How to Create Certificates and CA Certificates

Introduction

To avoid a warning when you log into your mPower device that your connection is not private or that the source can't be verified, you must have a signed certificate using a verifiable signing certificate (typically from a third-party Certifying Authority) for that particular device. This document reviews the basics of certificates and describes two methods of creating certificates (including how to be your own Certifying Authority which is helpful if you are planning to create a secure network from scratch).

Basics

Certificates provide an added level of assurance for web users. They verify the subject of the certificate matches the hostname/DNS name and is the entity that it claims to be (this is commonly done through third party verification). This is not an indication of the degree of security features on the device or specific risks with using it. It's about authentication - verifying the identity of the organization behind the connection.

There are two types of certificates: 1) Certifying Authority (CA) certificates and 2) Signed certificates. Under signed certificates, they can be self-signed or signed by a signing authority using a verifiable CA certificate. Self-signed certificates are less reliable because they are not signed by a Certificate Authority, thus weakening authentication.

A CA certificate is used in conjunction with a signed certificate and public-private key pair. The signed certificate is generated based on the CA certificate creating a chain of trust for the client or server in question. The CA certificate verifies the signed certificate using its public key. The most common example of this is HTTPS. You need both certificates for this to work properly.

There are three ways to obtain certificates:

- pay to have your certificate signed by a third-party certifying authority such as DigiCert, Verisign, or others (NOTE: you may want to ask your IT department who they use for digital certificates if your company already has a relationship with a certifying authority firm.)
- create a self-signed certificate which provides less assurance of the certificate owner's identity than the other two methods (if you choose to do this, you can either generate your own or we recommend using the Generate Certificate feature in the device UI to automatically ensure the file is properly formatted). NOTE: This is the default on mPower devices.
- create your own CA and corresponding signed certificate files using a software tool like openssl or others.

NOTE: Do **NOT** use a Microsoft Windows-based tool unless the file is saved in the proper format (.pem). You must first create and upload the CA certificate to the device UI before the corresponding signed certificate. If you do not use the proper format for each certificate, the system does not upload the file.

For more information about certificates, refer to the following:

https://darutk.medium.com/illustrated-x-509-certificate-84aece2c5c2e

https://adamtheautomator.com/x509-certificates/

This document reviews the steps for two different methods:

1. Creating a self-signed certificate
2. Creating a CA Certificate and corresponding signed certificate.

Method 1: Create a self-signed certificate

Prerequisites

Before starting, you need:

1. A target device using mPower (including MTR, Conduit, MTCAP, IP67, or Conduit3) with an IP address.
2. A Windows client machine (for this example, a PC using windows 10).
3. To assign an IP address via DHCP or static but the DNS server should assign a DNS name to the device (for this example, my device has a DNS name device.mts.test).
4. An Ubuntu machine with openssl on it.

Self-signed certificates are typically used internally within labs or business environments. These certificates are not used externally for commercial use as they're not from a trusted third-party certificate authority. Only trusted certificate authorities (CA) can issue SSL/TLS certificates for commercial use in the public domains.

If you install a self-signed certificate on a public website or entity, upon accessing the IP address, a user's web browser displays a message that the resource can't be trusted (i.e. the certificate installed isn't signed by a trusted third-party) and prompts you to not advance or not.

When creating a self-signed certificate, you must first create a server private key. This key should stay private and be stored on the server. It should not be shared externally. The private key is used to then generate a public certificate that you can share with others.

A Certificate signing request or CSR is the mechanism used to provide details of the entity and the resource you want to incorporate into the request.

1. To create a private key and CSR, run the following command below:

```
openssl req -new -days 365 -key webserver.pem -out webserver.csr
```

What the above command means:

-new: create a new request

-days: the number of days for which the certificate should be valid. Use as high a number as you feel comfortable with for your development environment.

-key: Generate private key with filename webserver.pem

-out: the name of the target .csr file to which the command writes.

NOTE: This command can be done all in one programmatically rather than interactively.

Example terminal output:

```
root@user:~/Documents/certificates# openssl req -new -days 365 -key
webserver.pem -out webserver.csr 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]:MN Locality Name (eg,
city) []:MINNEAPOLIS
Organization Name (eg, company) [Internet
Widgits Pty Ltd]:MULTITECH Organizational Unit
Name (eg, section) []:SUPPORT
Common Name (e.g. server FQDN or YOUR name)
[]:device.mts.test Email Address
[]:user.foobar@multitech.com

Please enter the following
'extra' attributes to be
sent with your certificate
request
A challenge password []:
An optional company name []:
```

2. Create a v3.ext file. Only an X.509 v3 certificate carries SAN information. This requires an additional file containing the v3 information when creating an X.509 v1 certificate. Create a file named v3.ext with the following information:

```
root@user:~/Documents/certif
icates # cat v3.ext
authorityKeyIdentifier=keyid
,issuer subjectAltName =
@alt_names
[alt_names]
DNS.1 = device.mts.test
```

The alt_names section specifies the domains which are valid for this certificate.

3. After the private key, CSR, and v3.ext files have been generated, create a Self-Signed Certificate. Run the following commands to create a self-signed SSL certificate.

   ```
   openssl x509 -in webserver.csr -out webserver.crt -req -signkey
   webserver.pem -days 500 -extfile v3.ext
   ```

   NOTE: v3.ext file is not required to create a self-signed certificate. You may include the organizational details from the file in the command as shown in this alternative example.

   ```
   openssl req x509 -nodes -days 3650 –subj '/c=US/ST=MN/L=St.
   Paul/CN=my.domain.com' –new key rsa=2048 –keyout=key.pem -out crt.pem
   ```

   Example terminal output:

   ```
   root@user:~/Documents/certificates# openssl x509 -in webserver.csr -out
   webserver.crt -req -signkey webserver.pem -days 500 -extfile v3.ext
   Signature ok
   subject=C = US, ST = MN, L = MINNEAPOLIS, O = MULTITECH, OU =
    SUPPORT, CN = device.mts.test, emailAddress =
    darshan.maiya@multitech.com
   Getting Private key
   ```

