

Instructions to Convert OpenSSL to PKCS v1.0

November 12, 2013

Convert “.CER” and “.PFX” Digital Certs to “.CRT” and “.KEY” Format

Purpose: This document is for the system administrator(s) who will be downloading and configuring FTP Client to use Digital Certificates. If your FTP Client doesn't support “.cer” and “.pfx” format of Digital Certificates, please follow these instructions to have the Certificates converted into “.crt” and “.key” format. You will need OpenSSL – a tool to convert Digital Certificates into the proper format.

Step 1: Download OpenSSL

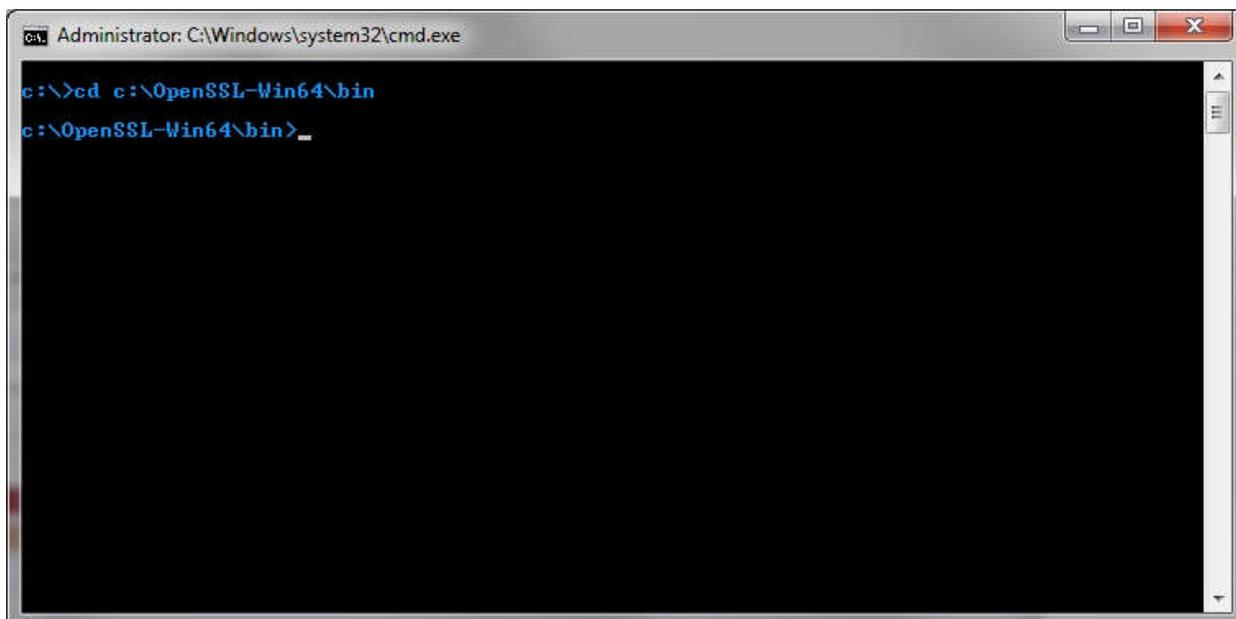
- OpenSSL can be downloaded from <http://slproweb.com/products/Win32OpenSSL.html>
- **Note:** You may be prompted to download and install the [Visual C++ 2008 Redistributables](#), which can also be downloaded from the link above.

Step 2: Navigate to OpenSSL on your machine

Option 2a:

OpenSSL tool needs to be run from the command prompt. By default, the executable installs to, and resides in the \OpenSSL-Win64 or Win32\bin folder depending upon which Windows version (64 bit or 32 bit) you are running on.

