

FEITIAN

ePass2003 User Guide



V2.0

Feitian Technologies Co., Ltd.

Website: www.FTsafes.com

Revision History:

Date	Revision	
June 2013	V1.0	Release of the first version
Oct 2019	V2.0	

Software Developer's Agreement

All Products of Feitian Technologies Co., Ltd. (Feitian) 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 Feitian provided enhancement or upgrade to the Product.
3. Warranty – Feitian 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, Feitian's sole obligation is to replace or repair, at the discretion of Feitian, any Product free of charge. Any replaced Product becomes the property of Feitian.

Warranty claims must be made in writing to Feitian 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 Feitian. Any Products that you return to Feitian, or a Feitian 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 Feitian's Liability – Feitian'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 Feitian 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 Feitian 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.....	3
1.1	Supported Platform.....	3
1.2	Preparing for Installing ePass2003	3
1.3	Installing ePass2003 Runtime	4
1.4	Uninstalling ePass2003 Runtime	7
Chapter 2	ePass2003 Token Manager	11
2.1	Prerequisite	11
2.2	Overview.....	11
2.2.1	Interface without USB Key Insertion	11
2.2.2	Interface with USB Key Insertion.....	12
2.2.3	Interface Buttons	12
2.3	Login.....	12
2.4	Certificate Management	14
2.4.1	Viewing Certificate Information.....	15
2.4.2	Importing.....	16
2.4.3	Exporting	17
2.4.4	Deletion	18
2.4.5	Single Sign On (SSO).....	19
2.4.6	Analysis Tool.....	19
2.5	Changing Token Name.....	21
2.6	Changing User PIN.....	21
Chapter	Unlock/Rest User Pin	24
Appendix:	Terms and Abbreviations	26

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 ePass2003

Before installing ePass2003 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)
- ePass2003 Token available

1.3 Installing ePass2003 Runtime

1. Before you can use the ePass2003, you must install the Runtime library. Execute ePass2003-Setup.exe. The following select language interface appears:

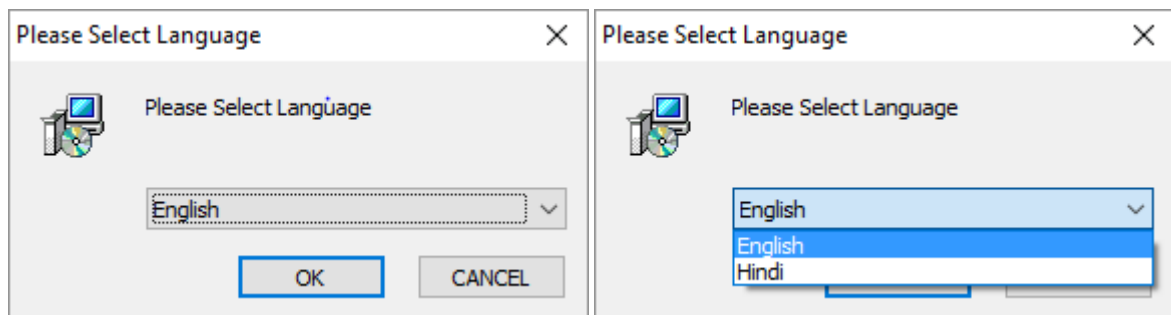


Figure 1 select language

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

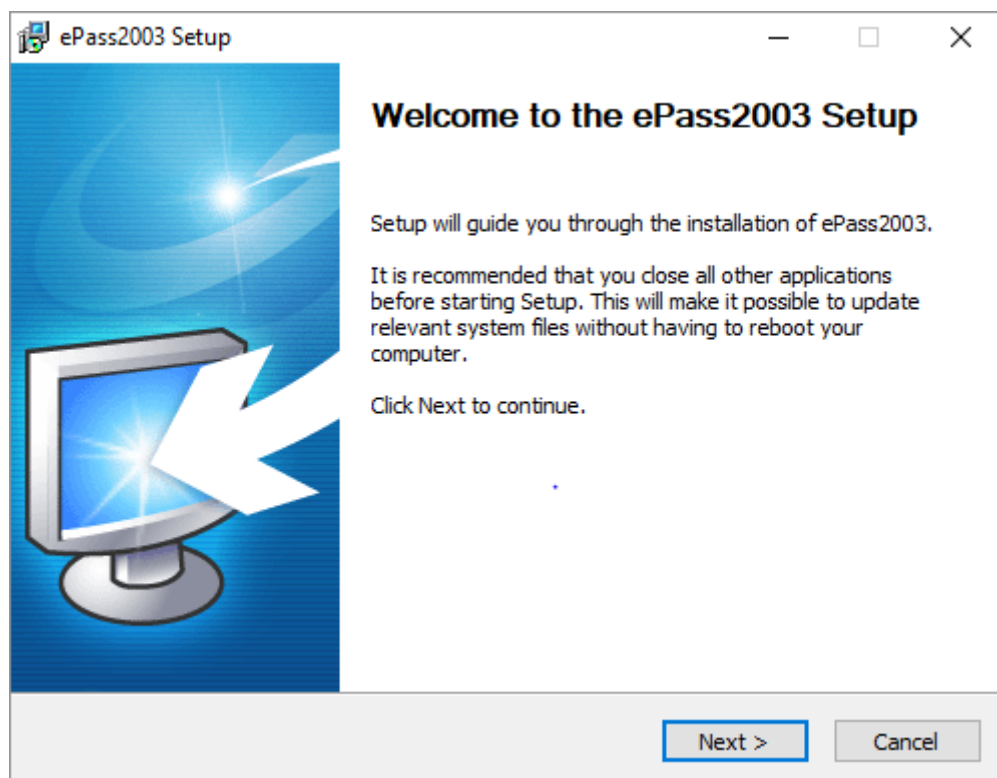


Figure 2 welcome interface

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

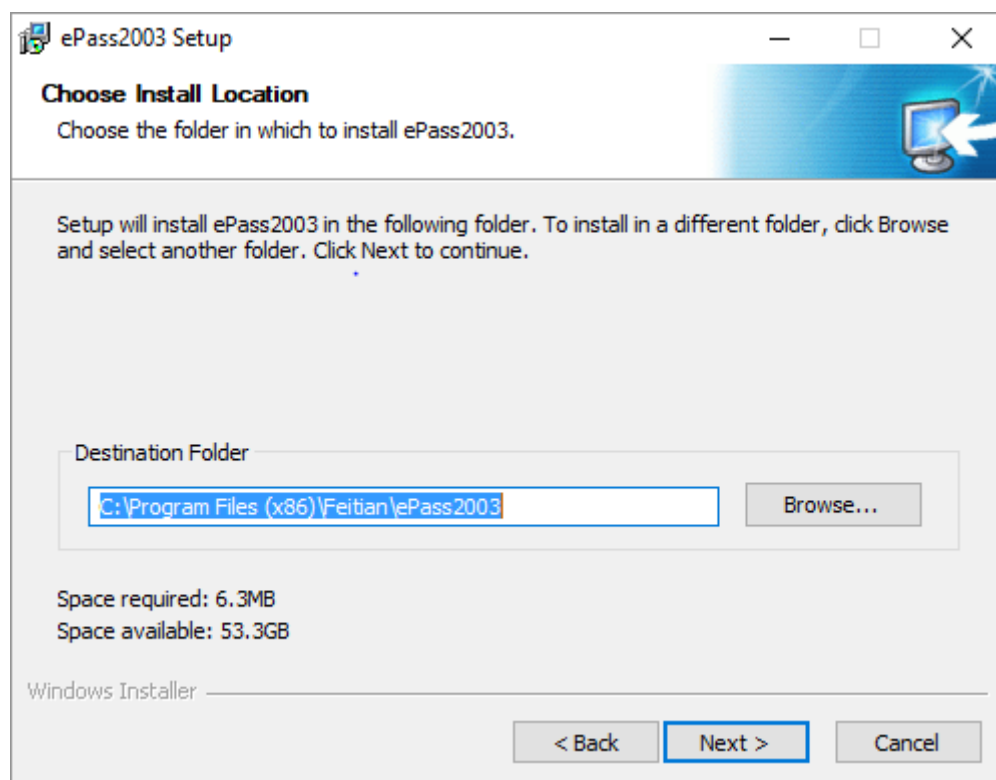


Figure 3 select install path

