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

|  |
| --- |
|  |

## Before you begin

if worldwide Developer Relations Certificate - G2 is missing download from there .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.

https://www.apple.com/certificateauthority/



The Register App identifier is pass.com.flyingtiger

File names Are:

certificate.pem

LCDigital.p12

Password should be : 123

Apple Credentials:

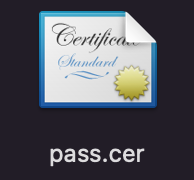
[damian@loyicard.com](mailto:damian@loyicard.com)

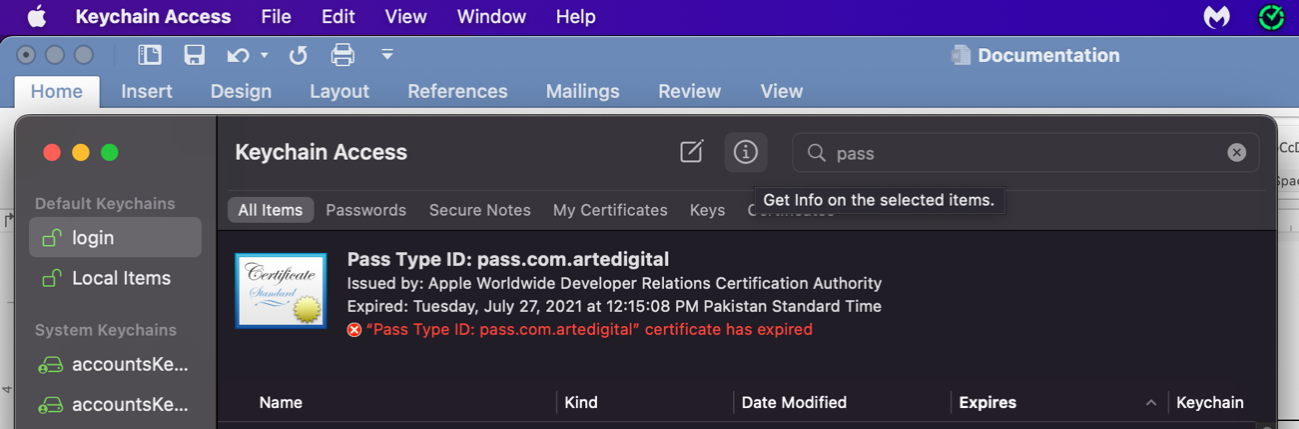
Netflix12

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

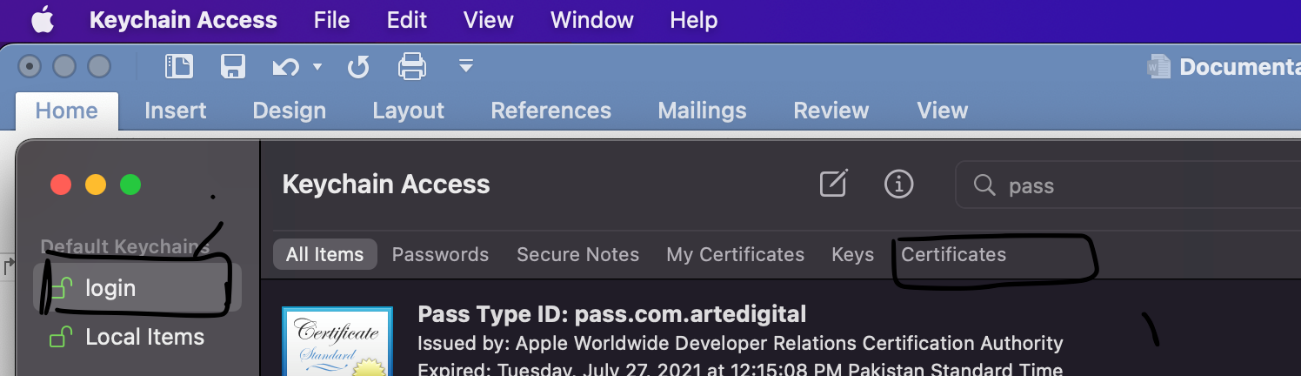
<https://www.skycore.com/help/creating-pass-signing-certificate/>

after successfully following all steps you should have a .cer file e.g pass.cer



Open keychain access in application/utilities.