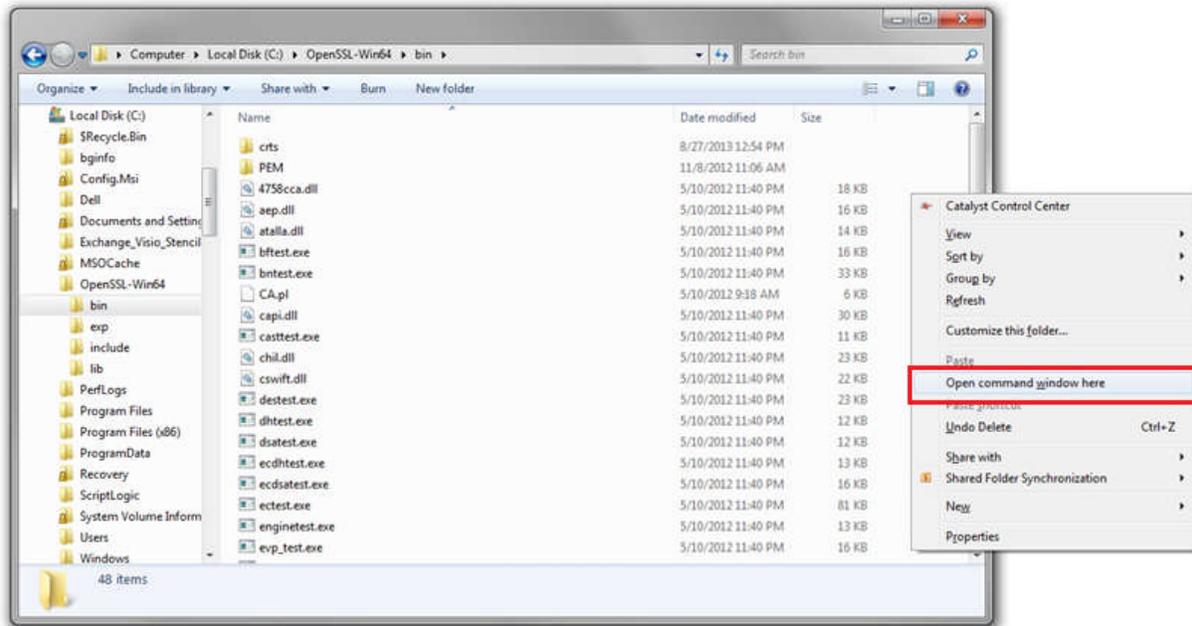
Open a command window and navigate to the bin folder with the command **cd c:\OpenSSL-Win64\bin** or **cd c:\OpenSSL-Win32\bin**



```
Administrator: C:\Windows\system32\cmd.exe
c:\>cd c:\OpenSSL-Win64\bin
c:\OpenSSL-Win64\bin>_
```

Option 2b:

Alternatively, a command window can be opened directly from a specified directory (“C:\OpenSSL-Win64\Bin” or “C:\OpenSSL-Win32\Bin”) in the Windows Explorer. Hold the Shift key and right click in the blank area and click on “Open command window here”.