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

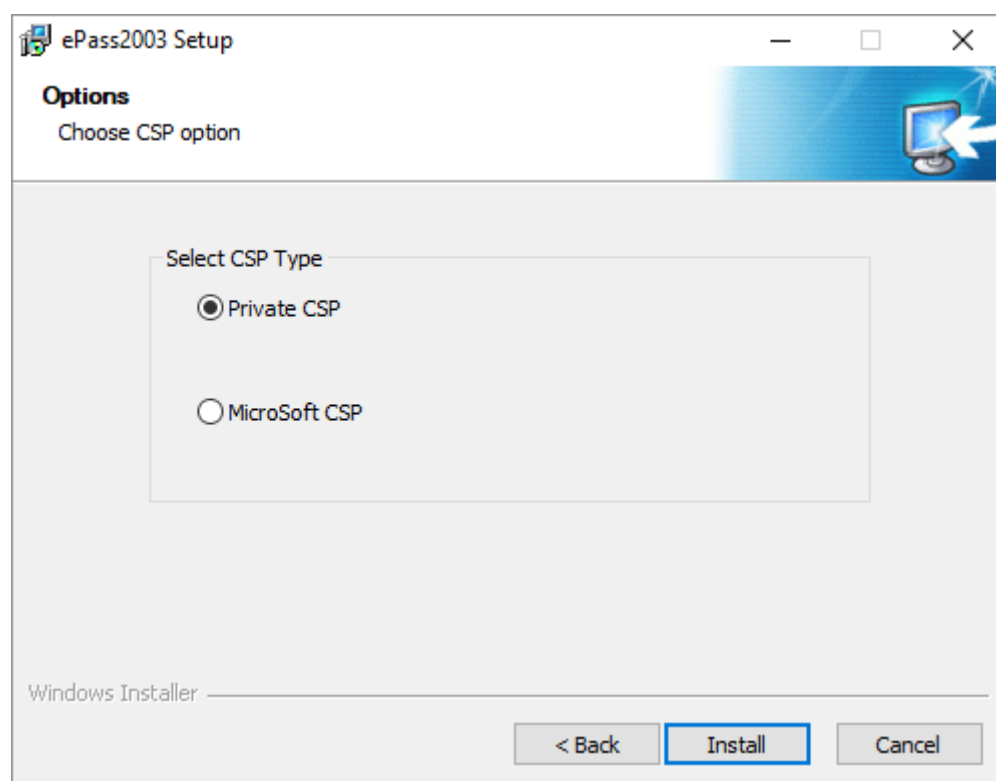


Figure 4 choose CSP

Note: ePass2003 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 FEITIAN, the CSP name is "EnterSafe ePass2003 CSP v1.0".
- 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:

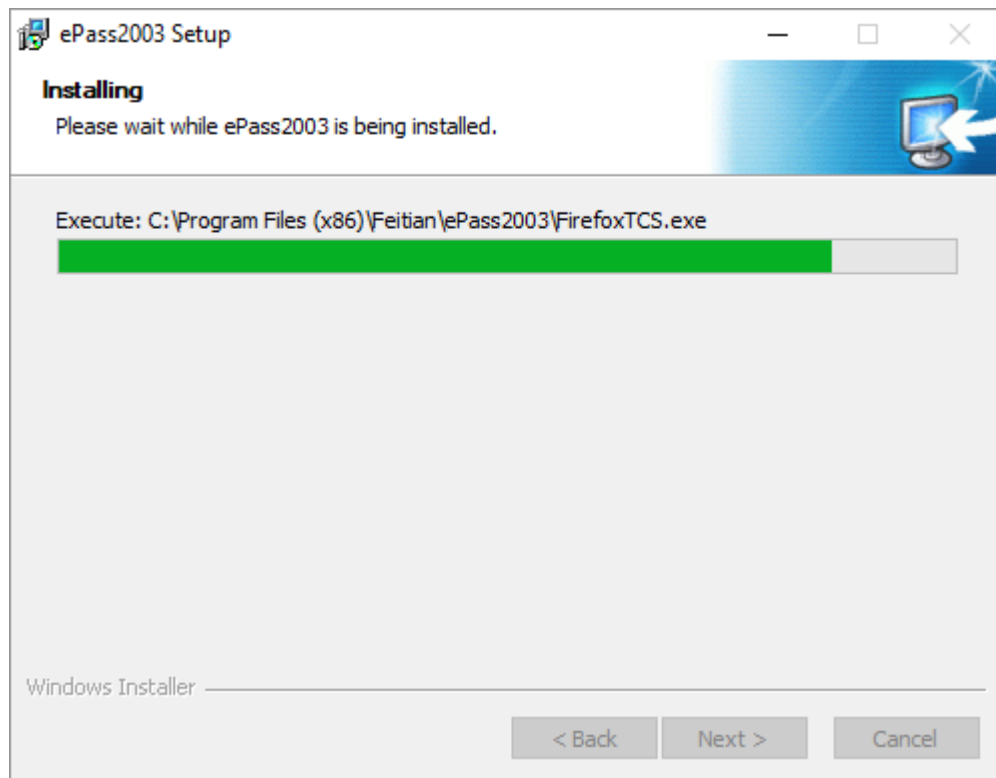


Figure 5 install process

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

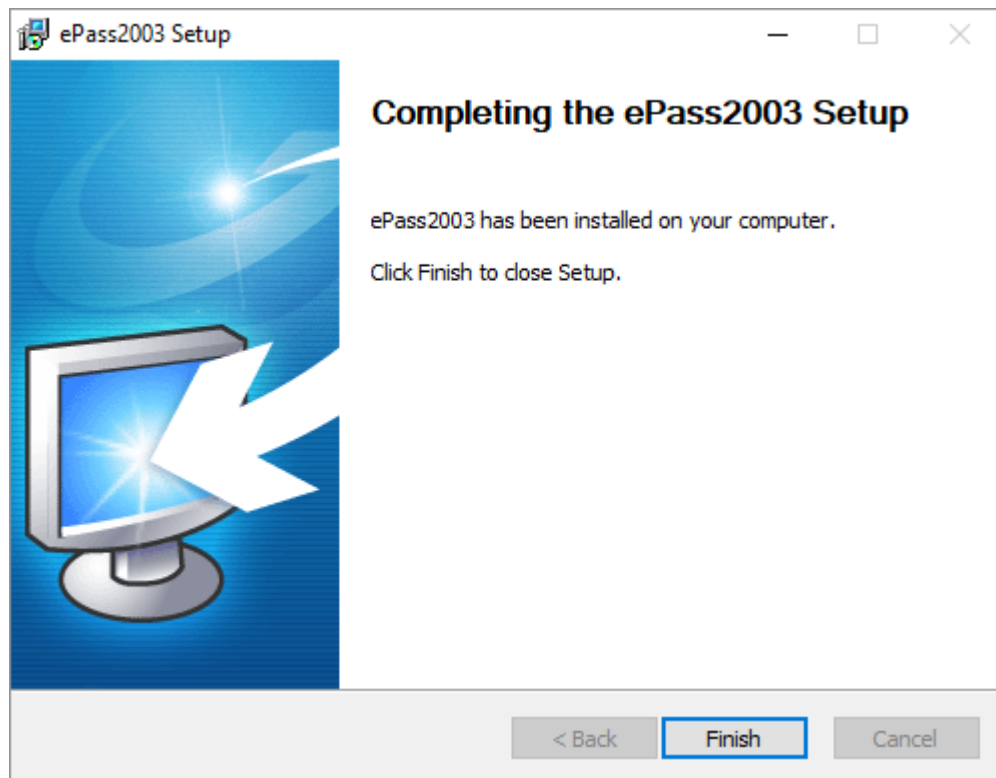


Figure 6 install completed

7. Click "Finish" to finish the installation.

1.4 Uninstalling ePass2003 Runtime

After install the ePass2003 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 "ePass2003 (Remove only)" in the "Currently installed programs" list, then click "Change/Remove".

- Uninstall it from start menu

Open "start" menu → "All Programs" → "Feitian" → "ePass2003" → "Uninstall ePass2003".

