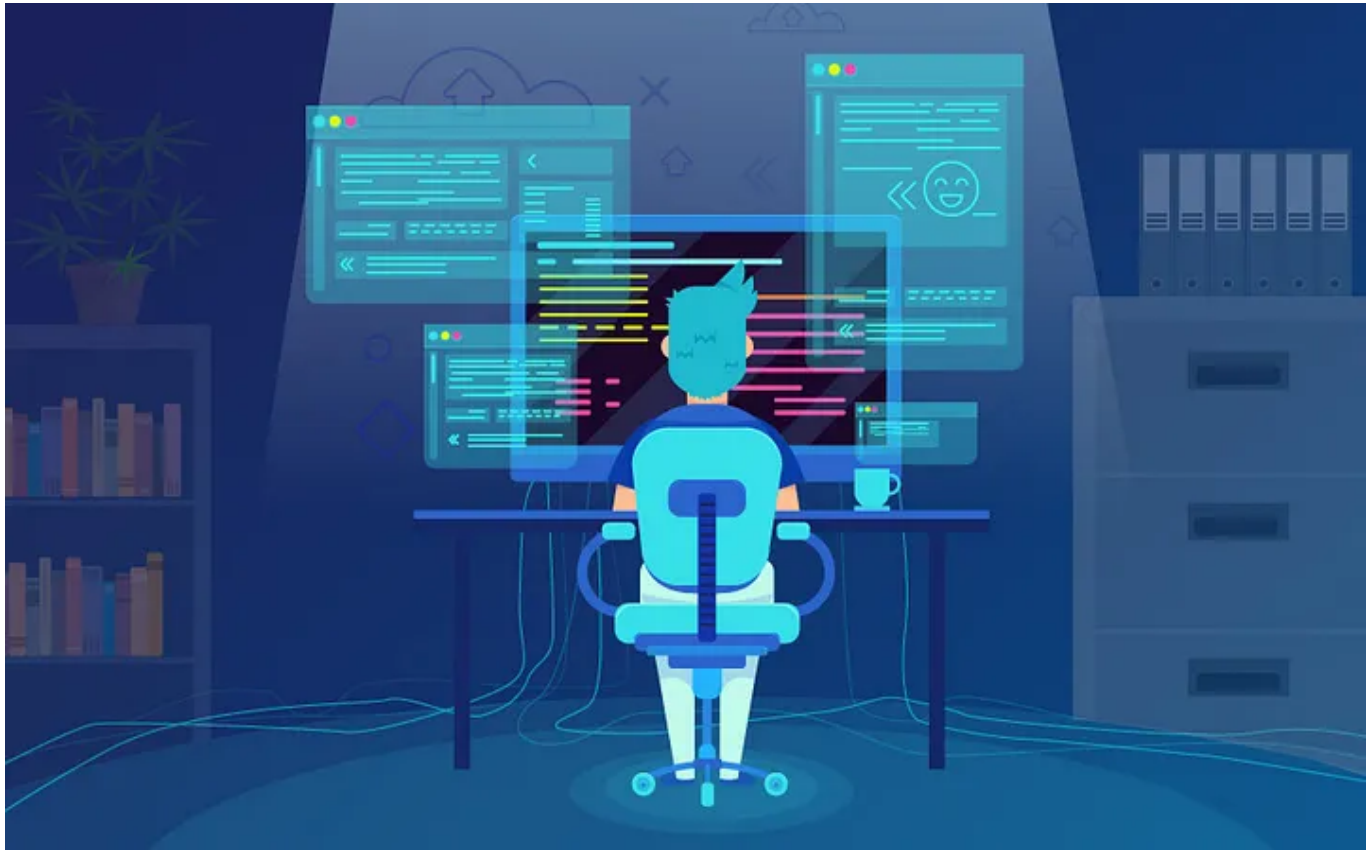
Self-signed certificate for Msi

Adarsh Kumar · Following

Published in Fnplus Club · 5 min read · Aug 14, 2019



Developer in his Natural Habitat

Being a Computer Science student, I always try to find more about software and how things work.

While working on a project I came across the concept of Certification.

Intrigued by this, I wanted to make my own “Self-signed certificate”.

General Idea

Certificate are used for security as they authenticate a software or a website of it's credibility and trustworthiness.

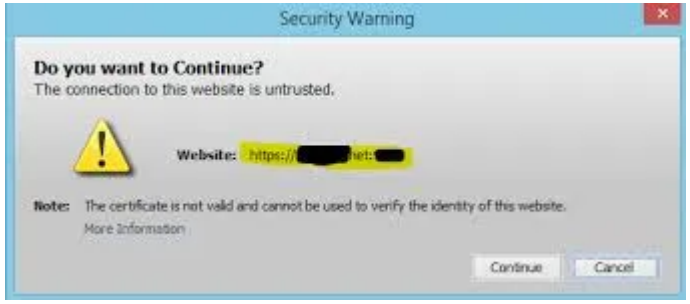
> *Any general user who has used internet knows that most of the website starts with-: https://*

The 's' in it stands for Secure, and your browser knows this because the website has a SSL certificate. SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details.{More Info}

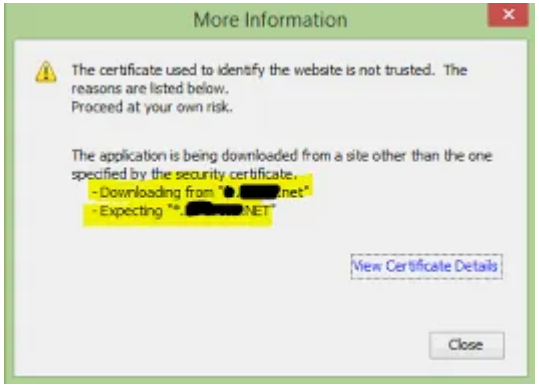
What If we don't have one?

Well if you visit a lot of websites and download a lot of software, you might already know what it looks like when a software isn't ensured by a certificate.