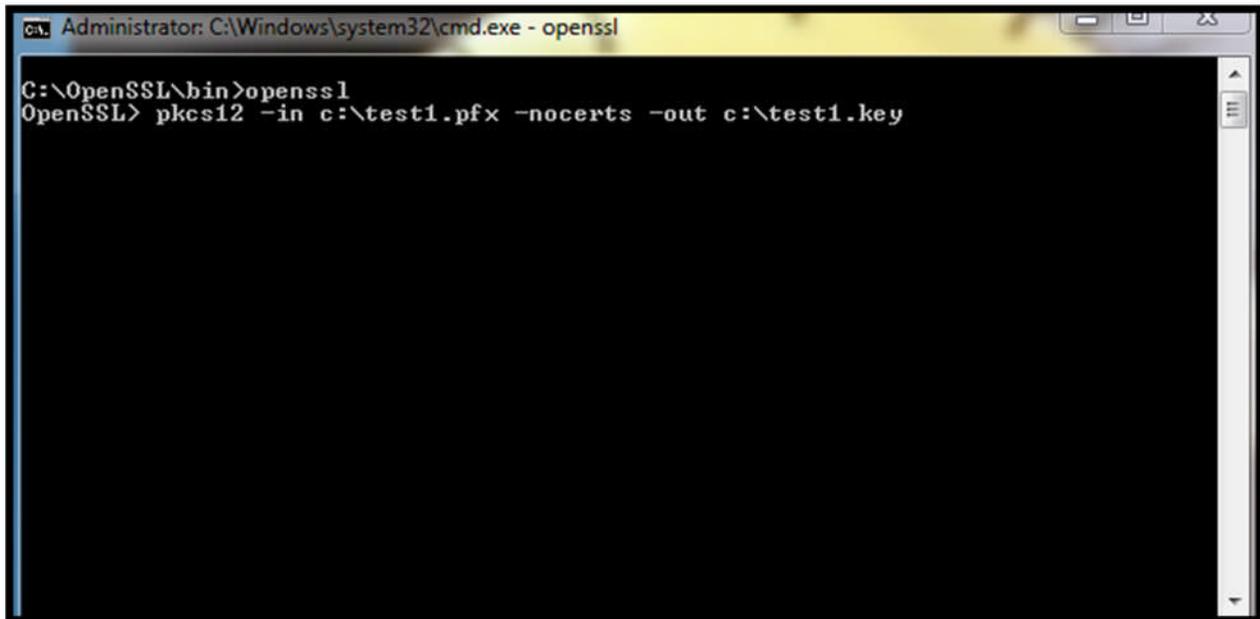


Step 3: Execute the command

Once the Digital Cert has been backed up/extracted into a .pfx file, it is ready to be converted. **Note:** Please remember the password used to extract the Digital Cert. In order for you to execute the command, you need to have the source file location of the “*.pfx” file and the destination location of the desired output file in the converted format. In the example below, the command will convert “certificate.pfx” file into “certificate.key”.

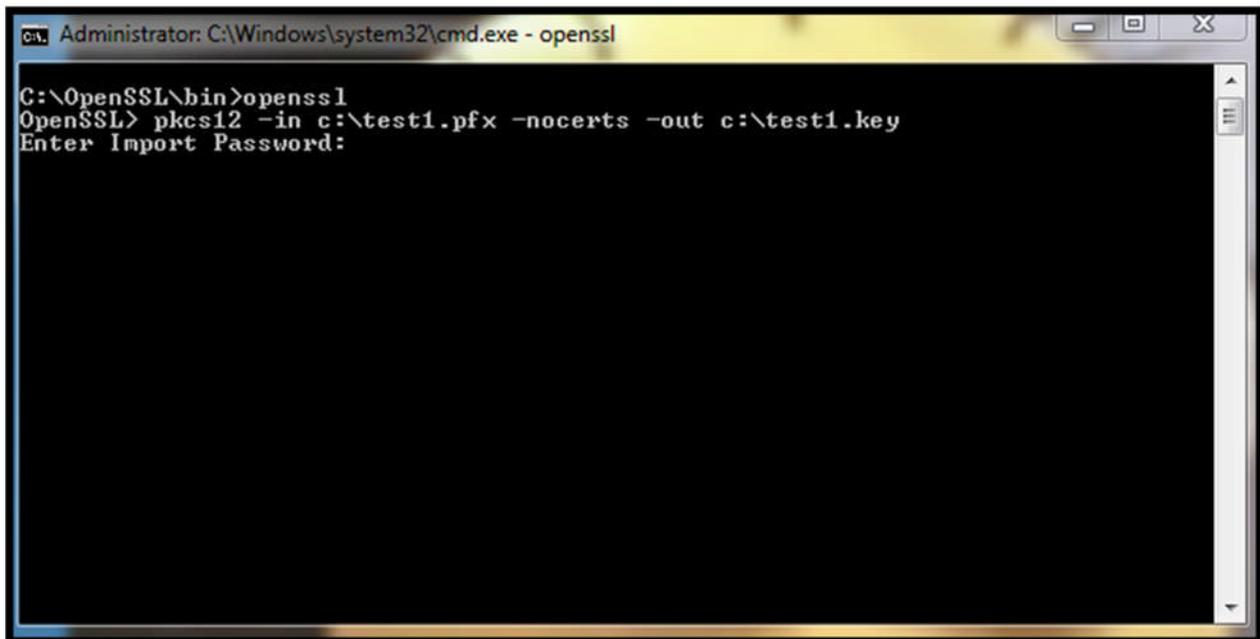
Enter the command **OpenSSL** and hit enter.

