**Most Popular**

- SSL Host Headers in IIS 7
- More Discussion About How Firefox 3 Handles SSL Certificates
- Free SSL Certificates from a Free Certificate Authority
- SSL VPN Servers
- SSL Certificates in Google Chrome

**Login:**

Click here to login

# The Most Common OpenSSL Commands

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. A compiled version of OpenSSL for Windows can be found here.

If you don't want to bother with OpenSSL, you can do many of the same things with our SSL Certificate Tools. 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 for more info)**

```
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.

- **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 CACe
```



Posted on January 11, 2008



Rohit Sijwali
Posts: 34

### Re: The Most Common OpenSSL Commands
**Reply #50 on :** Tue October 23, 2012, 00:33:51

Hi,
I want to know that how the passphrase is stored in the Private key file and how openssl or other utility can erify the password.

Alan
Posts: 34

### FireFox Cert Backup
**Reply #49 on :** Wed August 29, 2012, 10:45:01

I have a user cert (.cer) that I've imported onto my Windows machine. I use FireFox to Backup (not export) the cert as pkcs12, and it asks for a certificate backup password to be entered.

If I then run the openssl command on the resulting pkcs12 file:

openssl pkcs12 -in cert.p12

And it has a private key section.

Where did the private key come from?

Mikhail
Posts: 34

### Re: The Most Common OpenSSL Commands
**Reply #48 on :** Sat August 11, 2012, 08:55:53

Awesome article been trying to work out how to get my SAN SSL working on a unix box other servers are windows apps and this little number gave me what I had been searching for for almost 2 weeks never had to use openssl before.

pfx converted and got me my priv key generated on II6 so I could get it onto the unix box.
Might be an old article but it works for me.

Mikhail
Melbourne, Australia
www.hostingworx.com.au

**Robert**
Posts: 15

### Re:.crt to .key
**Reply #47 on :** Fri July 27, 2012, 09:16:27

Hi Nick,

There is no way to convert a .crt to a .key file. If you can't locate the .key file you will need to generate a new key and CSR and re-key your certificate.

Nick
Posts: 34

### .crt to .key
**Reply #46 on :** Fri July 27, 2012, 01:13:44

Hi All.

Would like to know how to convert .crt file to .key file.

snow6oy
Posts: 34

### Re: The Most Common OpenSSL Commands
**Reply #45 on :** Mon July 09, 2012, 14:06:50

Very handy reference. The command to sign a certificate using your own CA might help too.

openssl ca -in x.csr -out x.crt -config openssl.conf

**Robert**
Posts: 15

### Re: How to convert .PEM to PFX or .Cer to .PFX dont have key for certificate
**Reply #44 on :** Fri June 15, 2012, 08:57:16

Hi Prasad,

If you don't have the private key, you won't be able to covert it to a pfx file. You will need to generate a new certificate.

Prasad
Posts: 34

### How to convert .PEM to PFX or .Cer to .PFX dont have key for

### certificate
**Reply #43 on :** Thu June 14, 2012, 09:35:56

Hi
would like to do following
convert .PEM to PFX or .Cer to .PFX
however dont have key for certificate only .pem and .cer file is available

Help appriciated

Jana
Posts: 34

### Verify Certificate against a CA bundle file using openssl
**Reply #42 on :** Fri March 02, 2012, 02:02:13

openssl verify -CAfile <CA-bundle.crt> <Certificate.crt>

Ramesh
Posts: 34

### How to import the certificate
**Reply #41 on :** Tue February 21, 2012, 07:55:10

I would like to know how to import the received .cer file into the already existing .crt file.

bryant
Posts: 34

### in reply to #39
**Reply #40 on :** Thu January 26, 2012, 12:36:36

use the -batch option to suppress the command line interaction

Adam
Posts: 34

### Convert from crt to pfx
**Reply #39 on :** Fri December 02, 2011, 22:46:16

i'm using openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -certfile CACert.crt
and it works perfectly
but when i want to run it from php like this

system("openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -certfile CACert.crt");

my output file is always 0 bytes.
i tried

system('echo "Password" | openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -certfile CACert.crt');

with password, with no password ... when i run it from php it doenst work
i think its because i can't seem to be able to send parameters when it asks me to input export password

Any Suggestions ?

El-Shazli
Posts: 34

### convert to apk
**Reply #38 on :** Sun October 16, 2011, 05:26:00

How could I convert SSL certificate from CER and P7B to apk to be able to set up on mobile Samsung Galaxy Tap p1000.

