Cheatography

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 privateKey.key
```

Generate a self-signed certificate

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

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

```
openssl req -out CSR.csr -key privateKey.key -new
```

Generate a certificate signing request based on an existing certificate

```
openssl x509 -x509toreq -in certificate.crt -out CSR.csr -signkey privateKey.key
```

Remove a passphrase from a private key

```
openssl rsa -in privateKey.pem -out newPrivateKey.pem
```

Check Files

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

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

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

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

Debugging

Print certificate

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

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

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

Remove Passphrase

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

```
openssl pkcs12 -in keyStore.p12 -out keyStore.pem -nodes
```

Remove Passphrase from key-file

```
openssl rsa -in example.key -out example.nocrypt.key
```

Performance

Check the SSL performance

```
openssl speed sha1
openssl speed aes-256-cbc
openssl speed -evp aes-256-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

SSLHonorCipherOrder On
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-E
SSLProtocol -ALL +TLSv1 +TLSv1.1 +TLSv1.2
SSLCertificateFile /etc/ssl/www.example.com.pem
SSLCertificateKeyFile /etc/ssl/www.example.com.key
SSLCertificateChainFile /etc/ssl/chain.pem

SSLStrictSNIVHostCheck On

Header always set Strict-Transport-Security "max-age=63072000; includeSubdomains; preload"

<FilesMatch "\.(cgi|shtml|phtml|php)$">
SSLOptions +StdEnvVars
</FilesMatch>
<Directory /usr/lib/cgi-bin>
SSLOptions +StdEnvVars
</Directory>

BrowserMatch "MSIE [2-6]" \
nokeepalive ssl-unclean-shutdown \
downgrade-1.0 force-response-1.0
```

How to get a A+ at SSL-Labs (cont)

```
# MSIE 7 and newer should be able to use keepalive
BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
```