HYPERPKI™

HYP2003 USB TOKEN User Guide

THE #1 USB TOKEN IN
THE INDIAN MARKET

#200-6191 Westminster Hwy, Richmond BC V7C 4V4, CANADA
hypersecu.com | 1 (604) 279-2000

HYPERSECU®

Revision History:

Date	Revisi	
Jan 2021	V1.0	Release of the first version
Jun 2022	V1.1	Update for HYP2003

Software Developer's Agreement

All Products of Hypersecu Information Systems Inc. including, but not limited to, evaluation copies, diskettes,

CD-ROMs, hardware and documentation, and all future orders, are subject to the terms of this Agreement. If you do not agree with the terms herein, please return the evaluation package to us, postage and insurance prepaid, within seven days of their receipt, and we will reimburse you the cost of the Product, less freight and reasonable handling charges.

1. Allowable Use – You may merge and link the Software with other programs for the sole purpose of protecting those programs in accordance with the usage described in the Developer's Guide. You may make archival copies of the Software.

2. Prohibited Use – The Software or hardware or any other part of the Product may not be copied, reengineered, disassembled, decompiled, revised, enhanced or otherwise modified, except as specifically allowed in item 1. You may not reverse engineer the Software or any part of the product or attempt to discover the Software's source code. You may not use the magnetic or optical media included with the Product for the purposes of transferring or storing data that was not either an original part of the Product, or a Hypersecu provided enhancement or upgrade to the Product.

3. Warranty – Hypersecu warrants that the hardware and Software storage media are substantially free from significant defects of workmanship or materials for a time period of twelve (12) months from the date of delivery of the Product to you.

4. Breach of Warranty – In the event of breach of this warranty, Hypersecu's sole obligation is to replace or repair, at the discretion of Hypersecu, any Product free of charge. Any replaced Product becomes the property of Hypersecu.

Warranty claims must be made in writing to Hypersecu during the warranty period and within fourteen (14) days after the observation of the defect. All warranty claims must be accompanied by evidence of the defect that is deemed satisfactory by Hypersecu. Any Products that you return to Hypersecu, or a Hypersecu authorized distributor, must be sent with freight and insurance prepaid.

EXCEPT AS STATED ABOVE, THERE IS NO OTHER WARRANTY OR REPRESENTATION OF THE PRODUCT, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

5. Limitation of Hypersecu's Liability – Hypersecu's entire liability to you or any other party for any cause whatsoever, whether in contract or in tort, including negligence, shall not exceed the price you paid for the unit of the Product that caused the damages or are the subject of, or indirectly related to the cause of action. In no event shall Hypersecu be liable for any damages caused by your failure to meet your obligations, nor for any loss of data, profit or savings, or any other consequential and incidental damages, even if Hypersecu has been advised of the possibility of damages, or for any claim by you based on any third-party claim.

6. Termination – This Agreement shall terminate if you fail to comply with the terms herein. Items 2, 3, 4 and 5 shall survive any termination of this Agreement.

Contents

Chapter 1 Runtime Installation

1.1 Supported Platform

Windows Platform:

- Windows 2000
- Windows XP x86/x64
- Windows 2003 x86/x64
- Windows Vista x86/64
- Windows 2008 x86/x64
- Windows 7 x86/x64
- Windows8 x86/x64
- Windows10 x86/x64

Linux Mac OS

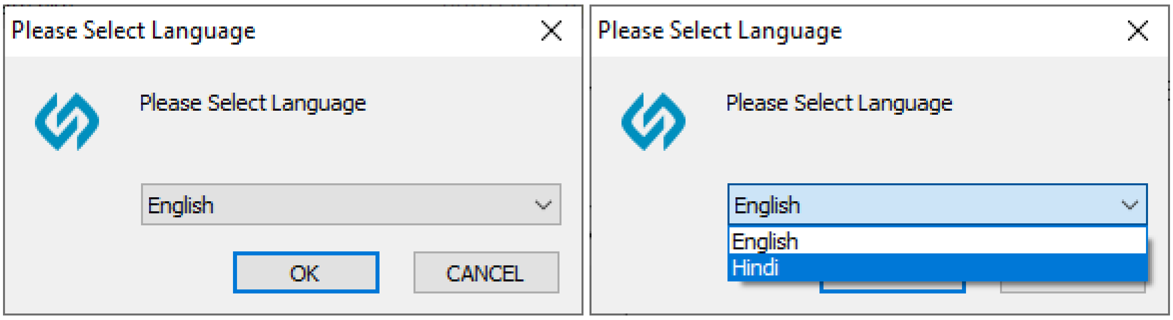
1.2 Preparing for installing HYP2003

Before installing HYP2003 Runtime, make sure the following requirements are satisfied:

- Your operating system is one in the above list
- Your computer has at least one USB port available
- Your BIOS supports the USB device, and USB support has been enabled in CMOS settings
- USB extension or hub available (optional)
- HYP2003 Token available

1.3 Installing HYP2003 Runtime

1. Before you can use the HYP2003, you must install the Runtime library. Execute HYP2003-Setup.exe. The following select language interface appears:



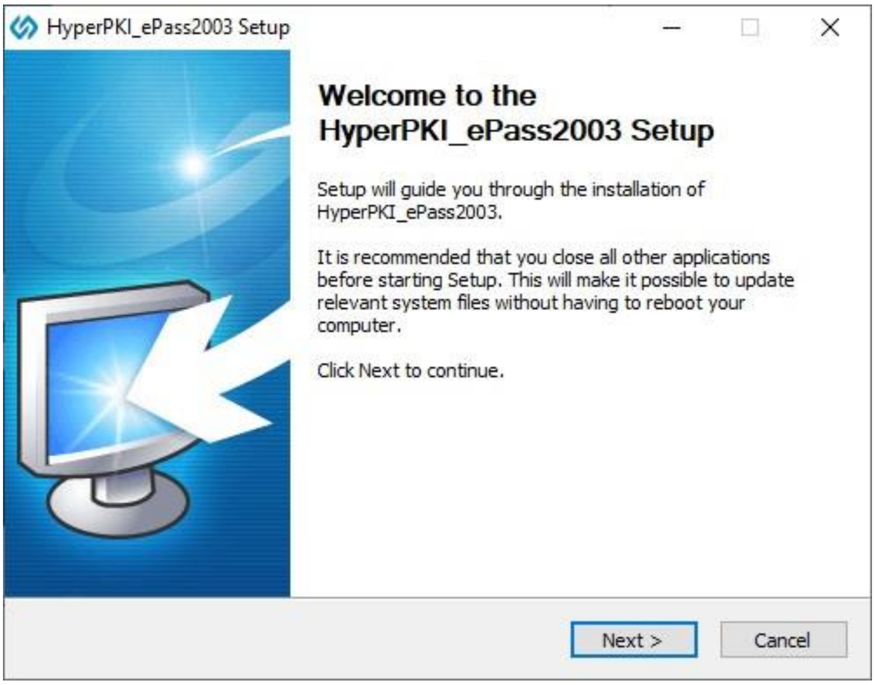
Please Select Language

Please Select Language

English

Figure 1 select language

2. After select language, click “OK”, the following welcome interface appears:



HyperPKI_ePass2003 Setup

Welcome to the HyperPKI_ePass2003 Setup

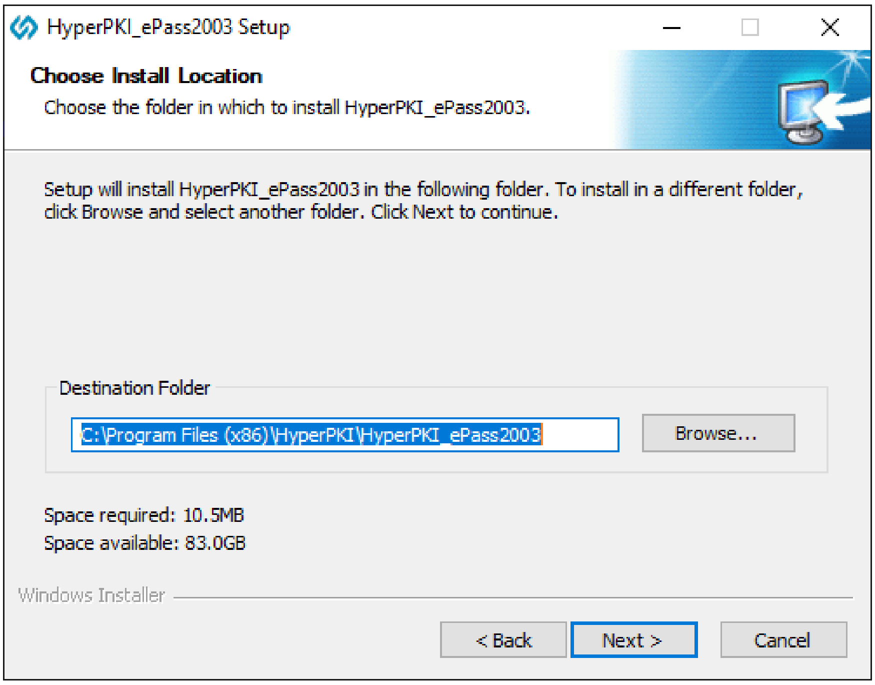
Setup will guide you through the installation of HyperPKI_ePass2003.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Figure 2 welcome interface

3. Click “Next”, the following select install path interface appears:



HyperPKI_ePass2003 Setup

Choose Install Location

Choose the folder in which to install HyperPKI_ePass2003.

