|  |  |
| --- | --- |
| |  | | --- | | [Apple Developer](https://developer.apple.com/) | |

## Before you begin

Step 1: Download worldwide Developer Relations Certificate - G2 (If it’s is missing in your OS).  
<https://www.apple.com/certificateauthority/> Image Ref: Image= 1.0  
  
Details: Apple established the Apple PKI in support of the generation, issuance, distribution, revocation, administration, and management of public/private cryptographic keys that are contained in CA-signed X.509 Certificates.

Image: 1.0



The registered app identifier is pass.com.flyingtige.

File names:   
-certificate.pem

-LCDigital.p12

Password for the cert is: **123**

Apple Credentials:

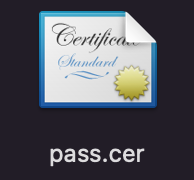
[damian@loyicard.com](mailto:damian@loyicard.com)

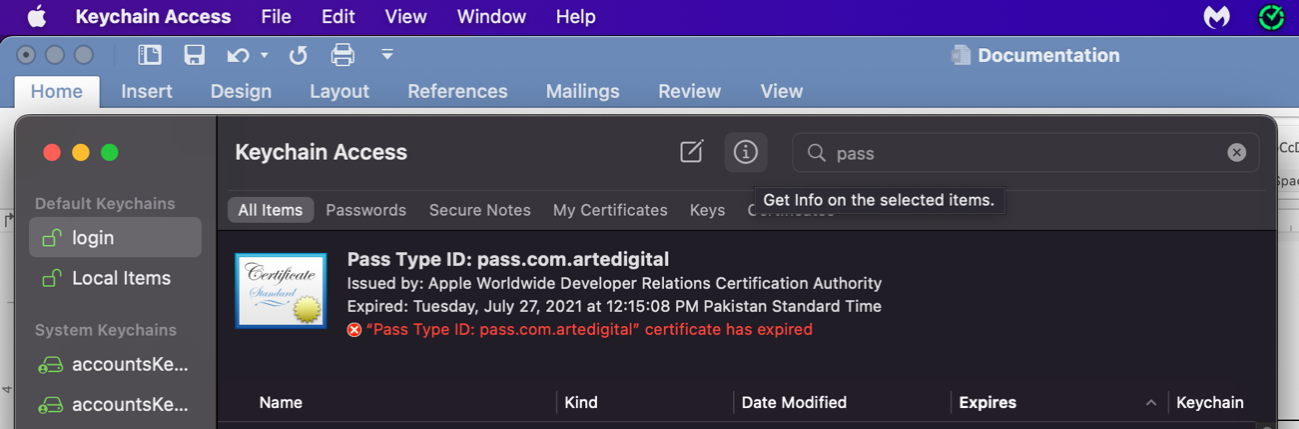
Netflix12

Follow this link step by step in both cases (create new pass type id or renew pass type id), scroll down for renew pass type id;

<https://www.skycore.com/help/creating-pass-signing-certificate/>

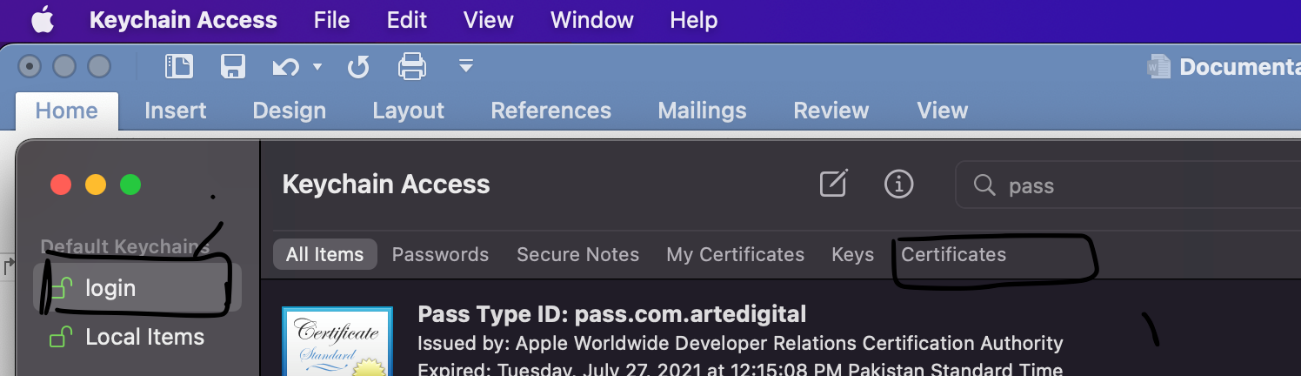
After following all the mentioned steps you should have a **.cer** file, e.g “**pass.cer**” (Ref Image: 1.1)

