



MAC OS User Guide for HYP2003/ePass2003 Tokens

1. Installation of Token Drivers in MAC OS
2. Certificate Trust Policies in MAC OS
3. How to load and unload PKCS#11 module in Mozilla Firefox on MAC OS
4. How to load and unload PKCS#11 module in Adobe Reader for signing PDF on MAC OS

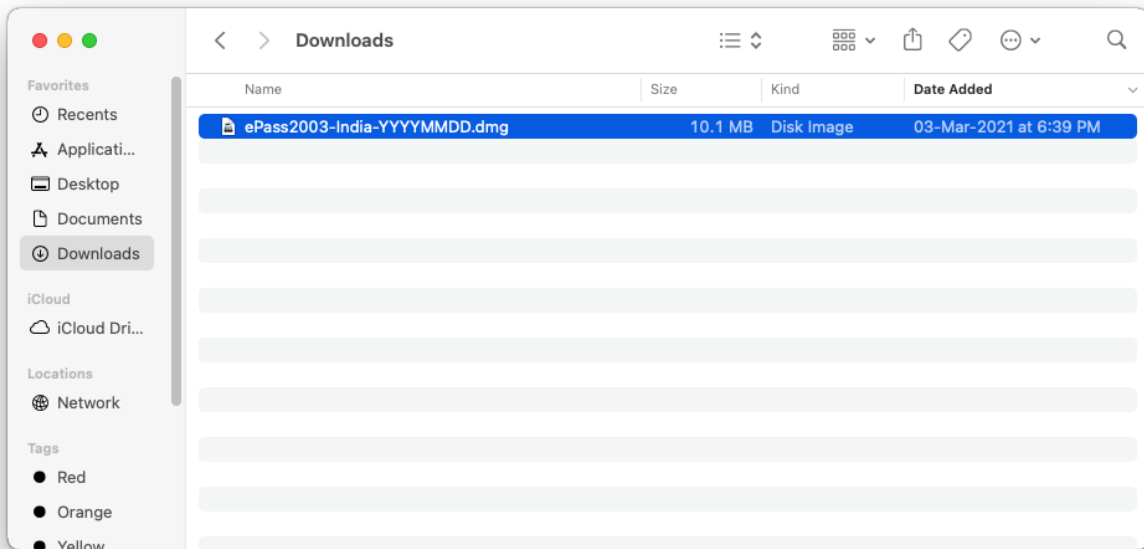
INSTALLATION OF **HYP2003/EPASS2003** TOKEN DRIVER IN MAC OS

From below link, you will able to download device driver for MAC system.

[Downloads and Updates \(India\) | Hypersecu](#)

Once Download is complete, extract the Zip folder and you will find the ePass2003-India.dmg file.

Select the file and open it by double click on it.

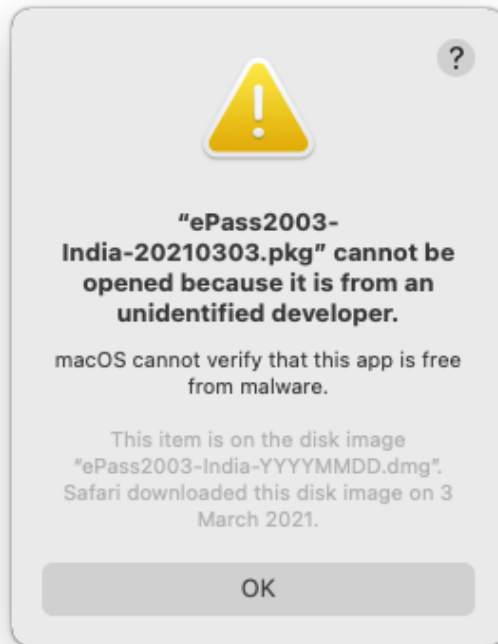


Disk Image package of ePass2003-India having the list of content

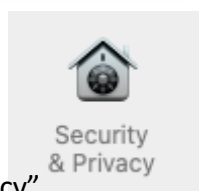
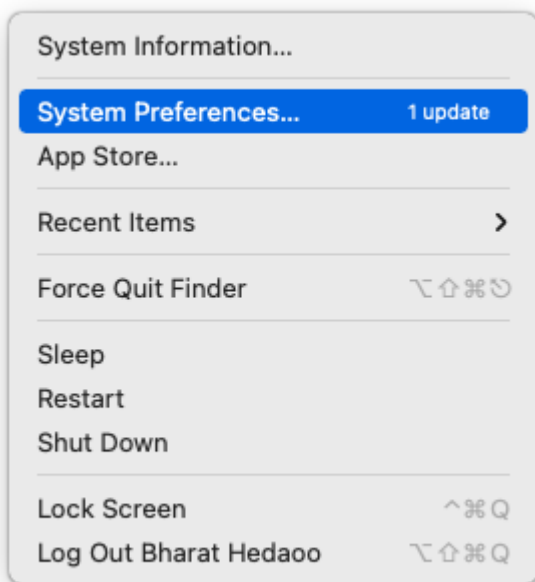
1. EnterSafeAdminMgr:- Manager Tool of Administrator version
2. ePass2003-India-YYYYMMDD.pkg:- it will install EnterSafe middleware and manager
3. License Agreement
4. ReadMe.rtf:- Readme document
5. uninstall.sh:- Uninstall Castle Mac.



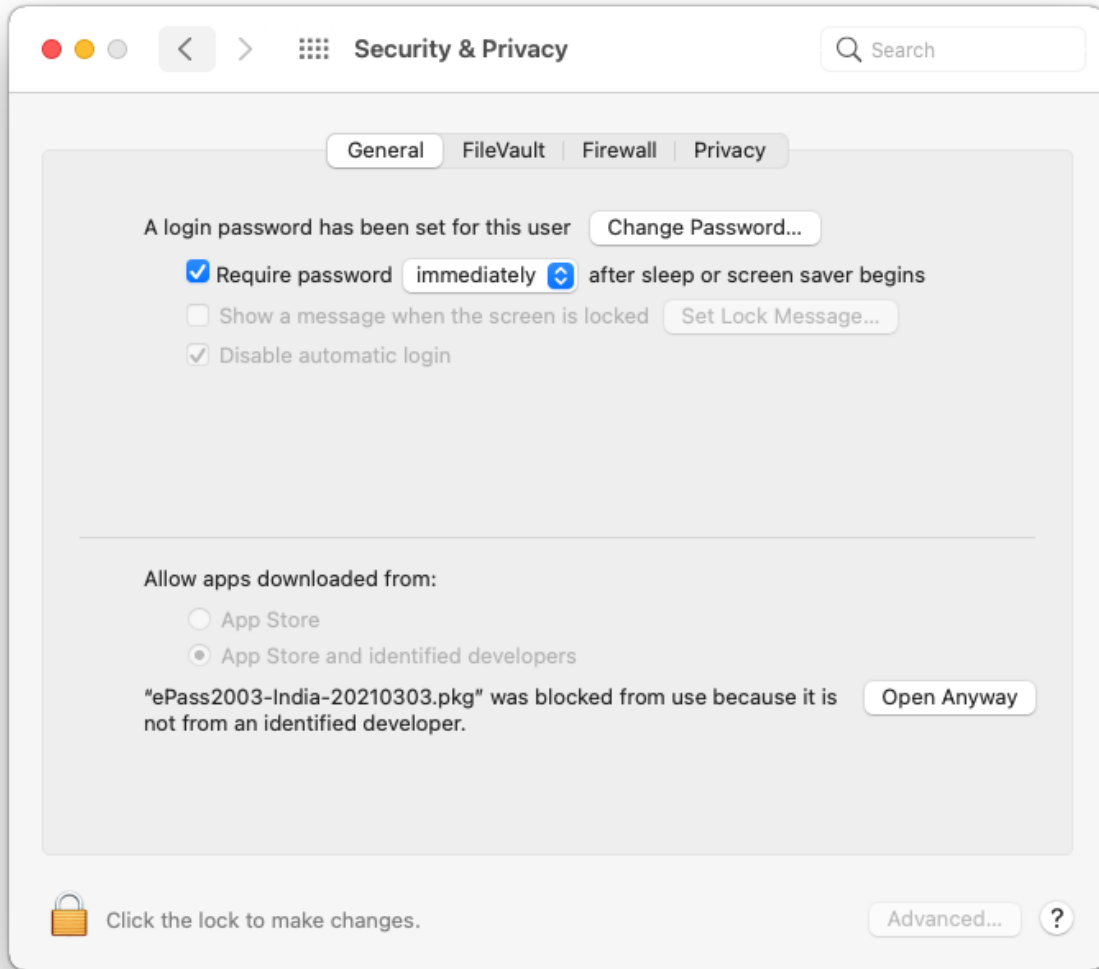
Executing the Package file with double click on it, you will get the message Package is from unidentified developer.