Type `pkcs12 -in c:\filename.pfx -nocerts -out c:\filename.key` to convert the private key from a .pfx to .key (private key) format.



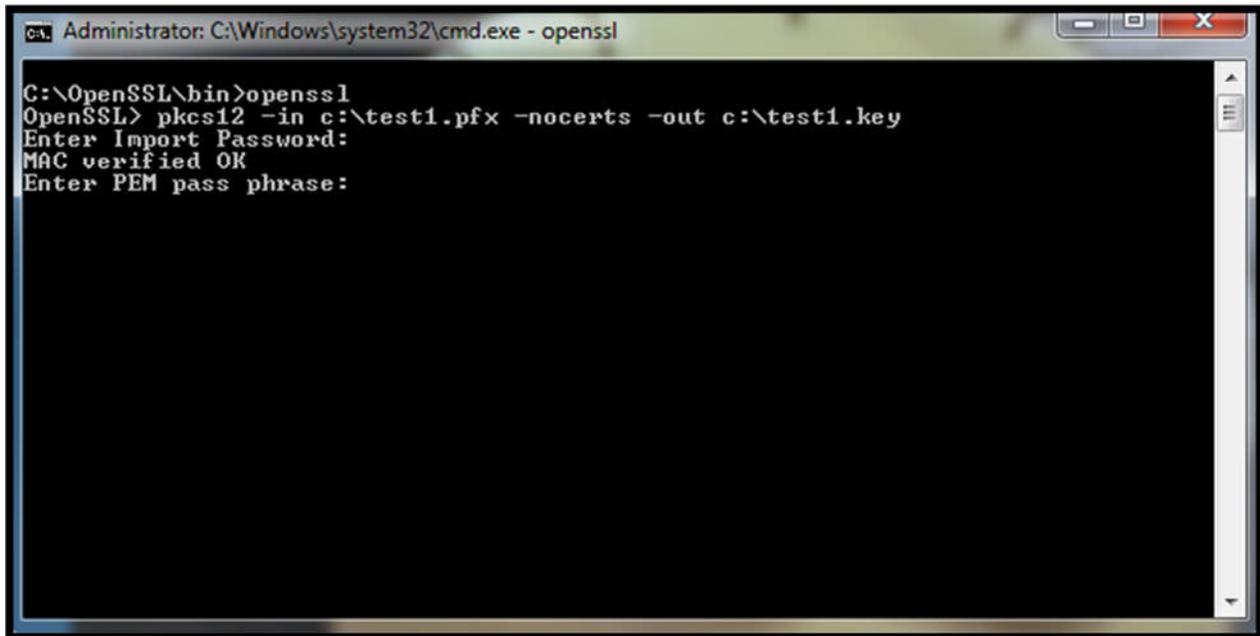
```
Administrator: C:\Windows\system32\cmd.exe - openssl
C:\OpenSSL\bin>openssl
OpenSSL> pkcs12 -in c:\test1.pfx -nocerts -out c:\test1.key
```

When prompted, please enter the password used while exporting the Digital Cert into a file – when the “.pfx” file was created.



