**GROUP: Harshal Bhole, Adesh Padwal , Ashwit**

**PROJECT2**

**PROBLEM 1**

**Task 1** : As per mentioned in the problem statement we ran the following commands and created the directories.

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

After running the following commands CA.cert CA.crt and CA.key was generated after entering the organization information and some other details.

CA.crt we got is as follows:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

The CA.key we found was as follows:

A screenshot of a computer

Description automatically generated

Task 2: In this we had to issue the CA certificate to PKLabServer.com

Step 1:

A screenshot of a computer

Description automatically generated

Step 2:

A screenshot of a computer

Description automatically generated

Step 3:

A screenshot of a computer

Description automatically generated

Graphical user interface, text

Description automatically generated

And hence the connection was successful!

The Server.csr file we found was like this:

A screenshot of a computer

Description automatically generated

Graphical user interface, text

Description automatically generated

The Server.crt file we found was like this:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The server.pem file was found as :

A screenshot of a computer

Description automatically generated

1. As we use modified the hosts file in the /etc and mentioned the ip and PKLabServer.com it now points to the local host. So even if we use <https://localhost:4433> we will get the same output.

Also we got the output like this after following all the above steps :

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

1. **It had no effect at all.** The actual PEM-format certificate is the lines from ----BEGIN to -----END **only**; everything else is comment data intended to be possibly helpful to a human reader, but ignored by programs.

To change the certificate actually used in a program, you need to change the base64 data inside the PEM block. This is not easy, and you may find it easier to just generate different certs from scratch.