Setup will install HyperPKI_ePass2003 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder

C:\Program Files (x86)\HyperPKI\HyperPKI_ePass2003

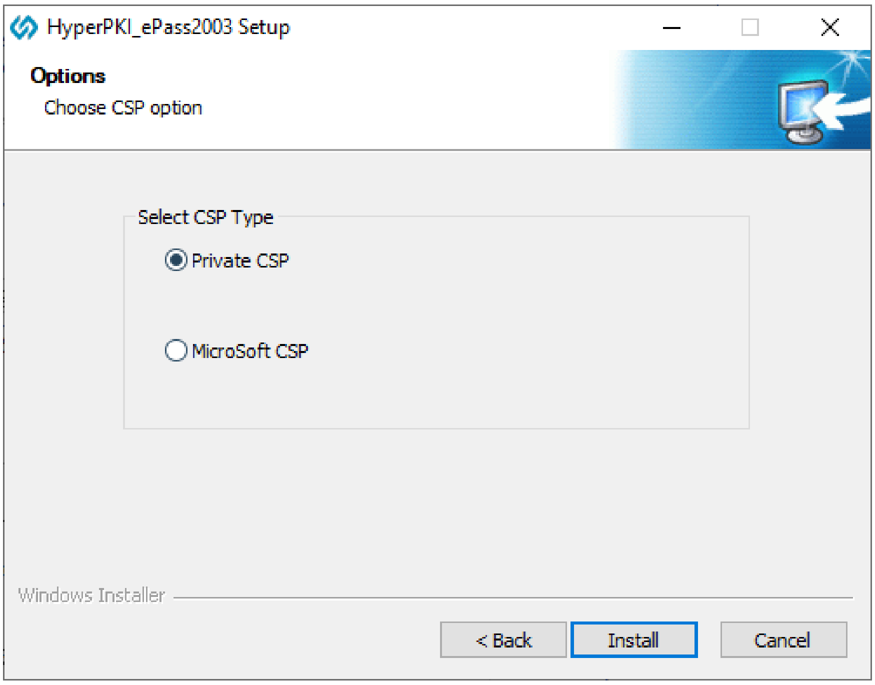
Space required: 10.5MB

Space available: 83.0GB

Windows Installer

Figure 3 select install path

4. Click "Next", the following choose CSP interface appears:



HyperPKI_ePass2003 Setup

Options

Choose CSP option

Select CSP Type

● Private CSP

○ MicroSoft CSP

Windows Installer

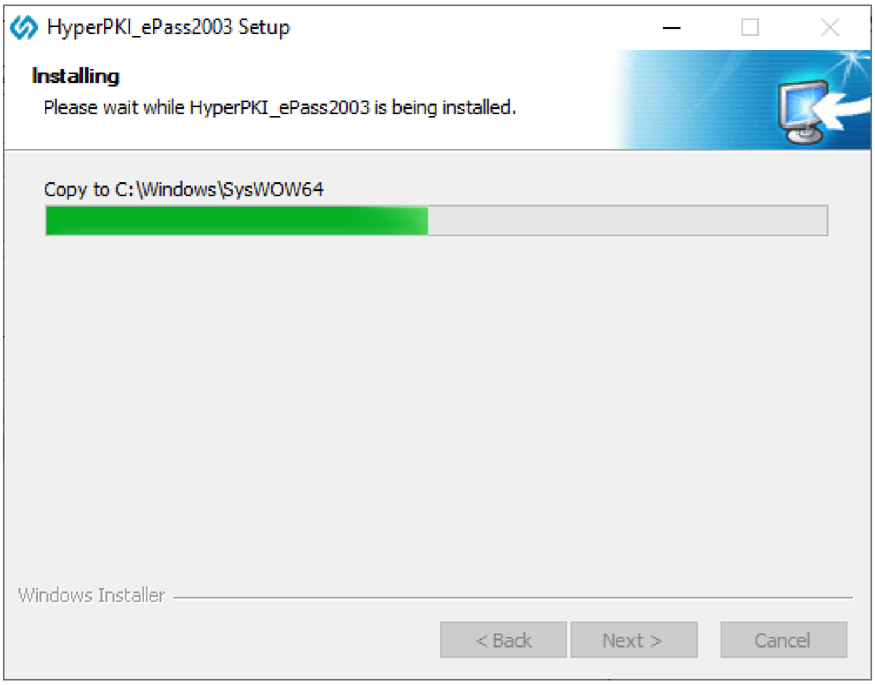
Figure 4 choose CSP

Note: HYP2003 supports Private CSP and Microsoft CSP.

For older windows systems such as Windows2000/XP, users must install patch KB909520 to enable the option 'Microsoft CSP'.

- Private CSP is provided by HYPERSECU, the CSP name is "EnterSafe ePass2003 CSP v2.0".
- Microsoft CSP means Microsoft Base CSP (Microsoft Base Smart Card Crypto Provider), it supports Minidriver, and user can install the middleware through system update, no redundant installation package, no complicated installation process; we also have installation package for the user who doesn't have the Internet. But please pay attention, from Vista and above, Microsoft has integrated Minidriver into Windows system, for XP and below, Windows system doesn't install Base CSP (Microsoft CSP option disable), user can add Base CSP through system patch KB909520.

5. After select CSP, click "Install" to continue, the following interface appears:



HyperPKI_ePass2003 Setup

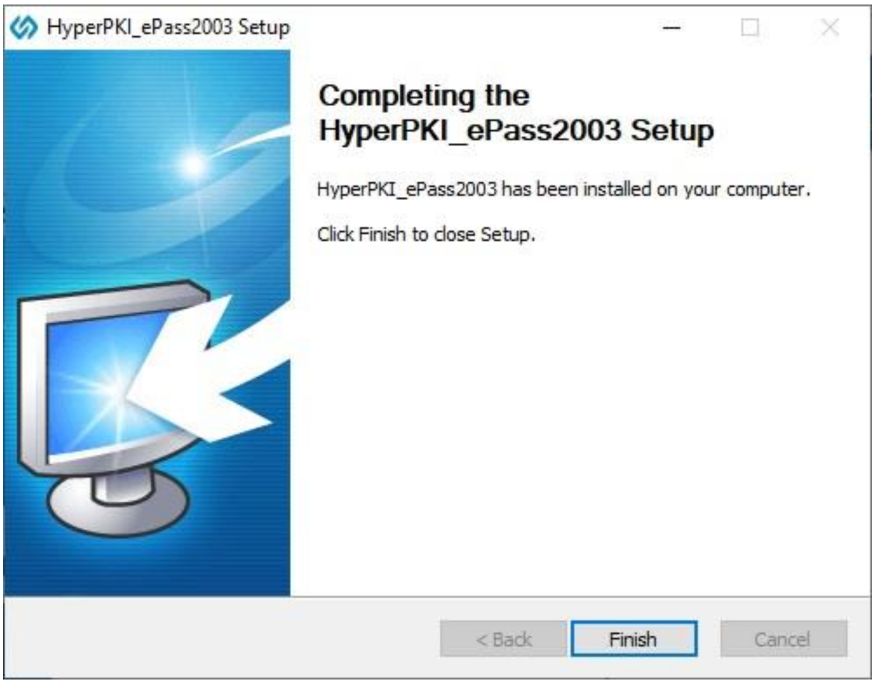
Installing

Please wait while HyperPKI_ePass2003 is being installed.

Copy to C:\Windows\SysWOW64

Figure 5 install process

6. After install process finish, the following interface appears:


HyperPKI_ePass2003 Setup

Completing the HyperPKI_ePass2003 Setup

HyperPKI_ePass2003 has been installed on your computer.

Click Finish to close Setup.

Figure 6 install completed

7. Click “Finish” to finish the installation.

1.4 Uninstalling HYP2003Runtime

After install the HYP2003 runtime, you can uninstall it through following methods:

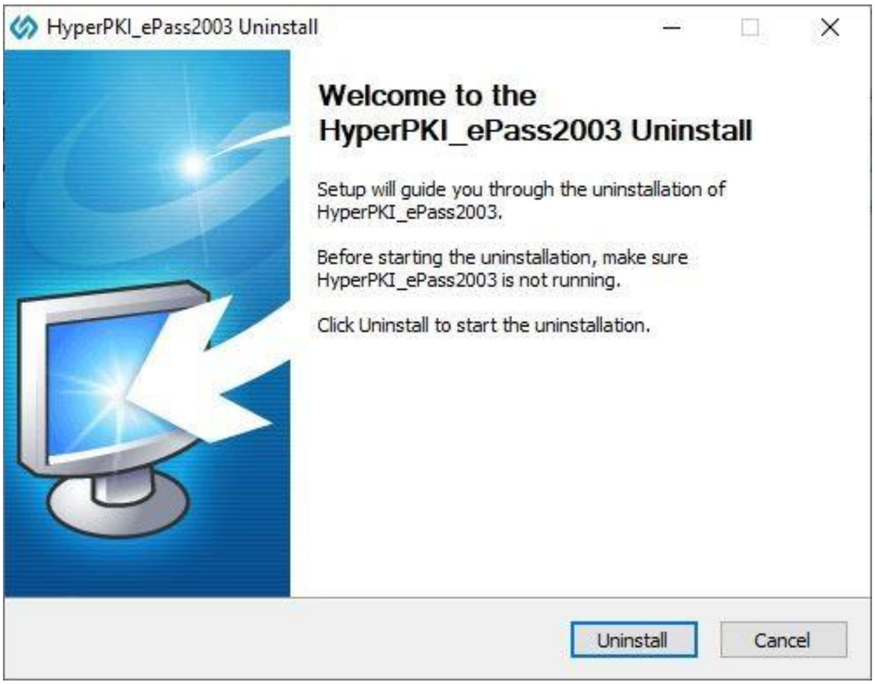
- Use “Add or Remove Programs” to uninstall

  Open “start” menu →select “Control Panel”, double click “Add or Remove Programs”, choose “HYP2003 (Remove only)” in the “Currently installed programs” list, then click “Change/Remove”.

- Uninstall it from start menu

  Open “start” menu → “All Programs” → “Hypersecu” → “HYP2003” → “Uninstall HYP2003”.

1. Both of above two methods can launch the Uninstall Wizard of HYP2003, see following interface:



HyperPKI_ePass2003 Uninstall

Welcome to the HyperPKI_ePass2003 Uninstall

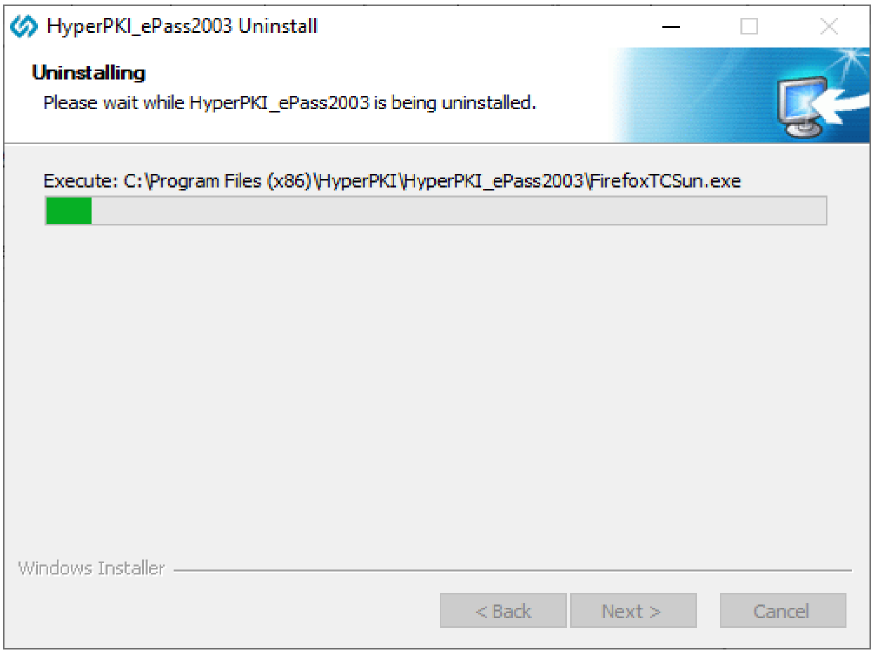
Setup will guide you through the uninstallation of HyperPKI_ePass2003.