4. After you have generated all the required files, upload the private key and the certificate to the target device.

   Example terminal output:

```
root@user:~/Documents/certificates# cat webserver.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAnVPwf5OxEdmKyf38F0uyki0GP80D3PF5Zb4
FYGtj1SayseJgZXC8kIzyoNb0/ksLqpSzV1J//aJwSKhpTUrJJaD1uqK
gPNk/3qS/RpI8ioq3BrIIxd5RQCaL63t2cnUG1xCWk/ezT7aYer0du
Bt18fEtBts7kyY7zTD4RjCm80SgRb0yOvHiz0TxLGSMUk5ViUFsKv4
p0zElqUkTViFeGW23nfmB+mWVGoLwp10HSLCRt36UTWj4EwH
DXsBElK2JOlJOc93XIwnWvxyu8r9Gcxds5ECdgZFZnAQWAj0d0RE
d6rfp9/w/sM5KcFyJLNPEehTPepoVwHnNvxL4nPYsxQIDAQABAoI
BAQCXdzOoL5Ge5LiY5VxpNSiTUKOekwtwEE7W5A2bGWjA0oPhf
Fdf8hyocfo5XRn7JFb0ADt1C2lLz7KYUQMoNaLYBlHtQBpS2rmB6
Ux5bdq5avjwikCl9vZ0c2fr6y5K3V4bec3uYOASE3JTYHUXReDUcG
PwIOsHLR0P3GB6euaQdvPf5wFnDza/TxJEyIRSrPHyqQUf1obU8g
WQkDGyLOyGc4A+kn9ISrODDTn2ORbCoBldV8bcdkIVPttA8waw
dZr6Daq+KkZ8/WJ3O7No6x1WzG7gEPe1UkCUHsjMHVXf+RxGlvJ
flyqPDRaUR5CqyvfmobIHANUn8zkUMmyuW3gBAoGBAM5F5Zx
QEcCegaDF3n/6pCFylL/BLsQ5WxgorQ+Vr5xOqtkt7rIzUjH4IMgL4
YJyVB7Mp6H5vnuoE0GAGS2lLK5oigTttNsG17ttTyZqCzlNtaKqd4S
9fJLiUIMlG33Y05oCHO9lzSGrDPi0YQjXGuX2z9K9jCAIRCiZSGsLJPI
BAoGBAMNBZtNuWisAP+nmTrN+SCeNihn6rhp5ASTf4bDdv43m
mD1DIuJ2c6QgVu6LZRHLtQBJYDkTA+mRL1FZMDS5C0hQKbOWq
2Lam9op6gWH81lx/ocR8mKvodTOmXocM+MdKZanp29hcdcWJ
```

```
wXdLeTkL6ZpwA+bQ+oF5gsaib/Gw/LFAoGAXcl+GtJ1H+Vx/w24
muv1UJfudjl58BI8DwH/ngRrMmC6YcD2tOOMzdeJ4Cs2v78H7HE
VDxqkt0i2aKO7zvs5E5vIlXEXODcmQ7vxrv+sVsO0gF+NtDcLuyVXg
imPFGtP2sh3K4pX+KTzYulw7ToQqtrLp4AzhCT+CI+ZU8JfbAECgYB
McXyKZnfSwgRD1LEXQOeK5LUeurATGTDDeQtpLUfjjFYqFfDAbN
OVfDvMpLJrJy+z7wZHEhTECt1Voe9nlNK/+vJ4pxJuX1wJK8O9ap5
xdFnME9Crpktbf49C6Wu/DRnNK9I3nxTsunWIrDFdnaCyLFDPS2B
pbOnFixxHAtCQaQKBgQCYRI1tH0kOYBr4yY4pRMoW4DPWrVWb
m/J6szjR9hffzZeP4ue9ste4fCESoiAzhjqGzPJl7dmBaTFD0OR5gPs6
imtBGUrbCg8PBKUDMzqZu2rJUE8T11SnhQVs9bIAeVWJjj1Y1l6P
HsyPMWgYvbjP80i1IVExSINJtRsz2q0dgQ==
-----END RSA PRIVATE KEY-----
root@user:~/Documents/certificates# cat webserver.crt
-----BEGIN CERTIFICATE-----
MIIErTCCA5WgAwIBAgIJALkDZPqJ1+17MA0GCSqGSIb3DQEBCwUAMI
GcMQswCQYDVQQGEwJVUzELMAkGA1UECAwCTU4xFDASBgNVBAc
MC01JTk5FQVBPTElTMRIwEAYDVQQKDAlNVUxUSVRFQ0gxEDAOBgN
VBAsMB1NVUFBPUlQxGDAWBgNVBAMMD2RldmljZS5tdHMudGVzd
DEqMCgGCSqGSIb3DQEJARYbZGFyc2hhbi5tYWl5YUBtdWx0aXRlY2gu
Y29tMB4XDTE5MDYxODIwMTQxNVoXDTIwMTAzMDIwMTQxNVowg
ZwxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJNTjEUMBIGA1UEBwwLT
UlOTkVBUE9MSVMxEjAQBgNVBAoMCU1VTFRJVEVDSDEQMA4GA1U
ECwwHU1VQUE9SVDEYMBYGA1UEAwwPZGV2aWNlLm10cy50ZXN0
MSowKAYJKoZIhvcNAQkBFhtkYXJzaGFuLm1haXlhQG11bHRpdGVjaC5
jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCdU/B/
k7ER2YrJ/fwXS7KSLQY/zQPc8XllvgVga2PVJrKx4mBlcLyQjPKg1vT+Swu
qlLNXUn/9onBIqGlNSskloPW6oqA82T/epL9GkjyKircGsgjF3lFAJovre3Z
ydQbXEJaT97NPtph6vR24G3Xx8S0G2zuTJjvNMPhGMKbzRKBFvTI68e
LPRPEsZIxSTlWJQWwq/inTMSWpSRNWIV4Zbbed+YH6ZZUagvCnXQdI
sJG3fpRNaPgTAcNewESUrYk6Uk5z3dcjCda/HK7yv0ZzF2zkQJ2BkVmcB
BYCPR3RER3qt+n3/D+wzkpwXIks08R6FM96mhXAec2/Evic9izFAgMB
AAGjge8wgewwgbsGA1UdIwSBszCBsKGBoqSBnzCBnDELMAkGA1UE
BhMCVVMxCzAJBgNVBAgMAk1OMRQwEgYDVQQHDAtNSU5ORUFQT
0xJUzESMBAGA1UECgwJTVVMVElURUNIMRAwDgYDVQQLDAdTVVB
QT1JUMRgwFgYDVQQDDA9kZXZpY2UubXRzLnRlc3QxKjAoBgkqhkiG9
w0BCQEWG2RhcnNoYW4ubWFpeWFAbXVsdGl0ZWNoLmNvbYIJALk
DZPqJ1+17MCwGA1UdEQQlMCOCD2RldmljZS5tdHMudGVzdIIQZGV2
aWNlMS5tdHMudGVzdDANBgkqhkiG9w0BAQsFAAOCAQEAg823J
d65V7DhDIIjNjuUHgO1mmYNfLtlmKB5nT9rjRejAT1D/k4HDJH7En
YXOm/FB58KoWUKD5Wls0tmcmDVv2rMxTtcO1Y7I29L5h0jLeHU
HJgFuA7hx9/2Lwj/CW/rNsrDGM3q86MI3x4EjqO6Lmxl075j7dJz3
N4Z1wofwYgCmb5Z04fv4XirxkfXJ4IZXhiNpbLHk8LOdClHzlnEO864
BXxoy1Tz8HCcK+MGcKODrWEYB0EclYjINa9VqX1WaSoOXuUqiW7
YVYfWckjW5G8Dtt5djySXw3mB+DNhRWhKDYgEoLt0b0UEb6Li2I
N8DIxpJEAfjsCvTUkjDg 1w==
-----END CERTIFICATE-----
```

