

Generating a Certificate Signing Request (CSR) Using OpenSSL on Windows

Objective

This class activity aimed to generate a Certificate Signing Request (CSR) using OpenSSL on a Microsoft Windows system. This process is essential for creating a secure connection between a web server and a client by ensuring that a trusted certificate authority (CA) can authenticate the server's identity.

Introduction

A Certificate Signing Request (CSR) is a block of encoded text given to a Certificate Authority when applying for an SSL Certificate. It contains information such as the organization name, domain name, locality, and country. Generating a CSR is the first step in obtaining an SSL certificate, which is necessary for encrypting data transmitted over the internet.

This activity involved using OpenSSL, a robust and full-featured toolkit for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols, as well as a general-purpose cryptography library. The steps included installing OpenSSL, generating a private key, and creating a CSR that encapsulates the necessary information for certificate enrollment.

Class Activity

Environment:

- Operating System: Microsoft Windows 10
- OpenSSL Version: OpenSSL-Win32

Commands Executed:

```
cd \Program Files (x86)\OpenSSL-Win32\bin
```

```
openssl genrsa -out private-key.key 2048
```

```
openssl req -new -key private-key.key -out csr.txt
```

User Input:

- Country Name: KE
- State or Province Name: Nairobi
- Locality Name: Nairobi
- Organization Name: USIU
- Organizational Unit Name: APT3090
- Common Name: nairobi.com

File Management:

```
md c:\certificate
```

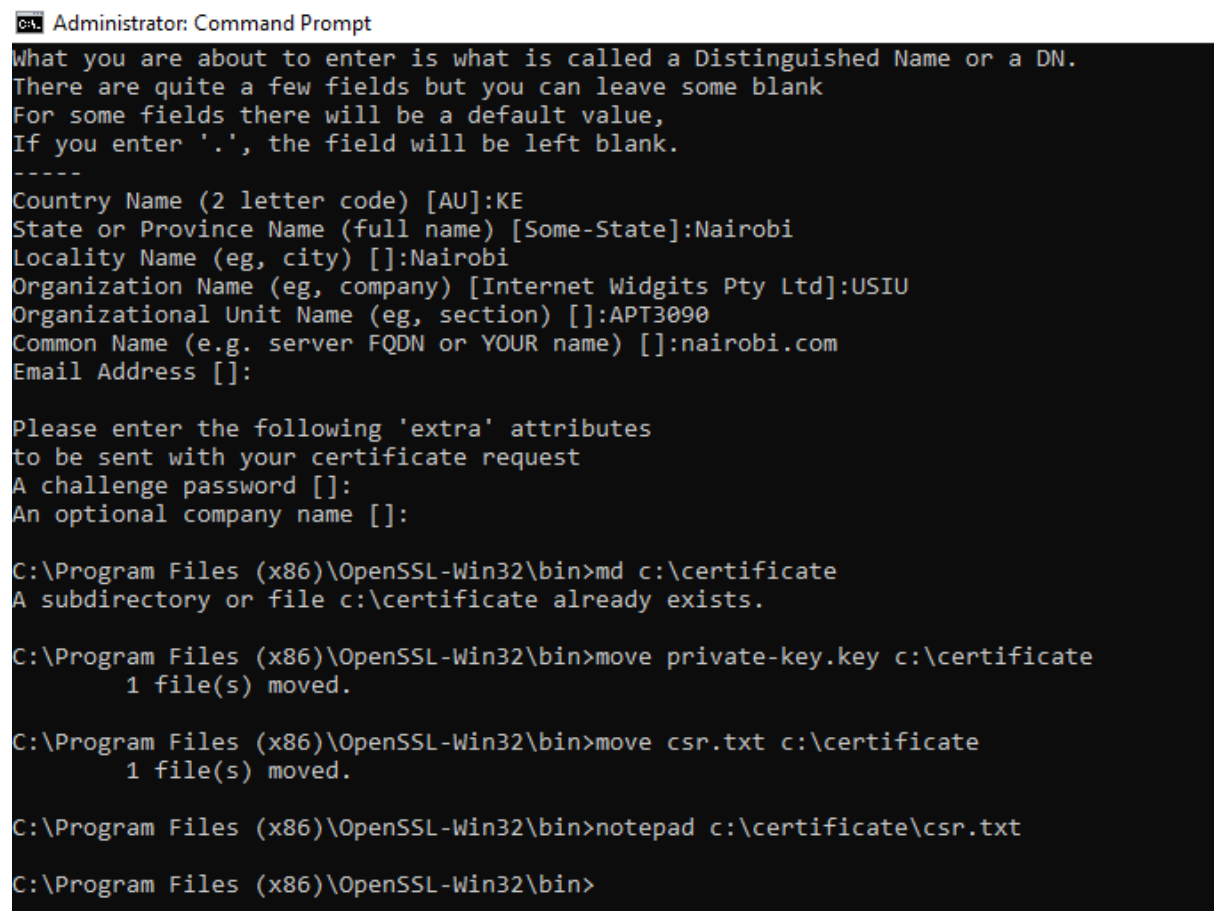
```
move private-key.key c:\certificate
```

```
move csr.txt c:\certificate
```

```
notepad c:\certificate\csr.txt
```