Before starting the uninstallation, make sure HyperPKI_ePass2003 is not running.

Click Uninstall to start the uninstallation.

Figure 7 uninstall wizard interface

2. Click “Uninstall”, the following uninstall process interface appears:



HyperPKI_ePass2003 Uninstall

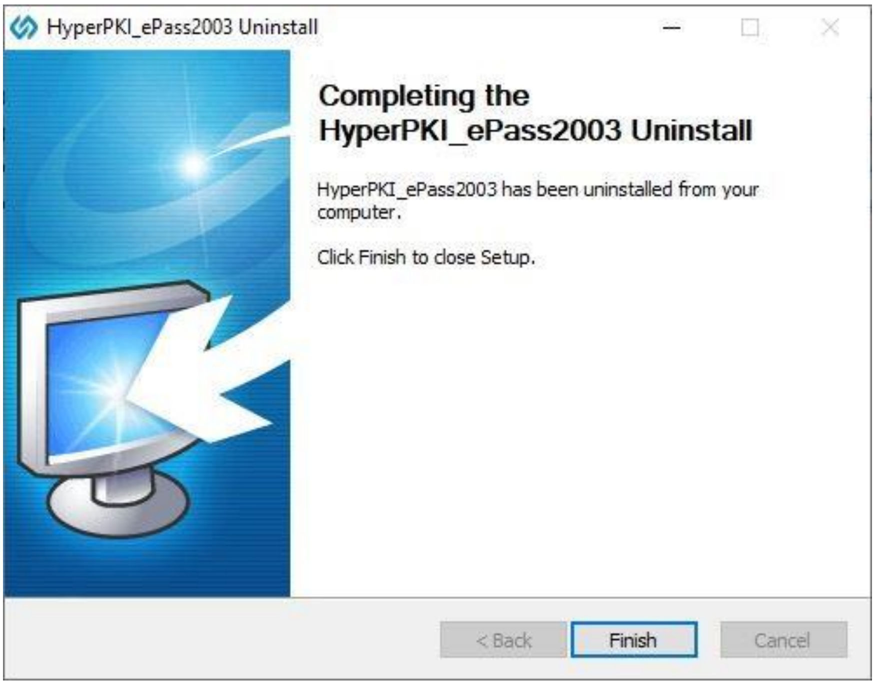
Uninstalling

Please wait while HyperPKI_ePass2003 is being uninstalled.

Execute: C:\Program Files (x86)\HyperPKI\HyperPKI_ePass2003\FirefoxTCSun.exe

Figure 8 uninstall process

3. After uninstall process finish, the following interface appears:



HyperPKI_ePass2003 Uninstall

Completing the HyperPKI_ePass2003 Uninstall

HyperPKI_ePass2003 has been uninstalled from your computer.

Click Finish to close Setup.

Figure 9 uninstall completed

4. Click “Finish” to close uninstall wizard, now HYP2003 has been already uninstalled from your computer.

Chapter 2 HYP2003 Token Manager

2.1 Prerequisite

Because the Manager is based on the middleware of HYP2003 and it needs to access the token, you must have installed HYP2003 product on your computer before using the Manager.

The token must be PKI initialized before use.

2.2 Overview

2.2.1 Interface without USB Key Insertion

You can find the shortcut for the Manager by clicking Start -> All Programs -> Hypersecu -> HYP2003. Click the shortcut to start the Manager. The following interface appears:

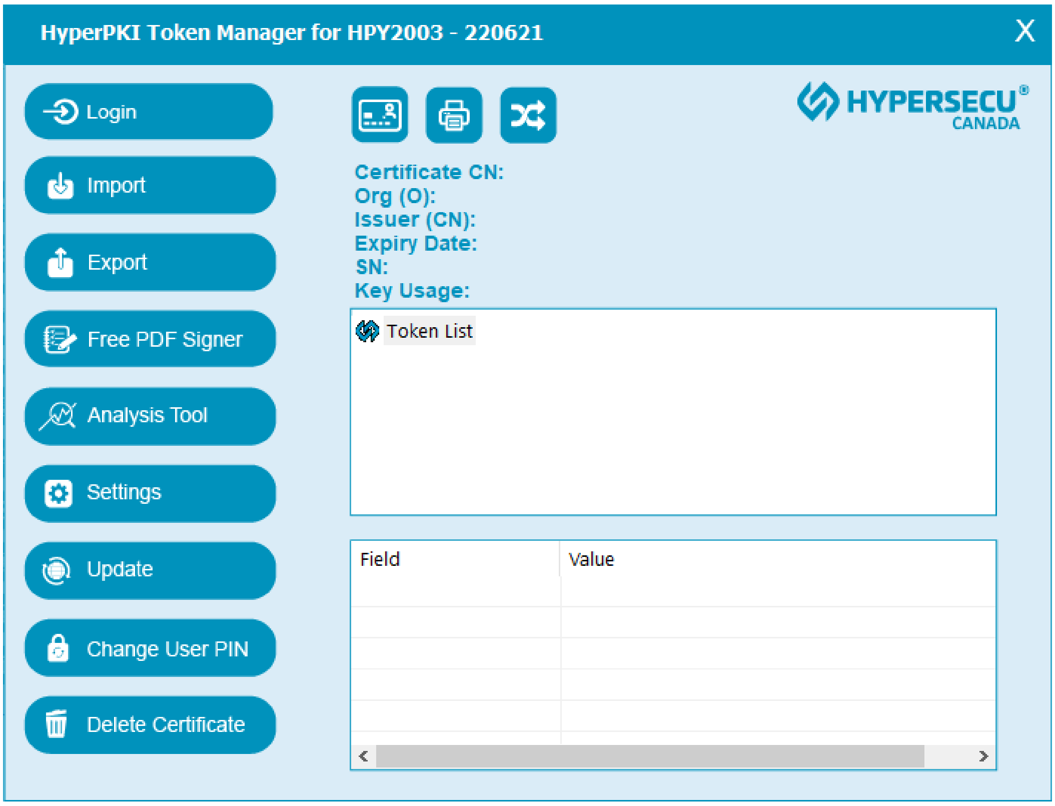
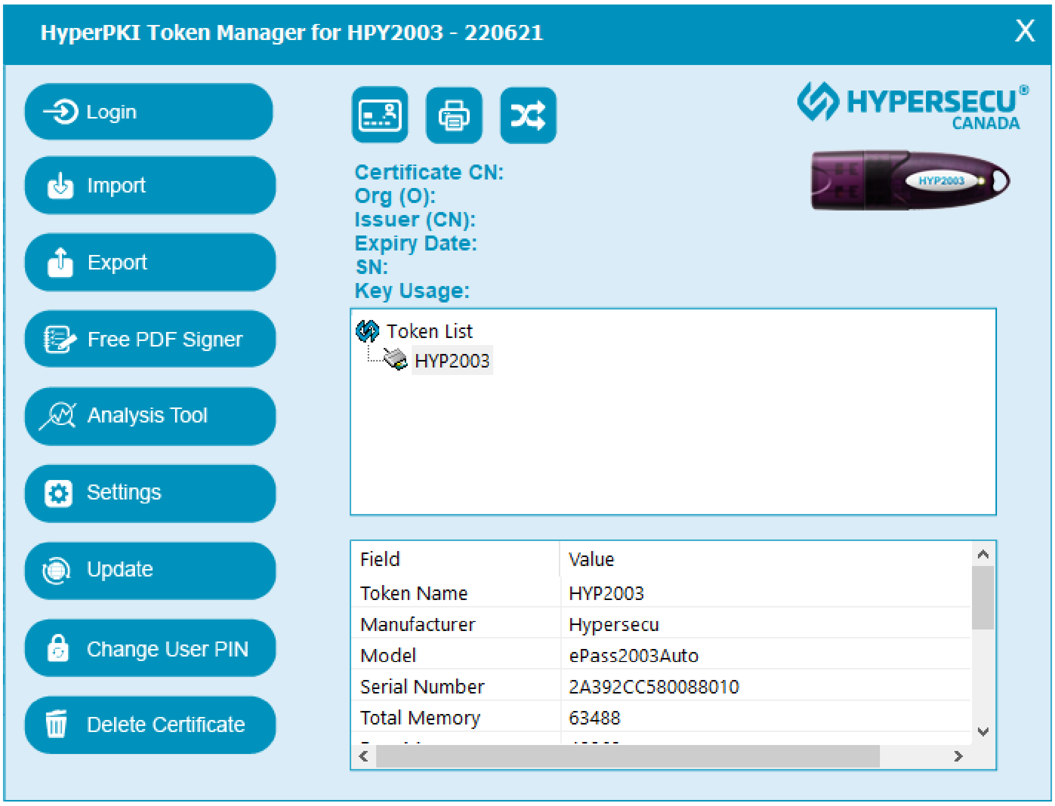


Figure 10 USB Key Not Inserted

2.2.2 Interface with USB Key Insertion

Connect HYP2003 to a USB port on your computer. The Manager will recognize it immediately as follows:



Certificate CN:
Org (O):
Issuer (CN):
Expiry Date:
SN:
Key Usage:

Field	Value
Token Name	HYP2003
Manufacturer	Hypersecu
Model	ePass2003Auto
Serial Number	2A392CC580088010
Total Memory	63488

Figure 11 USB Key Inserted

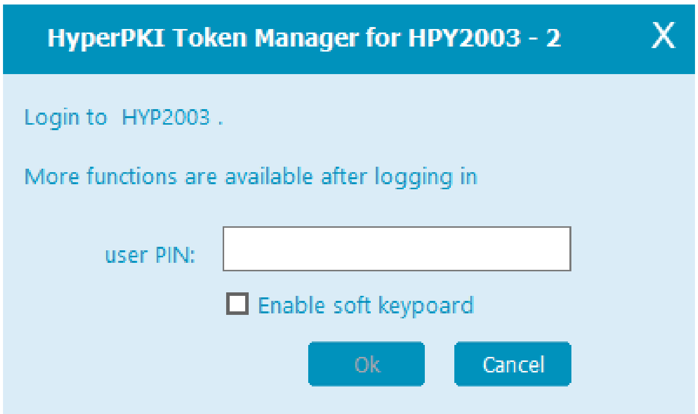
Note: The total private memory space and the free private memory space refer to the PIN protected spaces. Since the private key is extremely sensitive and it is managed by the COS, it doesn't show the total private memory space and the free private memory space.

