Website Hosting - Support #171

The Most Common OpenSSL Commands

08/14/2013 11:23 AM - Daniel Curtis

Status:	Closed	**Start date:**	08/14/2013
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:		**Estimated time:**	0.50 hour
Target version:		**Spent time:**	0.50 hour

Description

One of the most versatile SSL tools is OpenSSL which is an open source implementation of the SSL protocol. There are versions of OpenSSL for nearly every platform, including Windows, Linux, and Mac OS X. OpenSSL is commonly used to create the CSR and private key for many different platforms, including Apache. However, it also has hundreds of different functions that allow you to view the details of a CSR or certificate, compare an MD5 hash of the certificate and private key (to make sure they match), verify that a certificate is installed properly on any website, and convert the certificate to a different format.
Below, is a list of the most common OpenSSL commands and their usage:

General OpenSSL Commands

These commands allow you to generate CSRs, Certificates, Private Keys and do other miscellaneous tasks.

- Generate a new private key and Certificate Signing Request

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

- Generate a **stronger** private key and Certificate Signing Request

```
openssl req -sha512 -out CSR.csr -new -newkey rsa:4096 -nodes -keyout privateKey.key
```

- Generate a self-signed certificate

```
openssl req -x509 -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
```

Checking Using OpenSSL

If you need to check the information within a Certificate, CSR or Private Key, use these commands. You can also check CSRs and check certificates using our online tools.

- 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 Using OpenSSL

If you are receiving an error that the private doesn't match the certificate or that a certificate that you installed to a site is not trusted, try one of these commands. If you are trying to verify that an SSL certificate is installed correctly, be sure to check out the SSL Checker.

- Check an 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
```

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

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

Converting Using OpenSSL

These commands allow you to convert certificates and keys to different formats to make them compatible with specific types of servers or software. For example, you can convert a normal PEM file that would work with Apache to a PFX (PKCS#12) file and use it with Tomcat or IIS. Use our SSL Converter to convert certificates without messing with OpenSSL.

- Combining a .crt and .key into a .pem

```
cat example.com.key example.com.crt > example.com.pem
```

- Combinging a .crt and .key with an intermedate certificate into a .pem

```
cat example.com.key example.com.crt ca.bundle.example.com.crt > example.com.bundle.pem
```

- 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

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

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

- 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
```

History

#1 - 08/07/2014 08:54 AM - Daniel Curtis

- Description updated

#2 - 08/26/2014 04:20 PM - Daniel Curtis

- Description updated

#3 - 01/23/2015 02:15 PM - Daniel Curtis

- Description updated