For Web



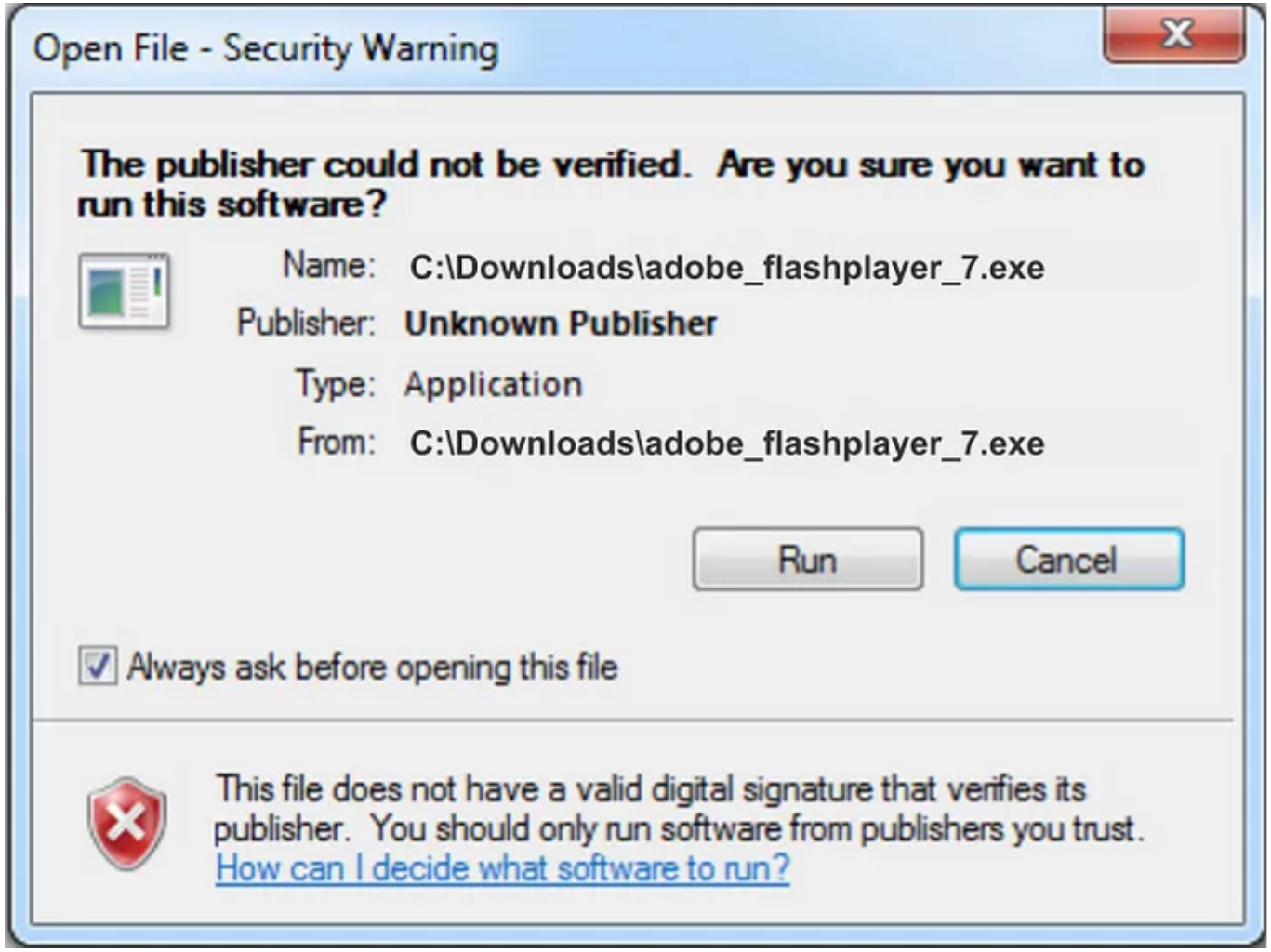
when not valid



when not trusted

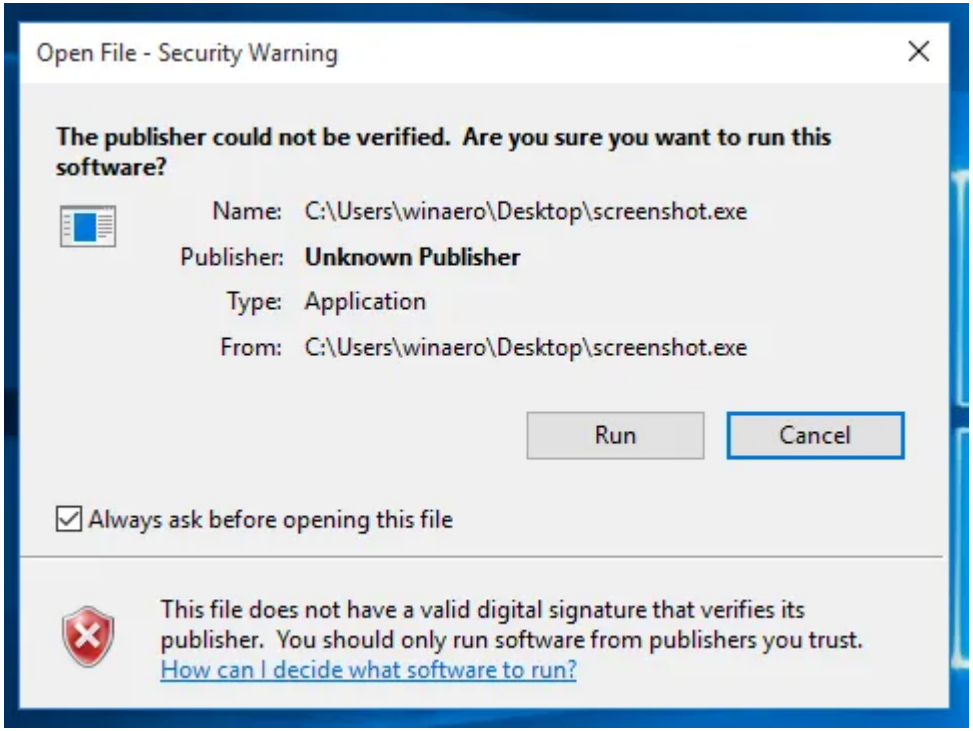
browser hesitates to proceed

For PC



You may trust the software and maybe fine to download it on your system,
But if the software doesn't have a digital signature. A.K.A Signed Certificate.