2.2.3 Interface Buttons

The buttons on the interface are: Login, Import, Export, Delete, Change User PIN, Change USB Key Name, View Certificate Information, Update, Analysis Tool and Setting.

2.3 Login

Select a USB key from the list on the right to which you want to log in and click Login. The following interface appears:



HyperPKI Token Manager for HPY2003 - 2

Login to HYP2003 .

More functions are available after logging in

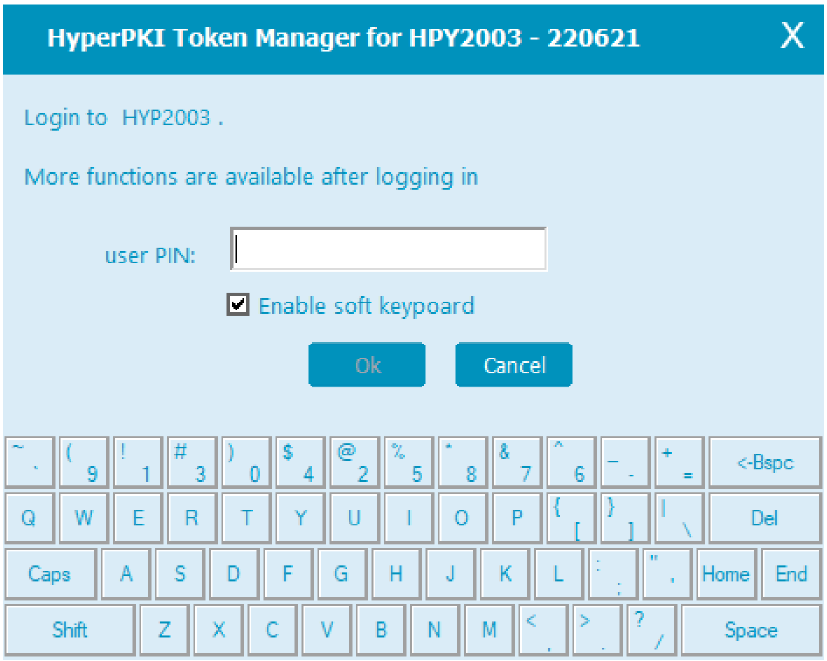
user PIN:

☐ Enable soft keypoard

Figure 12 Login dialog box

Note: When the PIN input dialog is displayed, the Manager will start the safe desktop. In this status, only the box is highlighted. Except input in the box, most of other operations are disabled. Default password is 12345678.

Optionally, you can use a soft keyboard by checking Soft keyboard option here to avoid monitoring of a potential Trojan program.



HyperPKI Token Manager for HPY2003 - 220621

Login to HYP2003 .

More functions are available after logging in

user PIN:

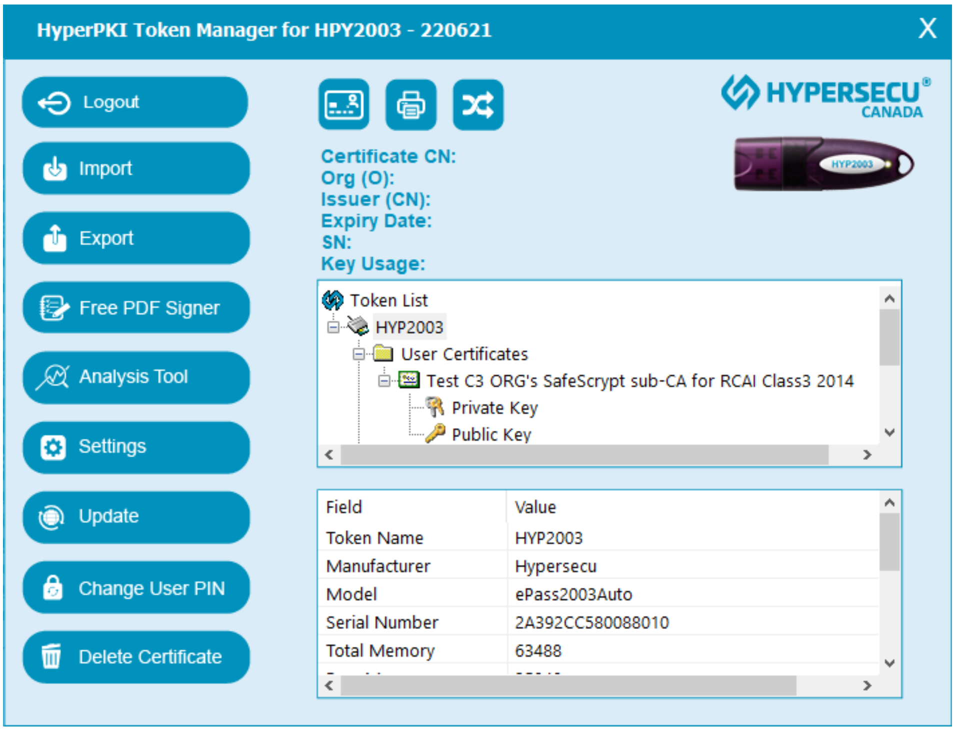
☑ Enable soft keypoard

X
Ok
Cancel
~ ` (9 ! 1 # 3) 0 $ 4 @ 2 % 5 * 8 & 7 ^ 6 _ - + = <-Bspc
Q W E R T Y U I O P { [}] | \ Del
Caps A S D F G H J K L : ; " , Home End
Shift Z X C V B N M < , > . ? / Space

Figure 13 Soft Keyboard

Note: The physical keyboard is disabled when you are using the soft keyboard.

After you enter a proper PIN and click OK, the interface as shown in Figure 5 appears. A token list is displayed on the top. Below are the properties and their values. By clicking Hide Details or More Details button, you can hide the details or show them. After you have logged in, you can view not only the public data but the private data. In addition, the Login button changes to Log out button. To securely log out, click this button.



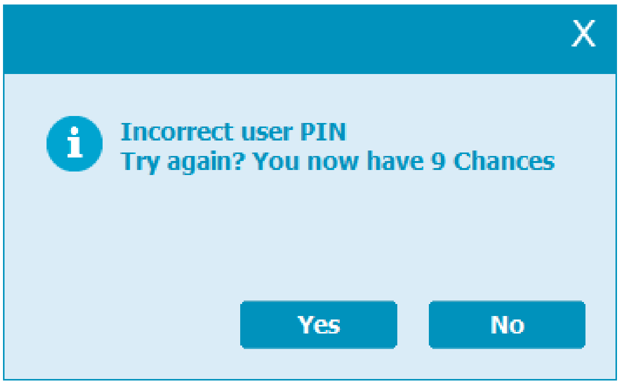
Certificate CN:
Org (O):
Issuer (CN):
Expiry Date:
SN:
Key Usage:

Token List
- HYP2003
  - User Certificates
    - Test C3 ORG's SafeScrypt sub-CA for RCAI Class3 2014
      - Private Key
      - Public Key

Field	Value
Token Name	HYP2003
Manufacturer	Hypersecu
Model	ePass2003Auto
Serial Number	2A392CC580088010
Total Memory	63488

Figure 14 Logged In

If you type an incorrect password in the PIN input box, the following interface appears:



Incorrect user PIN
Try again? You now have 9 Chances

Figure 15 Incorrect PIN Prompt

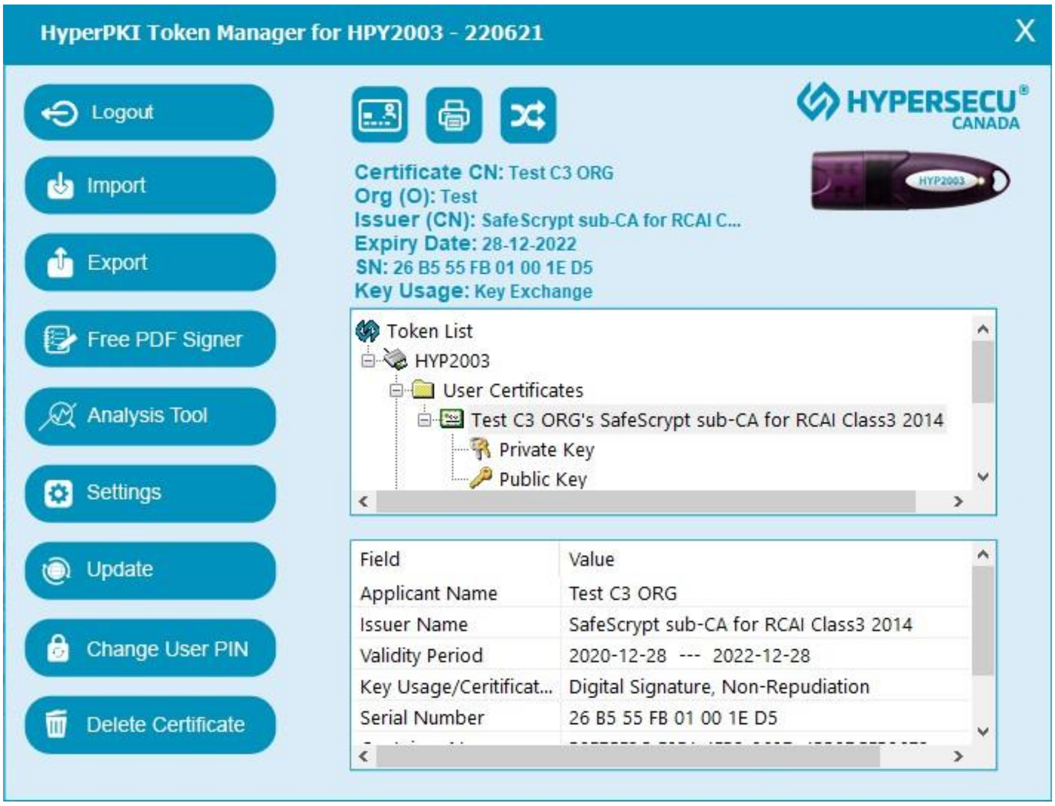
Note: There is a limit on the number of incorrect PIN inputs. If this number reaches 9, the token will be locked. You cannot perform any operations with it in this case.