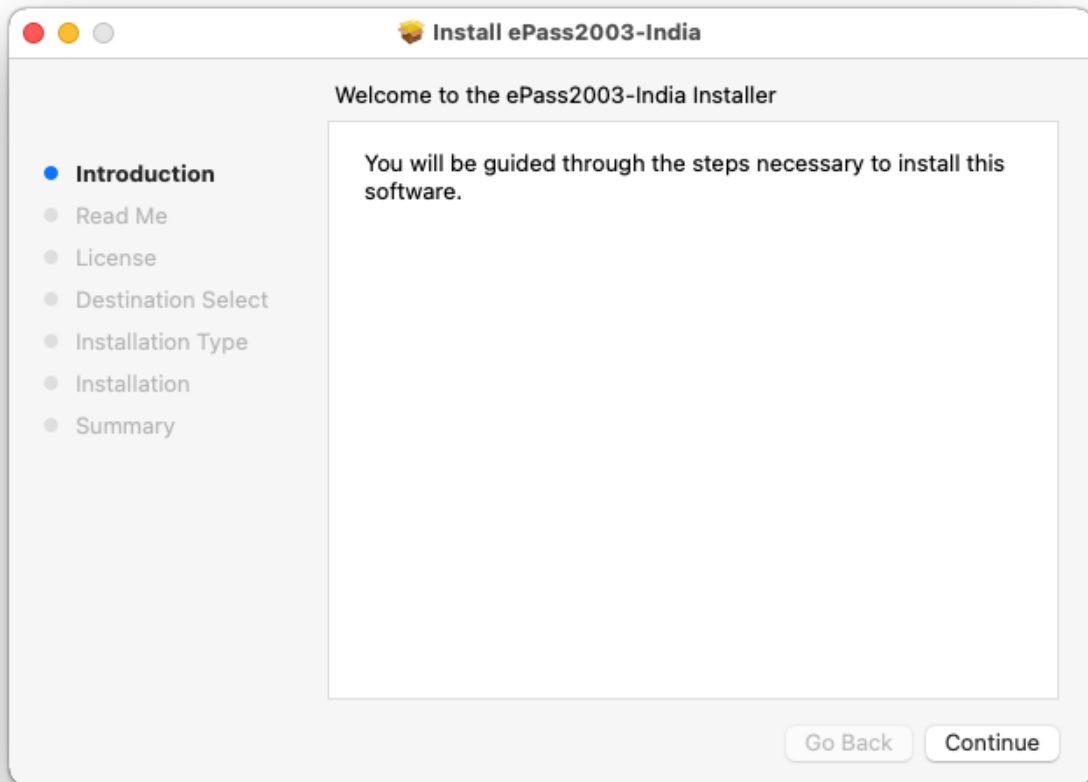
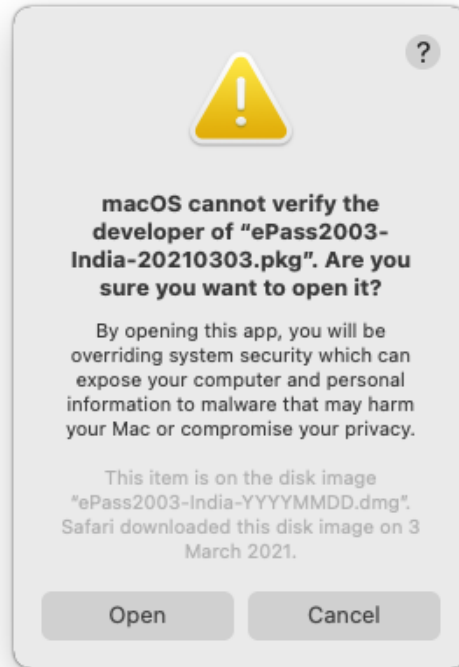


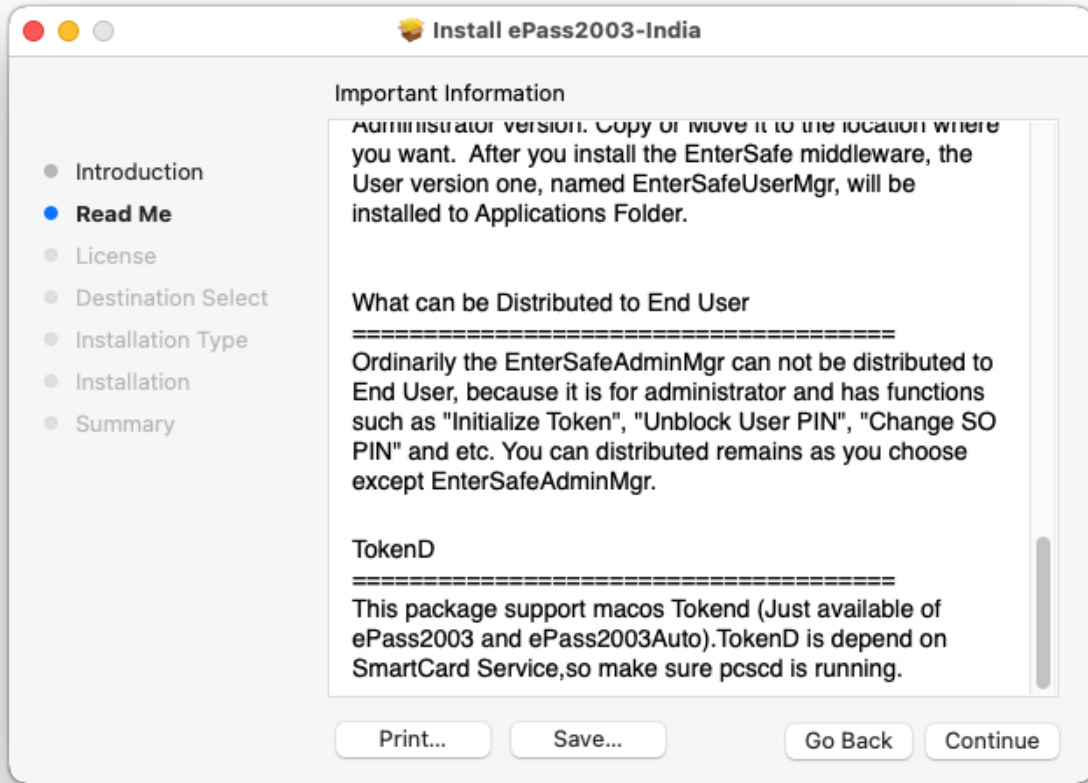
Click on ok and Launch System Preferences from the Apple Menu