Image: 1.1  


**Step 1:** You can find the **pass.cer** in Keychain, e.g. Open keychain access in application/utilities. (Ref image: 1.2)  
  
Image: 1.2  


**Step 2:** Select login and then certificates and then open your **pass.cer** file. (Ref image: 1.3)

Image 1.3



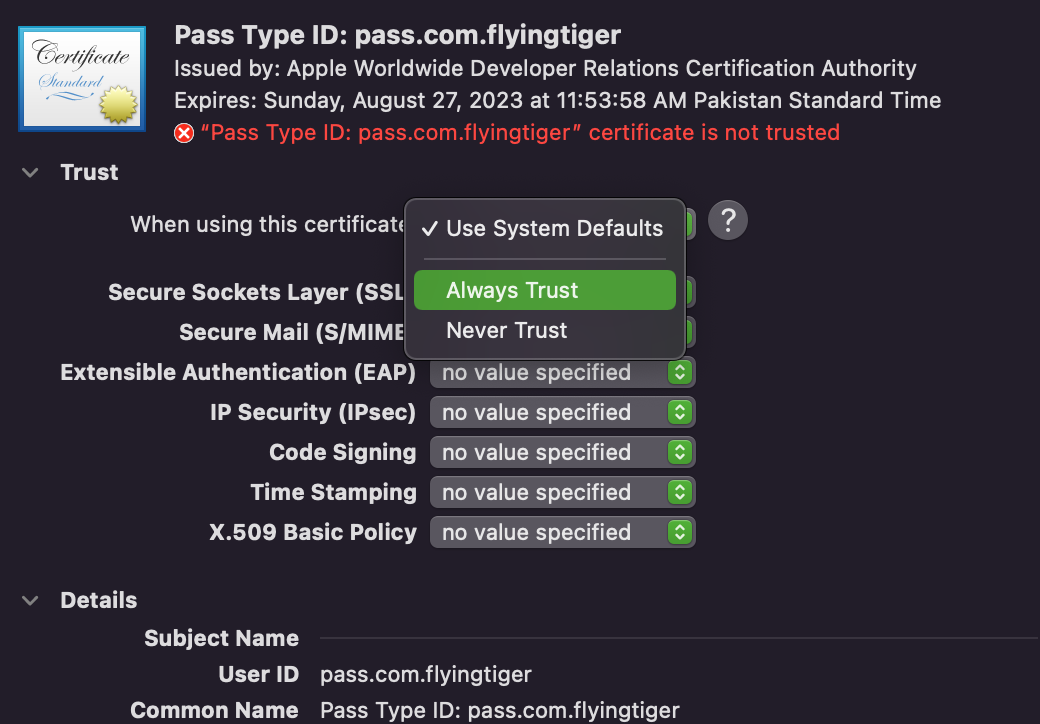
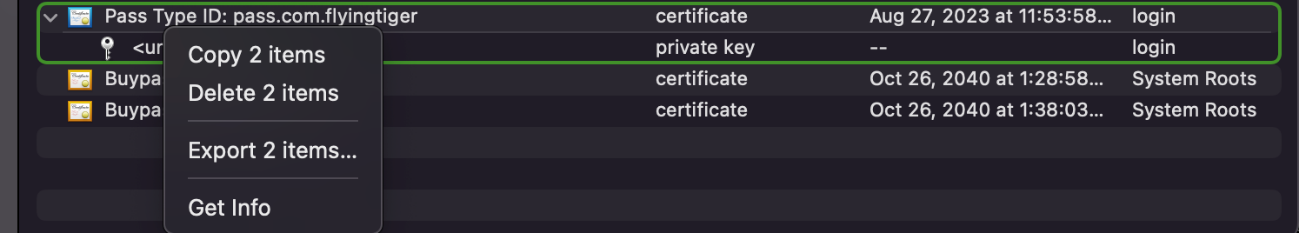
**Step 3:** Look for the latest/recent identifier. (According to expiry date and time.)

