



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.

Favorites	Name	Size	Kind	Date Added	`
 Recents 	ePass2003-India-YYYYMMDD.dmg	10.1 M	B Disk Image	03-Mar-2021 at 6:39	РМ
🙏 Applicati					
Desktop					
🗅 Documents					
⊕ Downloads ■					
iCloud					
iCloud Dri					
Locations					
Wetwork					
Tags					
• Red					
Orange					
 Yellow 					



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.

••		📗 ePass2003-India-20	210303	
.	*	RTF	5 mg	SHELL
EnterSafeAdminMgr.app	ePass2003- India-20210303.pkg	license_en.rtf	ReadMe_en.rtf	uninstall.sh

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





Click on ok and Launch System Preferences from the Apple Menu

System Information	
System Preferences	1 update
App Store	
Recent Items	>
Force Quit Finder	乙分米心
Sleep	
Restart	
Shut Down	
Lock Screen	^ % Q
Log Out Bharat Hedaoo	乙合業Q



Select the "Security & Privacy"

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

Www.hypersecu.com















interSafe ELOPER'S AGREEMENT
ELOPER 5 AGREEMENT
legal agreement between you (either an individual or a software that accompanies this SDA, which includes
ed media, printed materials, "online" or electronic
ftware").YOU AGREE TO BE BOUND BY THE TERMS OF WISE USING THE SOFTWARE. IF YOU DO NOT AGREE,
E; YOU MAY RETURN IT TO YOUR PLACE OF PURCHASE
e rights described in this SDA provided that you comply
license to use the Software, and to make and use copies
veloping and testing your software applications. Software with other programs for the sole purpose of usage described in the Developer's Guide.
Software. If EnterSafe makes a request via public e copies of the Software, you will comply immediately

Www.hypersecu.com

	Software License Agreement			
troduction	English			
ead Me	EnterSafe SOFTWARE DEVELOPER'S AGREEMENT			
software licens	stalling the software you must agree to the terms of the se agreement. continue or click Disagree to cancel the installation and quit			
	Disagree Agree			
	Disagree Agree of the Software, for the purposes of designing, developing and testing your software applications. 1.2 EnterSafe grants you to merge and link the Software with other programs for the sole purpose protecting those programs in accordance with the usage described in the Developer's Guide. 1.3 You may make archival copies of the Software. If EnterSafe makes a request via pul announcement or press release to stop using the copies of the Software, you will comply immedian			



	Standard Install on "macOSBigSur"
Introduction Read Me License Destination Select Installation Summary	This will take 17.2 MB of space on your computer. Click Install to perform a standard installation of this software for all users of this computer. All users of this computer will be able to use this software.
	Customize Go Back Instal



Enter your password	t to allow this.	
Password:		
	Cancel	Install Software

	💝 Install ePass2003-India
	Installing ePass2003-India
 Introduction Read Me License Destination Select Installation Type Installation Summary 	Running package scripts Install time remaining: Less than a minute
	Go Back Continue





Now installation of driver is completed.