Select login and then certificates and then open your pass.cer file



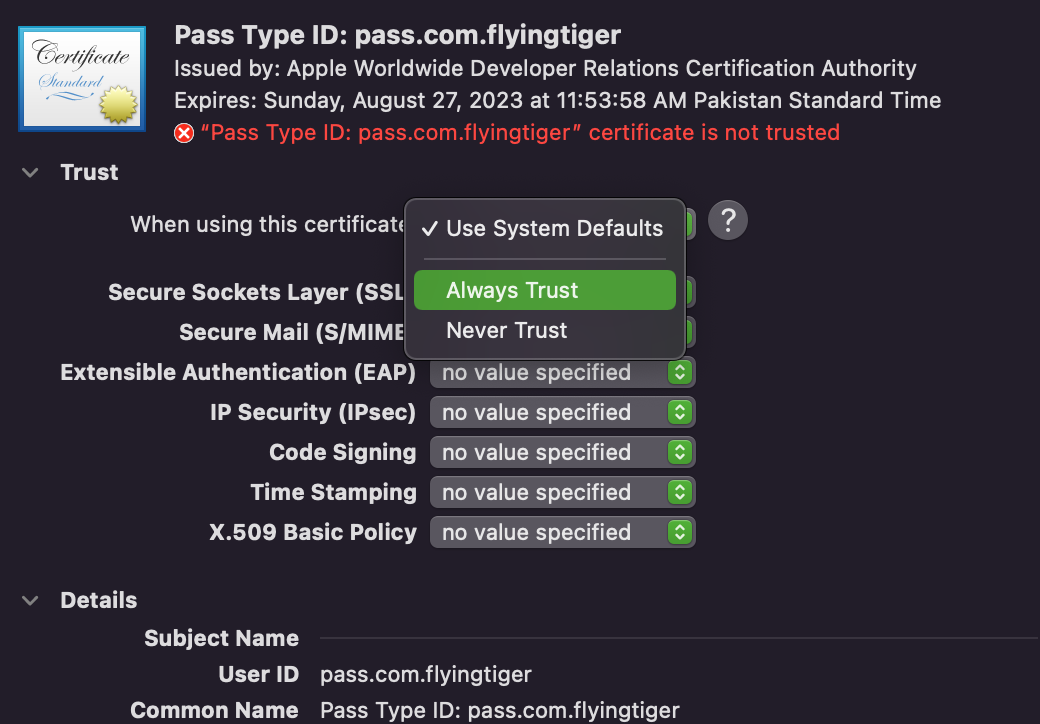
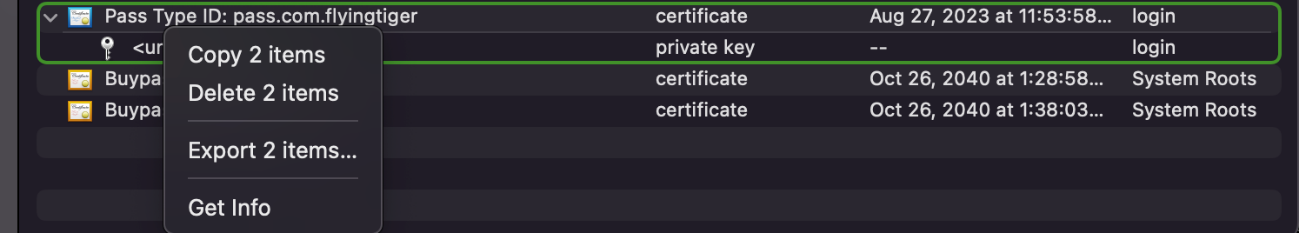
After opening look for your identifier, if multiple then you have to guess according to expiry date and time.