5. From the above two outputs, create a .crt file which looks like the following example. Upload this certificate to the target device in the UI under **Administration > x.509 Certificate > Upload**.

```
-----BEGIN CERTIFICATE-----
MIIErTCCA5WgAwIBAgIJALkDZPqJ1+17MA0GCSqGSIb3DQEBCwUAM
IGcMQswCQYDVQQGEwJVUzELMAkGA1UECAwCTU4xFDASBgNVBAc
MC01JTk5FQVBPTElTMRIwEAYDVQQKDAlNVUxUSVRFQ0gxEDAOBgN
VBAsMB1NVUFBPUlQxGDAWBgNVBAMMD2RldmljZS5tdHMudGVzd
DEqMCgGCSqGSIb3DQEJARYbZGFyc2hhbi5tYWl5YUBtdWx0aXRlY2gu
Y29tMB4XDTE5MDYxODIwMTQxNVoXDTIwMTAzMDIwMTQxNVowg
ZwxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJNTjEUMBIGA1UEBwwL
TUlOTkVBUE9MSVMxEjAQBgNVBAoMCU1VTFRJVEVDSDEQMA4GA1
UECwwHU1VQUE9SVDEYMBYGA1UEAwwPZGV2aWNlLm10cy50ZXN
0MSowKAYJKoZIhvcNAQkBFhtkYXJzaGFuLm1haXlhQG11bHRpdGVj
aC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCd
U/B/k7ER2YrJ/fwXS7KSLQY/zQPc8XllvgVga2PVJrKx4mBlcLyQjPKg1vT
+SwuqlLNXUn/9onBIqGlNSskloPW6oqA82T/epL9GkjyKircGsgjF3lFAJo
vre3ZydQbXEJaT97NPtph6vR24G3Xx8S0G2zuTJjvNMPhGMKbzRKBFv
TI68eLPRPEsZIxSTlWJQWwq/inTMSWpSRNWIV4Zbbed+YH6ZZUagvC
nXQdIsJG3fpRNaPgTAcNewESUrYk6Uk5z3dcjCda/HK7yv0ZzF2zkQJ2B
kVmcBBYCPR3RER3qt+n3/D+wzkpwXIks08R6FM96mhXAec2/Evic9iz
FAgMBAAGjge8wgewwgbsGA1UdIwSBszCBsKGBoqSBnzCBnDELMAk
GA1UEBhMCVVMxCzAJBgNVBAgMAk1OMRQwEgYDVQQHDAtNSU5
ORUFQT0xJUzESMBAGA1UECgwJTVVMVElURUNIMRAwDgYDVQQLD
AdTVVBQT1JUMRgwFgYDVQQDDA9kZXZpY2UubXRzLnRlc3QxKjAoBg
kqhkiG9w0BCQEWG2RhcnNoYW4ubWFpeWFAbXVsdGl0ZWNoLmNv
bYIJALkDZPqJ1+17MCwGA1UdEQQlMCOCD2RldmljZS5tdHMudGVzdII
IQZGV2aWNlMS5tdHMudGVzdDANBgkqhkiG9w0BAQsFAAOCAQEAg
823MJ+d65V7DhDIIjNjuUHgO1mmYNfLtlmKB5nT9rjRejAT1D/k4HDJ
H7EnYXOm/FB58KoWUKD5Wls0tmcmDVv2rMxTtcO1Y7I29L5h0jLeH
UHJgFuA7hx9/2Lwj/CW/rNsrDGM3q86MI3x4EjqO6Lmxl075j7dJz3N4
Z1wofwYgCmb5Z04fv4XirxkfXJ4IZXhiNpbLHk8LOdClHzlnEO864BXxoy
1Tz8HCcK+MGcKODrWEYB0EclYjINa9VqX1WaSoOXuUqiW7YVYfWck
jW5G8Dtt5djySXw3mB+DNhRWhKDYgEoLt0b0UEb6Li2IN8DIxpJEAfjs
CvTUkjDg 1w==
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAnVPwf5OxEdmKyf38F0uyki0GP80D3PF5Zb4FYGt
j1SayseJgZXC8kIzyoNb0/ksLqpSzV1J//aJwSKhpTUrJJaD1uqKgPNk/3q
S/RpI8ioq3BrIIxd5RQCaL63t2cnUG1xCWk/ezT7aYer0duBt18fEtBts7k
yY7zTD4RjCm80SgRb0yOvHiz0TxLGSMUk5ViUFsKv4p0zElqUkTViFeG
W23nfmB+mWVGoLwp10HSLCRt36UTWj4EwHDXsBElK2JOlJOc93XI
wnWvxyu8r9Gcxds5ECdgZFZnAQWAj0d0REd6rfp9/w/sM5KcFyJLNPE
ehTPepoVwHnNvxL4nPYsxQIDAQABAoIBAQCXdzOoL5Ge5LiY5VxpNS
iTUKOekwtwEE7W5A2bGWjA0oPhfFdf8hyocfo5XRn7JFb0ADt1C2lLz7
KYUQMoNaLYBlHtQBpS2rmB6Ux5bdq5avjwikCl9vZ0c2fr6y5K3V4bec
```