2.4 Certificate Management

After you have logged into the Manager, you can view certificate information, import a certificate, delete a certificate etc.

2.4.1 Viewing Certificate Information

1. Click the “+” on the left side of a container (folder icon) in the token list or double-click the icon to display its content. Click the “+” on the left side of a certificate icon to display the key-pair. When a certificate is selected, the Certificate View button is enabled.



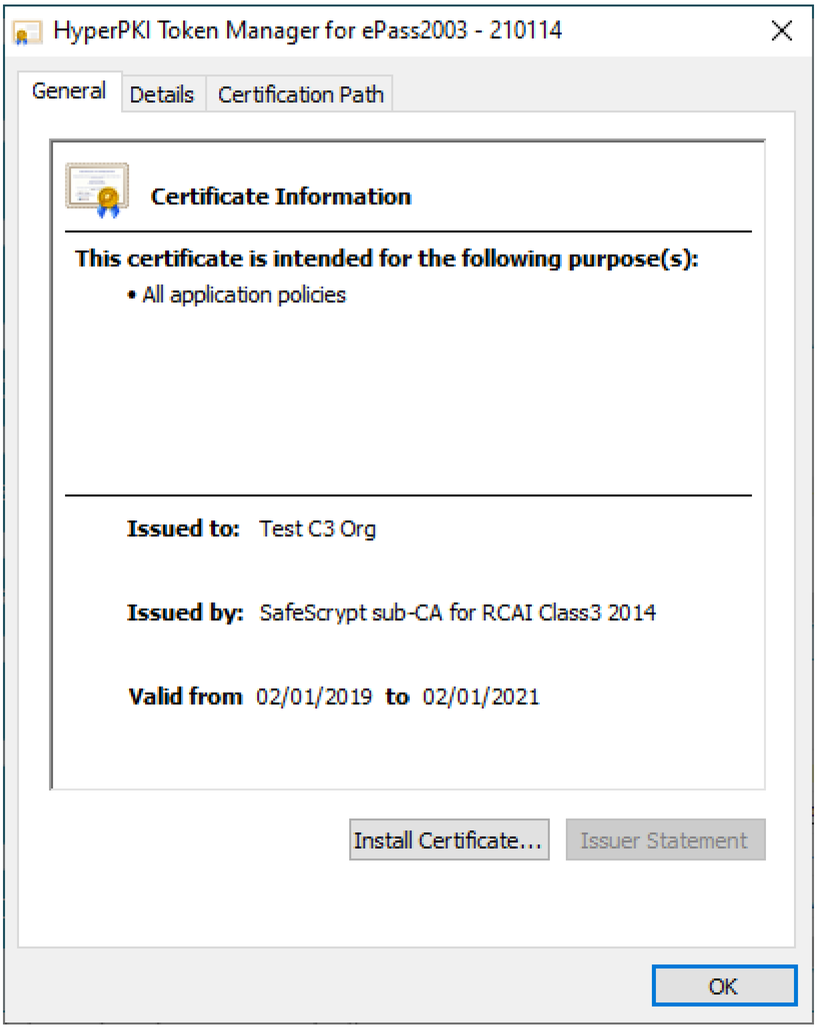
Certificate CN: Test C3 ORG
Org (O): Test
Issuer (CN): SafeScrypt sub-CA for RCAI C...
Expiry Date: 28-12-2022
SN: 26 B5 55 FB 01 00 1E D5
Key Usage: Key Exchange

- Token List
  - HYP2003
    - User Certificates
      - Test C3 ORG's SafeScrypt sub-CA for RCAI Class3 2014
        - Private Key
        - Public Key

Field	Value
Applicant Name	Test C3 ORG
Issuer Name	SafeScrypt sub-CA for RCAI Class3 2014
Validity Period	2020-12-28 --- 2022-12-28
Key Usage/Ceritificat...	Digital Signature, Non-Repudiation
Serial Number	26 B5 55 FB 01 00 1E D5

Figure 16 Viewing Certificate Information

2. By clicking Certificate View button or double-clicking a certificate icon, the following dialog box appears:



This certificate is intended for the following purpose(s):

- All application policies

Issued to: Test C3 Org

Issued by: SafeScrypt sub-CA for RCAI Class3 2014

Valid from 02/01/2019 to 02/01/2021

Figure 17 Certificate Information

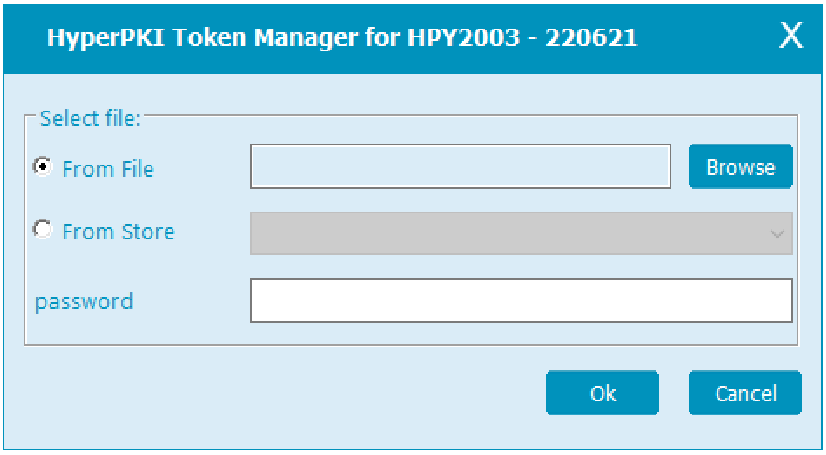
You can view the information of your interest.

2.4.2 Importing

Currently, HYP2003 supports to import the certificate from file or from Certificate Store. The following certificate types: P12, PFX and CER. The P12 and PFX types contain a key-pair (a public key and a private key), while the CER type does not. The PFX and CER types are used as examples below.

2.4.2.1 Importing the certificate from file

Click Import button in the main interface of the Manager. The following interface appears. Click Browse button to choose a certificate file to be imported. If necessary, enter a password below. Click OK.


HyperPKI Token Manager for HPY2003 - 220621

Select file:

● From File

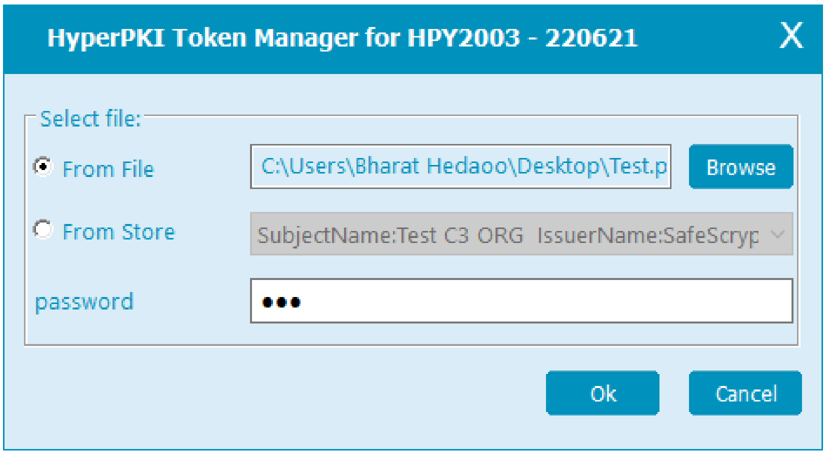
○ From Store

password

Figure 18 Certificate Import

2.4.2.2 Importing the certificate from Certificate Store

Click Import button in the main interface of the Manager. The following interface appears. Click "From Store" option to import a certificate from Certificate Store. It will list the certificates, and then you could choose one to import the certificate to the HYP2003 token. Click OK.


HyperPKI Token Manager for HPY2003 - 220621

Select file:

● From File: C:\Users\Bharat Hedaoo\Desktop\Test.p

○ From Store: SubjectName:Test C3 ORG IssuerName:SafeScryp

password: •••

Figure 19 Certificate Import

2.4.3 Exporting

You can export a certificate from HYP2003 token to a file.

From the tree view in the main interface of the Manager, choose the certificate to be exported and click Export button. A dialog box appears. Specify a path to the certificate file and its name.

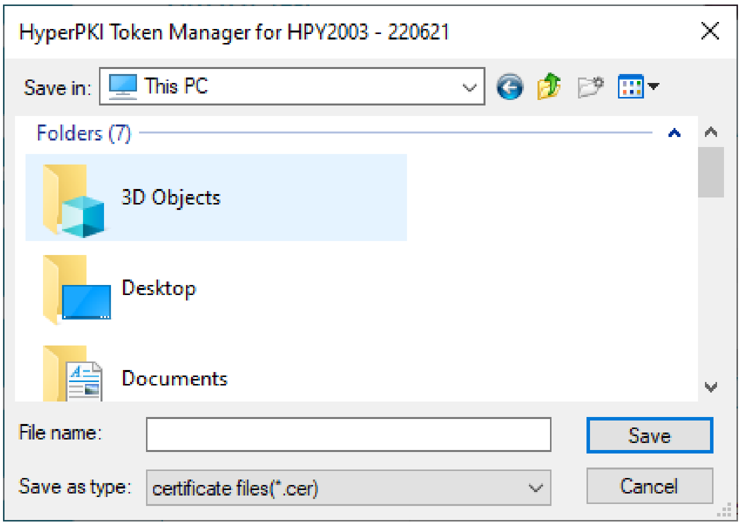
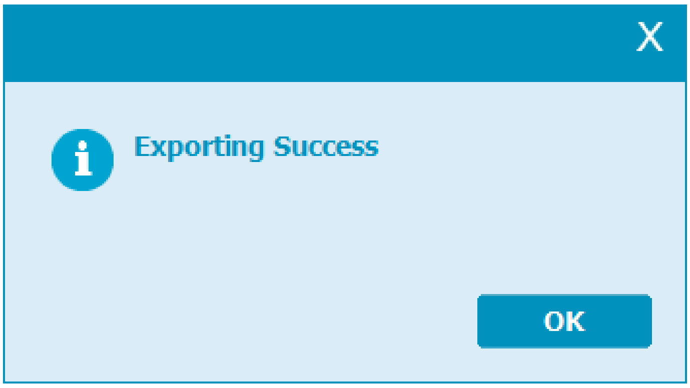


Figure 20 Certificate Export Path

Click Save. If the operation has succeeded, the following message will appear:



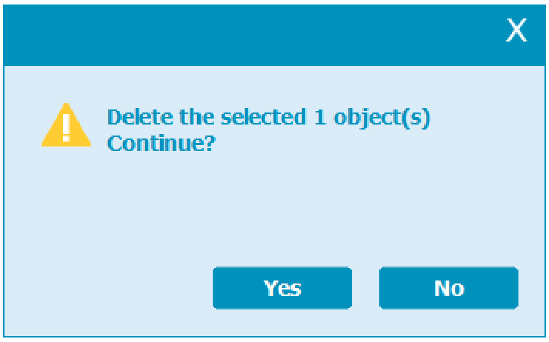
Exporting Success

Figure 21 Successful Export

Note: The private/public key-pair cannot be exported.