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



• • •	< > Applications	:= \$	… ~ Ĥ <⁄) ~ Q
Favorites	Name	A Date Modified	Size	Kind
 Recents 	Dictionary.app	01-Jan-2020 at 1:30 PM	2.8 MB	Application
🙏 Applicati	EnterSafeUserMgr.app	05-Jul-2021 at 4:38 PM	12.4 MB	Application
Desktop	💶 FaceTime.app	01-Jan-2020 at 1:30 PM	13.2 MB	Application
_	Find My.app	01-Jan-2020 at 1:30 PM	18.1 MB	Application
Documents	🏙 Font Book.app	01-Jan-2020 at 1:30 PM	7.1 MB	Application
Downloads	ຝ Home.app	01-Jan-2020 at 1:30 PM	5 MB	Application
0	🔚 Image Capture.app	01-Jan-2020 at 1:30 PM	3.2 MB	Application
iCloud	Launchpad.app	01-Jan-2020 at 1:30 PM	703 KB	Application
C iCloud Dri	🔤 Mail.app	01-Jan-2020 at 1:30 PM	26 MB	Application
	💫 Maps.app	01-Jan-2020 at 1:30 PM	55.7 MB	Application
Locations	🖸 Messages.app	01-Jan-2020 at 1:30 PM	7.3 MB	Application
⊖ Windo ≜	Mission Control.app	01-Jan-2020 at 1:30 PM	296 KB	Application
	🗾 Music.app	01-Jan-2020 at 1:30 PM	109.3 MB	Application
Network	Notes.app	01-Jan-2020 at 1:30 PM	23 MB	Application
Tags	🚱 Photo Booth.app	01-Jan-2020 at 1:30 PM	3.8 MB	Application
-	Photos.app	01-Jan-2020 at 1:30 PM	62.2 MB	Application
Red	📵 Podcasts.app	01-Jan-2020 at 1:30 PM	46.9 MB	Application
 Orange 	Review.app	01-Jan-2020 at 1:30 PM	10.8 MB	Application



After Open the EnterSafeUserMgr it will be look like that.

Slot list		I Manager(User)	
Soft list	Slots Information:		
	Description	Card Status	Manufacturer
	ES SLOT 1	<card found="" not=""></card>	EnterSafe

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



Slot list SS SLOT 1 [ePass2003]	Slots Information:	l Manager(User)	
ES SLOT T [ePass2003]	Description	Card Status	Manufacturer
	ES SLOT 1	Token is inserted and ready to	



 Slot list 	Slot detailed information:				
ES SLOT 1 [ePass2003]	Field		Turne		
🖼 Data management	Description		Type ES SLOT 1		
	Manufacturer		EnterSafe		
	Flags		[0x00000007] CKF_TC		
	Hardware Version		1.00	KEN_PRESENT CK	
	Firmware Version		1.00		
	Firmware version	n	100		
	Token detailed	information:			
	Field	Token Login			
	Token Name				
	Manufacturer	Please input user PIN:			
	Model				
	Serial number	••••••			
	Flags			CKF_LOGIN_RE	
	Max session nun	nb	OK Cancel		
	Max R/W session	number	0		
	Max PIN Length		255		
	Min PIN Length 8		8		
			63488	63488	
	Free public space		38912		
		Hardware Version 1.00			
	User Purview:				
eady	Login	Cha	nge User PIN Change	Foken Name	

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



	EnterSafe PKI Manager(User)				
 Slot list ES SLOT 1 <card li="" not="" recogniz<=""> </card>	Slots Information:				
	Description ES SLOT 1	Card Status Token is inserted but cannot be recognized	Manufacture EnterSafe		
ady					



eld		
	Туре	
escription	ES SLOT 1	
anufacturer	EnterSafe	
ags	[0x0000007] CKF_TOKEN_PRESENT CK	
ardware Version	1.00	
mware Version	100	
	Туре	
	<pre><pre><pre><pre>Card not recognized></pre></pre></pre></pre>	
	EnterSafe	
	Encloure	
erial number		
ags	[0xAAAAAA00] CKF_DUAL_CRYPTO_OPER	
ax session number	0	
ax R/W session number	0	
ax PIN Length	0	
n PIN Length	0	
Iblic space	0	
ee public space	0	
ardware Version	156.06	
	anufacturer ags ardware Version wware Version oken detailed information: eld iken Name anufacturer odel erial number ags ax session number ax R/W session number ax R/W session number ax PIN Length in PIN Length ublic space ee public space	

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.



www.hypersecu.com

HYPERSECU[®]