3uYOASE3JTYHUXReDUcGPwIOsHLR0P3GB6euaQdvPf5wFnDza/TxJE
yIRSrPHyqQUf1obU8gWQkDGyLOyGc4A+kn9ISrODDTn2ORbCoBldV8
bcdkIVPttA8wawdZr6Daq+KkZ8/WJ3O7No6x1WzG7gEPe1UkCUHsjM
HVXf+RxGlvJflyqPDRaUR5CqyvfmobIHANUn8zkUMmyuW3gBAoGBA
M5F5ZxQEcCegaDF3n/6pCFylL/BLsQ5WxgorQ+Vr5xOqtkt7rIzUjH4IM
gL4YJyVB7Mp6H5vnuoE0GAGS2lLK5oigTttNsG17ttTyZqCzlNtaKqd4S
9fJLiUIMlG33Y05oCHO9lzSGrDPi0YQjXGuX2z9K9jCAIRCiZSGsLJPIBAo
GBAMNBZtNuWisAP+nmTrN+SCeNihn6rhp5ASTf4bDdv43mmD1DIuJ
2c6QgVu6LZRHLtQBJYDkTA+mRL1FZMDS5C0hQKbOWq2Lam9op6g
WH81lx/ocR8mKvodTOmXocM+MdKZanp29hcdcWJwXdLeTkL6ZpwA
+bQ+oF5gsaib/Gw/LFAoGAXcl+GtJ1H+Vx/w24muv1UJfudjl58BI8Dw
H/ngRrMmC6YcD2tOOMzdeJ4Cs2v78H7HEVDxqkt0i2aKO7zvs5E5vIlX
EXODcmQ7vxrv+sVsO0gF+NtDcLuyVXgimPFGtP2sh3K4pX+KTzYulw7
ToQqtrLp4AzhCT+CI+ZU8JfbAECgYBMcXyKZnfSwgRD1LEXQOeK5LUe
urATGTDDeQtpLUfjjFYqFfDAbNOVfDvMpLJrJy+z7wZHEhTECt1Voe9nl
NK/+vJ4pxJuX1wJK8O9ap5xdFnME9Crpktbf49C6Wu/DRnNK9I3nxTsu
nWIrDFdnaCyLFDPS2BpbOnFixxHAtCQaQKBgQCYRI1tH0kOYBr4yY4p
RMoW4DPWrVWbm/J6szjR9hffzZeP4ue9ste4fCESoiAzhjqGzPJl7dmB
aTFD0OR5gPs6imtBGUrbCg8PBKUDMzqZu2rJUE8T11SnhQVs9bIAeV
WJjj1Y1l6PHsyPMWgYvbjP80i1IVExSINJtRsz2q0dgQ==
-----END RSA PRIVATE KEY-----

6. On a Windows-based PC, save the certificate (for this example, the file is saved as mycert.crt). Double click and install the certificate. **Install certificate > Current User > Place all certificates in the following store > Browse > Trusted Root Certification Authorities > ok > Next > Certificate store selected by user**.

   Once completed, the system displays a message indicating that the import was successful.

-----BEGIN CERTIFICATE-----
MIIErTCCA5WgAwIBAgIJALkDZPqJ1+17MA0GCSqGSIb3DQEBCwUAM
IGcMQswCQYDVQQGEwJVUzELMAkGA1UECAwCTU4xFDASBgNVBAc
MC01JTk5FQVBPTElTMRIwEAYDVQQKDAlNVUxUSVRFQ0gxEDAOBgN
VBAsMB1NVUFBPUlQxGDAWBgNVBAMMD2RldmljZS5tdHMudGVzd
DEqMCgGCSqGSIb3DQEJARYbZGFyc2hhbi5tYWl5YUBtdWx0aXRlY2gu
Y29tMB4XDTE5MDYxODIwMTQxNVoXDTIwMTAzMDIwMTQxNVowg
ZwxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJNTjEUMBIGA1UEBwwL
TUlOTkVBUE9MSVMxEjAQBgNVBAoMCU1VTFRJVEVDSDEQMA4GA1
UECwwHU1VQUE9SVDEYMBYGA1UEAwwPZGV2aWNLm10cy50ZXN0
MSowKAYJKoZIhvcNAQkBFhtkYXJzaGFuLm1haXlhQG11bHRpdGVjaC
5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCdU/
B/k7ER2YrJ/fwXS7KSLQY/zQPc8XllvgVga2PVJrKx4mBlcLyQjPKg1vT+S
wuqlLNXUn/9onBIqGlNSskloPW6oqA82T/epL9GkjyKircGsgjF3lFAJovr
e3ZydQbXEJaT97NPtph6vR24G3Xx8S0G2zuTJjvNMPhGMKbzRKBFvTI
68eLPRPEsZIxSTlWJQWwq/inTMSWpSRNWIV4Zbbed+YH6ZZUagvCn
XQdIsJG3fpRNaPgTAcNewESUrYk6Uk5z3dcjCda/HK7yv0ZzF2zkQJ2Bk
VmcBBYCPR3RER3qt+n3/D+wzkpwXIks08R6FM96mhXAec2/Evic9izF
AgMBAAGjge8wgewwgbsGA1UdIwSBszCBsKGBoqSBnzCBnDELMAkG

```
A1UEBhMCVVMxCzAJBgNVBAgMAk1OMRQwEgYDVQQHDAtNSU5O
RUFQT0xJUzESMBAGA1UECgwJTVVMVElURUNIMRAwDgYDVQQLDA
dTVVBQT1JUMRgwFgYDVQQDDA9kZXZpY2UubXRzLnRlc3QxKjAoBgk
qhkiG9w0BCQEWG2RhcnNoYW4ubWFpeWFAbXVsdGl0ZWNoLmNvb
YIJALkDZPqJ1+17MCwGA1UdEQQlMCOCD2RldmljZS5tdHMudGVzdII
QZGV2aWNlMS5tdHMudGVzdDANBgkqhkiG9w0BAQsFAAOCAQEAg
823MJ+d65V7DhDIIjNjuUHgO1mmYNfLtlmKB5nT9rjRejAT1D/k4HDJ
H7EnYXOm/FB58KoWUKD5Wls0tmcmDVv2rMxTtcO1Y7I29L5h0jLeH
UHJgFuA7hx9/2Lwj/CW/rNsrDGM3q86MI3x4EjqO6Lmxl075j7dJz3N4
Z1wofwYgCmb5Z04fv4XirxkfXJ4IZXhiNpbLHk8LOdClHzlnEO864BXxoy
1Tz8HCcK+MGcKODrWEYB0EclYjINa9VqX1WaSoOXuUqiW7YVYfWck
jW5G8Dtt5djySXw3mB+DNhRWhKDYgEoLt0b0UEb6Li2IN8DIxpJEAfjs
CvTUkjDg 1w==
-----END CERTIFICATE-----
```

Method 2: Becoming a Certifying Authority (CA): Creating a CA Certificate and Signed Certificate

The previous method using an unsigned certificate gets complicated to manage if you have multiple windows clients and multiple devices in your network. For multiple devices, it's better to become your own Certifying Authority (CA). That way you can create your own CA certificate and generate signed certificates from it. With this method, you install the same CA certificate on multiple windows hosts and generate a certificate for each device or possibly one certificate that you can have on all your devices.

