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

- **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
```

Originally posted on Sun Jan 13, 2008

81 Comments **SSL Shopper** **Oriol Rius**

Recommend 21 **Share** **Sort by Best**

Join the discussion…

Jana • 2 years ago
openssl verify -CAfile <ca-bundle.crt> <certificate.crt>
6 • Reply • Share ›

antoniok.spb • a year ago
DH parameter generation:

openssl dhparam -out dhparam.pem 2048
2 • Reply • Share ›

Jim ➚ antoniok.spb • a month ago
If you wanted 4096, add the -dsaparam so you're not waiting for 2 days for the command to complete.

openssl dhparam -dsaparam -out dhparam.pem 4096
• Reply • Share ›

Ye Wang • 8 months ago
Use this to check Diffie-Hellman primes via: `openssl dhparam -in dhparams.pem -text -noout` and `dhparams.pem` can be generated by `openssl dhparam -out dhparams.pem 2048`
1 • Reply • Share ›

NoelTheOne • a year ago
At this point, I strongly recommend adding '-sha256' when creating a new csr, to get a SHA256 certificate rather than an outdated SHA1 certificate.
1 • Reply • Share ›

intranovo Mod ➚ NoelTheOne • a year ago
Thanks. I added that to the self-signed certificate CSR command. I didn't add it to the others because certificate providers almost always ignore what is in the CSR and use whatever algorithm they want to sign the actual certificate when it is issued (and all certificate providers should be issuing SHA2 by default now because SHA1 certificates will soon stop working in web browsers).
1 • Reply • Share ›

NoelTheOne ➚ intranovo • a year ago
Sadly, "should" isn't necessarily "will." A number of providers are still issuing SHA1 certificates by default. Hopefully recent browser changes will force the change, but it hasn't happened yet.
• Reply • Share ›

Drummer Ubuntu • a month ago
This is pretty awesome, thank you!
• Reply • Share ›

David Valladares • 7 months ago
Nice post. Thank You!!!
• Reply • Share ›

Franck Dakia • 8 months ago
Thank You!
• Reply • Share ›

Swaroop • 8 months ago
I'm getting this issue, when i'm trying to connect to server through .pem file

curl: (58) unable to set private key file: '/tmp/.pem' type PEM
• Reply • Share ›

Sally Vuong • 10 months ago
Hi what does -des3 mean in openssl?
• Reply • Share ›

intranovo Mod ➚ Sally Vuong • 10 months ago
Using the -des3 option will encrypt private keys with triple DES which is the default so you don't need to specify it.
• Reply • Share ›

ewert59 • 2 years ago
There is also a "Check connection via SMTP" - STARTTLS or not - possible:

openssl s_client -starttls smtp &#91 -cipher 'ALL:!RC4' &#93 -connect alt1.gmail-smtp-in.l.google.co...:25

Here, openssl uses a connection to the mail server of google.com and checks the starttls option. With the switch -cipher, you can select between cipher algorithms, here, "all without RC4". Don't use the brackets. That means, you can use this switch or not.
• Reply • Share ›

Nisha • 2 years ago
Of course, for this to work, you'll need viartul hosts on ports 80 and 443 for your blog. Also, you'll need an SSL certificate for your blog. You can snag one from a reputable provider or make your own.
• Reply • Share ›

Manish • 2 years ago
I have created CA certificate using openssl commands
After successful generation, Certificate information has version V1 which i want to change to V2 or V3 but i didn't find any command to change it. Kindly let me know do we have command for this also
• Reply • Share ›

Merk • 2 years ago
I am no expert, but the version depends on cert extensions. A v1 cert has no extensions at all. So you will have to recreate your cert and supply some extensions.
• Reply • Share ›

Matt • 2 years ago
im using the following command:

openssl pkcs12 -export -in < CAfilename1.cer > -out < CAfilename.cer2.p12> -name < Ã¢Â €Âœalias nameÃ¢Â€Â> /nhin/nss-3.12.4/bin/pk12util -i < CAfilename.cer2.p12> -n < alias name> -d $AS_HOME/domains/nssdomain/config replacing with correct info in brackets, yet command does nothing... it just lists the options... any help here would be appreciated
• Reply • Share ›

Timothy • 2 years ago
Hi experts,
Im debugging OpenSSL code to rootcause BAD_RECORD_MAC error by ssl. by looking at the error it is digest failure. I just want to know what are the crypro algorithms and keys generated for the current session? Any API's are there to fetch this info???

Thanks
Timothy
• Reply • Share ›

Sreedhar • 2 years ago
May i know what is the procedure to generate .crt and .key files for an existing .csr file. When i requested the Cybertrust Public SureServer Standard SSL Certificate they issued me two .pem files(cert.pem and chainp7.pem). Is there any possibility to create .crt and .key files using those .pem files?