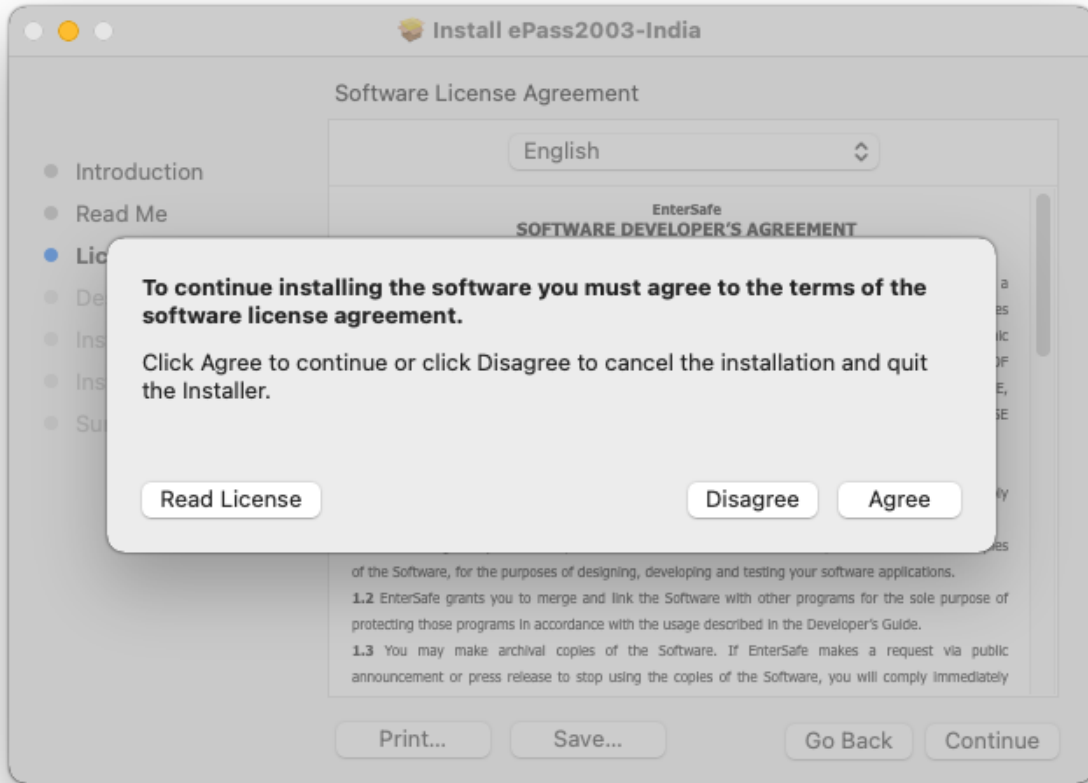
Select the "Security & Privacy" and go to "General" tab. Continue installation by click on Open Anyway button, which is showing, into next image.

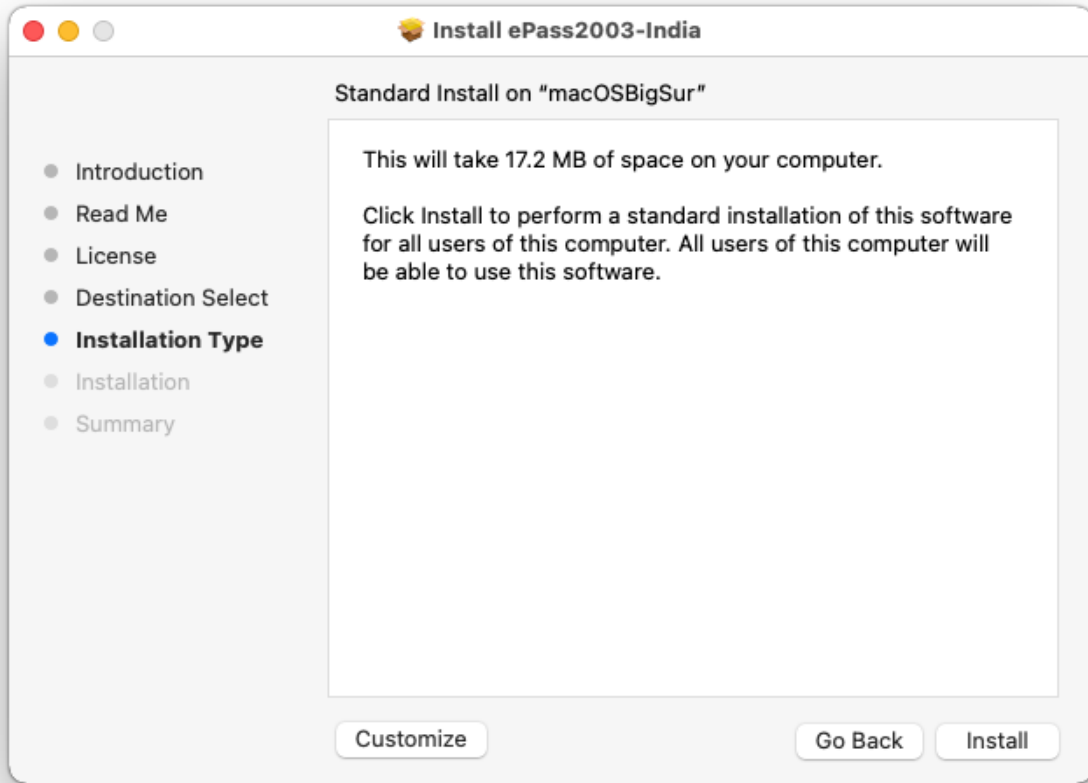


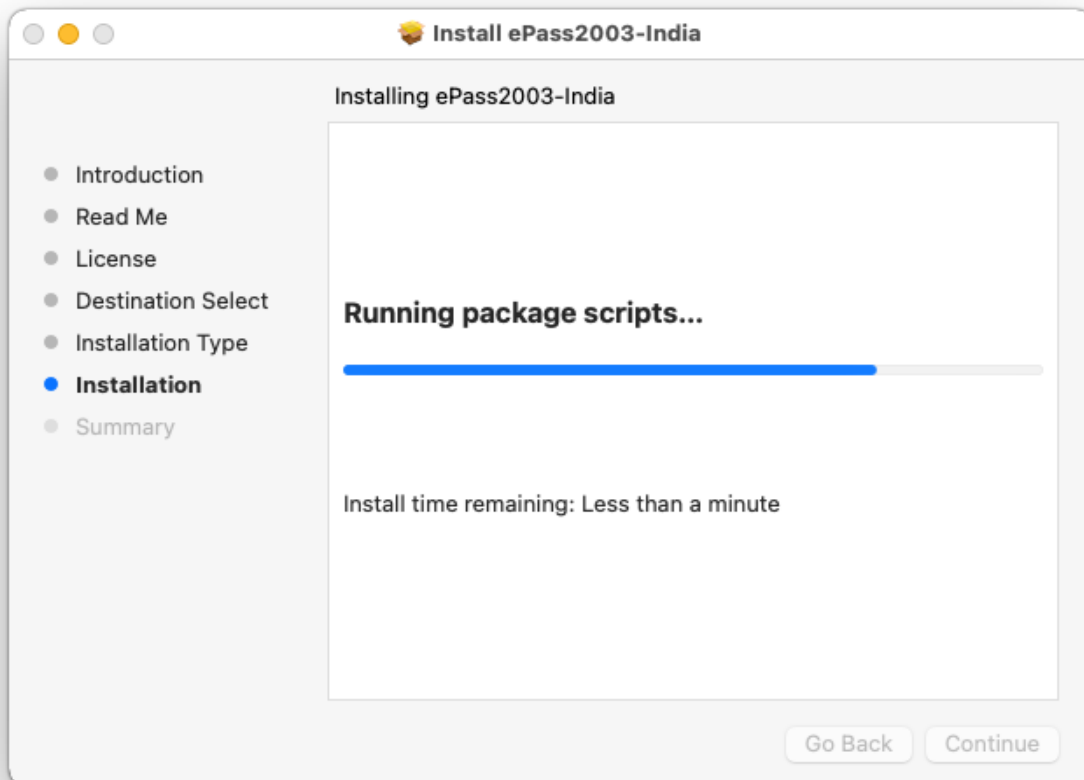
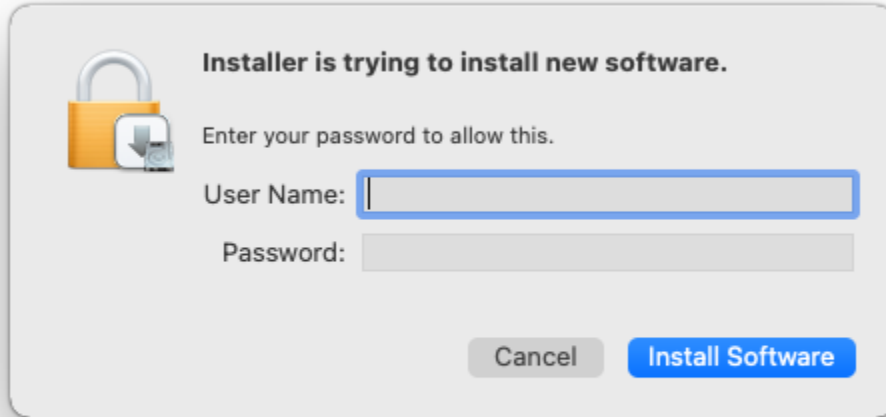