Prerequisites

Before starting, you need:

1. A target device using mPower (including MTR, Conduit, MTCAP, IP67, or Conduit3) with an IP address.
2. A Windows client machine (for this example, a PC using windows 10).
3. To assign an IP address via DHCP or static but the DNS server should assign a DNS name to the device (for this example, my device has a DNS name device.mts.test).
4. An Ubuntu machine with openssl on it.

1. Create a root key.

```
openssl genrsa -out rootCA.key 2048
```

Example terminal output:

```
root@user:~/Documents/certificates# openssl
genrsa -out rootCA.key 2048 Generating RSA
private key, 2048 bit long modulus
.............+++

.......................+++
e is 65537 (0x010001)
```

This creates a key, 2048 bits long.

2. Generate the root certificate.

```
openssl req -x509 -new -nodes -key rootCA.key -days 1024 -out

rootCA.pem
```

What the above command means:

- new: create a new request

-x509: specifies the kind of certificate to make

-key: the file with the private key to use

-days: the number of days for which the certificate should be valid. Use as high a number as you feel comfortable with for your development environment.

-out: the name of the target file to which the commands writes the certificate
.

Example terminal output:

```
root@user:~/Documents/certificates # openssl req -x509 -new -nodes -key rootCA.key -days 1024
- out rootCA.pem
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]:MN Locality Name (eg, city) []:MINNEAPOLIS
Organization Name (eg, company) [Internet Widgits Pty
Ltd]:MULTITECH Organizational Unit Name (eg, section) []:SUPPORT
Common Name (e.g. server FQDN or YOUR name)
[]:device.mts.test Email Address []:user.foobar@multitech.com
```

3. Upload this certificate onto the target device from the UI. Go to **Administration -> x.509 CA certificates -> Choose File -> Import**.

4. Copy this file into your windows machine or all of your windows machines (for this example, the certificate is named rootCA.crt). See example .crt file below.

```
-----BEGIN CERTIFICATE-----
MIIEEDCCAvigAwIBAgIJAKhMOu2HKvgWMA0GCSqGSIb3DQE
BCwUAMIGcMQswCQYDVQQGEwJVUzELMAkGA1UECAwCTU
4xFDASBgNVBAcMC01JTk5FQVBPTElTMRIwEAYDVQQKDAlNV
UxUSVRFQ0gxEDAOBgNVBAsMB1NVUFBPUlQxGDAWBgNVB
AMMD2RldmljZS5tdHMudGVzdDEqMCgGCSqGSIb3DQEJARYb
ZGFyc2hhbi5tYWl5YUBtdWx0aXRlY2guY29tMB4XDTE5MDYx
OTE1MzMxOVoXDTIyMDQwODE1MzMxOVowgZwxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJNTjEUMBIGA1UEBwwLTUlOTk
VBUE9MSVMxEjAQBgNVBAoMCU1VTFRJVEVDSDEQMA4GA1
UECwwHU1VQUE9SVDEYMBYGA1UEAwwPZGV2aWNlLm10cy
50ZXN0MSowKAYJKoZIhvcNAQkBFhtkYXJzaGFuLm1haXlhQG1
1bHRpdGVjaC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDw
AwggEKAoIBAQDWDJDaZRPD6Ap8NB3M8t5CdrtCW5ig1KfO1
KYMkUlkcKCgB0OQj8NQR0iFJVjXrOxZ8NxK2VuTf51ozCl47rqw
hbtROTUxSMBjHkZ1Or8QMt5sSXUB+issgYjAFs0w5clHFpjNQh
FyGTbOx0JOWiMJ1k8hUJPpEMf4Ne8DVSSMn1h8OjmqM24U
Jw/ZSNMjm7Bcw5BVUlkUmOG+La4LwCSYwbwXtVUs270aIfy
Arnhr/nfjbKSrfeHS5B/XCzLVSSx9gvfGJG9lzW4qEQjwUXqFJus
D1aXawaBIR0GrEZmOklLeyhy36lZZ7XLmnixl1ltDnUGCI0A/QO
MQxDKTY0IXAgMBAAGjUzBRMB0GA1UdDgQWBBSxwfFTzi8d
wuNPhGfxBs6TUBJxAjAfBgNVHSMEGDAWgBSxwfFTzi8dwuNP
hGfxBs6TUBJxAjAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb
3DQEBCwUAA4IBAQDSfJKNqxglA/OeFDF4UcAyhRC+eqjJGESZ
1RikhkgY5WXKrSWPB6XDyT5x2X14zuGWOfYqvA2fUWDH4O
WGXQB5qXJ1saKaSMj3sCVtV7HpVC69XhyM5cTBmnCUW0KS
LUE5mqPFRAjzQuRLxwg2GN6ubiUBqXobCvYPu6DHZgW2EIO
o0Jgc8Et/SRhlc0+zBV/fzmqqsmcXO9tZgto+TyulZwkUJBAk/qb
UzcUnVF2jRfVCp86L9b4jKLhBdRfRqkp5XWmBuFI7o0FRrdo4d
oxAhRaUnZCvAvz6T2ec9opyBS6DnvX3cki4WnIvs+RhQ5mZAs
67pNfMRJyFyl6sdi3G
-----END CERTIFICATE-----
```

5. On the Windows client, save the certificate. Double click and install the certificate. **Install certificate -> current user -> Place all certificates in the following store -> Browse -> Trusted Root Certification Authorities -> ok -> Next -> Certificate store selected by user**. The system displays a warning message which you can accept.

   Once completed, the system displays a message indicating that the import was successful. Now you have successfully become a Certifying Authority (CA). Next, you must create an RSA private key and CSR.

6. Create an RSA private key and certificate signing request (CSR) using the following command:

   NOTE: This private key should stay private, stored on the server, and not shared externally. The private key is used to then create a public certificate that you can share with others. Certificate signing request or CSR is used to provide some details of the entity and the resource you want to incorporate into the request.

   ```
   openssl req -new -nodes -out server.csr -newkey rsa:2048 -keyout server.key
   ```

The -newkey and -keyout specify the kind of private key to generate and the file where it’s stored, respectively.