This may show up on your system while installing the MSI.



This applies to any other software which doesn't have a certificate. As they could be malicious and our systems are designed so that they can warn us from such software.

Hence, a bit of caution is needed, only install those software which can be trusted by user.

Making a Self-signed certificate

Let's Do this

Well, honestly, It's really easy. Just that without proper information it could take hours. So here are 3 parts to make Self-Signed Certificate. These will be done on a Windows System. If you have any other OS like Linux or IOS. The steps will be the same.

Step 1) *Install OpenSSL* **Step 2)** *Follow instruction to make a signed certificate*
Step 3) *Attach it using Ksign software*

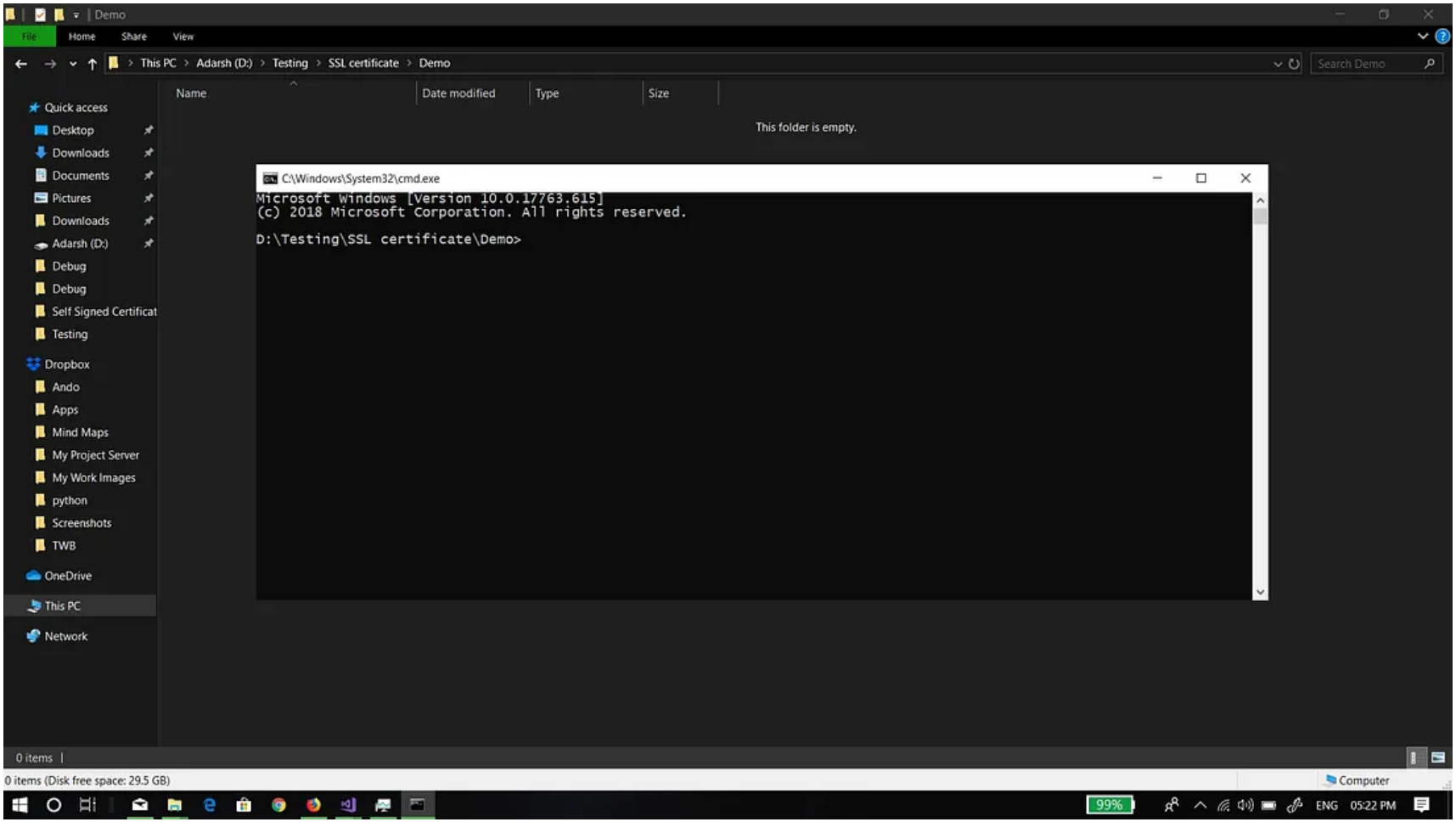
Step 1: Install OpenSSL

For windows you need to download it from here. See the install file, Or follow this Video for easy install.