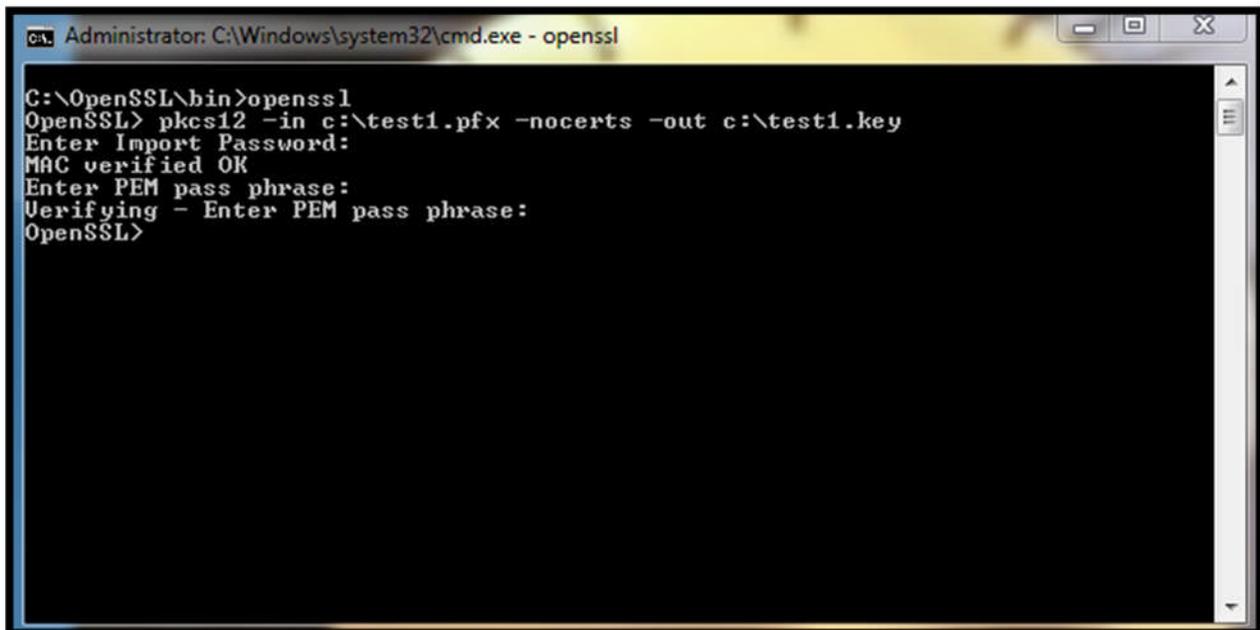
```
Administrator: C:\Windows\system32\cmd.exe - openssl
C:\OpenSSL\bin>openssl
OpenSSL> pkcs12 -in c:\test1.pfx -nocerts -out c:\test1.key
Enter Import Password:
```

If the password is accepted, the verification will be printed on the screen. If asked please enter the PEM pass phrase. This can be a new or same password that was used for the Import Password.



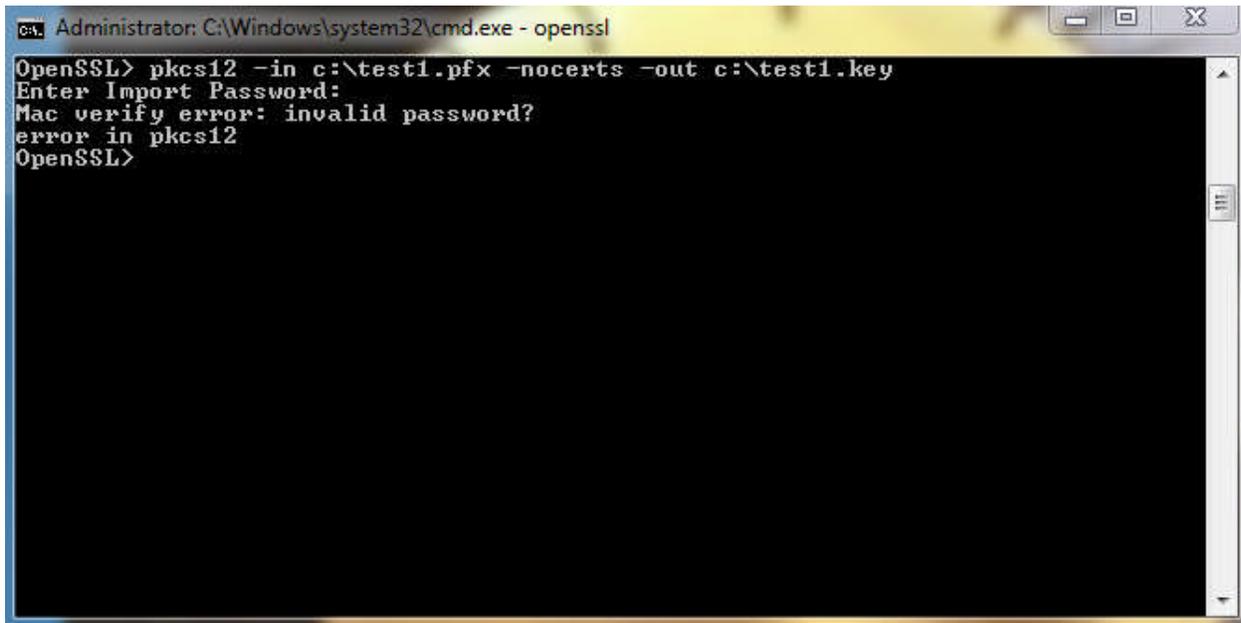
```
Administrator: C:\Windows\system32\cmd.exe - openssl
C:\OpenSSL\bin>openssl
OpenSSL> pkcs12 -in c:\test1.pfx -nocerts -out c:\test1.key
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
```

