Jacques Durandt

ST10242724

APDS7311 ICE Task 3

1. Explain the process of creating a self-signed SSL certificate with a physical example.

Step 1: Install OpenSSL

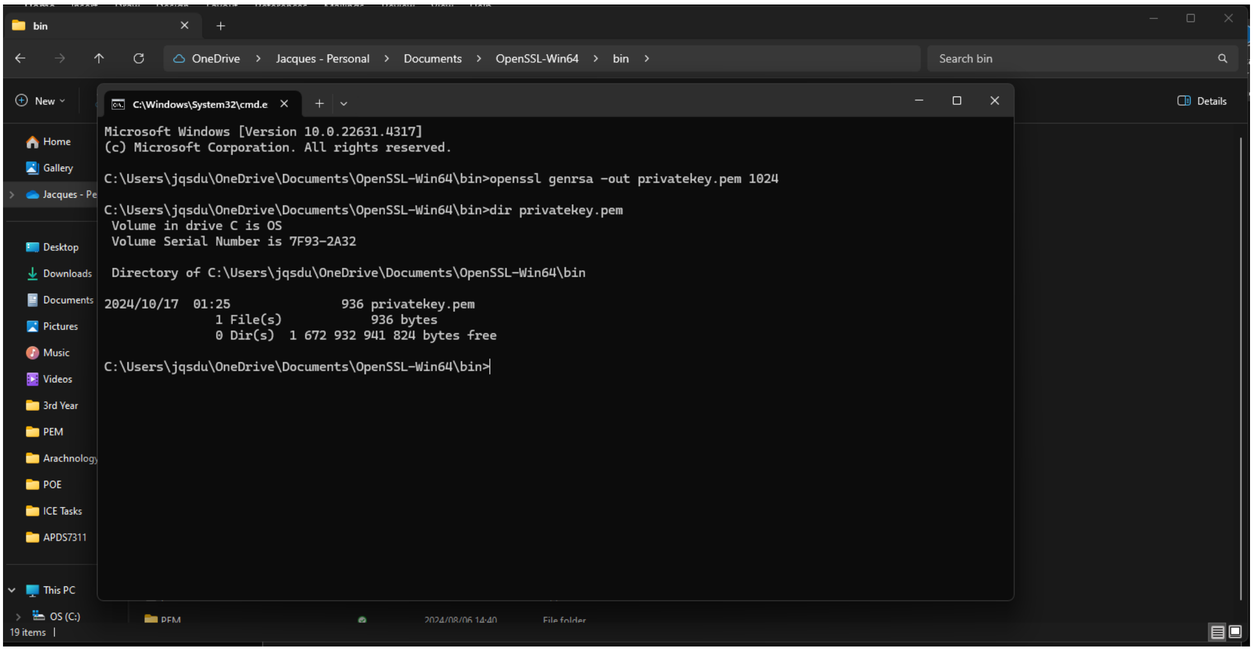
Make sure you have OpenSSL installed. You can download the installation file from the internet, then follow the on-screen instructions to install.

Step 2: Generate a Private Key

OpenSSL will require a private key to create a self-signed certificate. Run the following commands on the command prompt within the bin folder of where OpenSSL is installed to generate a 1024-bit RSA private key:

>openssl genrsa -out privatekey.pem 1024

>dir privatekey.pem



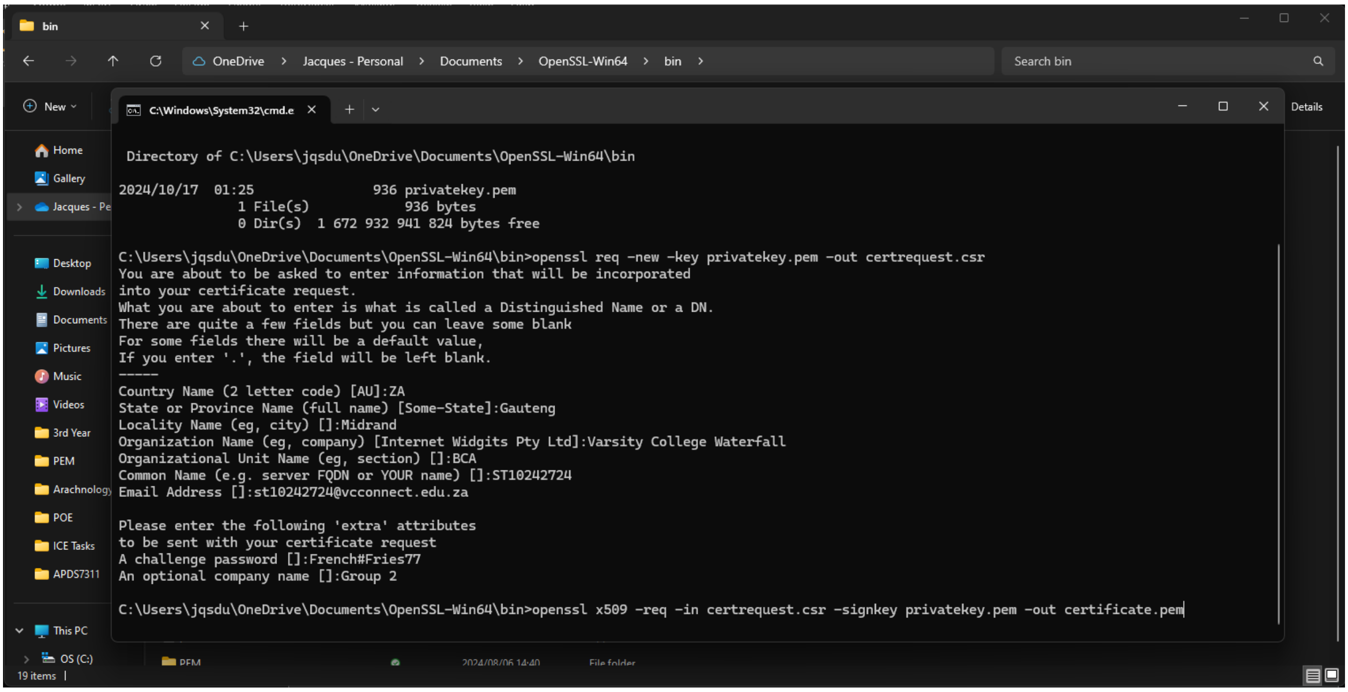
```
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\jqsdu\OneDrive\Documents\OpenSSL-Win64\bin>openssl genrsa -out privatekey.pem 1024

C:\Users\jqsdu\OneDrive\Documents\OpenSSL-Win64\bin>dir privatekey.pem
 Volume in drive C is OS
 Volume Serial Number is 7F93-2A32

 Directory of C:\Users\jqsdu\OneDrive\Documents\OpenSSL-Win64\bin

2024/10/17  01:25               936 privatekey.pem
               1 File(s)            936 bytes
               0 Dir(s)  1 672 932 941 824 bytes free

C:\Users\jqsdu\OneDrive\Documents\OpenSSL-Win64\bin>
```

Step 3: Create an “openssl.cfg” file in the bin folder

Create a notepad file in the SSL bin folder called “openssl.cfg”, then copy the required text from https://www.openssl.org/docs/man1.1.1/man1/req.html and paste it into the file and save.