OpenSSL install Process

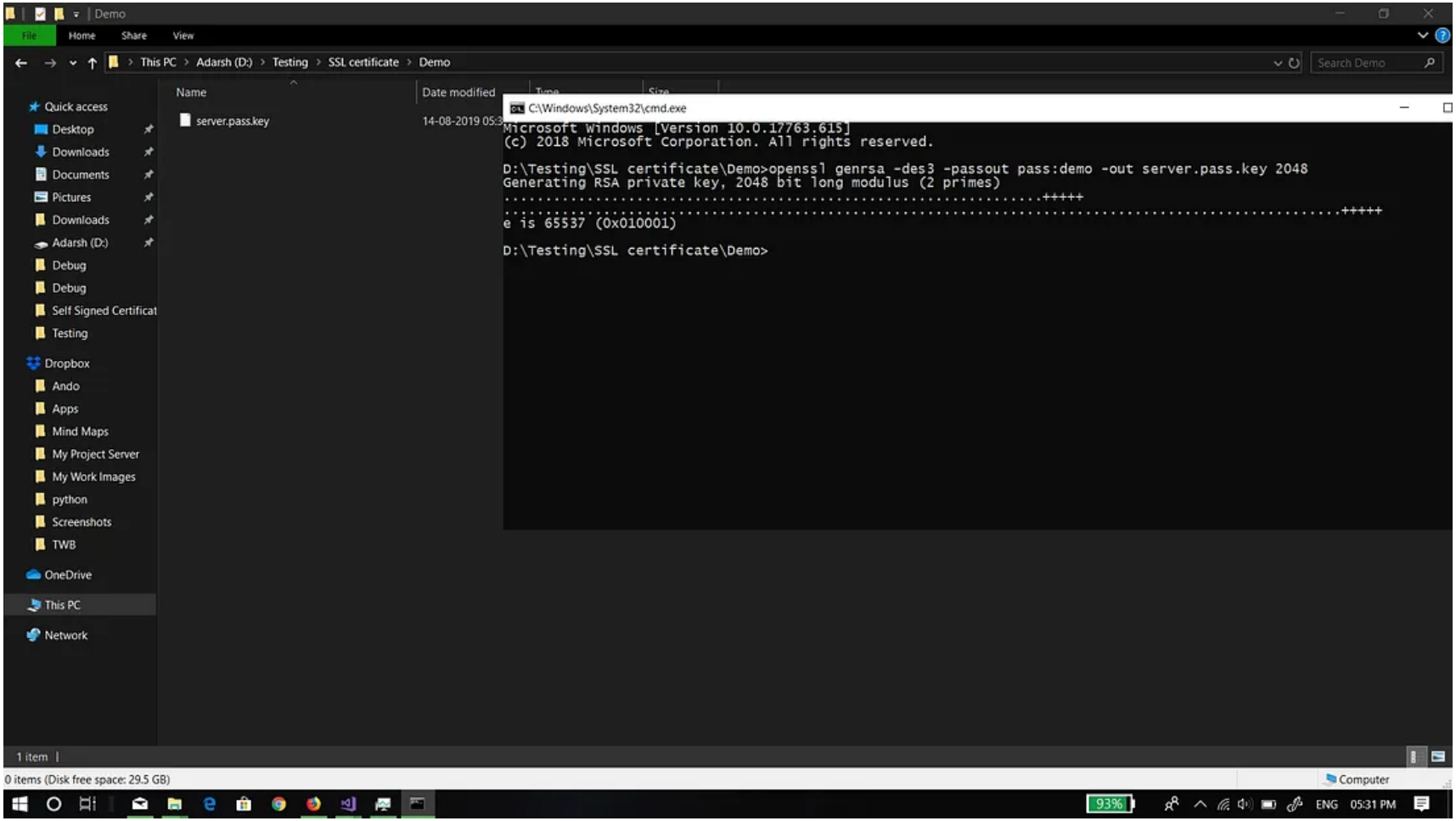
Step 2: Instruction to follow

> *Restart the cmd after each step!!*



Root location

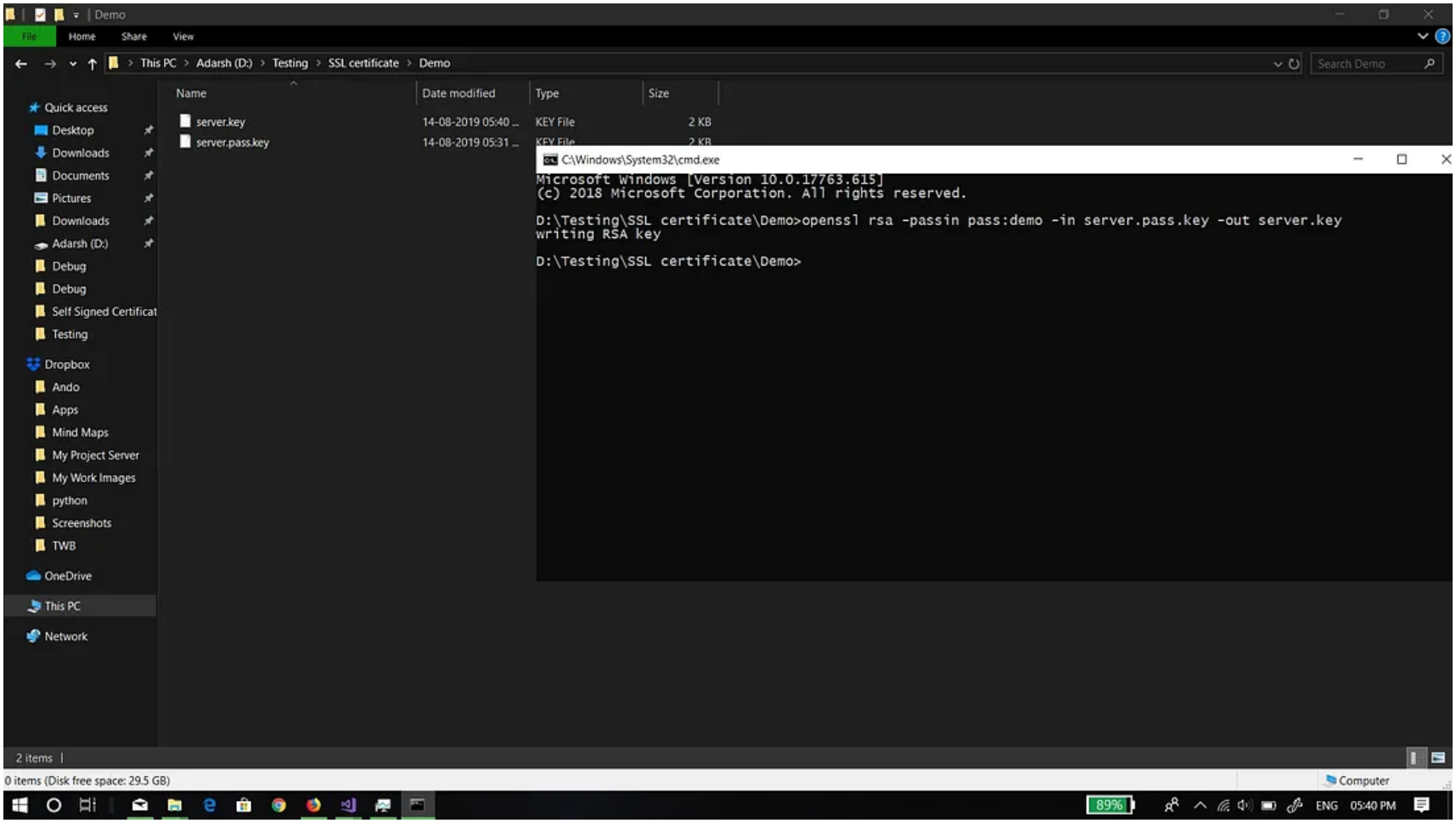
Step 1: Go the the folder you want to use for the certificate creation.