2.4.4 Deletion

From the tree view of the main interface of the Manager, choose the certificate you want to delete and click Delete. The following interface appears:



Delete the selected 1 object(s)
Continue?

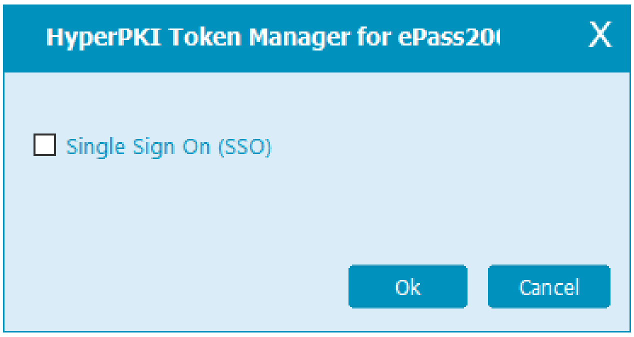
Figure 22 Deleting Certificate

Click Yes to delete the selected certificate if you do want.

2.4.5 Single Sign On (SSO):

HYP2003 has introduced a new feature Single Sign On (SSO).

Click Setting button Settings in the main interface of the Manager. The following interface appears:



HyperPKI Token Manager for ePass20(

X

□ Single Sign On (SSO)

Figure 23 Enabling SSO

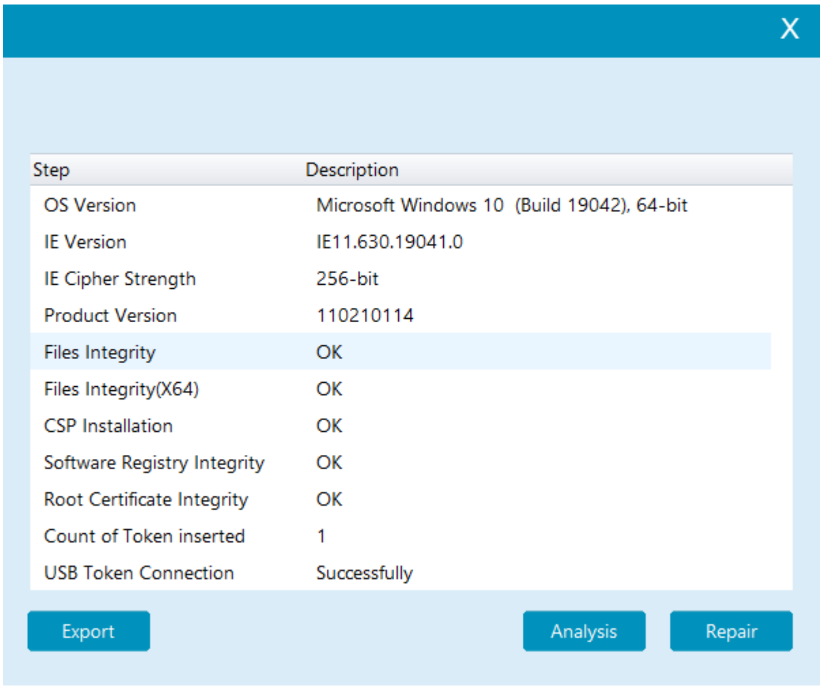
Click Ok to enable this feature.

2.4.6 Analysis Tool:

New Enhancements & Features added to Analysis Tool:

1. Check and Repair ActiveX setting in Windows System.
2. Check Java Version Installed and if there is no Java installed on current system, open link to install the Java.
3. Check and Repair Java Plug-in setting in Windows System.
4. Check and Install necessary DLL Files for using Digital Certificate in Windows System.

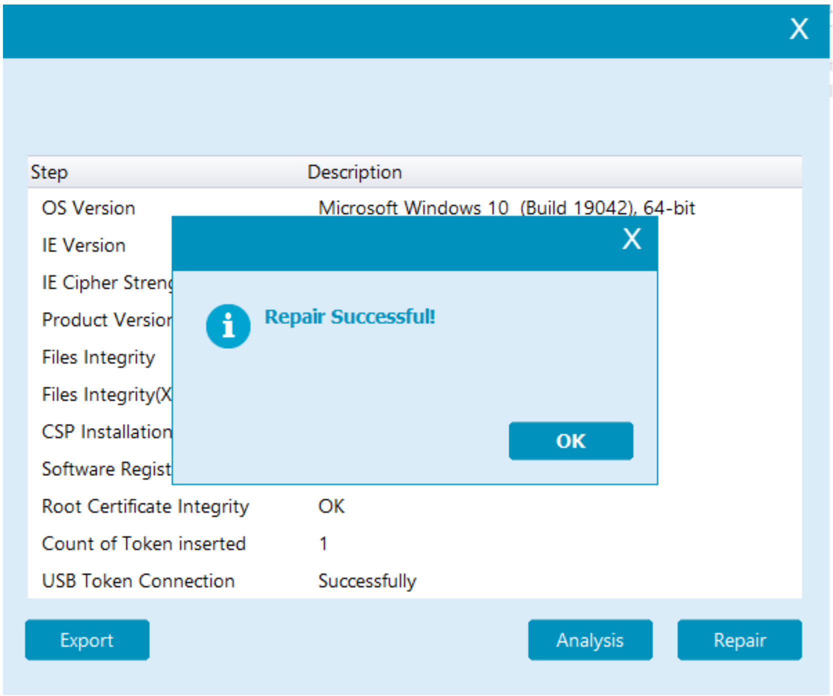
To run Analysis Tool, click on Analysis Tool button in Analysis Tool the main interface of the Token Manager and then click on Analysis. The following interface appears:



Step	Description
OS Version	Microsoft Windows 10 (Build 19042), 64-bit
IE Version	IE11.630.19041.0
IE Cipher Strength	256-bit
Product Version	110210114
Files Integrity	OK
Files Integrity(X64)	OK
CSP Installation	OK
Software Registry Integrity	OK
Root Certificate Integrity	OK
Count of Token inserted	1
USB Token Connection	Successfully

Figure 24 Running Analysis Tool

After Clicking on Repair button, following Interface appears:



Step	Description
OS Version	Microsoft Windows 10 (Build 19042), 64-bit
IE Version	
IE Cipher Streng	
Product Versior	
Files Integrity	
Files Integrity(X	
CSP Installation	
Software Regist	
Root Certificate Integrity	OK
Count of Token inserted	1
USB Token Connection	Successfully

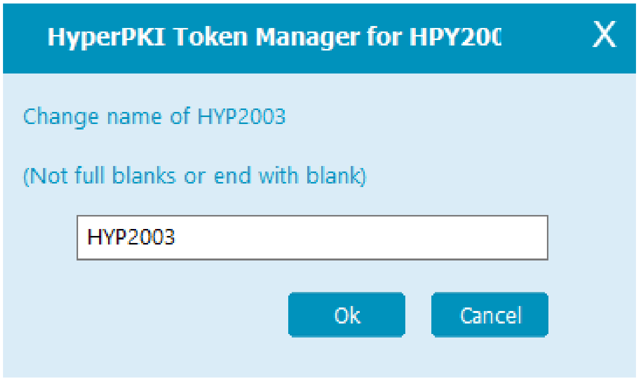
Repair Successful!

Figure 25 Running Repair Tool

2.5 Changing Token Name

Generally, the token is distinguished by serial number. For intuitive purpose, the token can be given a common name.

1. Click Change Token Name button. The following interface appears:
2.



HyperPKI Token Manager for HPY20(

Change name of HYP2003

(Not full blanks or end with blank)

HYP2003

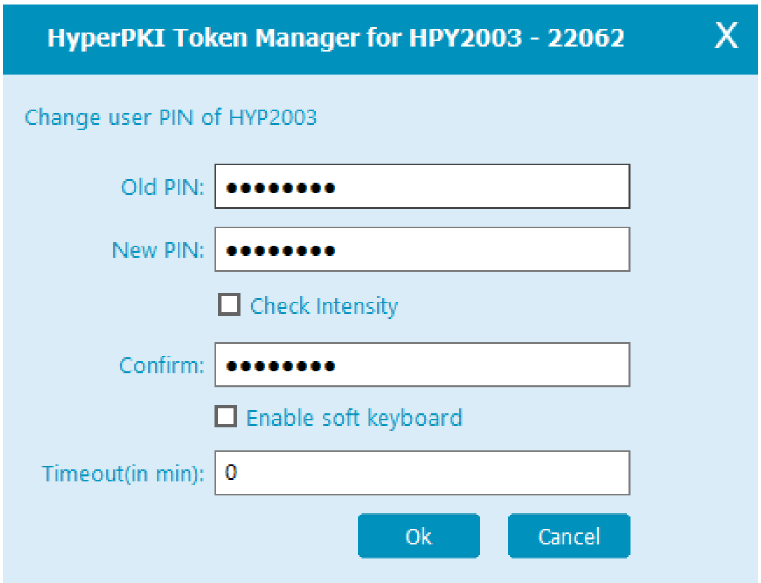
Figure 26 Changing Token Name

3. Enter a name for the token and click OK.

Note: At most a 32-character name can be provided.

2.6 Changing User PIN

You can change the PIN of your token. In the main interface of the Manager, click Change User PIN button. The following interface appears. Enter the old and new PINs and confirm the new PIN. Click OK.