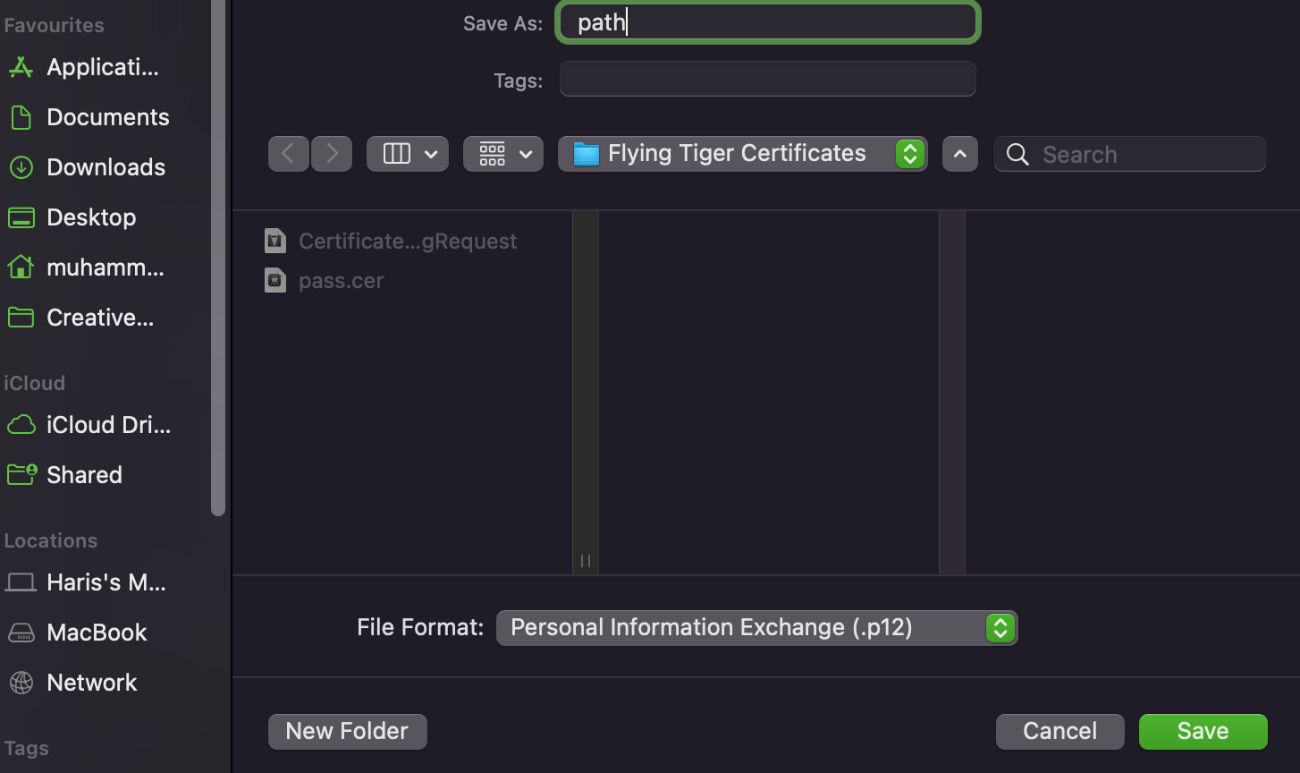


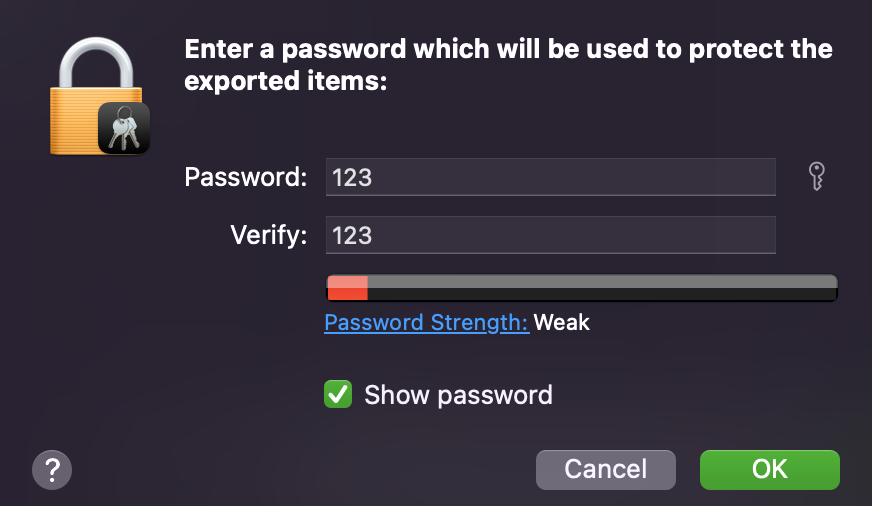
***Note:*** *The certificate must be trusted.*