Making Key

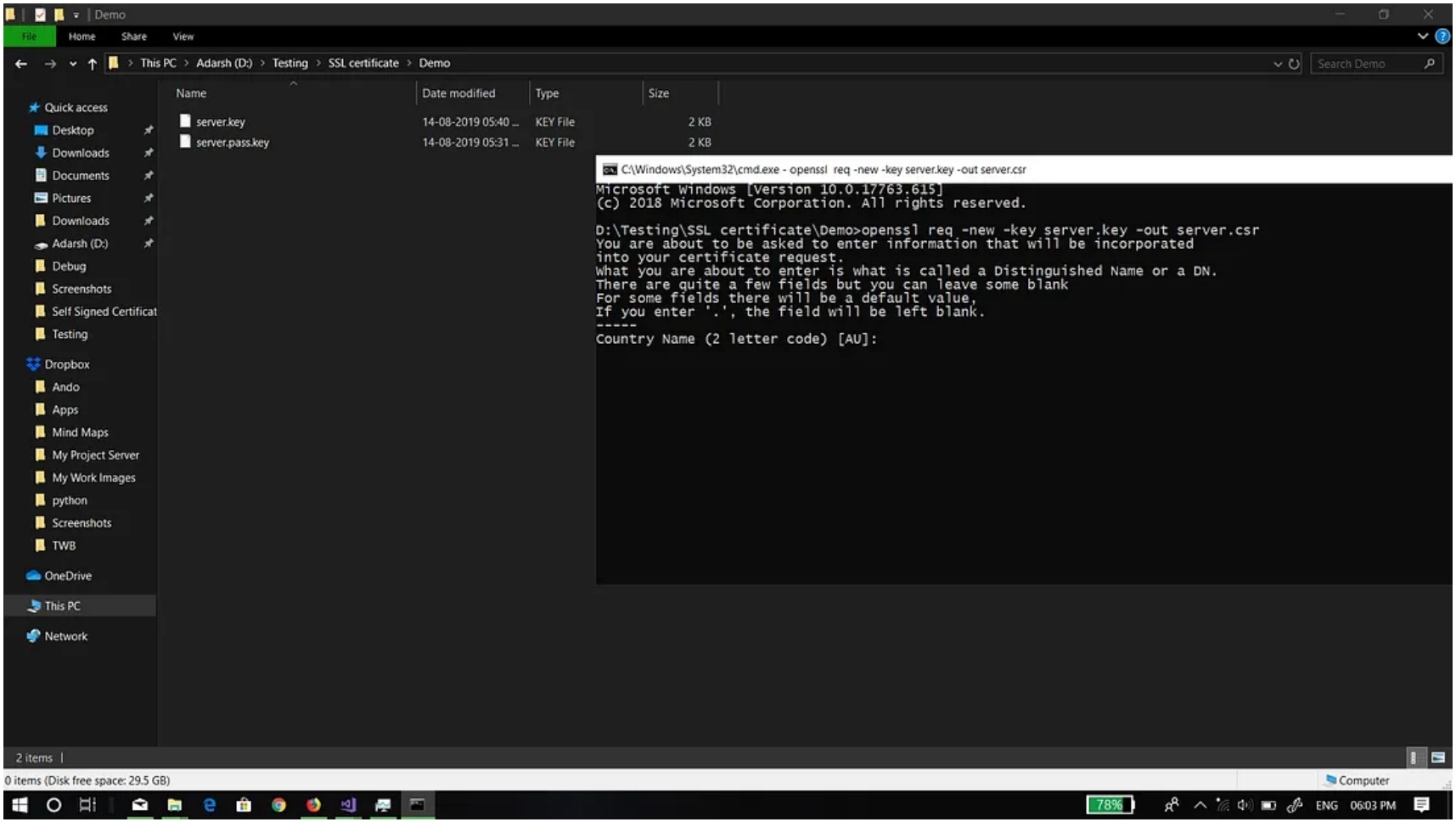
Step 2: Use this command " openssl genrsa -des3 -passout pass:x -out server.pass.key 2048 ". *{x: is the password of your choice}.* This will make a key

that will be used to create your certificate.



