**Example using my OpenSSL CA to sign a Clearwell keystore certificate**JeremyC 20/2/2016  
  
**Summary**We created our own CA using OpenSSL. We created a root CA, with an intermediate CA, which we use to sign any CSRs. The steps here demonstrate how our own CA was used to sign a CSR from Clearwell and then the signed cert was installed into the Clearwell keystore. Testing was done on Clearwell v811. Part of the motivation behind doing this was that the existing GSL 811 Clearwell cert had expired, and I wanted to re-test the workaround steps for the HTTPS download issue (ET-3816296) in a realistic HTTPS environment (i.e. with a chain of trust).  
  
  
**o Create a new Clearwell keystore (i.e. a private key).**C:\jdk-8u45-windows-x64\bin>.\keytool.exe -genkey -alias clearwellkey -keyalg RSA -keystore new-server.keystore

Enter keystore password:

Re-enter new password:

What is your first and last name?

[Unknown]: clearwell1.cwlab.local

What is the name of your organizational unit?

[Unknown]: my\_org\_unit

What is the name of your organization?

[Unknown]: my\_org

What is the name of your City or Locality?

[Unknown]: Reading

What is the name of your State or Province?

[Unknown]: Berkshire

What is the two-letter country code for this unit?

[Unknown]: GB

Is CN=clearwell1.cwlab.local, OU=my\_org\_unit, O=my\_org, L=Reading, ST=Berkshire, C=GB correct?

[no]: yes

Enter key password for <clearwellkey>

(RETURN if same as keystore password):

Re-enter new password:  
  
  
**o Create a CSR.**C:\jdk-8u45-windows-x64\bin>.\keytool.exe -certreq -keyalg RSA -alias clearwellkey -file my.csr -keystore .\new-server.keystore

Enter keystore password:  
  
  
**o Use our intermediate CA to sign the CSR and create the signed cert.**C:\ca>c:\users\administrator.CWLAB\Cygwin\home\administrator\CW\_Tools\tools\openssl\OpenSSL-Win32\_0\_9\_8k\bin\openssl.exe ca -config intermediate/openssl.cnf -extensions usr\_cert -days 375 -notext –md sha256 -in c:\jdk-8u45-windows-x64\bin\my.csr -out c:\clearwell1cert.pem

Using configuration from intermediate/openssl.cnf

Loading 'screen' into random state - done

Enter pass phrase for c:/ca/intermediate/private/intermediate.key.pem:

Check that the request matches the signature

Signature ok

Certificate Details:

Serial Number: 4097 (0x1001)

Validity

Not Before: Feb 20 14:35:29 2016 GMT

Not After : Mar 1 14:35:29 2017 GMT

Subject:

countryName = GB

stateOrProvinceName = Berkshire

localityName = Reading

organizationName = my\_org

organizationalUnitName = my\_org\_unit

commonName = clearwell1.cwlab.local

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

Netscape Comment:

OpenSSL Generated Certificate

X509v3 Subject Key Identifier:

A7:50:A5:87:49:97:41:87:9D:E0:34:F1:55:04:56:2B:08:94:EF:9D

X509v3 Authority Key Identifier:

keyid:60:66:4E:74:48:61:65:9D:B1:8D:D5:2E:6A:80:BA:44:94:6D:5D:42

Certificate is to be certified until Mar 1 14:35:29 2017 GMT (375 days)

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y

Write out database with 1 new entries

Data Base Updated

**o Verify our new cert.**  
C:\ca>c:\users\administrator.CWLAB\Cygwin\home\administrator\CW\_Tools\tools\openssl\OpenSSL-Win32\_0\_

9\_8k\bin\openssl.exe verify -CAfile intermediate/certs/ca-chain.pem c:\clearwell1cert.pem

c:\clearwell1cert.pem: OK

**o Install all the certs into the Clearwell keystore.**C:\jdk-8u45-windows-x64\bin>.\keytool.exe -import -trustcacerts -alias root -file c:\ca\cacert.pem -

keystore .\new-server.keystore  
  
C:\jdk-8u45-windows-x64\bin>.\keytool.exe -import -trustcacerts -alias inter -file c:\ca\intermediate\intermediate.cert.pem -keystore .\new-server.keystore

C:\jdk-8u45-windows-x64\bin>.\keytool.exe -import -trustcacerts -alias clearwellkey -file c:\clearwell1cert.pem -keystore .\new-server.keystore

