Setup directory and components for each test:

- mkdir ~/Desktop/<folder name>
- cd ~/Desktop/<folder name>
- mkdir newcerts certs crl private requests
- cp /etc/ssl/openssl.cnf ./config.txt
- touch index.txt
- sudo bash –c ‘echo “01” > serial’

Generate root CA certificate

- openssl genrsa -out private/cakey.pem 4096
- openssl req –new –x509 –key private/cakey.pem –out cacert.pem –days 3650 –set_serial 0 -nodes

Country Name: Ca
State: Quebec
Locality Name: Montreal
Org Name: Concordia Ltd.
Org Unit Name: My Apache CA
Common Name: APACHE
Email Address: lol@lol.com

- sudo gedit config.txt

UNDER [CA_default]

➔ dir = ~/Desktop/<folder name>

UNDER [policy_match]

➔ countryName = supplied
➔ stateOrProvinceName = supplied
➔ organizationUnitName = supplied

Generate Leaf certificate

- openssl genrsa –out webserverkey.pem 2048
- openssl req -new -key webserverkey.pem -out webserverreq.csr -days 365

Country Name: Ca
State: Quebec
Locality Name: Montreal
Org Name: Concordia Ltd. - leaf
Org Unit Name: My Apache Certificate
Common Name: apache.host (must be the hostname that you use)
Email Address: lol@lol.com

- openssl ca -in webserverreq.csr -out webservercert.pem -config ../config.txt

Notes

1- This sequence is the standard procedure applied to generate the certificate chain. Specific certificate validation tests might require different alterations in the config file for the root, intermediate or leaf certificate; or in the OpenSSL commands.

2- To test if the network appliance accepts its own key pair for externally delivered content, use the appliance’s public and private key pairs to sign a leaf certificate instead of generating a new CA key pair.

3- Insights on each certificate validation test are found in the ‘Appendix A’ of the ASIA CCS 2018 paper.