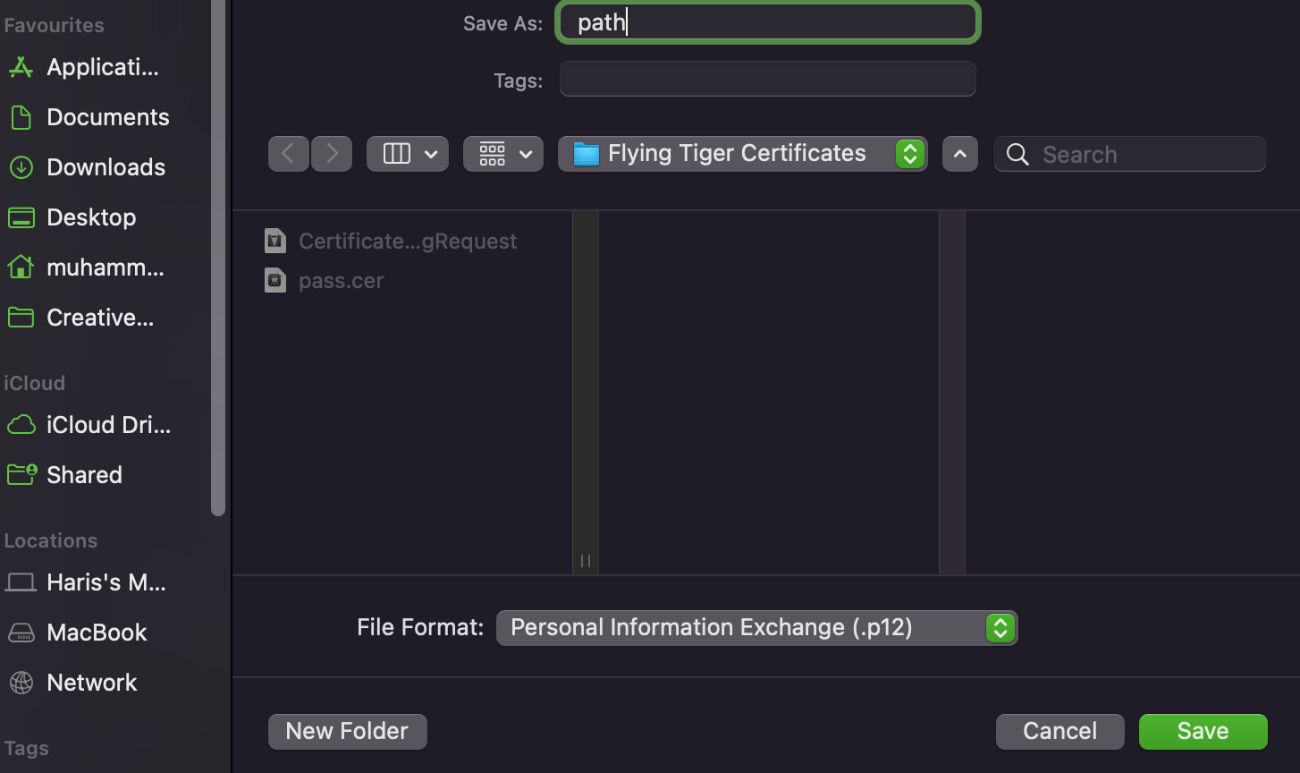


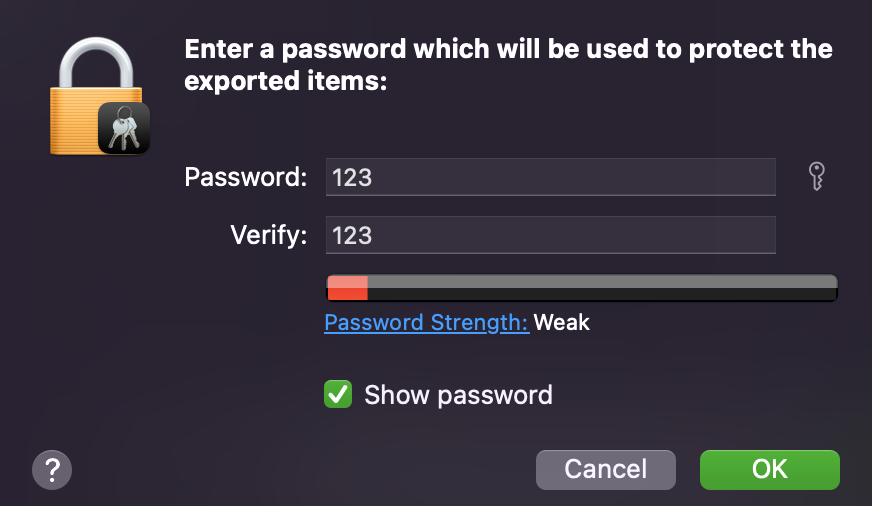
Certificate must be trusted



Double click on certificate and following menu will open up …select always trust…it will ask for mac password please provide it

now look at the arrow at the left of certificate press this arrow and it will open a scroll down menu in which there will be a key section…select both and export to disk in p.12 format. 