JayOdom
Posts: 34

### convert pfx to pem
**Reply #37 on :** Fri September 16, 2011, 14:08:06

Solution to Reply to #22:

Move the '-nodes' option from this:
C:\OpenSSL\bin>openssl pkcs12 -in cert.pfx -out cag.pem -nodes

To This:
C:\OpenSSL\bin>openssl pkcs12 -in cert.pfx -nodes -out cag.pem

JayOdom
Posts: 34

### convert pfx to pem
**Reply #36 on :** Fri September 16, 2011, 13:43:24

I am having the same issue Heinz is having in the post below mine.

Anyone know what could be wrong?

Heinz
Posts: 34

### convert pfx to pem
**Reply #35 on :** Tue September 06, 2011, 08:29:18

Hello,

running on a win2008 r2 as an administrator:

What could be the reason that the following error occurs:

C:\>cd C:\OpenSSL\bin

C:\OpenSSL\bin>dir C:\OpenSSL\bin\cert.pfx
Volume in Laufwerk C: hat keine Bezeichnung.
Volumeseriennummer: 7CD4-6EAD

Verzeichnis von C:\OpenSSL\bin

06.09.2011 14:53 2.709 cert.pfx
1 Datei(en), 2.709 Bytes
0 Verzeichnis(se), 92.737.318.912 Bytes frei

C:\OpenSSL\bin>openssl pkcs12 -in cert.pfx -out cag.pem -nodes
Usage: pkcs12 [options]
where options are
-export output PKCS12 file
-chain add certificate chain
-inkey file private key if not infile
-certfile f add all certs in f
-CApath arg - PEM format directory of CA's
-CAfile arg - PEM format file of CA's
-name "name" use name as friendly name
-caname "nm" use nm as CA friendly name (can be used more than once).
-in infile input filename
-out outfile output filename
-noout don't output anything, just verify.
-nomacver don't verify MAC.
-nocerts don't output certificates.
-clcerts only output client certificates.
-cacerts only output CA certificates.
-nokeys don't output private keys.
-info give info about PKCS#12 structure.
-des encrypt private keys with DES
-des3 encrypt private keys with triple DES (default)
-idea encrypt private keys with idea
-aes128, -aes192, -aes256
encrypt PEM output with cbc aes
-nodes don't encrypt private keys
-noiter don't use encryption iteration
-maciter use MAC iteration
-twopass separate MAC, encryption passwords
-descert encrypt PKCS#12 certificates with triple DES (default RC2-40)
-certpbe alg specify certificate PBE algorithm (default RC2-40)
-keypbe alg specify private key PBE algorithm (default 3DES)
-keyex set MS key exchange type
-keysig set MS key signature type
-password p set import/export password source
-passin p input file pass phrase source
-passout p output file pass phrase source
-engine e use engine e, possibly a hardware device.
-rand file;file;...
load the file (or the files in the directory) into
the random number generator
-CSP name Microsoft CSP name
-LMK Add local machine keyset attribute to private key

C:\OpenSSL\bin>

It would be very helpful, when you could help me to solve this issue.

Thanks a lot

Regards

Heinz

**Robert**
Posts: 15

### Re: covert RSA private key to X509
**Reply #34 on :** Wed August 24, 2011, 18:38:39

Hi Madan,

The key may already be in X509 format if you can read it in a text editor. If you cannot, it is probably in binary format (der). In that case you can convert it to x509 using the converter or running the OpenSSL command.

Madan
Posts: 34

### covert RSA private key to X509
**Reply #33 on :** Wed August 24, 2011, 07:09:13

Hi,

Is it possible to convert key the private key in RSA format to X509 format... Kindly advise on the possibility.

sara sat
Posts: 34

### cross certification
**Reply #32 on :** Mon May 09, 2011, 06:08:52

hi all
how can i cross certify 2 self sign certificates

SafeTinspector
Posts: 34

### Good, concise, just what I needed. Thanks
**Reply #31 on :** Thu April 28, 2011, 14:04:02

Had need to get a cert into eDirectory and it only wanted PKCS#12 while all I had was CER and KEY from when I got a cert for their SMTP daemon.
Problem solved and I didn't need to do a bunch of reading to get there from here.

Showing comments **1** to **20** of **50** | Next | Last

## Write a comment

Name:

Email: (not published)

Subject:

Comment:


Security Code:

Post Comment