Once PEM pass phrase is entered it will ask to verify. Enter the password again.



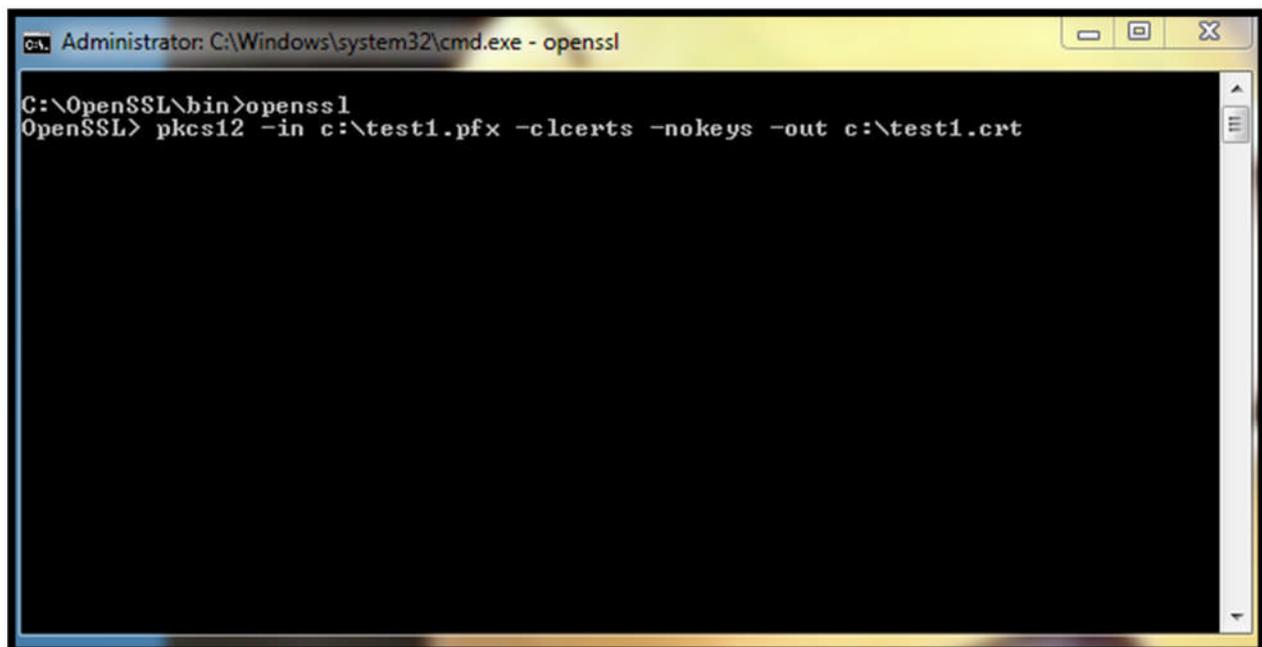
```
Administrator: C:\Windows\system32\cmd.exe - openssl
C:\OpenSSL\bin>openssl
OpenSSL> pkcs12 -in c:\test1.pfx -nocerts -out c:\test1.key
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
OpenSSL>
```

If the password is incorrect, a notification will be printed on the screen.



