Creating a Self-Signed SSL Certificate

These steps require that you have OpenSSL installed on your computer. OpenSSL is available for any operating system. Do an Internet search for instructions for installing on your OS.

1. Create an extension file with the following text:

authorityKeyIdentifier = keyid,issuer

extendedKeyUsage = serverAuth, clientAuth

basicConstraints=CA:FALSE

keyUsage=digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment

subjectAltName = @alt\_names

[alt\_names]

DNS.1 = [www.yourdomain.com](http://www.yourdomain.com)

Make sure to replace “www.yourdomain.com” with your domain name.

Name the file v3.ext and save it in the current folder. (The folder where you want all your keys and certs created.)

The OpenSSL commands should all be run from a terminal/console/PowerShell console that is in the folder where you saved the extension file. (You’ll need to configure OpenSSL in Windows so that its location is in the path.)

2. Create an RSA key for your root CA using the following command:

openssl genrsa -out ca.key 4096

You can also use the -des3 option in order to password protect the key.

3. Create a self-signed root CA cert using the following command:

openssl req -new -x509 -days 365 -key ca.key -out ca.crt

Answer the questions asked. For the "Common Name", do NOT use your domain name.

4. Create a subordinate CA that will be used for signing.

openssl genrsa -out ia.key 4096

5. Request a cert from the subordinate CA.

openssl req -new -key ia.key -out ia.csr

Make sure that the "Common Name" is the domain name you want for the cert.

Make sure that the "Common Name" matches the domain in alt\_names in your ext file

6. Process the cert request and sign it with the root CA.

openssl x509 -req -days 365 -in ia.csr -CA ca.crt -CAkey ca.key -extfile v3.ext -set\_serial 01 -out yourcert.crt

7. Export the file as a PFX.

openssl pkcs12 -export -out yourcert.pfx -inkey ia.key -in yourcert.crt -chain -CAfile ca.crt

You can now upload this cert to App Service and use it with your app.