SSL Shopper

The Most Common OpenSSL Commands

One of the most versatile SSL tools is OpenSSL (http://www.openssl.org/) which is an open source implementation of the SSL protocol. There are versions of OpenSSL for nearly every platform, including Windows (http://www.slproweb.com/products/Win32OpenSSL.html), Linux, and Mac OS X. OpenSSL is commonly used to create the CSR (/what-is-a-csr-certificate-signing-request.html) 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. A compiled version of OpenSSL for Windows can be found here (http://www.slproweb.com/products/Win32OpenSSL.html).

Compare SSL Certificates ❯ (/ssl-certificate-wizard.html)

If you don't want to bother with OpenSSL, you can do many of the same things with our SSL Certificate Tools (/ssl-certificate-tools.html). Below, we have listed 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 self-signed certificate (see How to Create and Install an Apache Self Signed Certificate (/article-how-to-create-and-install-an-apache-self-signed-certificate.html) for more info)**

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

- **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 (csr-decoder.html) and check certificates (certificate-decoder.html) 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 (ssl-checker.html).

- **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 (ssl-converter.html) without messing with OpenSSL.

- **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.cr
```

Compare SSL Certificates ❯ (/ssl-certificate-wizard.html)

Originally posted on Sun Jan 13, 2008

Buy DigiCert Certificate ❯ (https://www.digicert.com/order/order-1.php?rid=011592&rkey=8727e6b5) x

Join the discussion…

LOG IN WITH | **OR SIGN UP WITH DISQUS** ?

Ⓓ Ⓕ Ⓣ Ⓖ | Name

Deryck Henson • 4 years ago

8 years later and still relevant. I love it. Spent hours on this and now all of a sudden I'm finished.

74 ⌃ | ⌄ 1 • Reply •

> **Jan Lund** ➔ Deryck Henson • 2 years ago
>
> 10 years - and counting...
> Excellent stuff :-)
>
> 19 ⌃ | ⌄ • Reply •

>> **Benedict Tesha** ➔ Jan Lund • a year ago • edited
>>
>> 11 years and counting. Cool stuff
>>
>> 5 ⌃ | ⌄ • Reply •

>>> **Luke** ➔ Benedict Tesha • 4 months ago
>>>
>>> 4319 days or 11 years, 9 months, 28 days. Still relevant.
>>>
>>> 1 ⌃ | ⌄ • Reply •

>>> **Michael P.** ➔ Benedict Tesha • a year ago
>>>
>>> 11 years 2 months 1 week 1 day and counting....
>>>
>>> 1 ⌃ | ⌄ • Reply •

>>>> **Dinesh verma** ➔ Michael P. • 9 months ago
>>>>
>>>> 11 years, 4 months, 22 days Still relevant.
>>>>
>>>> ⌃ | ⌄ • Reply •

>>>>> **Alex** ➔ Dinesh verma • 5 months ago
>>>>>
>>>>> 11 years, 8 months and Still relevant.
>>>>>
>>>>> ⌃ | ⌄ • Reply •

>>> **Akos Korsos** ➔ Benedict Tesha • 2 months ago • edited

Q Top Resources

Buy from the highest-rated provider

Buy DigiCert Certificate ➊ (https://www.digicert.com/order/order-1.php?rid=011592&rkey=8727e6b5)   X

🪄 SSL Wizard (/ssl-certificate-wizard.html)
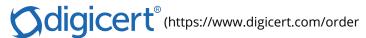
$ Cheap SSL Certificates (/cheapest-ssl-certificates.html)

</> Code Signing Certificates (/cheap-code-signing-certificates.html)

✳ Wildcard Certificates (/best-ssl-wildcard-certificate.html)

🔧 SSL Tools (/ssl-certificate-tools.html)

#1 Rated Certificate Provider

digicert® (https://www.digicert.com/order

/order-1.php?rid=011592&rkey=8727e6b5)

★★★★★

$ Get Pricing (https://www.digicert.com/order/order-1.php?rid=011592&rkey=8727e6b5)

Home (https://www.sslshopper.com/)   SSL Wizard (ssl-certificate-wizard.html)   **SSL FAQ (ssl-faq.html)**

SSL Reviews (certificate-authority-reviews.html)   SSL News (ssl-security-news.html)   Site Map (site-map.html)

About (about-ssl-shopper.html)   SSL Tools (ssl-certificate-tools.html)