**o Validate the new server keystore.**C:\jdk-8u45-windows-x64\bin>.\keytool.exe -list -keystore .\new-server.keystore

Enter keystore password:

Keystore type: JKS

Keystore provider: SUN

Your keystore contains 3 entries

inter, Feb 20, 2016, trustedCertEntry,

Certificate fingerprint (SHA1): 96:A8:AD:E9:E1:FA:10:A9:DF:2E:13:08:B7:08:A2:7C:D9:79:DE:15

root, Feb 20, 2016, trustedCertEntry,

Certificate fingerprint (SHA1): CE:13:59:B0:4B:70:AB:92:6E:86:96:3E:BA:E9:D4:AA:45:01:12:42

clearwellkey, Feb 20, 2016, PrivateKeyEntry,

Certificate fingerprint (SHA1): B2:F4:24:C2:65:DE:21:5C:89:23:AE:23:6A:48:FA:A9:4B:79:4E:63  
  
  
**o Install the new server keystore.**C:\jdk-8u45-windows-x64\bin>copy new-server.keystore d:\cw\v811\config\templates\tomcat\server.keystore

Overwrite d:\cw\v811\config\templates\tomcat\server.keystore? (Yes/No/All): Yes

1 file(s) copied.  
  
Then run “Clearwell Utility” option 7.  
  
  
**o Verify that Clearwell starts up and then check the certificates and chain, using openssl.exe.**$ openssl s\_client -showcerts -connect clearwell1.cwlab.local:443

Loading 'screen' into random state - done

CONNECTED(00000168)

depth=2 C = GB, ST = England, O = JeremyC, OU = JeremyC CA, CN = JeremyC Root CA

verify error:num=19:self signed certificate in certificate chain

verify return:0

---

Certificate chain

0 s:/C=GB/ST=Berkshire/L=Reading/O=my\_org/OU=my\_org\_unit/CN=clearwell1.cwlab.local

i:/C=GB/ST=England/O=JeremyC/OU=JeremyC CA/CN=JeremyC Intermediate CA

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

MIIE2jCCAsKgAwIBAgICEAEwDQYJKoZIhvcNAQELBQAwaDELMAkGA1UEBhMCR0Ix

EDAOBgNVBAgTB0VuZ2xhbmQxEDAOBgNVBAoTB0plcmVteUMxEzARBgNVBAsTCkpl

cmVteUMgQ0ExIDAeBgNVBAMTF0plcmVteUMgSW50ZXJtZWRpYXRlIENBMB4XDTE2  
…  
UGyCsrb5klG5UjFL3BJk1UwQrPSEK015OnUGaWYeKuZ8S+Xl5GBfdpuNgRrQzZYc

zeQFN2eRW1MudJMKhH2eoHahDz9gig8fUi41QbhVcAAJD/Hcqccjto++Q17ufdvl

dIagyV+mqxE+83sYfud1koYp0U0DGu29AWSPSnoqwALekbb5ZG59QfchF/7wCg==

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

1 s:/C=GB/ST=England/O=JeremyC/OU=JeremyC CA/CN=JeremyC Intermediate CA

i:/C=GB/ST=England/O=JeremyC/OU=JeremyC CA/CN=JeremyC Root CA

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

MIIFqjCCA5KgAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwYDELMAkGA1UEBhMCR0Ix

EDAOBgNVBAgTB0VuZ2xhbmQxEDAOBgNVBAoTB0plcmVteUMxEzARBgNVBAsTCkpl

cmVteUMgQ0ExGDAWBgNVBAMTD0plcmVteUMgUm9vdCBDQTAeFw0xNjAyMjAxMzE0

MzFaFw0yNjAyMTcxMzE0MzFaMGgxCzAJBgNVBAYTAkdCMRAwDgYDVQQIEwdFbmds

YW5kMRAwDgYDVQQKEwdKZXJlbXlDMRMwEQYDVQQLEwpKZXJlbXlDIENBMSAwHgYD

VQQDExdKZXJlbXlDIEludGVybWVkaWF0ZSBDQTCCAiIwDQYJKoZIhvcNAQEBBQAD

ggIPADCCAgoCggIBAOCA3IIgNw2YgrUGDGTc8bx233C/YS8hva0zwJDettKHNAhh

FRH5C8OTaDppMZCbTxKQZ/pfHOlkLu+UQvUUYKpa2WLl0JZ4PGBdvqJbl2TLRi7c  
…  
cimlNtWxX56jJOj2Z2v7DDjBg00Lioq9sNynRUUIuoQWvbLTvUrfGTi/3SpZnxa9