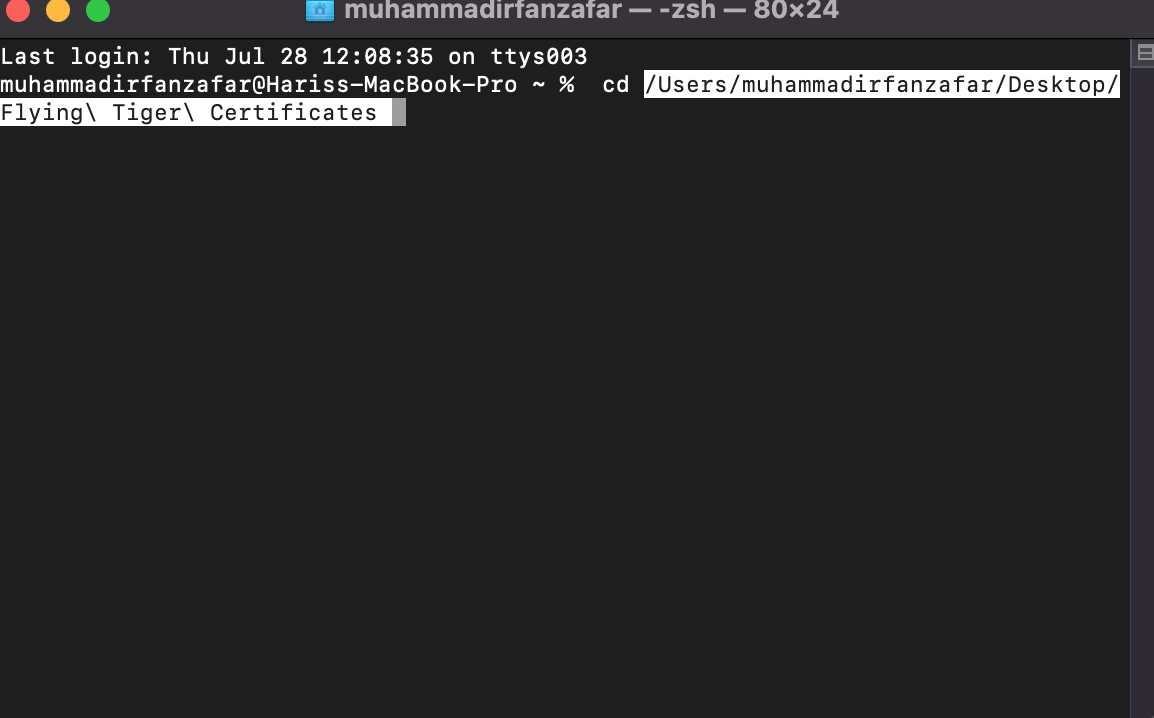
**Step 4:** Double-click on the certificate and the following menu will be opened. Select **Always Trust** from the dropdown. it will ask for a Mac password (it will same one used for login into your MacBook. (Ref image: 1.4)  
  
Image: 1.4

  
  
**Step 5:** Click the dropdown arrow at the left of the certificate. There will be a key section and then Select **Export 2 Items** to the download /export to disk in p.12 format. (Ref image: 1.5)  
  
Image: 1.5  


**Step 6:** For your ease name this file **“path”**. And save it to the project folder. (Ref image: 1.6)  
  
Image1.6  
  


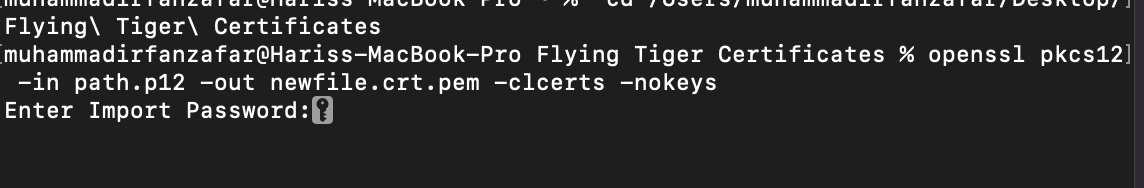
**Step 7:** Click **OK** to save. It will ask for the password. In our case is **“123**” (Ref image: 1.7)  
  
