PKI / openSSL Cheat Sheet

by mdoehle via cheatography.com/23234/cs/5082/

Certificate Signing Request (CSR)

Generate a new private key and Certificate Signing Request

```
openssl req -out CSR.csr -new -newkey rsa:2048 -nodes -sha256 -keyout privat eKe y.key
```

Generate a self-signed certificate

```
openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:2048 -keyout privat eKe y.key -out certif ica te.crt
```

Generate a certificate signing request (CSR) for an existing private key

```
openssl req -out CSR.csr -key privat eKe y.key -new
```

Generate a certificate signing request based on an existing certificate

```
openssl x509 -x509toreq -in certif ica te.crt -out CSR.csr -signkey privat eKe y.key
```

Remove a passphrase from a private key

```
openssl rsa -in privat eKe y.pem -out newPri vat eKe y.pem
```

Check Files

Check a Certificate Signing Request (CSR)

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

Check a private key

```
openssl rsa -in privat eKe y.key -check
```

Check a certificate

```
openssl x509 -in certif ica te.crt -text -noout
```

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

```
openssl pkcs12 -info -in keySto re.p12
```

Debugging

Print certificate

```
openssl x509 -noout -text -in certif ica te.crt
```

Check an SSL connection. All the certificates (including Intermediates) should be displayed

```
openssl s_client -connect www.pa ypa l.c om:443
```

Remove Passphrase

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

```
openssl pkcs12 -in keySto re.p12 -out keySto re.pem -nodes
```

Remove Passphrase from key-file

```
openssl rsa -in exampl e.key -out exampl e.n ocr ypt.key
```

Performance

Check the SSL performance

```
openssl speed -evp aes-25 6-cbc
```

How to get a A+ at SSL-Labs

Check versions

```
# openssl version
OpenSSL 1.0.1e 11 Feb 2013
# apache2 -v
Server version: Apache /2.2.22 (Debian)
Server built:   Aug 18 2015 09:50:52
```

Enable mods

```
a2enmod ssl
a2enmod headers
a2enmod setenvif
```

Configure virtual host

```
   SSLEngine on

    SSLHon orC iph erOrder On
    SSLCip her Suite ECDHE- RSA -AE S12 8-G CM- SHA 2
6 :kE DH+ AES GCM :EC DHE -RS A-A ES1 28- SHA 256 :EC
    SSLPro tocol -ALL +TLSv1 +TLSv1.1 +TLSv1.2
    SSLCer tif ica teFile      /etc/s sl/ www.ex amp
    SSLCer tif ica teK eyFile   /etc/s sl/ www.ex amp
    SSLCer tif ica teC hai nFile /etc/s sl/ cha in.pe

    SSLStr ict SNI VHo stCheck On

    Header always set Strict -Tr ans por t-S ecurity

    <Fi les Match " \.( cgi |sh tml |ph tml |ph p)$ "
        SSLOptions +StdEn vVars
    </F ile sMa tch>
    <Di rectory /usr/l ib/ cgi -bi n>
        SSLOptions +StdEn vVars
    </D ire cto ry>

    Browse rMatch "MSIE [2-6]" \
        nokeep alive ssl-un cle an- shu tdown \
        downgr ade-1.0 force- res pon se-1.0
    # MSIE 7 and newer should be able to use keepali
    Browse rMatch "MSIE [17-9] " ssl-un cle an- shu t
```