Click to unlock the	Feitian ePass2003 [Nikita] keychain.			Q Search				
Keychains		e renar er desseee printaj negenario						
Feitia3 [Nikita]		CA India 2014						
login	Certificate	ot certificate autho	prity					
Local Items			March 2024 15:40:49	India Standard Time				
		This root certificate						
System								
System Roots	Name		^ Kind	Date Modified	Expires	Keychain		
	[] (n)Code Solu	utions CA 2014	certificate		05-Mar-2024 12:00:00	Feitian ePa		
	<pre></pre>		private key			Feitian ePa		
	<pre> variable </pre>		private key			Feitian ePa		
Category	<pre> {unknown> } </pre>		private key			Feitian ePa		
All Items	<pre>vunknown></pre>		private key			Feitian ePa		
	Rhorat C Har	CA India 2014	cortificato	-	11-Feb-2018 15:19:15	Feitian ePa		
	0	CA India 2014			05-Mar-2024 15:40:49	Feitian ePa		
	04 1-1- 0044				07-Feb-2015 15:31:50	Feitian ePa		
	CA India 2014							
" Certificate		v			13-Mar-2015 13:58:59	Feitian ePa		
Certificate Real	oot certificate authority		India Standard Time		13-Mar-2015 13:58:59 13-Mar-2015 00:00:00			
Certificate Ref E		ch 2024 15:40:49 I	ndia Standard Time			Feitian ePa		
Certificate Ref E	oot certificate authority xpires: Tuesday, 5 Mar	ch 2024 15:40:49 I	India Standard Time		13-Mar-2015 00:00:00	Feitian ePa Feitian ePa		
Trust	oot certificate authority xpires: Tuesday, 5 Mar This root certificate is	ch 2024 15:40:49 I s not trusted			13-Mar-2015 00:00:00 27-Sep-2016 15:32:00	Feitian ePa Feitian ePa Feitian ePa		
Trust	oot certificate authority xpires: Tuesday, 5 Mar	ch 2024 15:40:49 I s not trusted			13-Mar-2015 00:00:00 27-Sep-2016 15:32:00 	Feitian ePa Feitian ePa Feitian ePa Feitian ePa		
Trust When a	oot certificate authority xpires: Tuesday, 5 Mar This root certificate is	ch 2024 15:40:49 I s not trusted			13-Mar-2015 00:00:00 27-Sep-2016 15:32:00 05-Mar-2024 12:00:00	Feitian ePa Feitian ePa Feitian ePa Feitian ePa		
Trust When a Secure S	oot certificate authority xpires: Tuesday, 5 Mare This root certificate is using this certificate:	ch 2024 15:40:49 i a not trusted ✓ Use System Def Always Trust	aults		13-Mar-2015 00:00:00 27-Sep-2016 15:32:00 05-Mar-2024 12:00:00	Feitian ePa Feitian ePa Feitian ePa Feitian ePa		
Trust When a Secure S	oot certificate authority prires: Tuesday, 5 Mar This root certificate is using this certificate: • Sockets Layer (SSL)	ch 2024 15:40:49 not trusted Use System Def Always Trust Never Trust	aults ?		13-Mar-2015 00:00:00 27-Sep-2016 15:32:00 05-Mar-2024 12:00:00	Feitian ePa Feitian ePa Feitian ePa Feitian ePa Feitian ePa Feitian ePa		
Trust When a Secure S	oot certificate authorit xpires: Tuesday, 5 Mar 9 This root certificate is using this certificate: Sockets Layer (SSL) accure Mail (S/MIME)	ch 2024 15:40:49 l a not trusted V Use System Def Always Trust Never Trust no value specifie	aults ? ed o		13-Mar-2015 00:00:00 27-Sep-2016 15:32:00 05-Mar-2024 12:00:00	Feitian ePa Feitian ePa Feitian ePa Feitian ePa		
Trust When a Secure S Extensible A	oot certificate authority prires: Tuesday, 5 Man 9 This root certificate is using this certificate: • Sockets Layer (SSL) ecure Mail (S/MIME) uthentication (EAP)	ch 2024 15:40:49 l a not trusted Use System Def Always Trust Never Trust no value specifie no value specifie	aults) ? ad o ad o		13-Mar-2015 00:00:00 27-Sep-2016 15:32:00 05-Mar-2024 12:00:00	Feitian ePa Feitian ePa Feitian ePa Feitian ePa		
Trust When a Secure S	oot certificate authority xpires: Tuesday, 5 Mar 9 This root certificate is using this certificate: Sockets Layer (SSL) becure Mail (S/MIME) uthentication (EAP) IP Security (IPsec)	ch 2024 15:40:49 l a not trusted Use System Def Always Trust Never Trust no value specifie no value specifie no value specifie	aults ? ed O ed O ed O ed O		13-Mar-2015 00:00:00 27-Sep-2016 15:32:00 05-Mar-2024 12:00:00	Feitian ePa Feitian ePa Feitian ePa Feitian ePa		
Trust When a Secure S Extensible A	oot certificate authority prires: Tuesday, 5 Man o This root certificate is using this certificate: • Sockets Layer (SSL) scure Mail (S/MIME) uthentication (EAP) IP Security (IPsec) iChat Security	ch 2024 15:40:49 l a not trusted Use System Def Always Trust Never Trust no value specifie no value specifie no value specifie no value specifie	aults ? ed o ed o ed o ed o		13-Mar-2015 00:00:00 27-Sep-2016 15:32:00 05-Mar-2024 12:00:00	Feitian ePa Feitian ePa Feitian ePa Feitian ePa		
Trust When a Secure S Extensible A	oot certificate authority xpires: Tuesday, 5 Mar 9 This root certificate is using this certificate: Sockets Layer (SSL) becure Mail (S/MIME) uthentication (EAP) IP Security (IPsec) iChat Security Kerberos Client	ch 2024 15:40:49 l not trusted Use System Def Always Trust Never Trust no value specifie no value specifie no value specifie no value specifie no value specifie	aults ? ed 0 ed 0 ed 0 ed 0 ed 0 ed 0 ed 0		13-Mar-2015 00:00:00 27-Sep-2016 15:32:00 05-Mar-2024 12:00:00	Feitian ePa Feitian ePa Feitian ePa Feitian ePa		