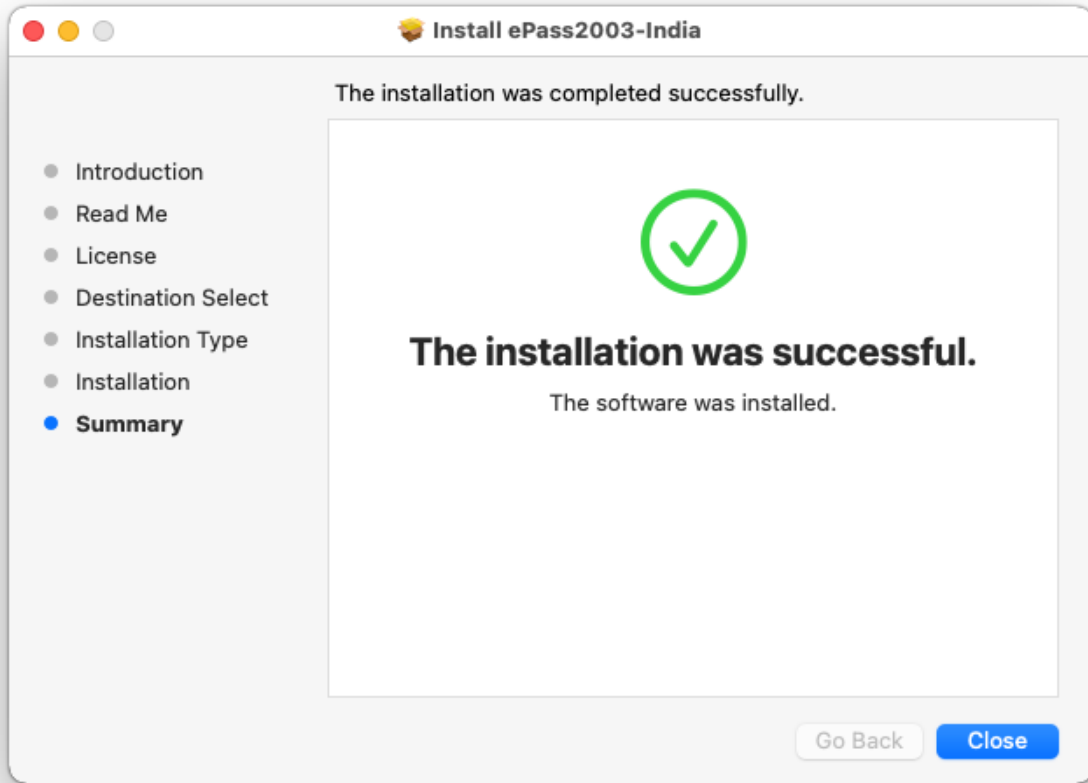






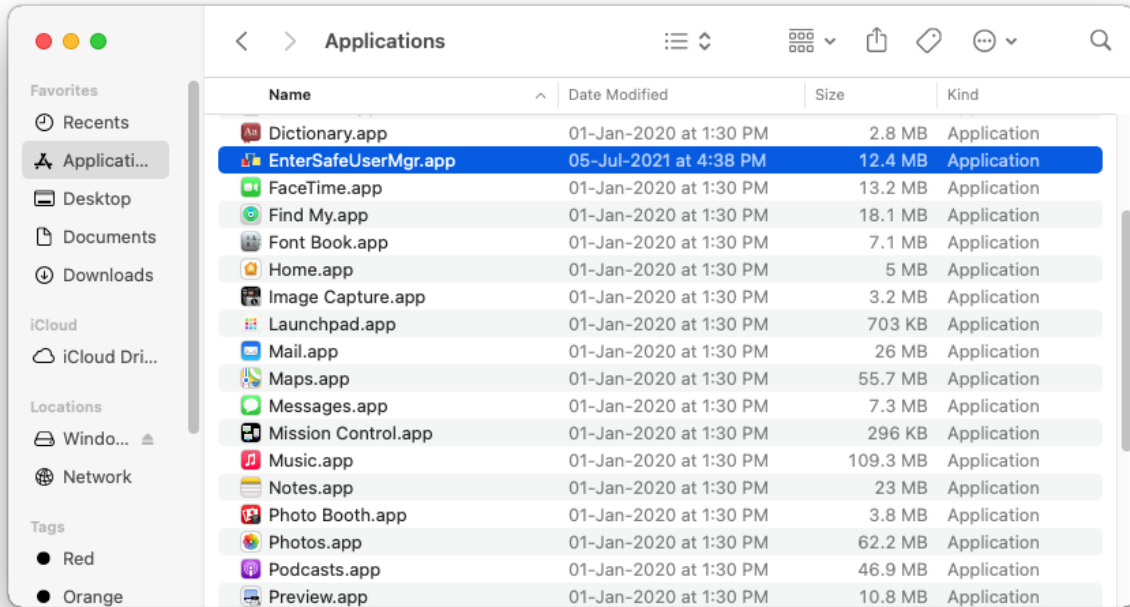




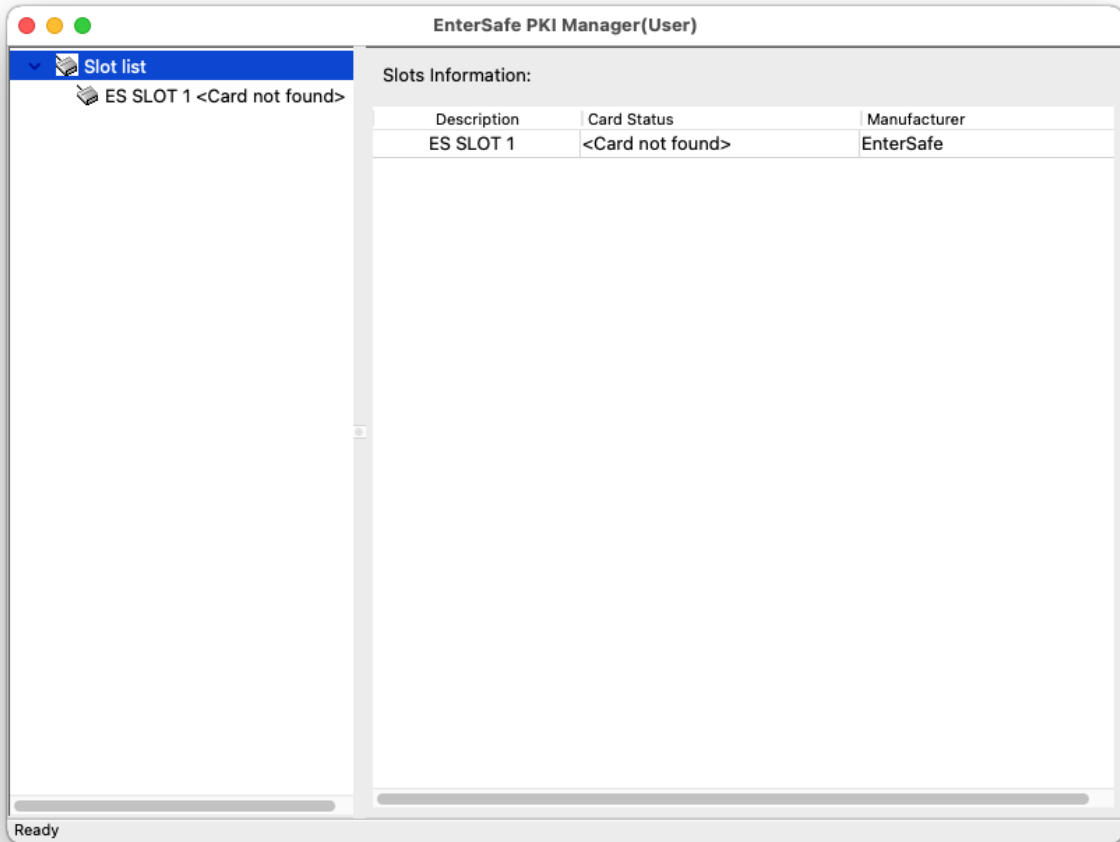


Now installation of driver is completed.