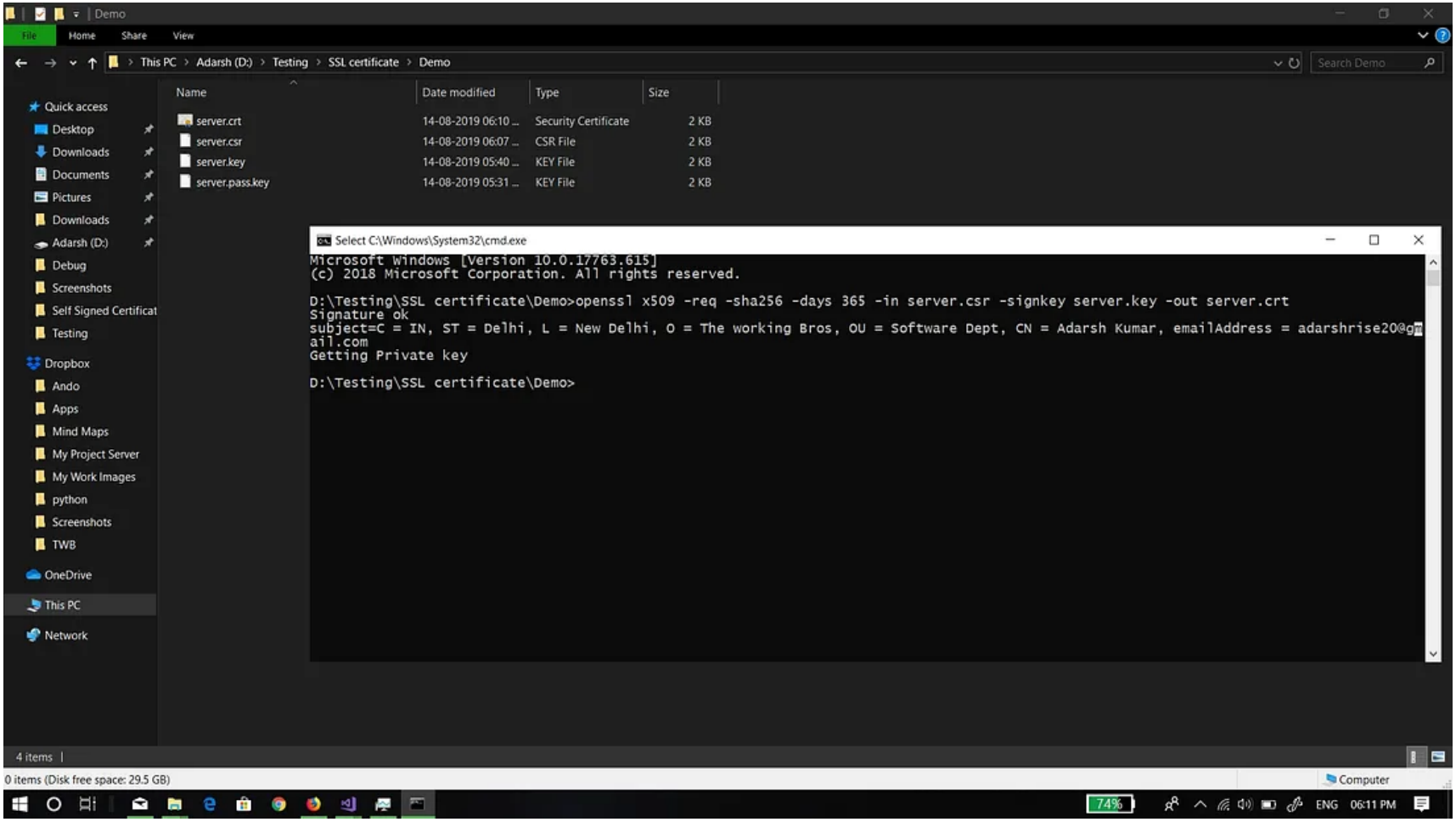
step 3

Step 3: Use this command “ openssl rsa -passin pass:x -in server.pass.key -out server.key “. *{x: is the password of your choice}.* This is the second phase of the same Key.



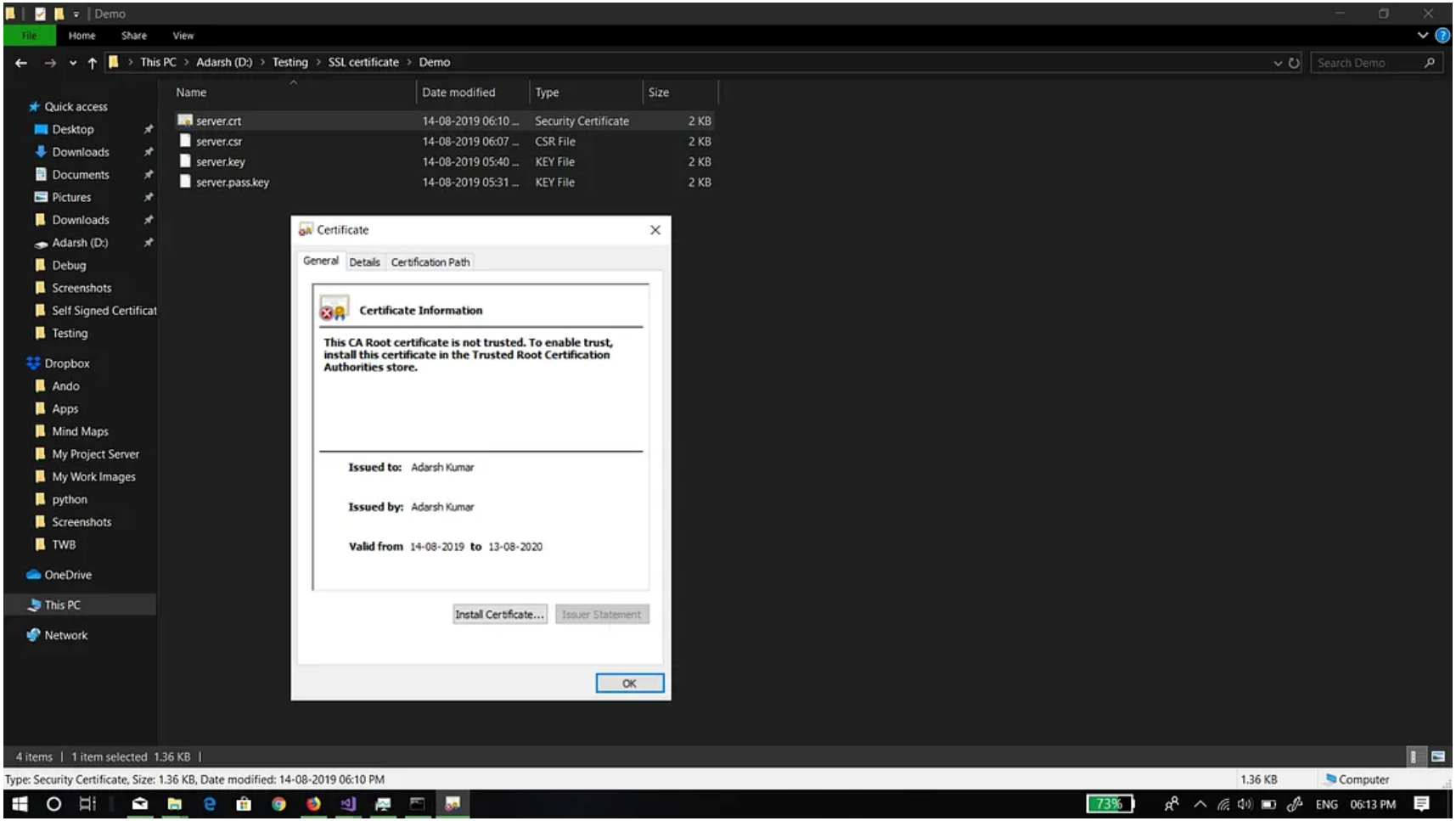
step 4

Step 4: Use this command " openssl req -new -key server.key -out server.csr". And fill the details. So that the certificate gets intertwined with the creator's details.