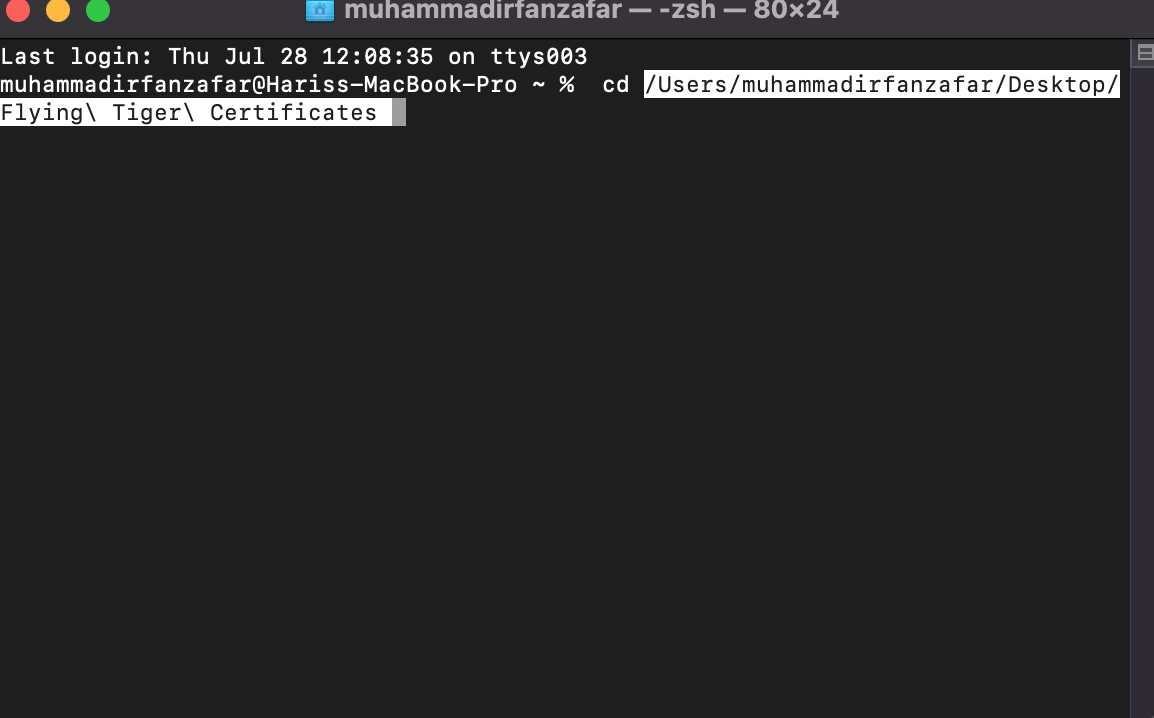
For your ease name this file “path”. And save it your folder.

After clicking save or ok…it will ask for password. In my case its 123 

Now you have this file at your saved destination.