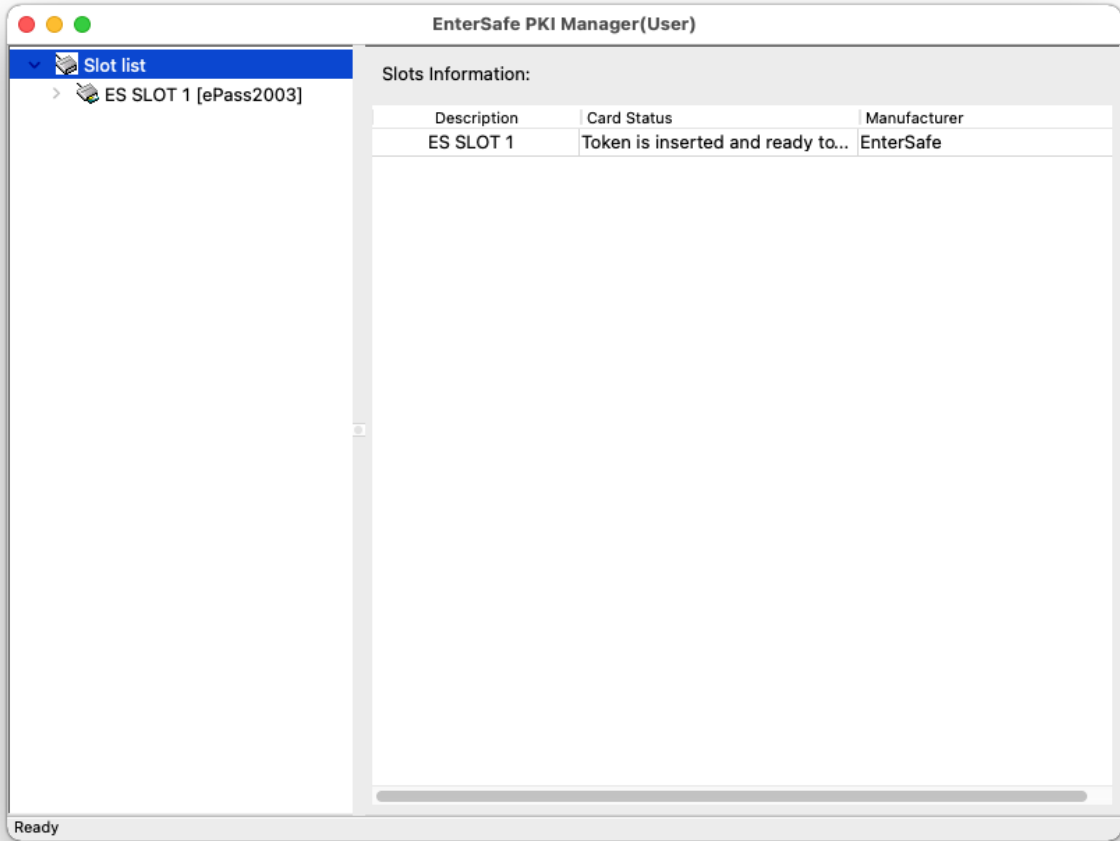
You will find the token manager from the Lanchpad and in the Application with Name "**EnterSafeUserMgr**"

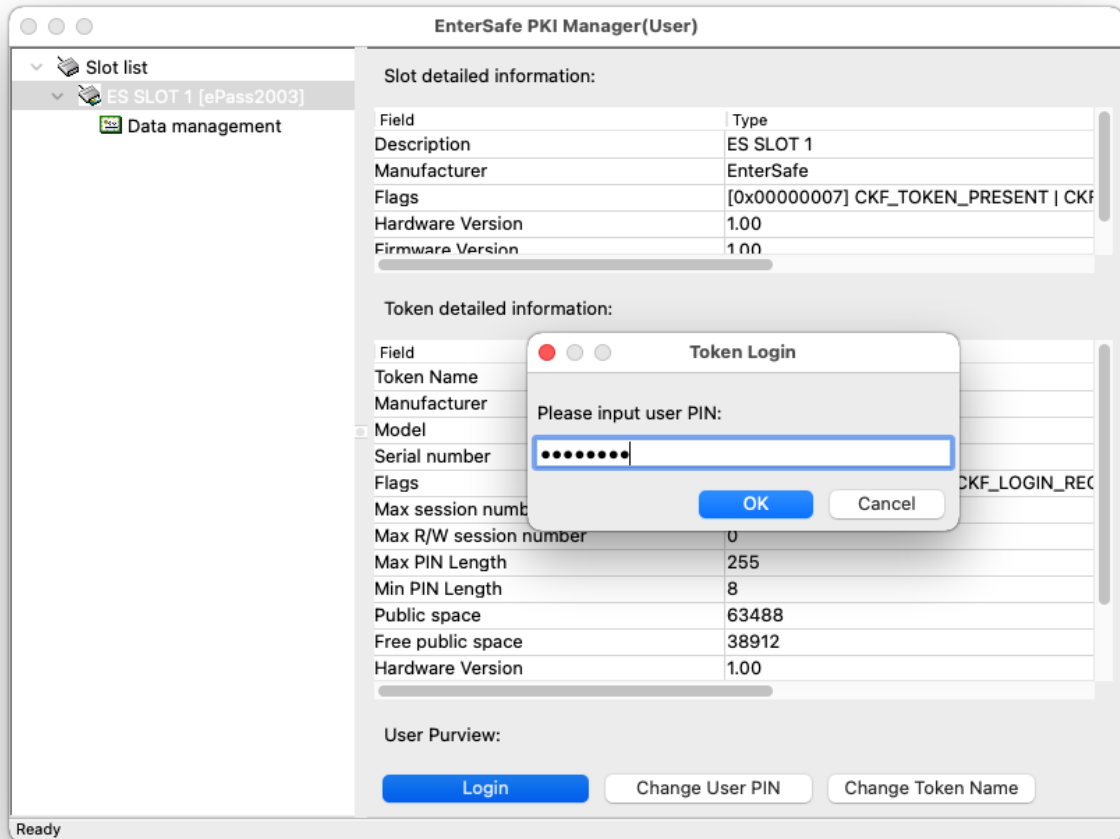


After Open the **EnterSafeUserMgr** it will be look like that.