Image: 1.7  
  


***Note:*** *Now you have this file at your saved destination.*

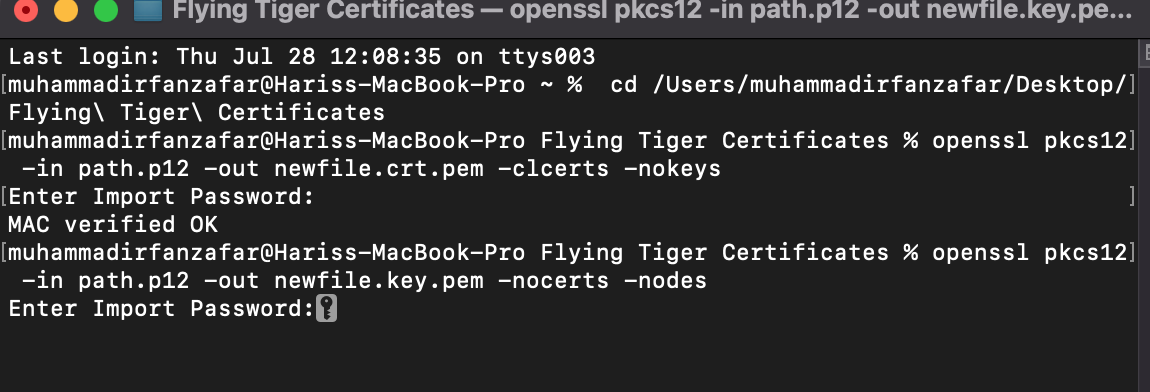
**Step 8:** Open the terminal and run command CD enter to your destination folder (Ref image: 1.8)  
  
Image: 1.8  


**Step 9:** You must run the following commands one by one…. (Ref image: 1.9)

**CMD 1:** openssl pkcs12 -in path.p12 -out newfile.crt.pem -clcerts -nokeys

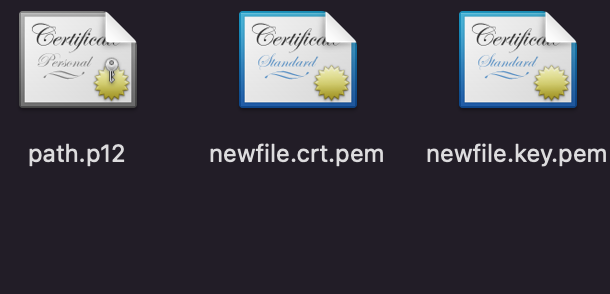


**SCMD2:**  openssl pkcs12 -in path.p12 -out newfile.key.pem -nocerts -nodes

  
***Note:*** *Provide the password for the file whenever the terminal asks*

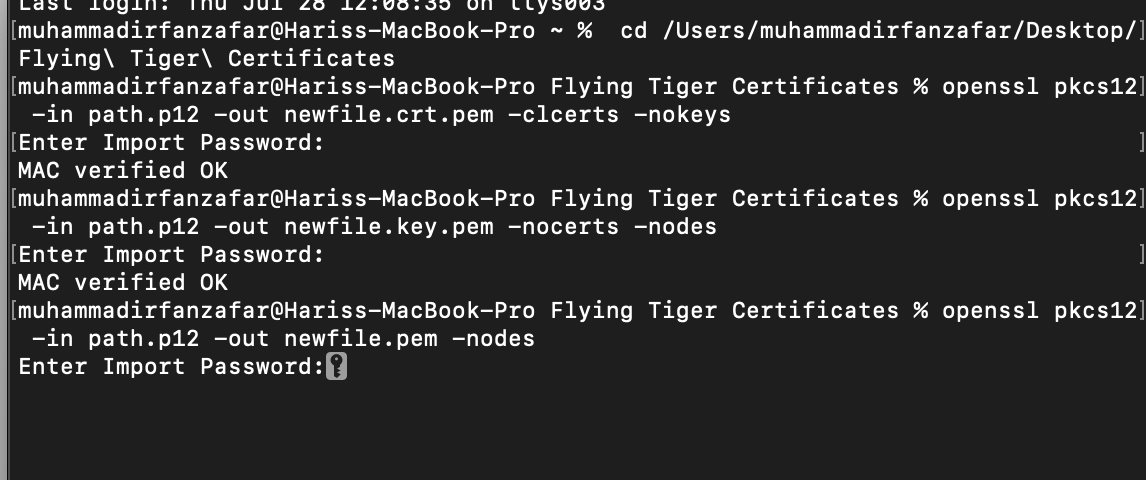
Now you’ll have the following files.

* certificate in **newfile.crt.pem**
* private key in **newfile.key.pem**



**Step 10:** To put the certificate and key in the same file without a password, use the following, as an empty password will cause the key not to be exported:

openssl pkcs12 -in path.p12 -out newfile.pem -nodes



Enter the same password while creating/importing the cert and key.   
now you have the complete **pem** file and p12 file (created earlier)   
  