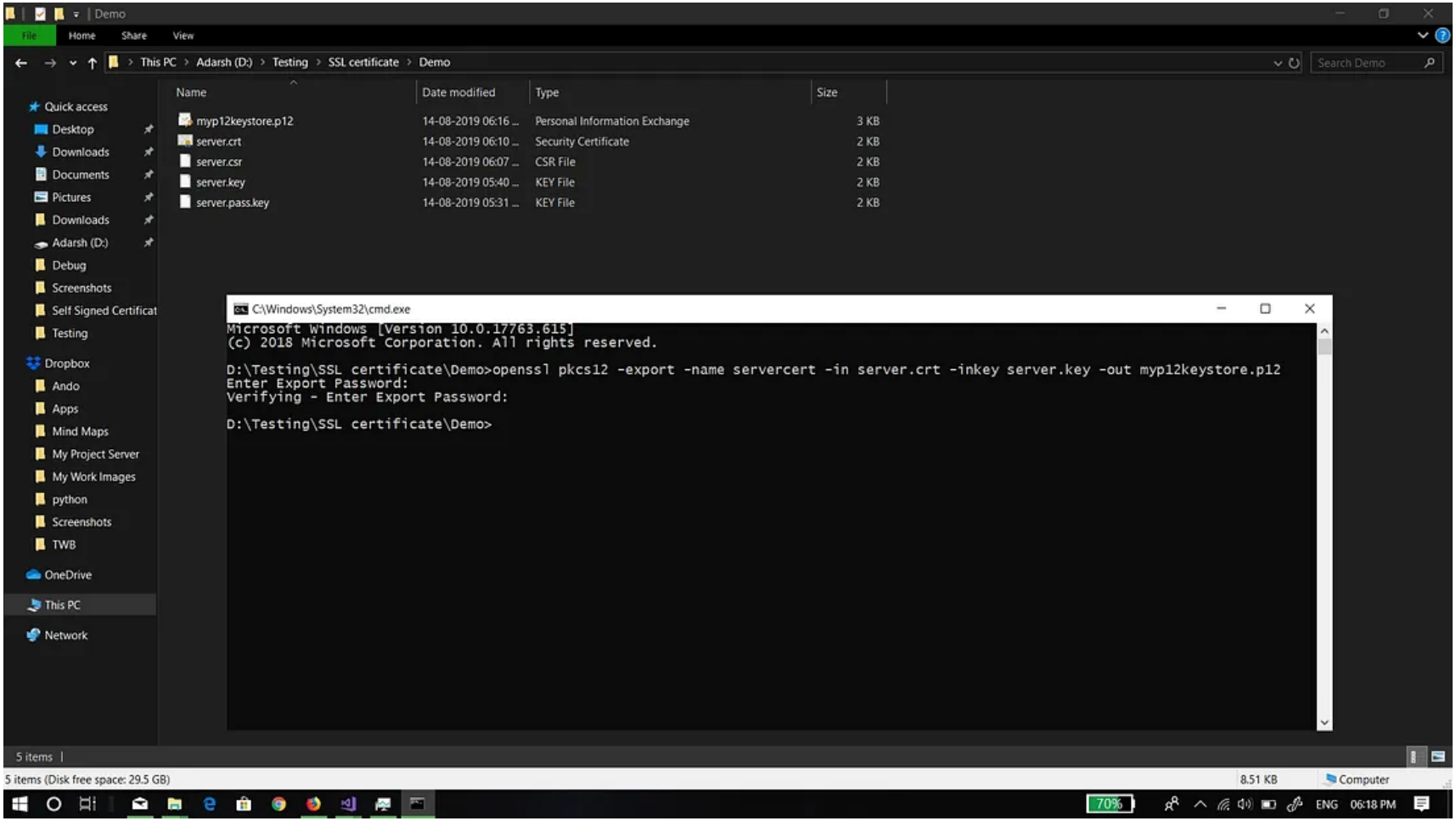
step 5

Step 5: Use this command “ openssl x509 -req -sha256 -days 365 -in server.csr -signkey server.key -out server.crt“. This step will give you your certificate.



step 6

Step 6: Install the certificate on the system, Now any software that has this certificate. Your system will consider it as trusted Software.



step 7

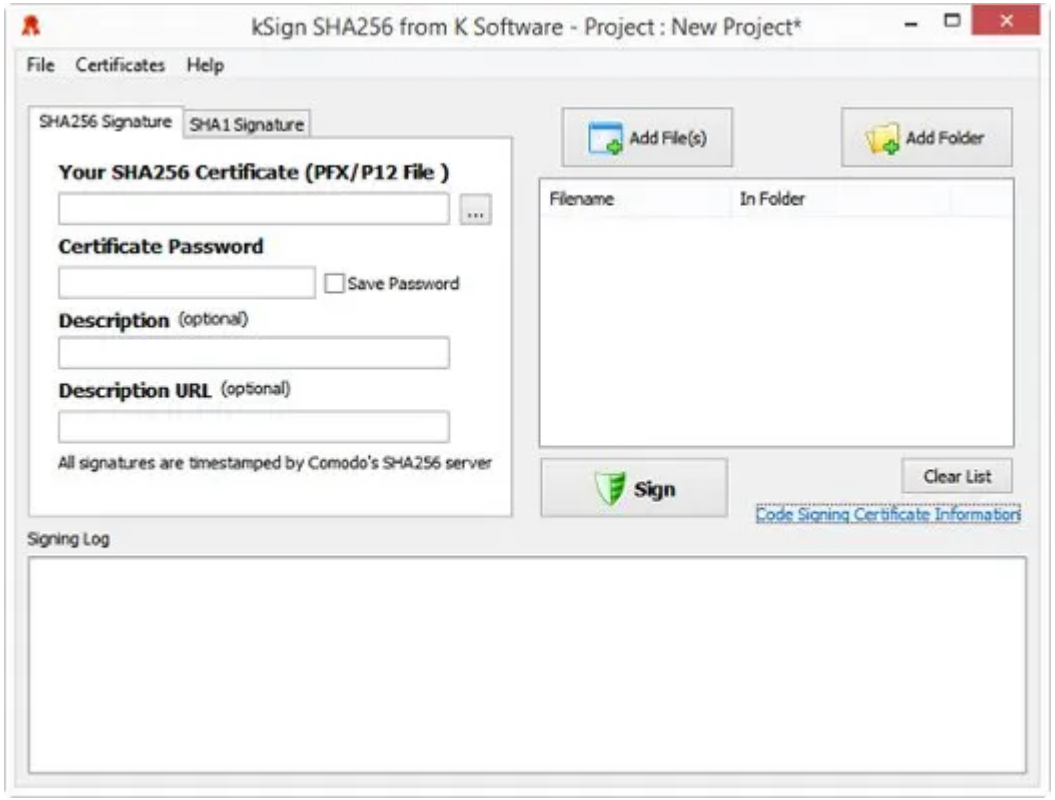
Step 7: Use this command “ openssl pkcs12 -export -name servercert -in server.crt -inkey server.key -out myp12keystore.p12“. P12 file can be easily