HyperPKI Token Manager for HPY2003 - 22062

Change user PIN of HYP2003

Old PIN: ●●●●●●●●

New PIN: ●●●●●●●●

□ Check Intensity

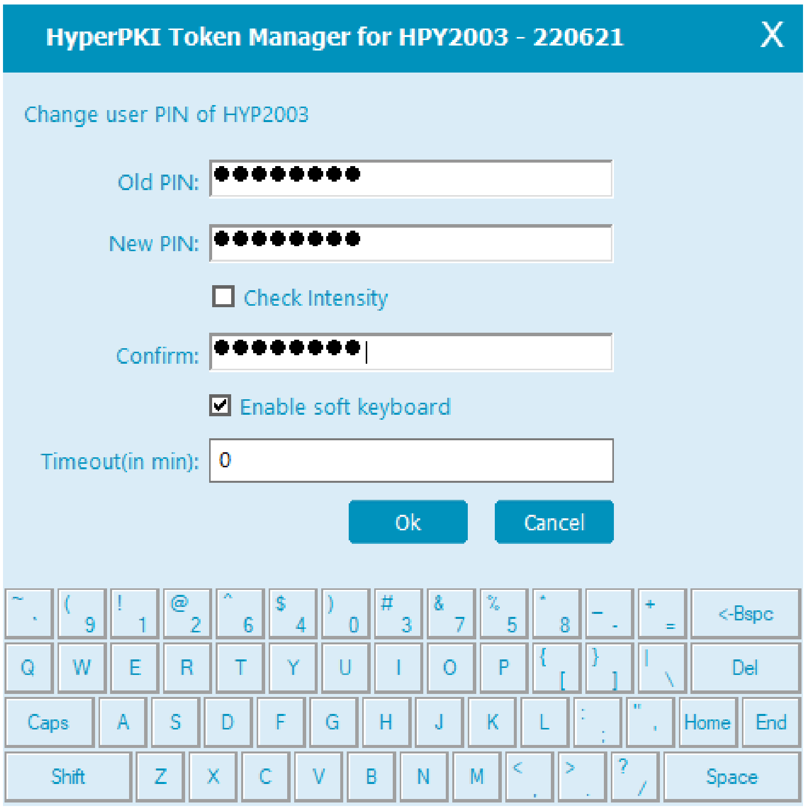
Confirm: ●●●●●●●●

□ Enable soft keyboard

Timeout(in min): 0

Figure 27 Changing User PIN

You can also enter the PINs by a soft keyboard. To do so, check Soft keyboard.



HyperPKI Token Manager for HPY2003 - 220621

Change user PIN of HYP2003

Old PIN: ●●●●●●●●●

New PIN: ●●●●●●●●●

□ Check Intensity

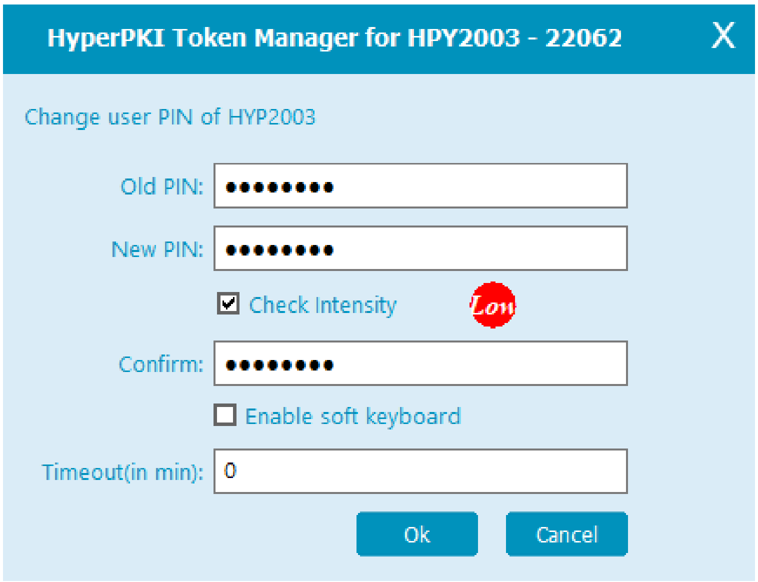
Confirm: ●●●●●●●●●

☑ Enable soft keyboard

Timeout(in min): 0

Figure 28 Soft Keyboard Input

You can check intensity option to get aware of the security strength of the PIN you have set. "L" surrounded by red means "Low".



HyperPKI Token Manager for HPY2003 - 22062

Change user PIN of HYP2003

Old PIN: ●●●●●●●●

New PIN: ●●●●●●●●

☑ Check Intensity Low

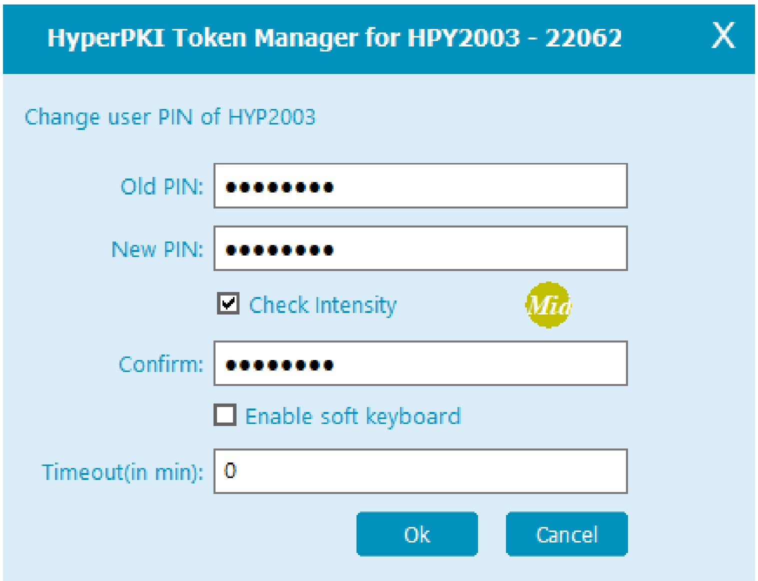
Confirm: ●●●●●●●●

□ Enable soft keyboard

Timeout(in min): 0

Figure 29 Low Strength

If the strength is higher, the following interface appears:



HyperPKI Token Manager for HPY2003 - 22062

Change user PIN of HYP2003

Old PIN: ●●●●●●●●

New PIN: ●●●●●●●●

☑ Check Intensity Mid

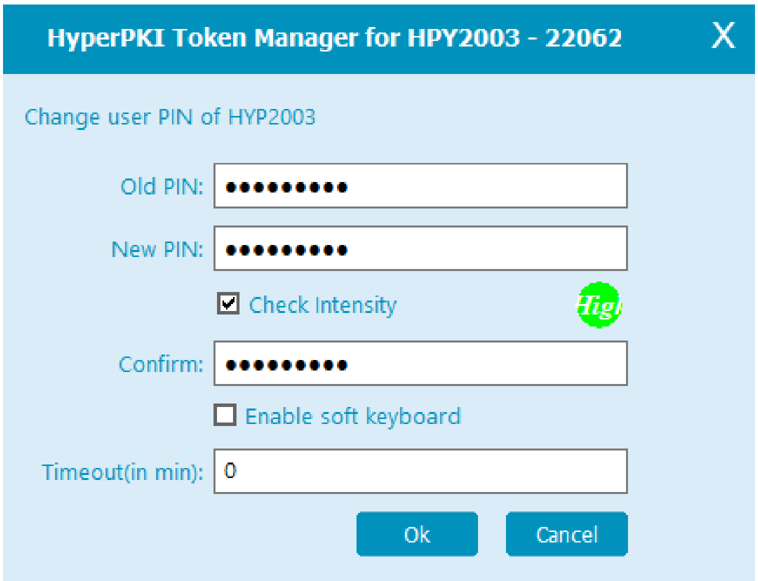
Confirm: ●●●●●●●●

□ Enable soft keyboard

Timeout(in min): 0

Figure 30 Medium Strength

We recommend long PINs made up of lower and upper-case letters, numbers and special characters.



HyperPKI Token Manager for HPY2003 - 22062

Change user PIN of HYP2003

Old PIN: ●●●●●●●●●

New PIN: ●●●●●●●●●

☑ Check Intensity High

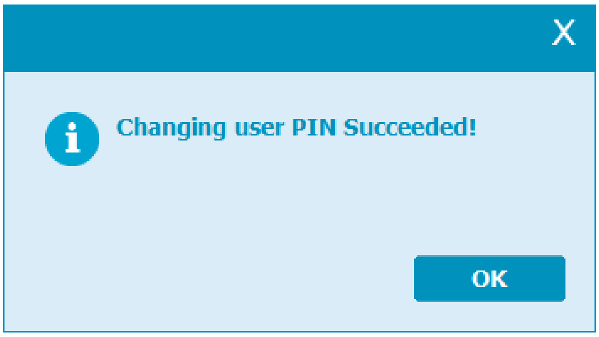
Confirm: ●●●●●●●●●

□ Enable soft keyboard

Timeout(in min): 0

Figure 31 High Strength

By clicking OK, the following interface may appear:

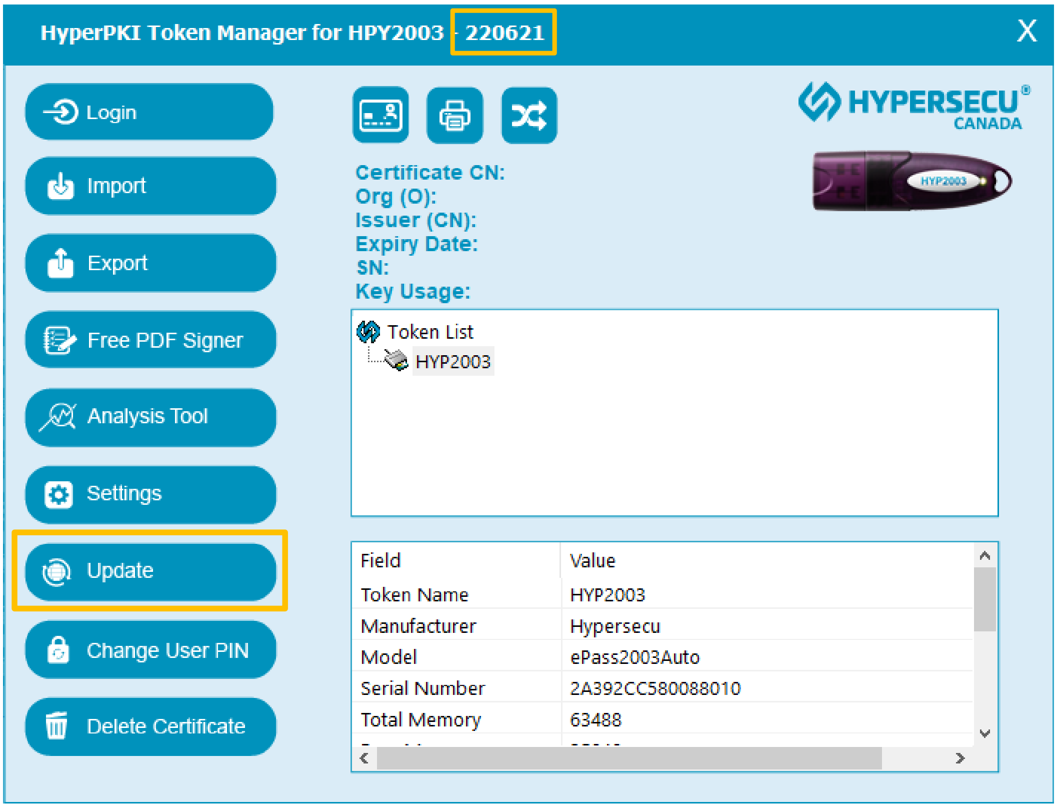


Changing user PIN Succeeded!