Example terminal output:

```
root@user:~/Documents/certificates# openssl req -new -nodes -out server.csr -newkey
rsa:2048 - keyout server.key
Generating a 2048 bit RSA private key
.................+++
...................................................................................+++
writing new private key to 'server.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]:MN Locality Name (eg, city)
[]:MINNEAPOLIS
Organization Name (eg, company) [Internet Widgits Pty
Ltd]:MULTITECH Organizational Unit Name (eg, section) []:SUPPORT
Common Name (e.g. server FQDN or YOUR name)
[]:device.mts.test Email Address []:user.foobar@multitech.com

Please enter the following 'extra'
attributes to be sent with your
certificate request
A challenge password []:
An optional company name []:
```

7. Create a v3.ext file containing the following information (Only an X.509 v3 certificate carries SAN information which requires an additional file versus creating an X.509 v1 certificate. That extra file contains v3 information.):

```
root@user:~/Documents/certificates # cat
v3.ext authorityKeyIdentifier=keyid,issuer
subjectAltName = @alt_names
[alt_names]
DNS.1 = device.mts.test
```

8. After generating a private key and CSR, create a server certificate by using the previously generated root certificate to issue it.

```
openssl x509 -req -in server.csr -CA rootCA.pem -CAkey rootCA.key -out server.crt -CAcreateserial -
days 500 -extfile v3.ext
```

```
root@user:~/Documents/certificates # openssl x509 -req -in server.csr -CA rootCA.pem -
CAkey rootCA.key -out server.crt -CAcreateserial -days 500 -extfile v3.ext
Signature ok
subject=C = US, ST = MN, L = MINNEAPOLIS, O = MULTITECH, OU = SUPPORT, CN = device.mts.test,
emailAddress =
user.foobar@multitech.com Getting CA
Private Key
```

```
root@user:~/Documents/certificates# ls -
lart total 36
drwxrwxr-x 13 dmaiya dmaiya 4096 Jun 19 10:31 ..
-rw-r--r--  1 root  root  151 Jun 19 10:31 v3.ext
-rw-------  1 root  root  1679 Jun 19 10:32 rootCA.key
-rw-r--r--  1 root  root  1468 Jun 19 10:33 rootCA.pem
-rw-------  1 root  root  1704 Jun 19 10:33 server.key
-rw-r--r--  1 root  root  1078 Jun 19 10:33 server.csr
-rw-r--r--  1 root  root  1480 Jun 19 10:33 server.crt
-rw-r--r--  1 root   root     17 Jun 19 10:33 rootCA.srl
drwxr-xr-x  2 root  root  4096 Jun 19 10:33 .
```

After this is complete, your generated files should look like the following example:

```
root@user:~/Documents/certificates# cat server.crt
-----BEGIN CERTIFICATE-----
MIIEGTCCAwGgAwIBAgIJAIgbPYeJ2639MA0GCSqGSIb3DQEBC
wUAMIGcMQswCQYDVQQGEwJVUzELMAkGA1UECAwCTU4x
FDASBgNVBAcMC01JTk5FQVBPTElTMRIwEAYDVQQKDAlNVUx
USVRFQ0gxEDAOBgNVBAsMB1NVUFBPUlQxGDAWBgNVBAM
MD2RldmljZS5tdHMudGVzdDEqMCgGCSqGSIb3DQEJARYbZG
Fyc2hhbi5tYWl5YUBtdWx0aXRlY2guY29tMB4XDTE5MDYxOTE
1MzM1MFoXDTIwMTAzMTE1MzM1MFowgZwxCzAJBgNVBAY
TAlVTMQswCQYDVQQIDAJNTjEUMBIGA1UEBwwLTUlOTkVBU
E9MSVMxEjAQBgNVBAoMCU1VTFRJVEVDSDEQMA4GA1UEC
wwHU1VQUE9SVDEYMBYGA1UEAwwPZGV2aWNlLm10cy50Z
XN0MSowKAYJKoZIhvcNAQkBFhtkYXJzaGFuLm1haXlhQG11b
HRpdGVjaC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDFUAxH8M3MsUq6ZVItD0TP6hFeVOJxOlmM4pj
0kvZq0CNn0xGe4G7v3e2Nm61RblLhU3Tc7InaSADQco9AB8G
vg5DS8K2f/t5ra/Z+94R6658/8rkctKcEc1Y6CAycZ+Y1Ybm8SVlC
```

```
NixawLlrJqRXyq29Dn7NHM/n3Uy6i7HExymtyx/s9QRN6PPCap
eMe+tSzgtE3Taq30Eoihft99/RN9Bz3M7LbeIczH9fRtio5ewQzy
bhZitZnLYHY+zlHxTUL2YighTSKpsQ276obmblF+944lrnnUlu/ca
jE733BiUxThM6yHaOaazuLeoAqvU2qYe8ppJRtnaGWT2H7YCP
AgMBAAGjXDBaMB8GA1UdIwQYMBaAFLHB8VPOLx3C40+EZ/
EGzpNQEnECMAkGA1UdEwQCMAAwLAYDVR0RBCUwI4IPZGV
2aWNlLm10cy50ZXN0ghBkZXZpY2UxLm10cy50ZXN0MA0GCS
qGSIb3DQEBCwUAA4IBAQBZnjmbTrm4JBf/fa5I6zp0vM7DKX4
d1TCrm2faExURKxZN16oGVNrYdUEdNTVF+MxvpC3AQkJaC7q
eZ2KLlV2CpnTG1eiwNwGpizhtvy/VKDa68luN3PlC+RuqKTa7dt
7wwOHOrSvrhmPQ3fYWfruj1sBl7/3D6hwI8COpdvhQLvIxNw+
LKRA8utOSvqNZJCZdGmzIhbmtSksTpka/UsDOr/o8QBcItMhTh
UB6M4UVvYHPebuJACl+YW3vS0Px22T+tntslhGT4Oem3qq0Tj
29K3Df4ZHtpMwbUiT3dhBJxyzRGM9hT4Nme4LBzFDm/gTW
m9nUKQ8IDf2zkwS3XdXY
-----END CERTIFICATE-----
root@user:~/Documents/certificates# cat server.key
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBA
QDFUAxH8M3MsUq6ZVItD0TP6hFeVOJxOlmM4pj0kvZq0CNn
0xGe4G7v3e2Nm61RblLhU3Tc7InaSADQco9AB8Gvg5DS8K2f/
t5ra/Z+94R6658/8rkctKcEc1Y6CAycZ+Y1Ybm8SVlCNixawLlrJq
RXyq29Dn7NHM/n3Uy6i7HExymtyx/s9QRN6PPCapeMe+tSzgt
E3Taq30Eoihft99/RN9Bz3M7LbeIczH9fRtio5ewQzybhZitZnLY
HY+zlHxTUL2YighTSKpsQ276obmblF+944lrnnUlu/cajE733BiUx
ThM6yHaOaazuLeoAqvU2qYe8ppJRtnaGWT2H7YCPAgMBAAE
CggEBAIx8UCIwu/cQDIrmdToL8wyuNauaeJfx2azL8efBc53dkD
fuOk+KsLIsq2T2ANNH3877Iuvhps06EwpXZtNKMoeK/2SRZK3
UQ/zsI9eG2FbEyOA5K7/aiEhM7onnDUOXXnuHlz0OZHUWKUJ
8kghOvRidAFLprTLRXt5R3L29lNbrTugyWFY6bujhPJNpCdwGb
pqIFhdjpnHIVdVlb1BtydD88B5u4WPAdc8e/eHXqs9q/QvVrbj9
8T6vnro1cukquqMv0Fg2Lug+yycxxAtSvog3KbHHfimX7YPHqi
wCmKUOdYqwely7KQAw8eDEfmFcEYs1nEl33Gk/YGxJikdU5yE
CgYEA6TXF6hplLQ5CDjkH9r1WXloNLtz6VyeyJndFJcm8IFIOQ0j
+Q2FgDB2t26hKZ4H75yvBaCN60GbwocA4GxuFmY2TKmlTgrv
q3ggK5wQmnJHHcPRi6tMWYVHsjWbLm2ANwONqrYFmb95Y
vJ0heguV78N3o+S4uW20KLgyE7bPDZcCgYEA2Jg6k+MHBKVP
xEwd5nfIJioxGHNJwJ3sRQxB7K2POcUyIDmF66PNo1mElzk14/
wI3D98Otky6rIPq0ho/DQzGRVJS2cozc7aNoLm7FoUc1+3Dg4T
ZxOmEAWwd9XklrmPg1x1rWPazVwga6va7EmwVRp/ZEgtXir4
MGaYMC/nc8kCgYB9wIQ/Lwp9mCGgX7pen0wSRoazTW8kTg
BvY4MC1FxAJV8RgyuwE7Lh9aMJPh8Y32uBBQQebntMIyYAYp
EedOG+oivIA9GHPmNwZG/UkFVtueIMk4s/SqHXyoA+4z5JQyt
HZpngg1VEX2YEFsq1b8fi6Mj7tFqzimdKScCfBsVxcwKBgAbvCK
EHWYgqip0sGqDwILYoD55KwoeqBpBHTiz3eWhOCcbCUKk0ez
bJfNcie7kqrlXuqllv7pNY0+uVy9aXDTO2XLxPNx0vjAjGtAHI+HK
hE8kdZj2cgWpt5DJR5Jl2o0N/SD0evzhnxJntzHpX+Y8f5Agfz2P+
WCekgSa5wd0RAoGBALrEwXO5KSzeY40WZtstHIUXpOBF5sfu
```

```
W0m8/UqAMIZzinuKEiQ8G8BQpUEZV4xmLMp6FWcWY2GcD
2dAO6CTxO+J1GE9G9m69tjRDZpnsA0ePPFBiBGM4yCZDdKRA
tHbBiHuE+udQIOZ31p/1vr o2HYV/PvzfMaGA6x4N5Ciza3
-----END PRIVATE KEY-----
```