C7QmlFNELnGCwaOnYIiwE9UqnjJvfK3fqBRaceImcvN7Mv/lrQod64VgM7fGdyPz

9adVFwt5U/AIC7/1J53V4HrzMctzrV3XrTi08/E8iP7G0r7p7e2cIhCzuTnrAhuU

B9iXARnhRTKXnFlTsElgN2fxDhW0lydReAuX7hJ48Ez2GlLFlGAzdxilMTxb47UX

FhAmXUh3qBSZwxkhG0U=

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

2 s:/C=GB/ST=England/O=JeremyC/OU=JeremyC CA/CN=JeremyC Root CA

i:/C=GB/ST=England/O=JeremyC/OU=JeremyC CA/CN=JeremyC Root CA

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

MIIGCTCCA/GgAwIBAgIJAMFAAdRGFyHcMA0GCSqGSIb3DQEBCwUAMGAxCzAJBgNV

BAYTAkdCMRAwDgYDVQQIEwdFbmdsYW5kMRAwDgYDVQQKEwdKZXJlbXlDMRMwEQYD

VQQLEwpKZXJlbXlDIENBMRgwFgYDVQQDEw9KZXJlbXlDIFJvb3QgQ0EwHhcNMTYw

MjIwMTE0NjE2WhcNMzYwMjE1MTE0NjE2WjBgMQswCQYDVQQGEwJHQjEQMA4GA1UE

CBMHRW5nbGFuZDEQMA4GA1UEChMHSmVyZW15QzETMBEGA1UECxMKSmVyZW15QyBD

QTEYMBYGA1UEAxMPSmVyZW15QyBSb290IENBMIICIjANBgkqhkiG9w0BAQEFAAOC

Ag8AMIICCgKCAgEAxkPbQXxXtctfCnV+xt71b7a/fOPzA+rLyq9JG93sbO7QwYs6

WG4G301t2eHR390qaWjZfw006gTYO8btkDIj+O3UhHTo9IT5gPlGHiTMf79Vk7Rb

mfdK1m6XXm9/j/ba/IVZiEEcxz4NyNxaGtspmn3KFrPGku1nt0Zuze1Y8TsGpyjF  
…  
q7dLGIfNl8eKzg5YdQLNExbawpMfkX6hZVidxS5mzyPzziYaD59TpgUjeOI45CuY

oWDWyBK+Hd625LTlU67FIcvmAadtBxxucTqz55cZjkeVWFxg9+Zhj2NsgoyyqxI7

dVdL425eYaMRgM7bbQ==

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

---

Server certificate

subject=/C=GB/ST=Berkshire/L=Reading/O=my\_org/OU=my\_org\_unit/CN=clearwell1.cwlab.local

issuer=/C=GB/ST=England/O=JeremyC/OU=JeremyC CA/CN=JeremyC Intermediate CA

---

No client certificate CA names sent

---

SSL handshake has read 5068 bytes and written 519 bytes

---

New, TLSv1/SSLv3, Cipher is EDH-RSA-DES-CBC3-SHA

Server public key is 2048 bit

Secure Renegotiation IS supported

Compression: NONE

Expansion: NONE

SSL-Session:

Protocol : TLSv1.2

Cipher : EDH-RSA-DES-CBC3-SHA

Session-ID: 56C87E177D3F6A64236819DE7379C4D967B7BD53C978F31E39835F7610A7A7C3

Session-ID-ctx:

Master-Key: AB18E6F9016E7D2D545EA6027CDBA9B9D5D5DF974FD7EBF18FAB47B4A562FC6E81E765D123D2089B07ED7EEED68F79F2

Key-Arg : None

PSK identity: None

PSK identity hint: None

SRP username: None

Start Time: 1455980055

Timeout : 300 (sec)

**Verify return code: 19 (self signed certificate in certificate chain)**

---  
  
…and if we use the “-Cafile” option to validate the chain (**NOTE**: Extra backslashes because I ran the following command from a Cygwin shell)…

openssl s\_client -showcerts -connect clearwell1.cwlab.local:443 -CAfile c:\\ca\\intermediate\\certs\\ca-chain.pem  
…