• Reply • Share ›

Robert • 2 years ago
You can't generate a .key file if you only have the CSR. You will need to generate a new CSR and Key and have your certificate provider sign the new key (by reissuing or rekeying the certificate).
• Reply • Share ›

jossy • 2 years ago
Hi,
I tried exporting my certificate to below format.
DER enabled X.509(cer)
Base64 encoded X.509(cer)

PKCS7(p7b)
Option to export private key is disabled for me in IE.
I was trying to convert the above files to PEM format using openSSL to be used in load runner Vugen for playback.
Any help would be appreciated.
I am getting some error

OpenSSL> pkcs12 -in M:/scripts/IBDFocus/WF01/cert/jossyB64.cer -out M:/scripts/IBDFocus/WF01/cert/jossy.pem
10272:error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag:.\crypto\asn1\tasn_dec.c:1316:
10272:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 error:.\crypto\asn1\tasn_dec.c:380:Type=PKCS12
error in pkcs12

see more

• Reply • Share ›

Ankit • 2 years ago
Hi All,

Can anyone help me in generating a CSR that has multiple State names. I am basically looking to get this for a Validation point. Please help if anyone is aware of how to achieve this.

• Reply • Share ›

Vlion • 2 years ago
Hi everyone. Hope you are great. Can you please help with this question? When converting a pem certificate to pkcs12 I'm asked for a export password. What is it?

Thanks and Regards

• Reply • Share ›

John Lin ➚ Vlion • a year ago
you can try to leave it blank. just ignore the request and return twice.

• Reply • Share ›

JRJ • 2 years ago
You make it up. The passphrase is used to protect the private key. When any application attempts to use the private key (or you import it into a keystore), the user will be prompted to supply the passphrase.

• Reply • Share ›

abraham • 2 years ago
For a Cisco Device I require a certificate which must include SAN (alternative subject names) so my Web authentication can work. I tried to open the certificate that I created using the following command but I am getting an error:

OpenSSL> x509 -text -in c:\openssl\MYCertificate.pem

I am running Openssl in a Win7 64bits laptop and created certificates in the past which are working fine.

ERROR:

Error opening Certificate :\openssl\MYCertificate.pem
4292:error:02001002:system library:fopen:No such file or directory:.\crypto\bio\bss_file.c:352:fopen('c:\openssl\MYCertificate.pem','rb')
4292:error:20074002:BIO routines:FILE_CTRL:system lib:.\crypto\bio\bss_file.c:354:
unable to load certificate
error in x509
OpenSSL>

• Reply • Share ›

Murthy • 2 years ago
Hi,
Is it possible to concatinate 3 pem files into 1 if so what is the command in pksc12.

Desc: we have 3 web servers above these 3 we have a load balancer, we need to give the keys of these 3 web servers to the load balancer site. As the site is accessible with the common URL we need to give all the 3 keys in a single pem file and upload.

Regards,
Murthy.

• Reply • Share ›

Mahean • 2 years ago

How to generate a new private key and Certificate Signing Request using DSA Algorithm from open SSL command

Reply • Share ›

mahesh • 2 years ago

how to verify the CRL certificate? and
Error 60: server certificate verification failed. CAfile: /etc/ssl/certs/ca-certificates.crt CRLfile: none.
any one get solution for this?

Reply • Share ›

Rohit Sijwali • 2 years ago

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.

Reply • Share ›

Mikhail • 2 years ago

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

Reply • Share ›

Alan • 2 years ago

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?

Reply • Share ›

Nick • 2 years ago

Hi All.

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

Reply • Share ›

snow6oy • 2 years ago

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

Reply • Share ›

Robert • 2 years ago

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.

Reply • Share ›

Prasad • 2 years ago

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

Reply • Share ›

Ramesh • 2 years ago

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

Reply • Share ›

Robert • 2 years ago

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.

Reply • Share ›

bryant • 2 years ago

use the -batch option to suppress the command line interaction

Reply • Share ›

El-Shazli • 2 years ago

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

Reply • Share ›

Heinz • 2 years ago

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]

see more

Reply • Share ›

JayOdom • 2 years ago

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

Reply • Share ›

JayOdom • 2 years ago

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

Anyone know what could be wrong?

Reply • Share ›

Adam • 2 years ago

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 ?

Reply • Share ›

powerhdeleon ➔ Adam • 6 months ago

you solved this?

Reply • Share ›

Madan • 2 years ago
Hi,

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

• Reply • Share ›

Robert • 2 years ago
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.

• Reply • Share ›

Robert • 2 years ago
Hi Will,

There is no way to restore the .key file. You will need to create a new one and then reissue your certificate.

• Reply • Share ›

sara sat • 2 years ago
hi all
how can i cross certify 2 self sign certificates

• Reply • Share ›

Load more comments