

# OpenSSL

## Check SSL

On domain

```
openssl s_client -connect www.domain.com:443
```

Check a Certificate Signing Request (CSR)

```
openssl req -text -noout -verify -in CSR.csr
```

Check a private key

```
openssl rsa -in privateKey.key -check
```

Check a certificate (crt or pem)

```
openssl x509 -in certificate.crt -text -noout
```

Check a PKCS#12 file (.pfx or .p12)

```
openssl pkcs12 -info -in keyStore.p12
```

## Create CSR+Key

Create a CSR

```
openssl req -out CSR.csr -new -newkey rsa:2048 -nodes -keyout privateKey.key
```

## Create Self-signed

```
openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:2048 -keyout privateKey.key -out certificate.crt
```

## Verify a CSR matches KEY

Check that MD5 hash of the public key to ensure that it matches with what is in a CSR or private key

```
openssl x509 -noout -modulus -in certificate.crt | openssl md5  
openssl rsa -noout -modulus -in privateKey.key | openssl md5  
openssl req -noout -modulus -in CSR.csr | openssl md5
```

## Convert

Convert a DER file (.crt .cer .der) to PEM

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

Convert a PEM file to DER

```
openssl x509 -outform der -in certificate.pem -out certificate.der
```

Convert a PKCS#12 file (.pfx .p12) containing a private key and certificates to PEM

You can add -nocerts to only output the private key or add -nokeys to only output the certificates.

```
openssl pkcs12 -in keyStore.pfx -out keyStore.pem -nodes
```

Convert a PEM certificate file and a private key to PKCS#12 (.pfx .p12)

```
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -certfile CACert.crt
```

---

Revision #4

Created 23 February 2018 06:59:05 by Dave

Updated 14 June 2019 00:41:38 by Dave