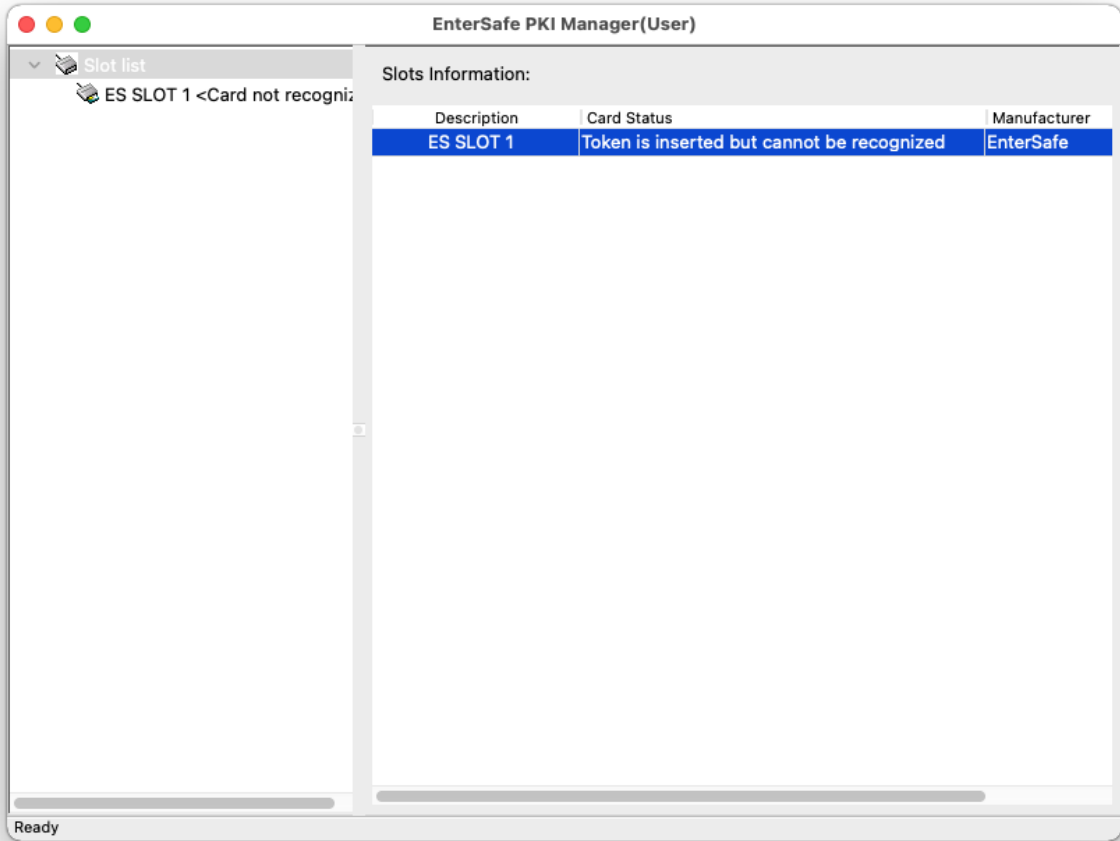


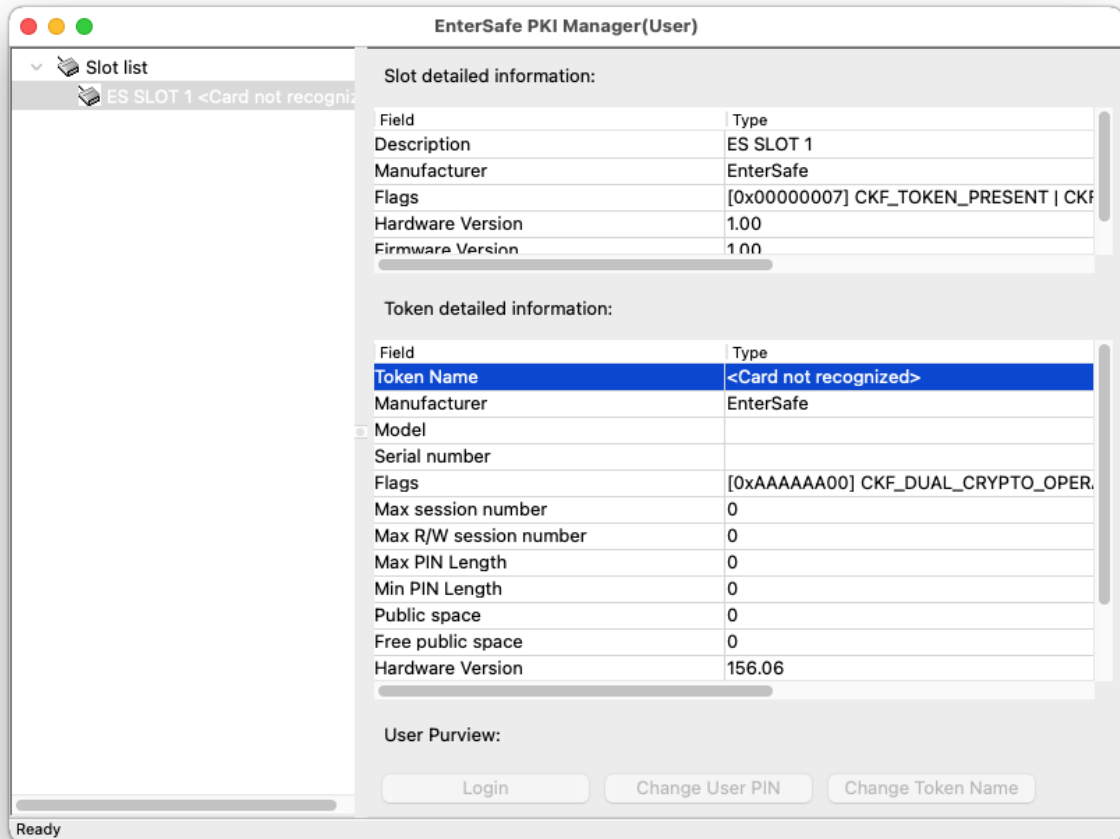
After Connecting token to USB Port ES SLOT follows the Token Name and you will able to access or view the details after login.





But if ePass2003 CSP version is 1.0 then you will get the card status “Token is inserted but cannot be recognized.”





In that case, you need to update the token firmware.

Firmware Process are available on link: -

<https://update.epasstokens.com/Content/ePassUpdateProcess.pdf>

CETIFICATE TRUST POLICIES IN MAC OS

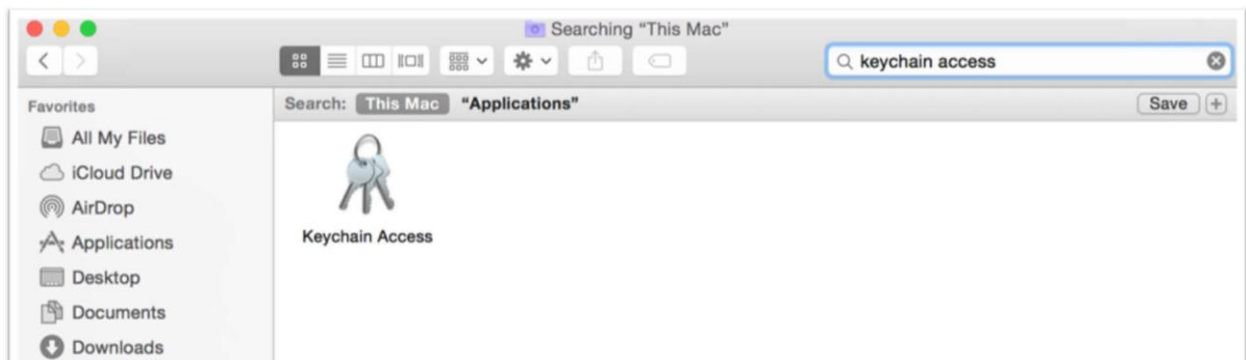
Some Root CA Certificate not Validate in trusted so that you need to set in Trust manually.

