

macOS User Guide for HYP2003

HyperPKI USB Token

09/09/2022

HSTE-NB0066-IND-RV1.0

HYPERSECU INFORMATION SYSTEMS INC

200-6191 Westminster Hwy, Richmond BC, V7C 4V4 Canada 1-604-279-2000 | hypersecu.com

Table of Contents

Getting Started	1
Requirements	1
Installing the HYP2003 Token Drivers	1
Logging In	5
Certificate Trust Policies	6
Types of Trust Policies	6
Set a Certificate's Trust Policy:	7
Digital Signing	8
Loading the PKCS#11 Module in Mozilla Firefox	8
Loading the PKCS#11 Module in Acrobat Reader DC for Digital Signing	8
Digitally Signing a PDF in Acrobat Reader DC	9

Document History

Version	Release Date	Description of Changes	Document Owner	Approved By
1.0	2022-09-09	Original document	NB	JL

Getting Started

Requirements

Before installing EnterSafe PKI Manager for the HYP2003 be sure the following requirements are fulfilled:

- The latest version of the HYP2003 drivers for macOS (go to hypersecu.com/updates-india to download)
- At least one available supported USB port
- HyperPKI HYP2003 USB token

Installing the HYP2003 Token Drivers

- 1. Extract the downloaded files, then locate ePass2003-India.dmg.
- 2. Double-click the file to open it and view the contents inside the disk image package:
 - EnterSafeAdminMgr: administrator version of EnterSafe PKI Manager
 - ePass2003-India-YYYYMMDD.pkg: installs EnterSafe PKI Manager
 - License Agreement
 - ReadMe.rtf: Readme document
 - uninstall.sh: Uninstalls Castle Mac.
- 3. Double-click ePass2003-India-YYYYMMDD.pkg to begin installation.
- 4. When you receive the message that the .pkg file is from an unidentified developer, click **OK** and open **System Preferences** form the Apple Menu.



5. Click Security & Privacy, then click on the General tab and click Open Anyway.

	General FileVault Firewall	Privacy
A login passwo	ord has been set for this user Change	Password
🗹 Require	e password immediately ᅌ after sleep	p or screen saver begins
Show a	a message when the screen is locked	Set Lock Message
Jisabi	o outomatio login	
Allow apps do	wnloaded from:	
O App St	tore	
 App St App St 	tore tore and identified developers	
App St App St Pass2003-Ir not from an id	tore tore and identified developers ndia-20210303.pkg" was blocked from us entified developer.	se because it is Open Anyway
App St App St "ePass2003-Ir not from an ide	tore tore and identified developers ndia-20210303.pkg" was blocked from us entified developer.	se because it is Open Anyway
App Si App Si "ePass2003-Ir not from an id	tore tore and identified developers ndia-20210303.pkg" was blocked from us entified developer.	se because it is Open Anyway
App Si App Si "ePass2003-Ir not from an id	tore tore and identified developers ndia-20210303.pkg" was blocked from us entified developer.	se because it is Open Anyway

6. Click **Open** to continue with the installation process.



- 7. Click **Continue** and follow the instructions on the installation guide.
- 8. Click Agree to proceed with the installation.



9. Click **Install**, then enter your user name and password if prompted and click **Install Software**.

\bigcap	Installer is t	rying to	install new	software.
	Enter your pas	sword to a	allow this.	
	User Name:			
	Password:			
			Cancel	Install Software

10. Click **Close** to complete the installation.

• •	😺 Install ePass2003-India
 Introduction Read Me License Destination Select Installation Type Installation Summary 	<text><image/><section-header><section-header><text><text></text></text></section-header></section-header></text>

Logging In

- 1. Open EnterSafe PKI Manager and connect the HYP2003 token.
- 2. If connected correctly, the HYP2003 token will appear on the Slot list

	EnterSafe PK	EnterSafe PKI Manager(User)				
 Slot list ES SLOT 1 [ePass2003] 	Slots Information:					
•	Description	Card Status	Manufacturer			
	ES SLOT 1	Token is inserted and ready to	EnterSafe			
	ES SLOT 1	Token is inserted and ready to	EnterSafe			

NOTE: If the HYP2003 token's CSP version is 1.0, the Card Status will display "Token is inserted but cannot be recognized." This means the HYP2003 token's firmware needs to be updated. To do so, see https://update.epasstokens.com/Content/ePassUpdateProcess.pdf.

