**IV. Configuring for Client Authentication**

1. Generate an X509 certificate specifically for use in client authentication over SSL

$ openssl req -x509 -nodes -days 3660 -newkey rsa:2048 -keyout mykey.key -out mycert.pem

Generating a 2048 bit RSA private key

.....+++

.....................................+++

writing new private key to 'mykey.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) [XX]:US

State or Province Name (full name) []:Wisconsin

Locality Name (eg, city) [Default City]:Madison

Organization Name (eg, company) [Default Company Ltd]:Organization Y

Organizational Unit Name (eg, section) []:Security

Common Name (eg, your name or your server's hostname) []:myre.y.org

Email Address []:

2. Examine contents of certificate

openssl x509 -text -in mycert.pem

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

d4:f6:c1:63:5b:6a:56:a2

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=US, ST=Wisconsin, L=Madison, O=Organization Y, OU=Security, CN=myre.y.org

Validity

Not Before: Apr 22 17:47:51 2013 GMT

Not After : Apr 30 17:47:51 2023 GMT

Subject: C=US, ST=Wisconsin, L=Madison, O=Organization Y, OU=Security, CN=myre.y.org

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:c2:d8:fb:03:4f:ab:a6:ea:13:6c:f0:77:e0:04:

ac:17:be:e1:5b:d3:03:b2:39:31:67:49:39:94:75:

02:08:ae:d3:3d:aa:be:99:02:60:0f:91:cf:f3:4d:

3a:f6:a9:a6:2b:22:40:2f:5b:4b:fe:d1:39:7c:41:

91:83:6c:19:aa:2f:b6:c7:9a:c7:b7:be:7a:c0:d6:

b4:54:5f:8d:7c:1c:4d:74:4d:e1:bf:4a:8a:aa:5e:

8c:00:04:a7:bf:b6:79:55:63:0b:62:09:df:66:70:

03:e0:71:dd:35:41:30:63:b8:3c:76:ab:45:26:c7:

44:5c:19:f6:f2:81:80:3f:63:94:f1:cb:5e:07:1a:

1e:c9:ea:c5:0c:61:fc:d2:72:e5:f8:70:d2:dc:a3:

16:d1:47:03:a0:f0:86:e7:75:df:32:5f:7c:d1:e7:

f5:30:ce:60:8b:01:4d:da:f8:2c:7d:41:da:2f:95:

a8:56:8c:31:f4:0b:70:0d:26:49:da:7b:e3:20:4c:

7f:b6:cc:0d:b6:ad:63:19:12:0a:16:6e:b1:6e:eb:

d4:b3:04:49:ca:95:f4:bd:b6:09:48:93:2c:d6:45:

bd:17:17:f3:72:48:03:84:e5:36:70:85:d2:e0:ee:

47:63:1a:f1:81:bf:c2:7f:c3:d6:3e:07:bb:c4:8f:

ee:1b

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

0D:5B:2D:95:1D:78:2A:21:87:8D:F9:39:5F:0C:7B:8C:09:DA:32:EC

X509v3 Authority Key Identifier:

keyid:0D:5B:2D:95:1D:78:2A:21:87:8D:F9:39:5F:0C:7B:8C:09:DA:32:EC

X509v3 Basic Constraints:

CA:TRUE

Signature Algorithm: sha1WithRSAEncryption

74:ee:6a:2a:55:b6:3f:4f:3a:ae:7c:d9:d6:8a:8d:3e:a5:f4:

17:b9:68:15:a1:12:b6:9c:c9:05:d7:3c:d7:71:3c:33:c2:b5:

77:df:3a:49:ff:bf:91:e1:c2:b0:db:17:d4:cf:d9:f9:78:1a:

ff:67:73:03:bf:6a:2a:32:e2:cc:0e:2a:14:24:69:e6:eb:12:

3c:cb:12:8b:de:6e:67:a8:02:97:bf:99:69:a9:99:ff:72:4d:

57:0a:13:78:c3:ef:e5:28:e5:fe:87:b7:d7:8a:1b:4c:f0:66:

0f:56:89:15:ff:98:36:94:b8:c6:ef:65:99:de:50:53:68:e5:

01:90:3f:65:5d:a6:e2:b3:f7:ea:39:d7:53:80:56:08:81:1b:

15:71:02:31:03:08:44:bf:29:29:64:ec:dd:0a:8f:04:33:ba:

a8:37:6f:c7:54:a3:02:b5:f4:00:3e:46:26:62:28:ac:36:3a:

35:bf:08:70:88:32:2b:48:01:1f:ee:1c:65:6b:f7:21:7e:a2:

36:ef:e3:19:25:9e:43:6b:ef:25:28:9f:13:d6:f2:83:ab:43:

46:4d:57:98:0d:01:1c:71:9b:6d:bb:68:75:b2:b3:15:92:0b:

f0:39:f6:7a:ca:9b:c4:d3:48:1a:79:2b:b1:3f:1c:cb:ad:64:

1d:5c:a7:eb

3. Extract the text-encoded representation of the certificate (the portion at the bottom of mycert.pem that looks like the following). Send it to the BSP admin so they can append it to the certificate bundle on BSP: bsp.test.../etc/pki/tls/certs/ca-bundle.crt. This will allow your new client certificate to verify:

-----BEGIN CERTIFICATE-----

MIIDuzCCAqOgAwIBAgIJANT2wWNbalaiMA0GCSqGSIb3DQEBBQUAMHQxCzAJBgNV

BAYTAlVTMRIwEAYDVQQIDAlXaXNjb25zaW4xEDAOBgNVBAcMB01hZGlzb24xFzAV

BgNVBAoMDk9yZ2FuaXphdGlvbiBZMREwDwYDVQQLDAhTZWN1cml0eTETMBEGA1UE

AwwKbXlyZS55Lm9yZzAeFw0xMzA0MjIxNzQ3NTFaFw0yMzA0MzAxNzQ3NTFaMHQx

CzAJBgNVBAYTAlVTMRIwEAYDVQQIDAlXaXNjb25zaW4xEDAOBgNVBAcMB01hZGlz

b24xFzAVBgNVBAoMDk9yZ2FuaXphdGlvbiBZMREwDwYDVQQLDAhTZWN1cml0eTET

MBEGA1UEAwwKbXlyZS55Lm9yZzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC

ggEBAMLY+wNPq6bqE2zwd+AErBe+4VvTA7I5MWdJOZR1Agiu0z2qvpkCYA+Rz/NN

OvappisiQC9bS/7ROXxBkYNsGaovtseax7e+esDWtFRfjXwcTXRN4b9KiqpejAAE

p7+2eVVjC2IJ32ZwA+Bx3TVBMGO4PHarRSbHRFwZ9vKBgD9jlPHLXgcaHsnqxQxh

/NJy5fhw0tyjFtFHA6Dwhud13zJffNHn9TDOYIsBTdr4LH1B2i+VqFaMMfQLcA0m

Sdp74yBMf7bMDbatYxkSChZusW7r1LMEScqV9L22CUiTLNZFvRcX83JIA4TlNnCF

0uDuR2Ma8YG/wn/D1j4Hu8SP7hsCAwEAAaNQME4wHQYDVR0OBBYEFA1bLZUdeCoh

h435OV8Me4wJ2jLsMB8GA1UdIwQYMBaAFA1bLZUdeCohh435OV8Me4wJ2jLsMAwG

A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAHTuaipVtj9POq582daKjT6l

9Be5aBWhEracyQXXPNdxPDPCtXffOkn/v5HhwrDbF9TP2fl4Gv9ncwO/aioy4swO

KhQkaebrEjzLEovebmeoApe/mWmpmf9yTVcKE3jD7+Uo5f6Ht9eKG0zwZg9WiRX/

mDaUuMbvZZneUFNo5QGQP2VdpuKz9+o511OAVgiBGxVxAjEDCES/KSlk7N0KjwQz

uqg3b8dUowK19AA+RiZiKKw2OjW/CHCIMitIAR/uHGVr9yF+ojbv4xklnkNr7yUo

nxPW8oOrQ0ZNV5gNARxxm227aHWysxWSC/A59nrKm8TTSBp5K7E/HMutZB1cp+s=

-----END CERTIFICATE-----