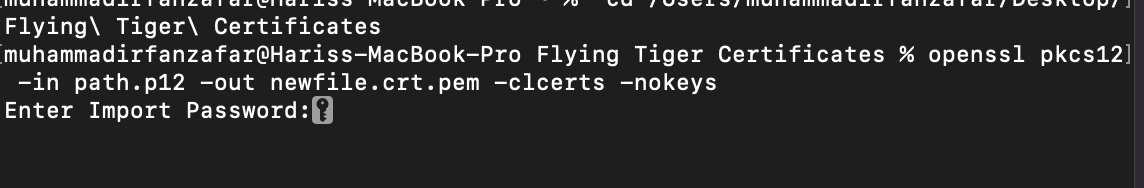


No open terminal and cd to your destination folder

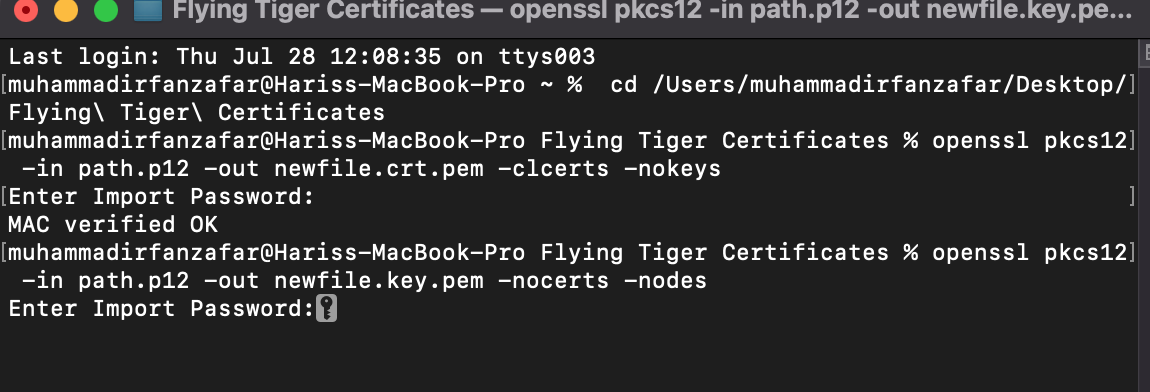


Hit enter and now you have to run the following commands one by one….

openssl pkcs12 -in path.p12 -out newfile.crt.pem -clcerts -nokeys



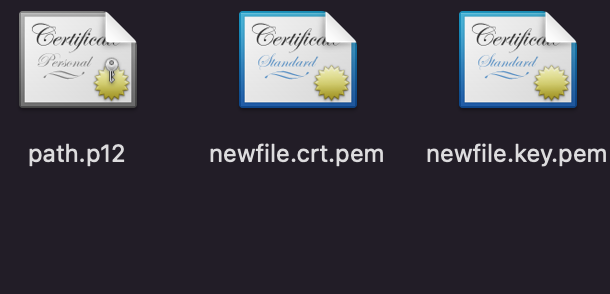
openssl pkcs12 -in path.p12 -out newfile.key.pem -nocerts -nodes



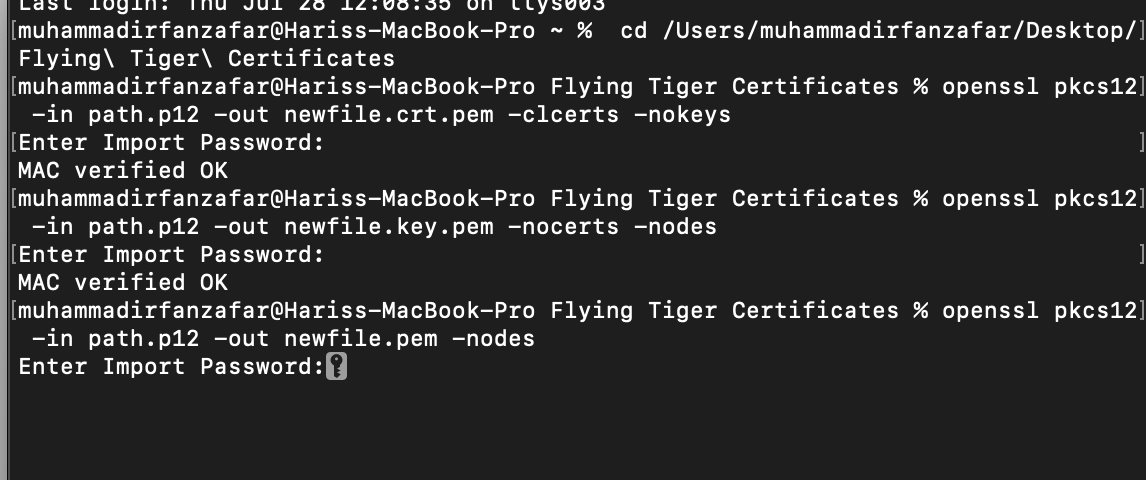
provide password for file whenever terminal asks

After that you have:

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



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

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

now you have complete pem file and p12 file (created earlier) 