- 3. Select the HYP2003 you inserted, then click **Login**.
- 4. Enter the user PIN and click **OK**.

🗸 词 Slot list	Slot detailed in	formation:			
SLOT 1 [ePass2003]	Slot detailed in	iormation.			
Data management	Field		Туре		
	Description		ES SLOT 1		
	Manufacturer		EnterSafe		
	Flags		[0x000000	07] CKF_TOK	EN_PRESENT CK
	Hardware Version		1.00	1.00	
	Firmware Versio	n	100		
	Field 🕒 🔿 Token Login				
	Token detailed	information.			_
	Tokon Namo	Token Name			
	Manufacturer Please input user PIN: Model				
			PIN:		
	Serial number	•••••			
	Flags				CKE LOGIN REC
	Max session nur	nb	ОК	Cancel	
	Max R/W session number		0		9
	Max PIN Length		255		
	Min PIN Length		8		
	Public space		63488		
	Free public space		38912		
	Hardware Version		1.00		
	User Purview:				
	Login	Chang	e User PIN	Change To	ken Name

Certificate Trust Policies

Some Root CA Certificates must be manually set to Trust. 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.

Types of Trust Policies

Certificates are widely used to secure electronic information. For example, a certificate might allow you to sign an 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.

macOS uses several 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.
NeverTrust	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 contain an appropriate value.
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

Trust Policy	Description
	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.

Set a Certificate's Trust Policy:

1. Search the **Application Keychain Access** and open it or navigate to the Utilities folder in the Applications folder and click **Open Keychain Access**.



- 2. Click and drag the certificate file to the Keychain Access icon or double-click the certificate file.
- 3. Click the keychain window, then choose a keychain and click **OK**.
- 4. If prompted, enter your user name and password.
- 5. Select the certificate, then select **File > Get Info**.
- 6. Click the **Trust** expandable menu to display the policies for the certificate, then select the trust policy you want to manually set.

Digital Signing

Loading the PKCS#11 Module in Mozilla Firefox

- 1. In the main Firefox menu, select Settings.
- 2. Click **Privacy & Security**, then navigate to Certificates and click **Security Devices**.
- 3. Click Load, then enter a name for the Module Name field.
- 4. In the Module filename field, enter the file path below:

```
/usr/local/lib/libcastle v2.1.0.0.dylib
```

5. Click **OK** to finish loading.

NOTE: Do not use browse to locate this file. Dynamic library files are protected by the macOS system so the file path must be entered manually.

NOTE: To unload the PKCS#11, go to **Settings > Privacy & Security > Security Devices**, and click **Unload**.

Loading the PKCS#11 Module in Acrobat Reader DC for Digital Signing

1. In Acrobat Reader DC, select **Preferences** from the Acrobat Reader menu.



- 2. Select **Signatures**, then click **More** under the category **Identities & Trusted Certificates**.
- 3. Click **Digital IDs**, then select **PKCS#11 Modules and Tokens**.
- 4. Click **Attach Module** and enter the file path below:

		Digital ID and Tru	sted Certificate Settings
Digital IDs	Attach Module	Detach Module	C Refresh
Roaming ID Accounts	Module Manuf ^ Lib	rary Path	
Digital ID Files			
Keychain Digital IDs			
PKCS#11 Modules and Tok	kens		
Trusted Certificates			
Trusted Certificates		Locate a F	PKCS#11 Module
Trusted Certificates		Locate a F	PKCS#11 Module
Trusted Certificates		Locate a F	PKCS#11 Module

- 5. Click **OK** to finish loading. The token will appear under the PKCS#11 Modules and Tokens menu.
- 6. Select the token, then click **Login**.

0 0	•	Digital ID an	Digital ID and Trusted Certificate Settings				
\sim	Digital IDs	Change F	Password	Login	Logout	2 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						
					(1)	

7. Enter the user PIN and click **OK**.

NOTE: If the Login button is not highlighted, click **Refresh**.

Digitally Signing a PDF in Acrobat Reader DC

1. Open the PDF document you want to sign.

- 2. Under Tools, click **Certificates**, then click **Digitally Sign**.
- 3. Draw the box on the document where you would like to place the digital signature.
- 4. Click **Sign**, then save the document.

IMPORTANT: This package supports macOS TokenD. TokenD is dependant on Smart Card Services, so be sure PC/SC is running. To test for PC/SC services, refer to: https://ludovicrousseau.blogspot.com/2014/03/level-1-smart-card-support-on-mac-os-x.html