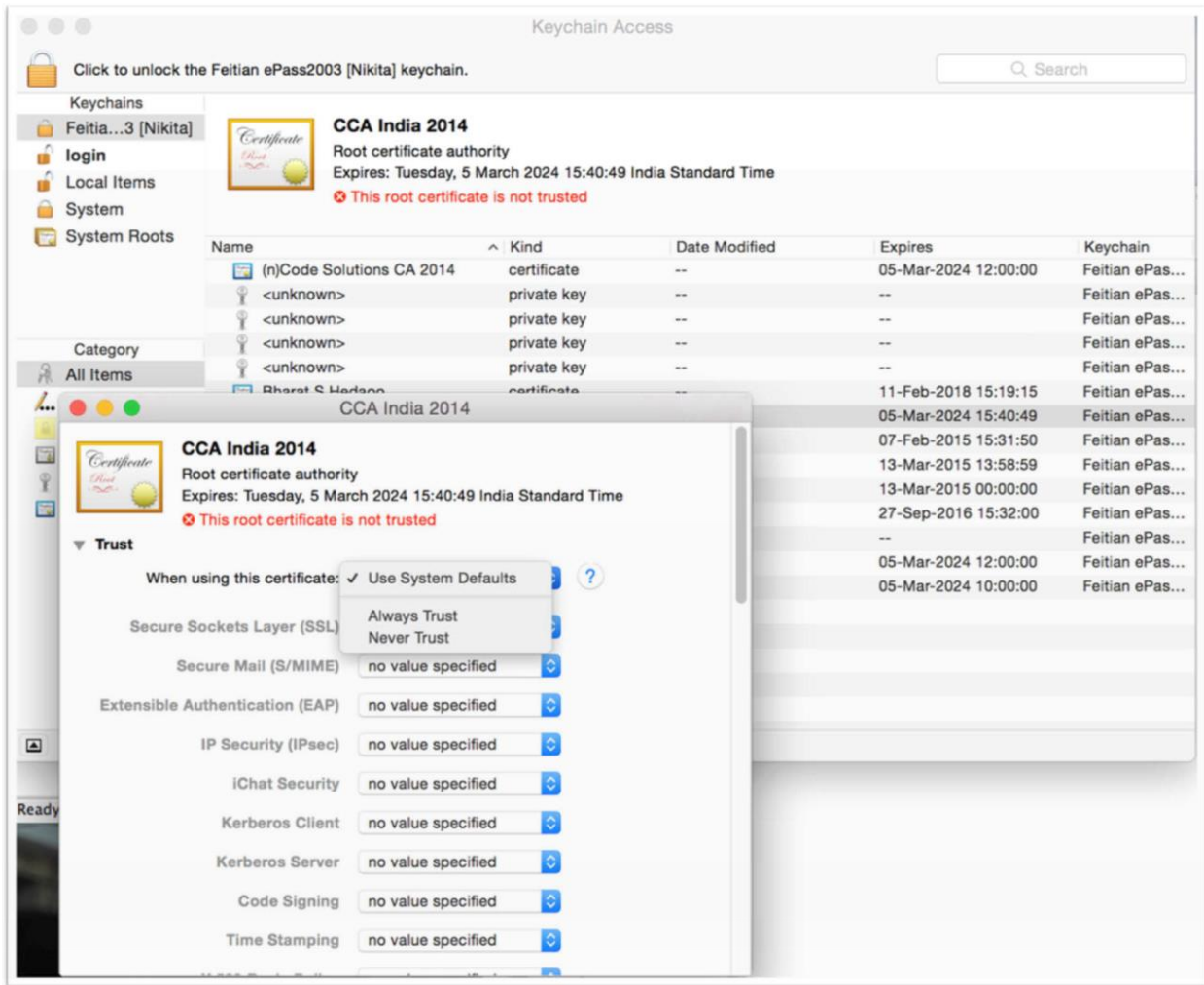
Search the Application Keychain Access and open it or Open Keychain Access, which is in the Utilities folder within the Applications folder.

If a certificate is not accepted, it may have expired or it may be invalid for the way it is being used. For example, some certificates may be used for establishing a secure connection to a server but not for signing a document.

The most common reason a certificate is not accepted is that system does not trust the certificate authority's root certificate. To have your computer trust a certificate authority, you must add the certificate authority to a keychain and set the certificate trust settings.

1. Drag the certificate file onto the Keychain Access icon, or double-click the certificate file.
2. Click the keychain pop-up menu, choose a keychain, and then click OK.
If system asked, enter the name and password for an administrator user on this computer.
3. Select the certificate, then choose File > Get Info.
4. Click the Trust disclosure triangle to display the trust policies for the certificate.
5. To override the trust policies, choose the trust settings you want to override from the pop- up menus.





Certificates are widely used to secure electronic information. For example, a certificate might allow you to sign email, encrypt a document, connect to a secure network, or identify yourself when using Messages. Each type of use is governed by a trust policy, which determines whether a certificate is valid for that use. A certificate may be valid for some uses but not for others.

Mac OS uses a number of trust policies to determine whether a certificate is trusted. You can choose a different policy for each certificate, providing a greater amount of control over how certificates are evaluated.

TRUST POLICY	DESCRIPTION
Use System Defaults or no value specified	Use the default setting for the certificate.
Always Trust	You trust the author and want to always allow access to the server or app.
Never Trust	You don't trust the author and don't want to allow access to the server or app.
Secure Sockets Layer (SSL)	The name in a server's certificate must match its DNS host name to successfully establish a connection. The host name check is not performed for SSL client certificates. If there is an extended key usage field, it must contain an appropriate value.
Secure Mail (S/MIME)	Email uses S/MIME to security sign and encrypt messages. The user's email address must be listed in the certificate, and key usage fields must be included.
Extensible Authentication Protocol (EAP)	When you connect to a network that requires 802.1X authentication, the name in the server's certificate must match its DNS host name. Host names for client certificates are not checked. If an extended key usage field is present, it must
IP Security (IPSec)	When certificates are used to secure IP communications (for example, in establishing a VPN connection), the name in the server's certificate must match its DNS host name. Host names for client certificates are not checked. If an extended key usage field is present, it must contain an appropriate value.
Messages Security	Certificates for messages must contain key usage settings.
Kerberos Client	This policy determines whether the certificate can be used to identify a user to a Kerberos server.
Kerberos Server	This policy determines whether a Kerberos server can use the certificate to identify itself to the system.
Code Signing	The certificate must contain key usage settings that explicitly permit it to sign code.

HOW TO LOAD AND UNLOAD PKCS#11 MODULE IN MOZZILA FIREFOX ON MAC

Start Mozilla; select the menu "Mozilla -> Preferences..." the "Preferences" dialog-box opens. At the left navigation bar, select "Privacy & Security", then "Certificates", the "Certificates" setting page shows at the right panel. Click the "Manage Security Devices..." button, the "Device Manager" dialog-box will pop up. Click the "Load" button to bring the "Load PKCS#11 Device" box. In the Module Name, enter "**EnterSafe**" or the name you like, in the Module filename enter "**/usr/local/lib/libcastle_v2.1.0.0.dylib**", then click "OK" button, all done.

You should not use "Browse..." button here, because the Mac OS protects the system file such as a dynamic library. Therefore, you should enter the module file name manually.

To unload PKCS#11 module, open the "Preferences" -> "Device Manager" dialog, and select the EnterSafe PKCS#11 Module, then click "Unload" button.

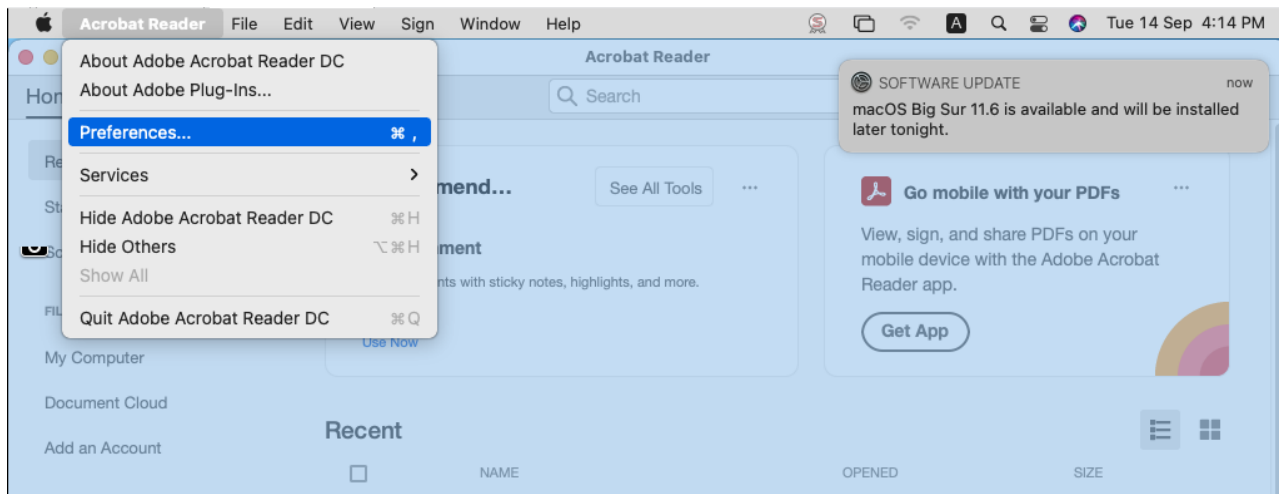
HOW TO LOAD AND UNLOAD PKCS#11 MODULE IN ADOBE READER FOR SIGNING PDF

How to Load PKCS#11 Module in Adobe Reader DC for Sign PDF

Add PKCS 11 Module in Adobe Reader (One Time Process)