9. Copy these two files and create a .crt or .txt file on a Windows client which looks like the following example. (NOTE: The change in text from **PRIVATE** to **RSA PRIVATE**.)

```
-----BEGIN CERTIFICATE-----
MIIEGTCCAwGgAwIBAgIJAIgbPYeJ2639MA0GCSqGSIb3DQEBC
wUAMIGcMQswCQYDVQQGEwJVUzELMAkGA1UECAwCTU4xF
DASBgNVBAcMC01JTk5FQVBPTElTMRIwEAYDVQQKDAlNVUxU
SVRFQ0gxEDAOBgNVBAsMB1NVUFBPUlQxGDAWBgNVBAMM
D2RldmljZS5tdHMudGVzdDEqMCgGCSqGSIb3DQEJARYbZGFyc
2hhbi5tYWl5YUBtdWx0aXRlY2guY29tMB4XDTE5MDYxOTE1Mz
M1MFoXDTIwMTAzMTE1MzM1MFowgZwxCzAJBgNVBAYTAlV
TMQswCQYDVQQIDAJNTjEUMBIGA1UEBwwLTUlOTkVBUE9MS
VMxEjAQBgNVBAoMCU1VTFRJVEVDSDEQMA4GA1UECwwHU1
VQUE9SVDEYMBYGA1UEAwwPZGV2aWNlLm10cy50ZXN0MSo
wKAYJKoZIhvcNAQkBFhtkYXJzaGFuLm1haXlhQG11bHRpdGVja
C5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBA
QDFUAxH8M3MsUq6ZVItD0TP6hFeVOJxOlmM4pj0kvZq0CNn0
xGe4G7v3e2Nm61RblLhU3Tc7InaSADQco9AB8Gvg5DS8K2f/t5
ra/Z+94R6658/8rkctKcEc1Y6CAycZ+Y1Ybm8SVlCNixawLlrJqRXy
q29Dn7NHM/n3Uy6i7HExymtyx/s9QRN6PPCapeMe+tSzgtE3Ta
q30Eoihft99/RN9Bz3M7LbeIczH9fRtio5ewQzybhZitZnLYHY+zlH
xTUL2YighTSKpsQ276obmblF+944lrnnUlu/cajE733BiUxThM6y
HaOaazuLeoAqvU2qYe8ppJRtnaGWT2H7YCPAgMBAAGjXDBa
MB8GA1UdIwQYMBaAFLHB8VPOLx3C40+EZ/EGzpNQEnECMA
kGA1UdEwQCMAAwLAYDVR0RBCUwI4IPZGV2aWNlLm10cy50
ZXN0ghBkZXZpY2UxLm10cy50ZXN0MA0GCSqGSIb3DQEBCwU
AA4IBAQBZnjmbTrm4JBf/fa5I6zp0vM7DKX4d1TCrm2faExURKx
ZN16oGVNrYdUEdNTVF+MxvpC3AQkJaC7qeZ2KLlV2CpnTG1ei
wNwGpizhtvy/VKDa68luN3PlC+RuqKTa7dt7wwOHOrSvrhmPQ
3fYWfruj1sBl7/3D6hwI8COpdvhQLvIxNw+LKRA8utOSvqNZJCZd
GmzIhbmtSksTpka/UsDOr/o8QBcItMhThUB6M4UVvYHPebuJA
Cl+YW3vS0Px22T+tntslhGT4Oem3qq0Tj29K3Df4ZHtpMwbUiT3
dhBJxyzRGM9hT4Nme4LBzFDm/gTWm9nUKQ8IDf2zkwS3XdXY
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBA
QDFUAxH8M3MsUq6ZVItD0TP6hFeVOJxOlmM4pj0kvZq0CNn0
xGe4G7v3e2Nm61RblLhU3Tc7InaSADQco9AB8Gvg5DS8K2f/t5
ra/Z+94R6658/8rkctKcEc1Y6CAycZ+Y1Ybm8SVlCNixawLlrJqRXy
q29Dn7NHM/n3Uy6i7HExymtyx/s9QRN6PPCapeMe+tSzgtE3Ta
q30Eoihft99/RN9Bz3M7LbeIczH9fRtio5ewQzybhZitZnLYHY+zlH
xTUL2YighTSKpsQ276obmblF+944lrnnUlu/cajE733BiUxThM6y
HaOaazuLeoAqvU2qYe8ppJRtnaGWT2H7YCPAgMBAAECggEBA
```

