI7/OePdG1Jr1xWsd+JAfBgNVHSM
EGBAwgBtpadyM/g5tI7/OePdG1Jr1xWsd+JAMBgNVHRMBETADAQH/MAOGCSqGSIb3
DQEBAQUAA4IBAQB81oTo1zN8cmGy209+oyB/AB+0bX3/abPYz21LsBgd01gEs/J
E7+/KZwskradIkgEAD1GKJtXUqRqGDRcH+pLF+FNR1WcmY/8sh/FtKpQ5Vv24
fXajxwY0Mvp908nuY3zD5z/1EyemUBcMfPytCCO+KBPShPG8F5dXAB1t3Uj3zy7k
t4zgt6oHL1IU1b533E9e2Ic5iH0Tgm5A2jq0BoN+DsfIRnoXGjJqH4Rov8UA500P
3QDxYbHtC1e40VYVX7hsS2JtWhFb1aC3oDZy7XdfN1NNVqSjmdRP3iVwoIKgG0
KpMNXJyx3ItKER1rTeUPY3NJ2S9nImbvas
-----END CERTIFICATE-----

~
~
~
~
~
~
~
~
~

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

```

server.key

server.crt

rootca.crt

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

The screenshot shows the 'USV Fernverwaltung' web interface. The top navigation bar includes 'Übersicht', 'USV', 'Protokoll', 'System' (highlighted with a red box), and 'Hilfe'. The left sidebar contains a menu with categories: 'Allgemein', 'Sicherheit', 'Netzwerkdienst', 'Benachrichtigung', and 'Über'. Under 'Netzwerkdienst', 'Webdienst' is highlighted with a red box. The main content area is titled 'Webdienst' and contains the following sections:

- Zugriff:** 'Zugriff erlauben' with radio buttons for 'Aktiviert HTTP' (selected), 'Aktiviert HTTPS', and 'Deaktiviert'.
- HTTP Einstellungen:** 'Http Port' set to '80' (range: [80 oder 5000-65535]).
- HTTPS Einstellungen:** 'Https Port' set to '443' (range: [443 oder 5000-65535]).
- Zertifikatsstatus:** 'Gültiges Zertifikat' and a link 'Zertifikat hochladen' (highlighted with a red box and a red arrow).
- Chiffresuiten:** A list of 14 TLS cipher suites, all of which are checked.

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

12. Laden Sie die Datei RMC.crt hoch.

The screenshot shows the 'USV Fernverwaltung' web interface. At the top right, there is a navigation bar with 'Übersicht', 'USV', 'Protokoll', 'System' (highlighted with a red box), and 'Hilfe'. Above 'System' is a user status bar: 'Administratoranmeldung von 192.188.188.100' with a user icon, '[Abmelden]', and a German flag. On the left is a dark blue sidebar menu with categories: 'Allgemein', 'Sicherheit', 'Netzwerkdienst' (highlighted with a red box), 'Konsolendienst', and 'Benachrichtigung'. Under 'Netzwerkdienst', 'Webdienst' is highlighted with a red box. The main content area is titled 'Hochladen und ersetzen' (highlighted with a red box) and contains the text 'Zertifikat hochladen' followed by a 'Datei auswählen' button and the text 'Keine ausgewählt'. Below this is an 'Absenden' button. At the bottom left of the main area is a '« Zurück' button.

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

USV Fernverwaltung | Administratoranmeldung von 192.168.188.100 [Abmelden]

Übersicht | USV | Protokoll | **System** | Hilfe

Allgemein
Sicherheit
Netzwerkdienst
TCP/IPv4
TCP/IPv6
SNMPv1 Service
SNMPv3 Service
Webdienst
Konsolendienst
FTP Dienst
Modbus TCP
Benachrichtigung
Reset/Neustart
Über

Installiertes Zertifikat

Ausgestellt an

Allgemeiner Name (CN)	RMCARD205
Organisation (O)	CyberPower System, Inc.
Organisation Einheit (OU)	RMCARD
Lokalität (L)	Unknown
Land	Unknown
Seriennummer	77:4B:46:A8

Ausgestellt von

Allgemeiner Name (CN)	RMCARD205
Organisation (O)	CyberPower System, Inc.
Organisation Einheit (OU)	RMCARD

Gültigkeit

Ausgestellt von	01/01/2020
Ablauf am	12/29/2029

Fingerabdrücke

SHA	F8 95 61 7F CC CF 0B 07 C1 32 C8 5F 4B B2 C5 0D 6D 55 5B E0
MD5	83 C5 51 43 09 F2 C0 77 67 DC 8D 19 00 3B 77 7D

[« Zurück](#)