Step 3: Create a Certificate Signing Request (CSR)

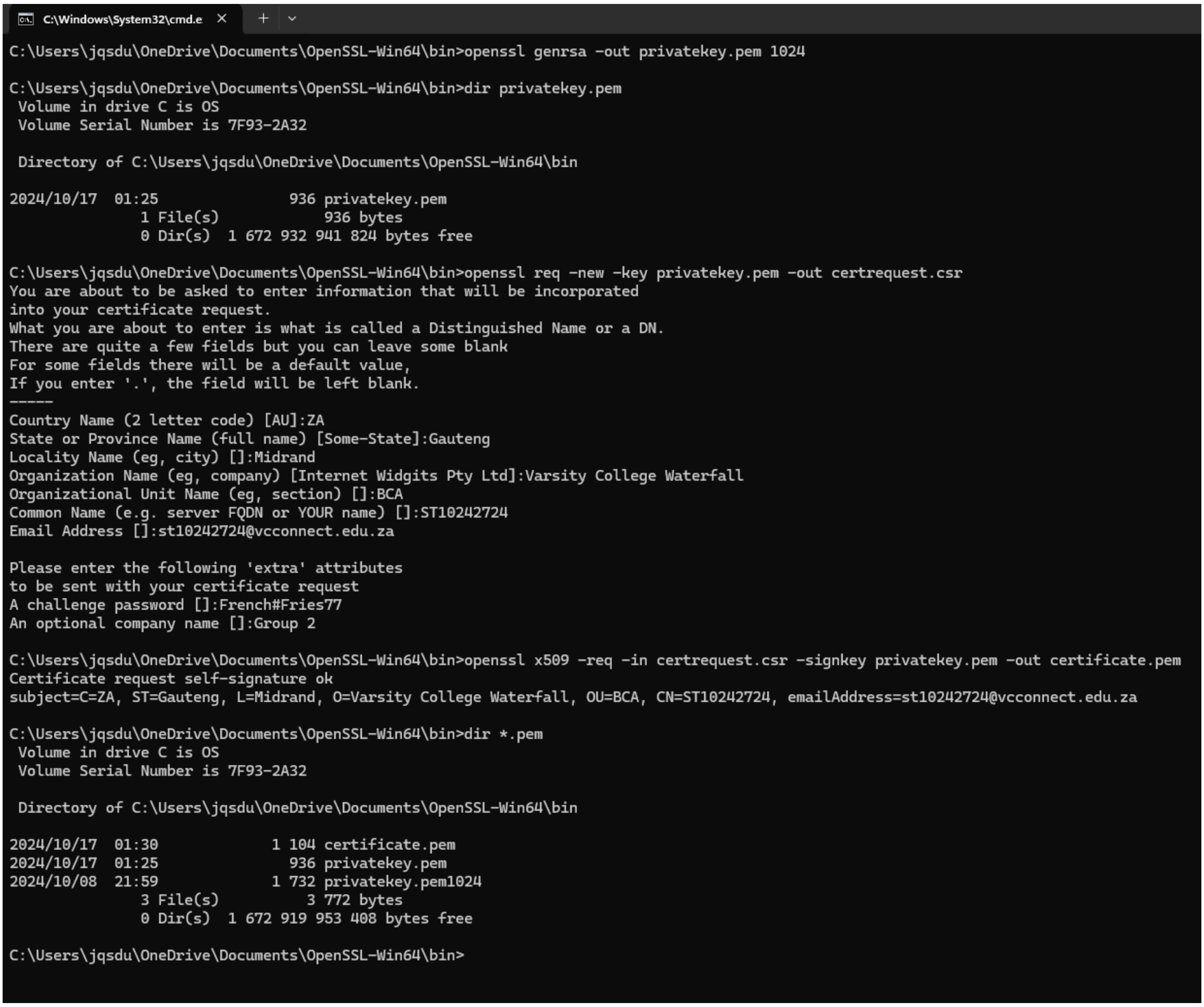
Type out the command within the open command prompt “openssl req -new -key privatekey.pem -out certrequest.csr”, then type in suitable information during the prompts to create the CSR.



```
 Directory of C:\Users\jqsdu\OneDrive\Documents\OpenSSL-Win64\bin

2024/10/17  01:25               936 privatekey.pem
               1 File(s)            936 bytes
               0 Dir(s)  1 672 932 941 824 bytes free

C:\Users\jqsdu\OneDrive\Documents\OpenSSL-Win64\bin>openssl req -new -key privatekey.pem -out certrequest.csr
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]:ZA
State or Province Name (full name) [Some-State]:Gauteng
Locality Name (eg, city) []:Midrand
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Varsity College Waterfall
Organizational Unit Name (eg, section) []:BCA
Common Name (e.g. server FQDN or YOUR name) []:ST10242724
Email Address []:st10242724@vcconnect.edu.za

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:French#Fries77
An optional company name []:Group 2

C:\Users\jqsdu\OneDrive\Documents\OpenSSL-Win64\bin>openssl x509 -req -in certrequest.csr -signkey privatekey.pem -out certificate.pem
```