ZmtEB5yWw7iykNT7G7+yhMQWIQjiKD5I6/VFX5pG8J/EvxdXt1IQeIiwGiHtI6WY

q7dLGIfNl8eKzg5YdQLNExbawpMfkX6hZVidxS5mzyPzziYaD59TpgUjeOI45CuY

oWDWyBK+Hd625LTlU67FIcvmAadtBxxucTqz55cZjkeVWFxg9+Zhj2NsgoyyqxI7

dVdL425eYaMRgM7bbQ==

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

---

Server certificate

subject=/C=GB/ST=Berkshire/L=Reading/O=my\_org/OU=my\_org\_unit/CN=clearwell1.cwlab.local

issuer=/C=GB/ST=England/O=JeremyC/OU=JeremyC CA/CN=JeremyC Intermediate CA

---

No client certificate CA names sent

---

SSL handshake has read 5068 bytes and written 519 bytes

---

New, TLSv1/SSLv3, Cipher is EDH-RSA-DES-CBC3-SHA

Server public key is 2048 bit

Secure Renegotiation IS supported

Compression: NONE

Expansion: NONE

SSL-Session:

Protocol : TLSv1.2

Cipher : EDH-RSA-DES-CBC3-SHA

Session-ID: 56C8820FF2997E2357DE211296B3C99EEC8433F10FD1791F28C034D05861B334

Session-ID-ctx:

Master-Key: 4DA482AC7D96E245D64AECF5D54A939A50BF4F5971953D7FBC431CF771C0337B510B0527D82C7A83A205

EA8D2041EC7F

Key-Arg : None

PSK identity: None

PSK identity hint: None

SRP username: None

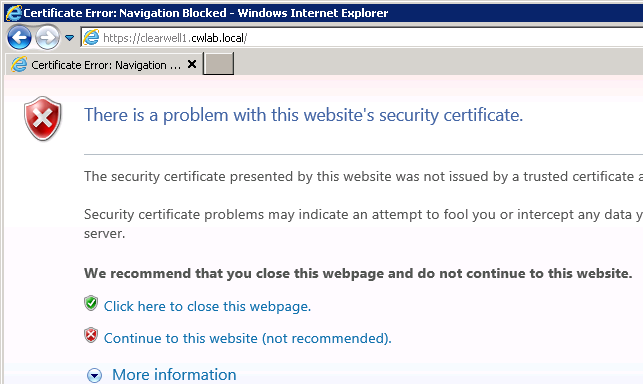
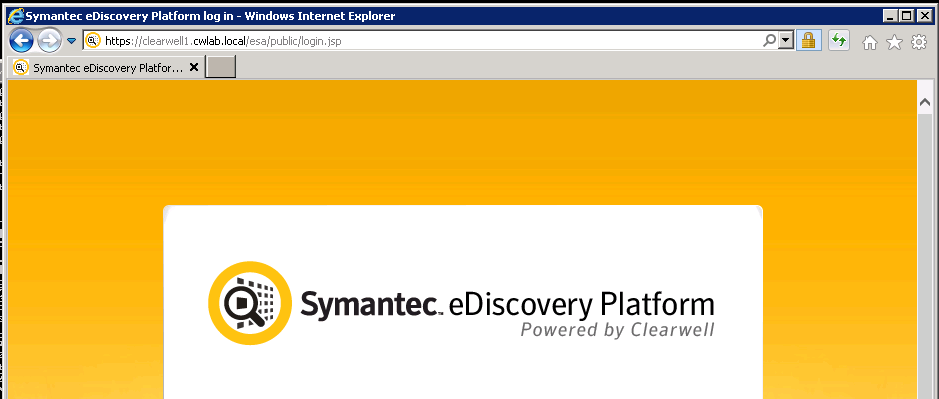
Start Time: 1455981071

Timeout : 300 (sec)

**Verify return code: 0 (ok)**

---  
  
  
**o Testing with IE.**

First we install our intermediate CA cert (intermediate.cert.pem), using “Internet options > Content > Certificates > Trusted Root Certificates > Import”.   
  
Then we test using IE, but it still fails:

  
=> It turns out that I had to add both my root CA cert \*and\* my intermediate CA cert. I guess this makes sense…  
  
…after all, just because Clearwell is also spitting out the root CA cert and intermediate CA cert, the client (IE) cannot simply trust them – it has to use it’s own CA certs, i.e. ones that it installed and trusts.

*JeremyC 20/2/2016***END**