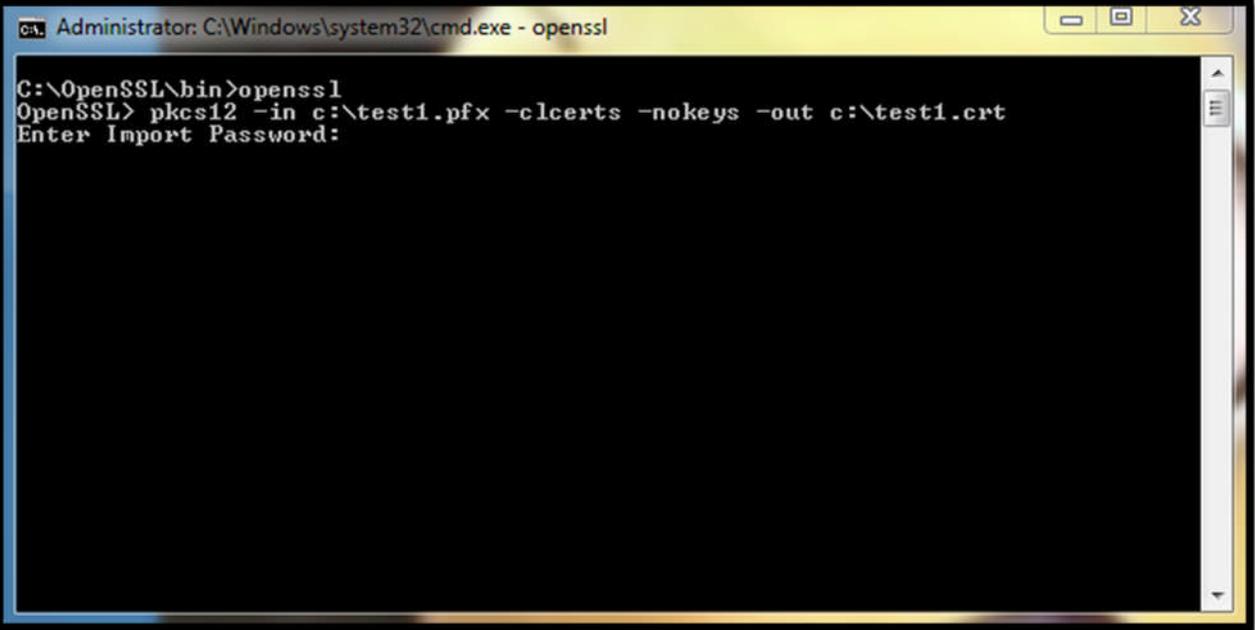
```
Administrator: C:\Windows\system32\cmd.exe - openssl
OpenSSL> pkcs12 -in c:\test1.pfx -nocerts -out c:\test1.key
Enter Import Password:
Mac verify error: invalid password?
error in pkcs12
OpenSSL>
```

Enter the command **pkcs12 -in c:\filename.pfx -clcerts -nokeys -out c:\filename.crt** to convert the private key from a .pfx to .crt (public key) format.



