Debugging SSL Certificates

Online Tools

Really nice set of tools to do a bunch of things, https://www.sslshopper.com/ssl-converter.html

Testing

Assuming that your CA certs are available, without a web server you can determine if a certificate is valid,

```
openssl s_server -cert www.krypton.com_server.crt -key
www.kryptong.com_server.key -CApath /etc/ssl/certs/ -www
```

The result will be an SSL http service listening on port 4433 with the follow response from the running the command,

```
Using default temp DH parameters
Using default temp ECDH parameters
ACCEPT
```

Further testing can be done by pointing your browser to, https://www.krypton.com:4433 where you will a page showing the various ciphers available and some statistics about your connection. Most modern browsers will also allow you to examine the certificate as well.

Getting Information

An SSL certificate contains information about, issuer, valid dates, subject, and crypto. The useful thing about this command is that you do not need CA certificates to view certificates,

```
openssl x509 -text -in www.krypton.com_server.crt
```