lx8UCIwu/cQDIrmdToL8wyuNauaeJfx2azL8efBc53dkDfuOk+Ks
LIsq2T2ANNH3877Iuvhps06EwpXZtNKMoeK/2SRZK3UQ/zsI9e
G2FbEyOA5K7/aiEhM7onnDUOXXnuHlz0OZHUWKUJ8kghOvRi
dAFLprTLRXt5R3L29lNbrTugyWFY6bujhPJNpCdwGbpqIFhdjpn
HIVdVlb1BtydD88B5u4WPAdc8e/eHXqs9q/QvVrbj98T6vnro1c
ukquqMv0Fg2Lug+yycxxAtSvog3KbHHfimX7YPHqiwCmKUOdY
qwely7KQAw8eDEfmFcEYs1nEl33Gk/YGxJikdU5yECgYEA6TXF6
hplLQ5CDjkH9r1WXloNLtz6VyeyJndFJcm8IFIOQ0j+Q2FgDB2t2
6hKZ4H75yvBaCN60GbwocA4GxuFmY2TKmlTgrvq3ggK5wQmn
JHHcPRi6tMWYVHsjWbLm2ANwONqrYFmb95YvJ0heguV78N3
o+S4uW20KLgyE7bPDZcCgYEA2Jg6k+MHBKVPxEwd5nflJioxGH
NJwJ3sRQxB7K2POcUyIDmF66PNo1mElzk14/wI3D98Otky6rIPq
0ho/DQzGRVJS2cozc7aNoLm7FoUc1+3Dg4TZxOmEAWwd9Xklr
mPg1x1rWPazVwga6va7EmwVRp/ZEgtXir4MGaYMC/nc8kCgYB
9wIQ/Lwp9mCGgX7pen0wSRoazTW8kTgBvY4MC1FxAJV8Rgyu
wE7Lh9aMJPh8Y32uBBQQebntMIyYAYpEedOG+oivIA9GHPmN
wZG/UkFVtueIMk4s/SqHXyoA+4z5JQytHZpngg1VEX2YEFsq1b8
fi6Mj7tFqzimdKScCfBsVxcwKBgAbvCKEHWYgqip0sGqDwILYoD
55KwoeqBpBHTiz3eWhOCcbCUKk0ezbJfNcie7kqrlXuqllv7pNY0
+uVy9aXDTO2XLxPNx0vjAjGtAHI+HKhE8kdZj2cgWpt5DJR5Jl2o
0N/SD0evzhnxJntzHpX+Y8f5Agfz2P+WCekgSa5wd0RAoGBALrE
wXO5KSzeY40WZtsItHIUXpOBF5sfuW0m8/UqAMIZzinuKEiQ8G
8BQpUEZV4xmLMp6FWcWY2GcD2dAO6CTxO+J1GE9G9m69tj
RDZpnsA0ePPFBiBGM4yCZDdKRAtHbBiHuE+udQIOZ31p/1vr
o2HYV/PvzfMaGA6x4N5Ciza3
-----END RSA PRIVATE KEY-----

10. Upload this certificate to the target device in the UI under **Administration > X.509 Certificate > Import**.

    Once completed successfully, you should not see the warning message in your browser when navigating to the device.

Troubleshooting

If you get an error or SSL is not able to read the certificate, the file is invalid and will not be accepted.

1. Check if you have uploaded your CA certificate under **Administration > x.509 CA certificates > Choose File > Import**
2. Check if the file format that you uploaded is right. The acceptable format (.pem) is:

```
   -----BEGIN CERTIFICATE-----
certificate_text
   -----END CERTIFICATE-----
   -----BEGIN RSA PRIVATE KEY-----
private_key_text
    -----END RSA PRIVATE KEY-----
```

3. Check your encryption algorithms versus the above example which used minimal encryption. Try to eliminate encryption like -des3, -sha1.

4. Check your X509v3 configuration in v3.ext file above keyUsage = digitalSignature is not supported.

5. The key and cert should be BASE64 encoded.

Using the mPower Device UI to Manage Certificates

Import a Certificate

To import a new certificate:

1. Go to **Administration > X.509 Certificate**. The Certificate window displays the details of the certificate that is currently used.
   NOTE: A certificate with a key size greater than 2048 bits causes a delay accessing the Web UI after the device starts. A certificate with a key size less than 2048 bits is not recommended since it is less secure and may become breakable in the near future.
2. Click **Upload** to open **Upload Certificate** window.
3. Click **Browse** to select a valid certificate to be uploaded.
4. Click **Upload**. Wait until the file is uploaded.
5. To save your changes, click **Save and Restart**.

Generate a New Certificate (Self-signed)

Because the router uses a self-signed website certificate, your browser shows a certificate error or warning. Ignore the warning and add an exception or add your device IP address to the trusted sites.

To generate a new certificate:

1. Go to **Administration > X.509 Certificate.** The X.509 Certificate window displays the details of the certificate that is currently used.
2. Click **Create** to open the **Generate Certificate** window.
3. In the Common Name field, enter the name, hostname, or IP address, depending on what you use to connect to the router. The web browser uses this field to check for a valid certificate.
4. In the **Days** field, enter the amount of days before the certificate will expire.
5. In the **Country** field, enter the 2-letter code for the country name.
6. In the **State/Province** field, enter the state or province for which the certificate is valid.
7. In the **Locality/City** field, enter the locality or the city for which the certificate is valid.
8. In the **Organization** field, enter the organization name for which the certificate is valid.
9. In the **Email Address** field, enter the email address of the person responsible for the router. Typically this is the administrator. This field may be left blank.
10. Click **Generate**. Wait until the certificate is generated. You may have to reboot to complete the operation.

11. If you are finished making changes, click **Save and Restart**.

Upload CA Certificate

To upload a CA certificate:

1. Go to **Administration > X.509 CA Certificates**.
2. Click **Browse** and choose the file for your CA certificate file.
3. Click **Open**.
4. Once your file is selected, click **Upload**.
5. Your CA certificate file displays in the certificate list along with relevant details.
6. You may delete or remove a certificate by clicking the trash can icon to the right under Options. **Note**: Both add and remove functions may take up to two minutes to update. Once updated, the changes are applied immediately. There is no need to restart the device after CA certificate is added or removed.