used for Signing the MSI/Exe file. This will make a PK12 file that will be used for signing the installer.

> *Assuming you have a MSI/Exe for this step, if you don't have you can make one using NSIS.*

Step 3: Download Ksign

Ksign is a free software which could be used to attach the certificate to the MSI/exe. installer file.



Ksign

Just fill the details, add the the MSI/exe File and click on Sign, And you have successfully made a installer with a Self-Signed Certificate.

Extras

Self-Signed Certificates are not trusted by other machines as, What you have made has no public awareness and has no way to tell if it's actually trust-able or not. Hence, Self-Signed certificate are used by companies within the company itself.

> *Otherwise you need to buy a Trusted certificate from an organization which sells such certificate.*

Although, you can get a Somewhat Trusted Certificate for Free By CAcert.

You may continue to gain more knowledge by visiting this web page.

Thanks For Reading

Ssl Openssl Installer Trusted Security

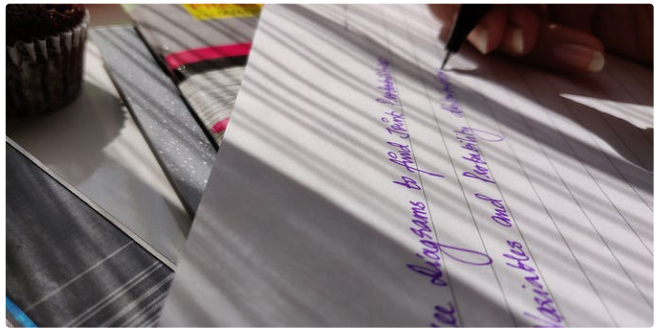
Written by Adarsh Kumar

Following

6 Followers · Writer for Fnplus Club

Aspiring Programmer;

More from Adarsh Kumar and Fnplus Club



Adarsh Kumar in Fnplus Club

The Emergence Of Web Technology

What is Web Tech?

8 min read · Jan 14, 2019

126 1

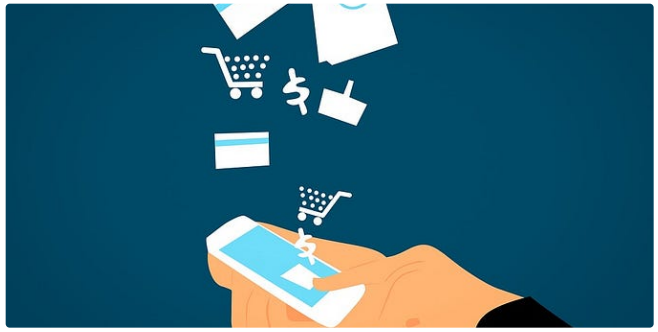
Madhura Joshi in Fnplus Club

DGIM Algorithm

I wanted to write a blog from the past few days. I did have some ideas but did not kno...

5 min read · Jun 4, 2019

452 5



Abdul Kadir in Fnplus Club

Integrating UPI payments inside your Android app

Alright, In this post I'll walk you guys through a toy app that will allow you to make...

3 min read · Apr 12, 2019

229 10

Adarsh Kumar

Source Control: Git The Console 1.0v

To all my aspiring programmer friends.

7 min read · Jan 27, 2019

137

See all from Adarsh Kumar

See all from Fnplus Club

Recommended from Medium

Mustafa Burak Aydın

Create Self -Signed Certificate With OpenSSL

What is Self-signet SSL certificate

2 min read · Nov 2

Bharath R

AES-GCM encryption and decryption for Python, Java, and...

AES-GCM is a block cipher mode of operation that provides high speed of authenticated...

3 min read · Jun 25

50

Lists

Staff Picks

530 stories · 510 saves

Stories to Help You Level-Up at Work

19 stories · 357 saves

Self-Improvement 101

20 stories · 1016 saves

Productivity 101

20 stories · 921 saves

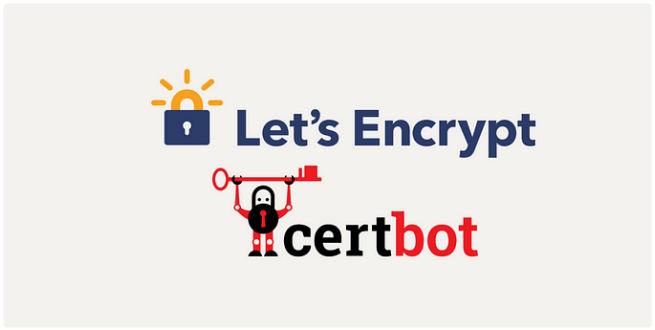
iabdullah

Self-Signed OpenSSL Certificates | MUHAMMAD ABDULLAH

In this blog I'll give a step by step tutorial on how to generate a self-signed OpenSSL...

3 min read · Dec 2

28



vijay chandamala

Creating an RSA-4096 SSL certificate

TLDR;

2 min read · Sep 11

6

REDFISH IA VEN

Prateek Bansal

SSL & TLS 3: AES and RSA

Port Forwarding in Windows and Ways to Set it Up

Learn how to set up port forwarding in Windows for remote access or to host...

7 min read · Jul 31

54

AES (Advanced Encryption Standard) and RSA (Rivest–Shamir–Adleman) are two...

4 min read · 6 days ago

See more recommendations