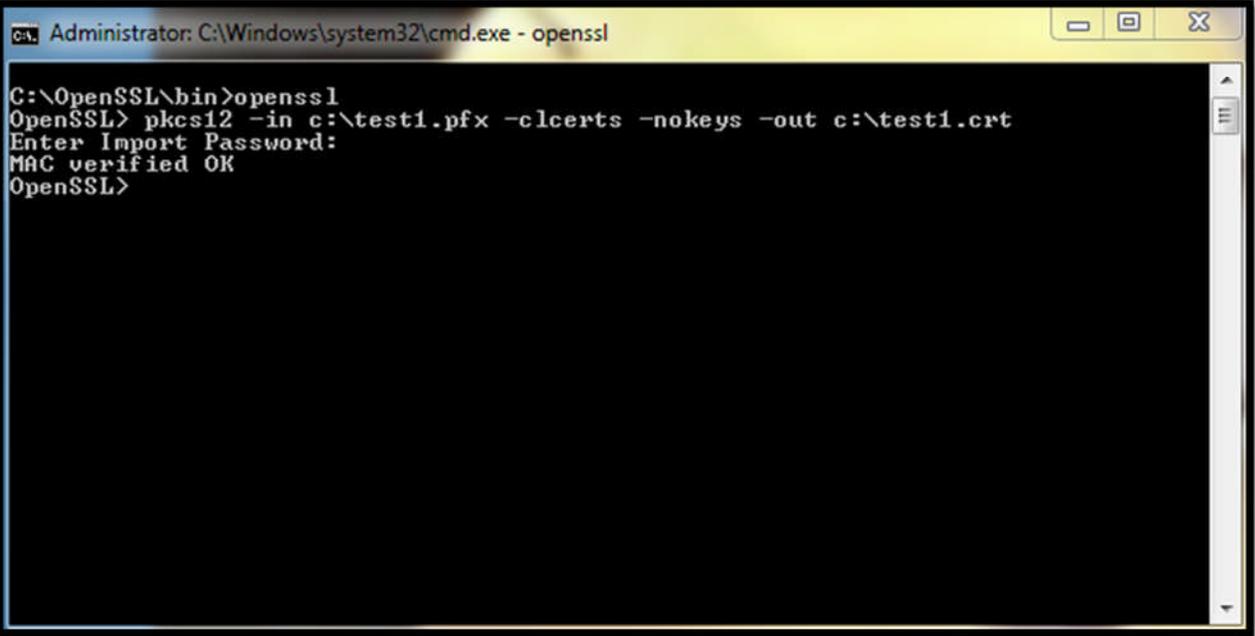
```
Administrator: C:\Windows\system32\cmd.exe - openssl
C:\OpenSSL\bin>openssl
OpenSSL> pkcs12 -in c:\test1.pfx -clcerts -nokeys -out c:\test1.crt
```

Enter the same password used for the .key conversion.



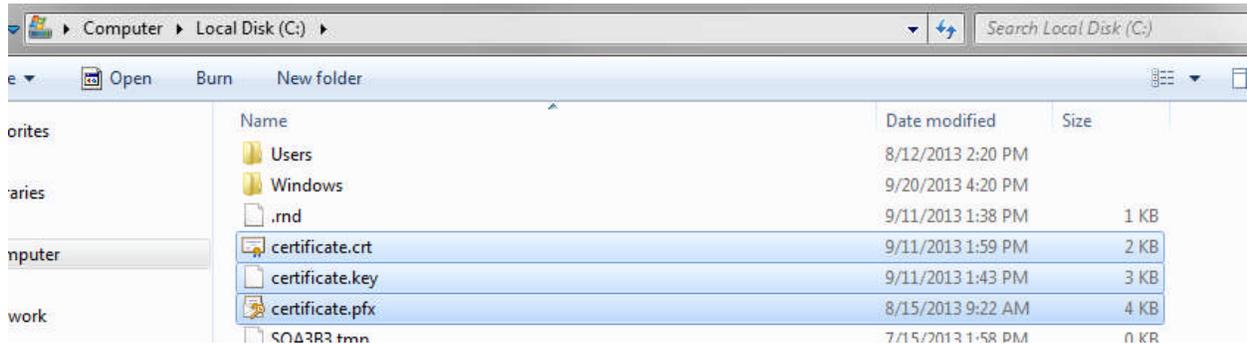
```
Administrator: C:\Windows\system32\cmd.exe - openssl
C:\OpenSSL\bin>openssl
OpenSSL> pkcs12 -in c:\test1.pfx -clcerts -nokeys -out c:\test1.crt
Enter Import Password:
```

Next you will see MAC verified OK



```
Administrator: C:\Windows\system32\cmd.exe - openssl
C:\OpenSSL\bin>openssl
OpenSSL> pkcs12 -in c:\test1.pfx -clcerts -nokeys -out c:\test1.crt
Enter Import Password:
MAC verified OK
OpenSSL>
```

Once both files have been generated they can be retrieved at the location specified in the commands.



Step 4: Reference(s)

For more information about OpenSSL and certificate formats click on the following links:

<http://www.openssl.org/>

<https://www.sslshopper.com/ssl-converter.html>

<http://www.sslshopper.com/article-most-common-openssl-commands.html>