Observations

- Successfully generated a private key and CSR.
- The csr.txt file contains the required information for certificate enrollment.
- Proper directory management was performed to store the generated files.



```
Administrator: Command Prompt
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]:KE
State or Province Name (full name) [Some-State]:Nairobi
Locality Name (eg, city) []:Nairobi
Organization Name (eg, company) [Internet Widgits Pty Ltd]:USIU
Organizational Unit Name (eg, section) []:APT3090
Common Name (e.g. server FQDN or YOUR name) []:nairobi.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

C:\Program Files (x86)\OpenSSL-Win32\bin>md c:\certificate
A subdirectory or file c:\certificate already exists.

C:\Program Files (x86)\OpenSSL-Win32\bin>move private-key.key c:\certificate
1 file(s) moved.

C:\Program Files (x86)\OpenSSL-Win32\bin>move csr.txt c:\certificate
1 file(s) moved.

C:\Program Files (x86)\OpenSSL-Win32\bin>notepad c:\certificate\csr.txt

C:\Program Files (x86)\OpenSSL-Win32\bin>
```

A new window (i.e. Notepad) opened which contains the information needed to enroll for a certificate as shown below



csr.txt - Notepad

File Edit Format View Help

-----BEGIN CERTIFICATE REQUEST-----

```
MIICrTCCAUAQAwDELMAkGA1UEBhMCU0UxEDAOBgNVBAgMB05haXJvYmkuEDAO
BgNVBAcMB05haXJvYmkuDTALBgNVBAoMBFVTSVUxEDAOBgNVBAcMB0FQVDMwOTAx
FDASBgNVBAMMC25haXJvYmkuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAlbngtmU0nIQidykCBn8Ahei1bj6e7xzACE/g7/I+rCaMR1QzWMUIbUa/
GtZdw40DSv8gFkQ4mKlWpXdw0Te/cLDf+doMwcc6P7focQoKPsggWb87euS/R/KC
fRgn6EIwxnn7VbaZCb6BfgKASHn7GYRjYm/Bz4AfcrmIttEWeROoQXChLOksj0/4
Misuwq0pXskgKtH0VeSAXva8BK1ILhvP7GwmT+kYXi9zB5XX9u/ta0MJAqjEadeY
N6Sfr3WZEwbuHEYU0xf0wmScFxs3bc+QxPE/CJJayz5nSJzmsDLnoq82MWTZ4VeF
S10Hd5nQib3ZV088ExtW4aPjX4XHbwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEB
AHMCPAxSdSRc3me0aLrVSWJGcuGeykzxJ9Bnt1rsFkYMyXFTZawLE3crwbIPhcw8
F9y170TA68ZhvRJ01LsS5QYLaAtI4XYaQ9rga/DKgtXZdZqK/5ejmhclV+IvIq4H
ztFD+3WAGVA48TsI+jpDLANaZXv5tdnJiXKJxY7NSIM7so7wkSzbAxX206tW3IA9
Wq0rRP5XNkHBb0vI2+61CmJ4R9Bz0ItHP6Y2HMNjLPM0ohFFLwC/Rahwk8eQ8ZeD
JLgdHahgjehLnepcxo3Rxosj9kvS+56h1f304Mt7UpidA0aoumVeCNFmwA8CGS
WxjecEf20YY2+NsfhAbSGPY=
```

-----END CERTIFICATE REQUEST-----

Conclusion

This activity demonstrated the process of generating a CSR using OpenSSL on a Windows system, which is a crucial step for securing web servers with SSL certificates. The detailed commands and user inputs provided a clear pathway to create and manage cryptographic keys and requests efficiently.