OpenSSL Cheat Sheet

by RomelSan (RomelSan) via cheatography.com/3953/cs/14102/

Create CA

Generate CA Private Key

openssl genrsa -out ca.key 4096

Self Sign CA (5 years)

openssl req -new -x509 -sha256 -days 1826 -key ca.key -out ca.crt

Create Certificate Request

Create a Private Key

openssl genrsa -out user.key 4096

Create a certificate request

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

Signing Requests

Process the request and get it signed by the CA

openssl x509 -req -days 730 -sha256 -in user.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out user.crt

Sign using v3 extension file

openssl x509 -req -days 730 -sha256 -in user.csr -extfile v3.txt -CA ca.crt -CAkey ca.key -set_serial 01 -out user.crt

Create Extension File

basicConstraints = CA:FALSE
authorityKeyIdentifier=keyid,issuer
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectAltName = @alt_names
[alt_names]
DNS.1 = server1.example.com
DNS.2 = mail.example.com
DNS.3 = www.example.com
DNS.4 = www.sub.example.com
DNS.5 = mx.example.com
DNS.6 = support.example.com
IP.1 = 192.168.0.100
URI.1 = https://www.myexample.com

Put the code in a file, modify it to reflect your site needs and save it as: v3.txt

Checking Certificates

Dump the Certificate

openssl x509 -in user.crt -text -noout

Check Purpose

openssl x509 -purpose -in user.crt -inform PEM

Inspect Certificate Request

openssl req -text -noout -verify -in user.csr

Export Certificate

Export as PKCS12 (PFX)

openssl pkcs12 -export -out user.pfx -inkey user.key -in user.crt

Export as PKCS12 with including CA public key

openssl pkcs12 -export -out user.pfx -inkey user.key -in user.crt -certfile ca.crt

Export as PKCS7 (P7B)

openssl crl2pkcs7 -nocrl -certfile user.crt -out certificate.p7b

Convert PFX to PEM

openssl pkcs12 -in user.pfx -out user.crt -nodes

While converting PFX to PEM format, openssl will put all the Certificates and Private Key into a single file.
You will need to open the file in Text editor and copy each Certificate & Private key (including the BEGIN/END statements)
to its own individual text file and save them as certificate.cer, CAcert.cer, privateKey.key respectively.

By **RomelSan** (RomelSan)
cheatography.com/romelsan/
keybase.io/romel

Published 26th December, 2017.
Last updated 26th December, 2017.