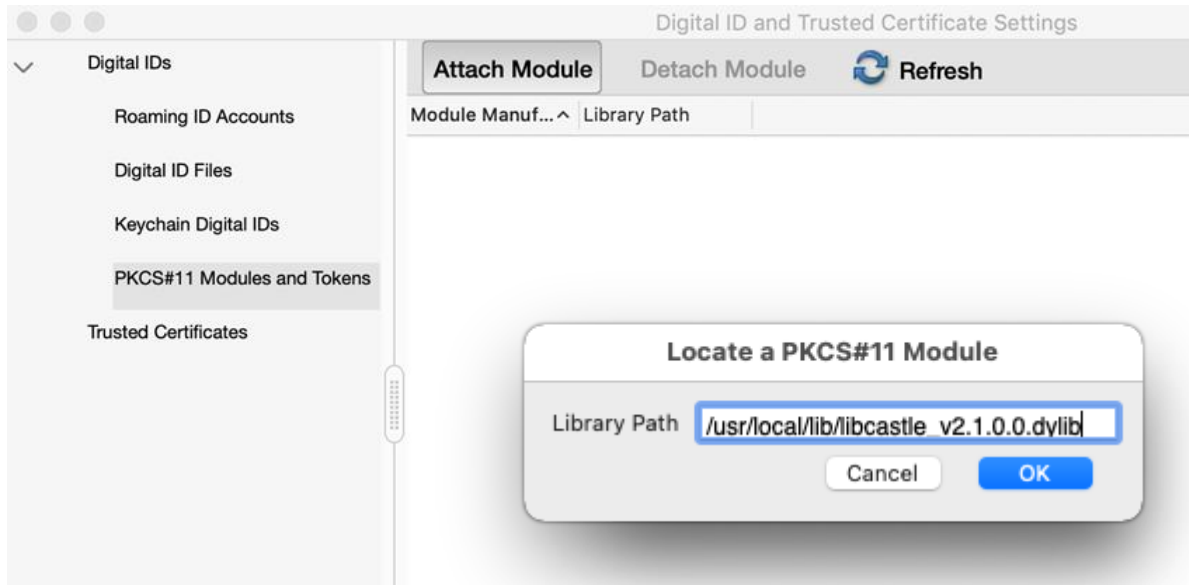
Configuration of a PDF signing certificate in Adobe Acrobat

1. Start Adobe Acrobat
2. Open the Preferences window (⌘ + ,) from the Menu bar

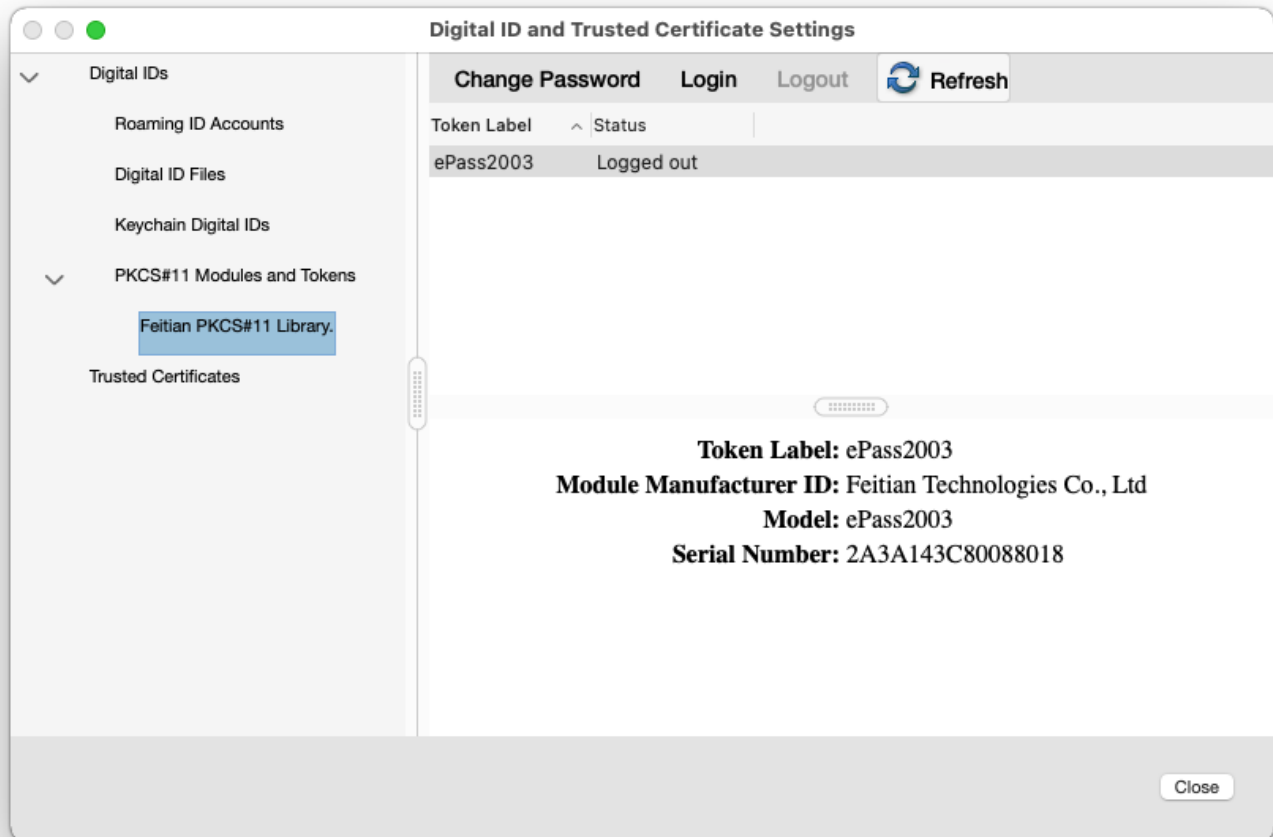


3. Select the category Signatures from left
4. Click on More... under the category **Identities & Trusted Certificates**
5. Click on Digital IDs > PKCS#11 Modules and Tokens

6. Click on **Attach Module**



7. Enter the path “/usr/local/lib/libcastle_v2.1.0.0.dylib” without quote to the PKCS#11 library path and Click On OK
8. After Click Ok. The driver should load, and the token will be shown below the PKCS#11 Modules and Tokens item on the right.



9. Select the correct token as per above image, by expanding the PKCS#11 Module and click Log in, fill in the token password and click OK. (Click on Refresh button if Login button is not Highlight)

Adobe Acrobat now configured to Sign PDF with the certificate, which is present into the token.

1. Open an existing PDF document using **Adobe Acrobat Reader DC**.
2. Click **Tools > Certificates**.
3. Click **Digitally Sign**.
4. Using the target cursor, drag and place the appropriate sized rectangle where you would like the digital signature placed.
5. Click **Sign**.

6. **Re-save** the document.

Note:

1. Step 9 need to perform when you plug the token and try to sign the PDF document.
2. This package support macOS Tokend (Just available of ePass2003 and ePass2003Auto)
TokenD is depend on SmartCard Service,so make sure pcscd is running.

For Test the PCSC service Reference, link

<https://ludovicrousseau.blogspot.com/2014/03/level-1-smart-card-support-on-mac-os-x.html>