

## Selbstsigniertes Code Signing Zertifikat erstellen

Mit diesem Befehl erstellen wir ein Schlüsselpaar sowie ein selbstsigniertes Zertifikat.

```
openssl req -new -newkey rsa:2048 -days 365 -nodes -x509 -keyout server.key -out server.crt
```

Mit diesem Befehl erstellen wir aus dem Privat.Key und dem selbstsignierten Zertifikat ein .pfx Zertifikat.

```
openssl pkcs12 -export -out codesign.pfx -inkey server.key -in server.crt
```

codesign.pfx	22.10.2016 21:06	Privater Informati...	3 KB
server.crt	22.10.2016 21:04	Sicherheitszertifikat	2 KB
server.key	22.10.2016 21:04	KEY-Datei	2 KB
.rnd	22.10.2016 21:04	RND-Datei	1 KB

```
Administrator: C:\Windows\system32\cmd.exe

C:\OpenSSL-Win64\bin>openssl req -new -newkey rsa:2048 -days 365 -nodes -x509 -keyout server.key -out server.crt
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'server.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:NRW
Locality Name (eg, city) []:Essen
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Der Windows Papst
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:https://der-windows-papst.de
Email Address []:info@der-windows-papst.de

C:\OpenSSL-Win64\bin>openssl pkcs12 -export -out codesign.pfx -inkey server.key -in server.crt
Enter Export Password:
Verifying - Enter Export Password:

C:\OpenSSL-Win64\bin>
```

Alternativ:

```
openssl req -subj /CN=der-windows-papst.de,/O=DerWindowsPapst,/C=DE -new -newkey rsa:2048 -days 365 -nodes -x509 -keyout server.key -out server.crt
```

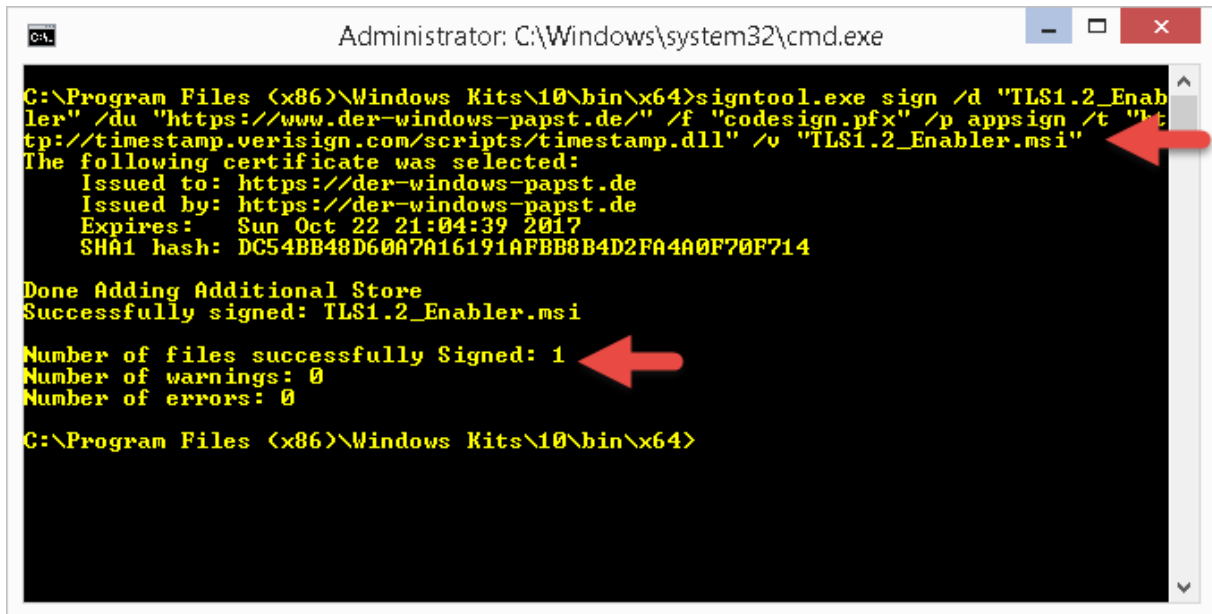
```
Administrator: C:\Windows\system32\cmd.exe

C:\OpenSSL-Win64\bin>openssl req -subj /CN=der-windows-papst.de,/O=DerWindowsPapst,/C=DE -new -newkey rsa:2048 -days 365 -nodes -x509 -keyout server.key -out server.crt
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'server.key'

C:\OpenSSL-Win64\bin>
```

## Selbstsigniertes Code Signing Zertifikat erstellen

```
signtool.exe sign /d "TLS1.2_Enabler" /du "https://www.der-windows-papst.de/" /f "codesign.pfx" /p appsign /t "http://timestamp.verisign.com/scripts/timestamp.dll" /v "TLS1.2_Enabler.msi"
```



```
Administrator: C:\Windows\system32\cmd.exe

C:\Program Files (x86)\Windows Kits\10\bin\x64>signtool.exe sign /d "TLS1.2_Enabler" /du "https://www.der-windows-papst.de/" /f "codesign.pfx" /p appsign /t "http://timestamp.verisign.com/scripts/timestamp.dll" /v "TLS1.2_Enabler.msi"
The following certificate was selected:
  Issued to: https://der-windows-papst.de
  Issued by: https://der-windows-papst.de
  Expires:   Sun Oct 22 21:04:39 2017
  SHA1 hash: DC54BB48D60A7A16191AFBB8B4D2FA4A0F70F714

Done Adding Additional Store
Successfully signed: TLS1.2_Enabler.msi

Number of files successfully Signed: 1
Number of warnings: 0
Number of errors: 0

C:\Program Files (x86)\Windows Kits\10\bin\x64>
```