Figure 32 PIN Changed

Chapter 3 Unlock/Rest User Pin

Please download the Remote Unblock Client from below: https://taxpro.co.in/DSC/TokenDrivers/RemoteUnlockClient.zip Make sure latest HYP2003 Drivers are installed in your system. Remote Unblock Client works only on 180929 and above driver version. If your system is having earlier driver version installed, then first update it by clicking on Update button as shown in image below.



HyperPKI Token Manager for HPY2003 - 220621

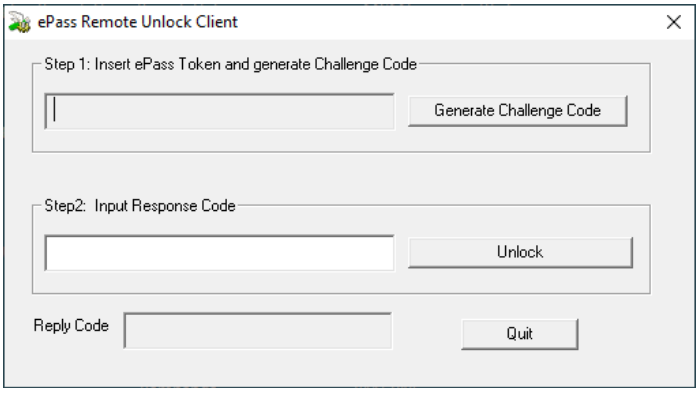
Certificate CN:
Org (O):
Issuer (CN):
Expiry Date:
SN:
Key Usage:

Token List
HYP2003

Field	Value
Token Name	HYP2003
Manufacturer	Hypersecu
Model	ePass2003Auto
Serial Number	2A392CC580088010
Total Memory	63488

Extract the downloaded Remote Unblock Client.

Now, open the RemoteUnlockClient.exe dialog Box showing as below.



ePass Remote Unlock Client

Step 1: Insert ePass Token and generate Challenge Code

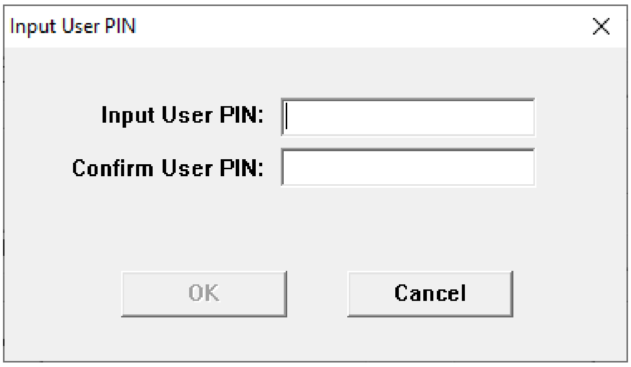
Step2: Input Response Code

Reply Code

Connect the Token which you want to unblock and Click on Generate Challenge Code button.

If you get Reply Code SN¡¢Cert Transmit Success, please check the eMail ID which is given in the DSC present in the token for Activation/Response Code. (Please refer last page of this document to know how to get/see eMail ID of DSC from blocked token.) Activation/Response code is sent from email ID tokenunblock@charteredinfo.com to registered email ID present into digital certificate which is available into the token.

Enter the Received Activation code in text box present in Input Response Code and Click on Unlock Button.



Enter the new Password which you Required and Confirm it. Password should be 8-digit alphanumeric character. After successful unblock you will get the message Unlock success!

Process of identify registered email ID into the Certificate:

- Plug-in token to USB Port. Open the Internet Explorer and Open Tool Menu Select Internet Option
- Select Content Tab
- Click on Certificate Button
- Find out present certificate into the token and Select it. Click on View Button
- Certificate Dialog Box is Opened.
- Click on Details Tab and find the field Subject Alternative Name
- On click on that field you will find the registered email id into the Digital Signature Certificate.

Chapter 4 Free PDF Sign

On successful installation of HyperPKI_HYP2003 driver, Signer.Digital Extension is added in your system chrome browser. On start or reopen Chrome its Prompted for enable.

For Firefox and New chromium-based Microsoft Edge browser need to add and enable extension manually.

Firefox - https://addons.mozilla.org/en-US/firefox/addon/signer-digital/

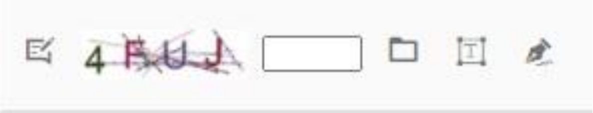
Microsoft Edge - https://chrome.google.com/webstore/detail/signerdigital/glghokcicpikglmflbbelbgeafpijkkf

Once enable the Signer.Digital extension on browser open the HyperPKI_HYP2003 Token Manager and click on Free PDF Signer button Free PDF Signer

On click on button URL: - https://web.signer.digital/InteractiveSigning is opened in default browser.

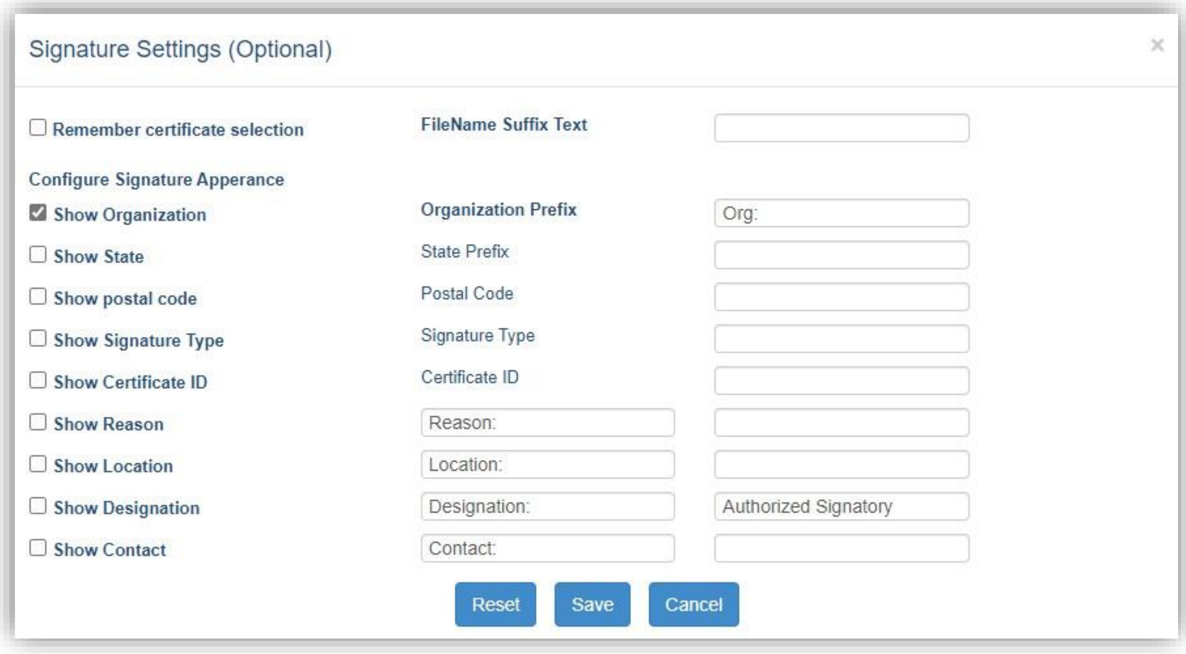
You will bookmark that URL in your browser and directly open it.

Once page is load you will see the below set of Icon in webpage.



First Icon from Left is Sign Setting (Optional). By click on it you will get the below dialog box.

Select the options by click on check box you need to show in singing appearance. Those settings are stored in your browser catch.



Signature Settings (Optional) ×

□ Remember certificate selection	FileName Suffix Text	
Configure Signature Apperance		
☑ Show Organization	Organization Prefix	Org:
□ Show State	State Prefix	
□ Show postal code	Postal Code	
□ Show Signature Type	Signature Type	
□ Show Certificate ID	Certificate ID	
□ Show Reason	Reason:	
□ Show Location	Location:	
□ Show Designation	Designation:	Authorized Signatory
□ Show Contact	Contact:	

Once Settings saved enter the showing captcha. You will refresh captcha by click on it.

Enter the captcha and click on browse button.

If need to Add text in open PDF document click on “Add Text Annotation” button and click on appropriate position where need to add, Its optional.

Once done its time to Sign PDF. Click on Sign PDF Icon draw the rectangle where you need to sign.

On release of mouse button after draw the rectangle you will get the certificate selection dialog box.

Select the certificate and enter the User PIN. On successfully sign PDF its prompt for saving.

All signing process perform in system memory catch and not shared over internet so that its secure.

Appendix: Terms and Abbreviations

Entry	Description
HYP2003	A smart card-based token with FIPS proved for PKI applications, introduced by Hypersecu Technologies. It is designed for PKI application
CryptoAPI Interface (CAPI)	An interface used for cryptography operations, provided by Microsoft. It provides cryptographic algorithm encapsulation of equipment irrelevant or implemented by software. With this interface, it is easy to develop PKI applications for data encryption/decryption, authentication and signature on Windows platforms.
Smart Card Minidriver Interface	An interface used for cryptography operations, provided by Microsoft. It provides cryptographic algorithm encapsulation of equipment irrelevant or implemented by software for Microsoft Base Smart Card Crypto Provider and Microsoft Smart Card Key Storage
PKCS#11 Interface	A programming interface introduced by RSA. It abstracts the cryptographic device into a universal logic view - Cryptographic Token, for use by upper-level applications, providing device independency and a manner of resource sharing.