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 <u>SSL</u> client certificates. If there is an extended key usage field, it must contain an appropriate value.				
Secure Mail (S/MIME)	Email uses <u>S/MIME</u> 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				
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 $${\rm PDF}$$

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 (\Re + ,) 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

		Digital ID and Tru	isted Certificate Settings
Digital IDs	Attach Module	Detach Module	C Refresh
Roaming ID Accounts	Module Manuf ^ Libr	ary Path	
Digital ID Files			
Keychain Digital IDs			
PKCS#11 Modules and Tokens			
Trusted Certificates		Locate a PKC	CS#11 Module
	Librar	y Path /usr/local/lik	p/libcastle_v2.1.0.0.dylib
			Cancel OK
		-	
	Digital IDs Roaming ID Accounts Digital ID Files Keychain Digital IDs PKCS#11 Modules and Tokens	Digital IDs Roaming ID Accounts Digital ID Files Keychain Digital IDs PKCS#11 Modules and Tokens Trusted Certificates	Digital IDs Roaming ID Accounts Digital ID Files Keychain Digital IDs PKCS#11 Modules and Tokens Trusted Certificates Locate a PKC

- 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.



• •	•	Digital ID and T	rusted Certificat	e Settings		
/	Digital IDs	Change Pass	sword Login	Logout	C Refresh	
	Roaming ID Accounts	Token Label 💦 🗠	Status			
	Digital ID Files	ePass2003	Logged out			
	Keychain Digital IDs					
\sim	PKCS#11 Modules and Tokens					
	Feitian PKCS#11 Library.					
	Trusted Certificates					
				(Ð	
		M	odule Manufact	Model: eP	itian Technologies Co., I	Ltd
						Close

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-osx.html