Step 4: Create a Self-Signed Certificate

In order to sign the certificate, type in “openssl x509 -req -in certrequest.csr -signkey privatekey.pem -out certificate.pem” and then “dir *.pem”.



```
C:\Users\jqsdu\OneDrive\Documents\OpenSSL-Win64\bin>openssl genrsa -out privatekey.pem 1024

C:\Users\jqsdu\OneDrive\Documents\OpenSSL-Win64\bin>dir privatekey.pem
 Volume in drive C is OS
 Volume Serial Number is 7F93-2A32

 Directory of C:\Users\jqsdu\OneDrive\Documents\OpenSSL-Win64\bin

2024/10/17  01:25               936 privatekey.pem
               1 File(s)            936 bytes
               0 Dir(s)  1 672 932 941 824 bytes free

C:\Users\jqsdu\OneDrive\Documents\OpenSSL-Win64\bin>openssl req -new -key privatekey.pem -out certrequest.csr
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]:ZA
State or Province Name (full name) [Some-State]:Gauteng
Locality Name (eg, city) []:Midrand
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Varsity College Waterfall
Organizational Unit Name (eg, section) []:BCA
Common Name (e.g. server FQDN or YOUR name) []:ST10242724
Email Address []:st10242724@vcconnect.edu.za

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:French#Fries77
An optional company name []:Group 2

C:\Users\jqsdu\OneDrive\Documents\OpenSSL-Win64\bin>openssl x509 -req -in certrequest.csr -signkey privatekey.pem -out certificate.pem
Certificate request self-signature ok
subject=C=ZA, ST=Gauteng, L=Midrand, O=Varsity College Waterfall, OU=BCA, CN=ST10242724, emailAddress=st10242724@vcconnect.edu.za

C:\Users\jqsdu\OneDrive\Documents\OpenSSL-Win64\bin>dir *.pem
 Volume in drive C is OS
 Volume Serial Number is 7F93-2A32

 Directory of C:\Users\jqsdu\OneDrive\Documents\OpenSSL-Win64\bin

2024/10/17  01:30             1 104 certificate.pem
2024/10/17  01:25               936 privatekey.pem
2024/10/08  21:59             1 732 privatekey.pem1024
               3 File(s)          3 772 bytes
               0 Dir(s)  1 672 919 953 408 bytes free

C:\Users\jqsdu\OneDrive\Documents\OpenSSL-Win64\bin>
```

Step 5: Paste the certificate.pem and privatekey.pem into the desired folder

2. Explain how this self-signed certificate will be used in your web application

After your self-signed certificate has been generated, it can be used in your web application. In order to apply it to a web server, the following steps must be taken:

Step 1: Configure the Web Server (Apache Example)

You must store the certificate and private key in a secure location within your solution and then update the Apache configuration to make use of these files.

Step 2: Accessing the Web Application

After you are done configuring your web server to use the SSL certificate, you will then be able to access your web application via HTTPS.

Please note that since a self-signed certificate is used, most browsers will display a security warning indicating that the certificate is not trusted by a recognized certificate authority.

The self-signed certificate can then be used to access the local development environment, test encryption, debug SSL issues and secure local communication.