1. Both of above two methods can launch the Uninstall Wizard of ePass2003, see following interface:

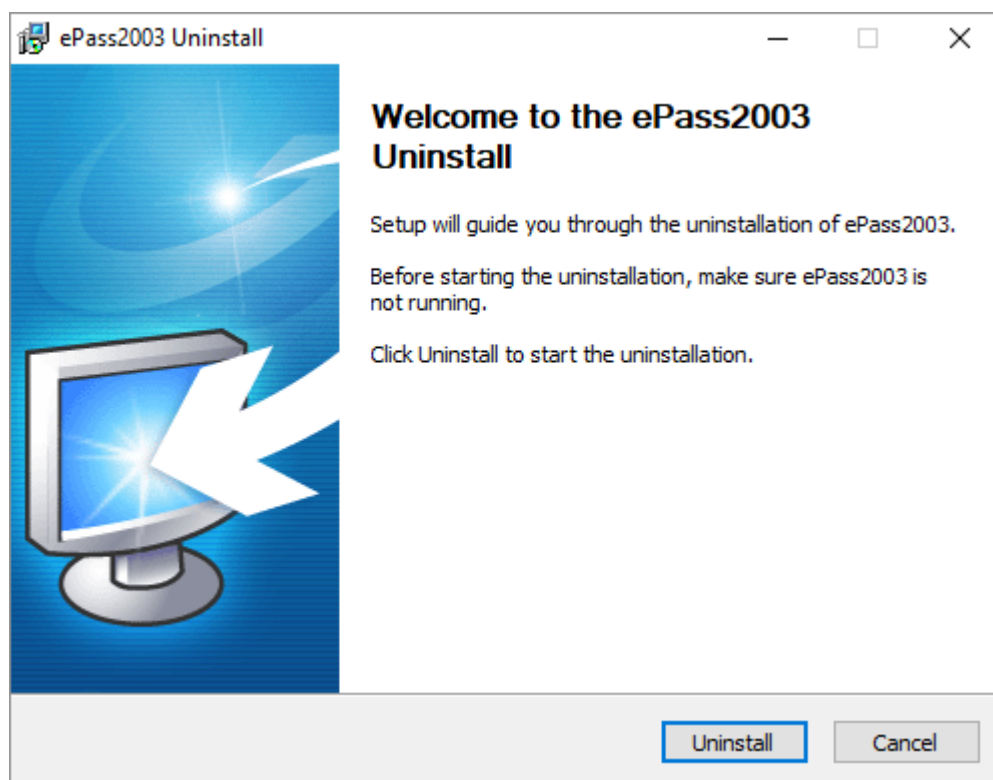


Figure 7 uninstall wizard interface

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

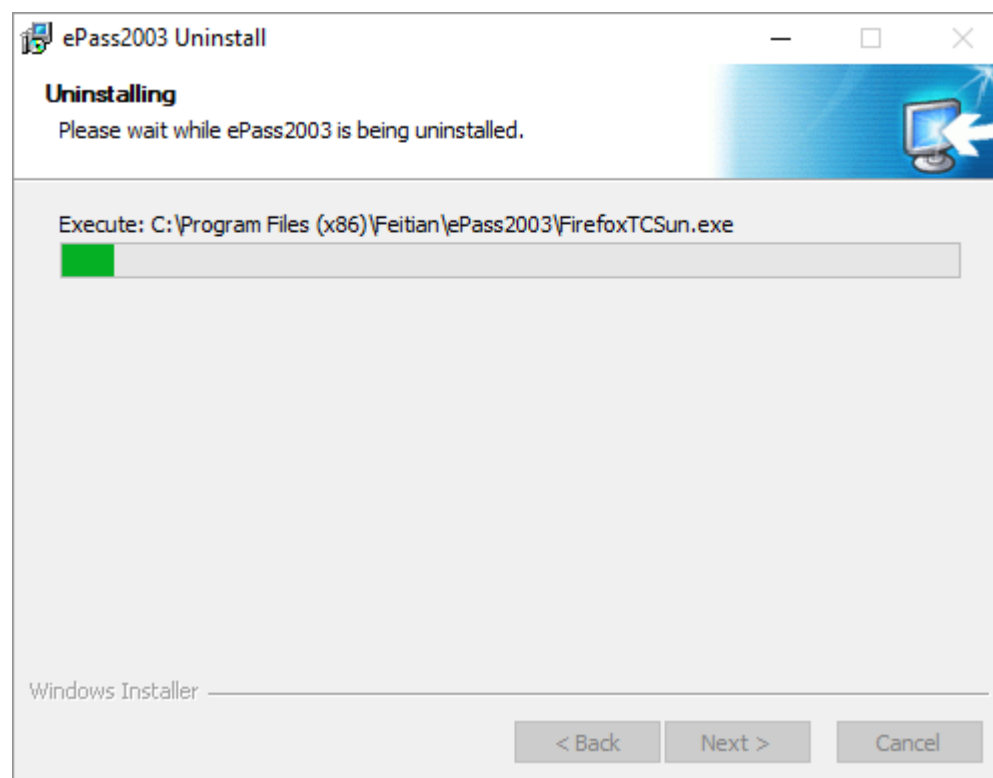


Figure 8 uninstall process

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

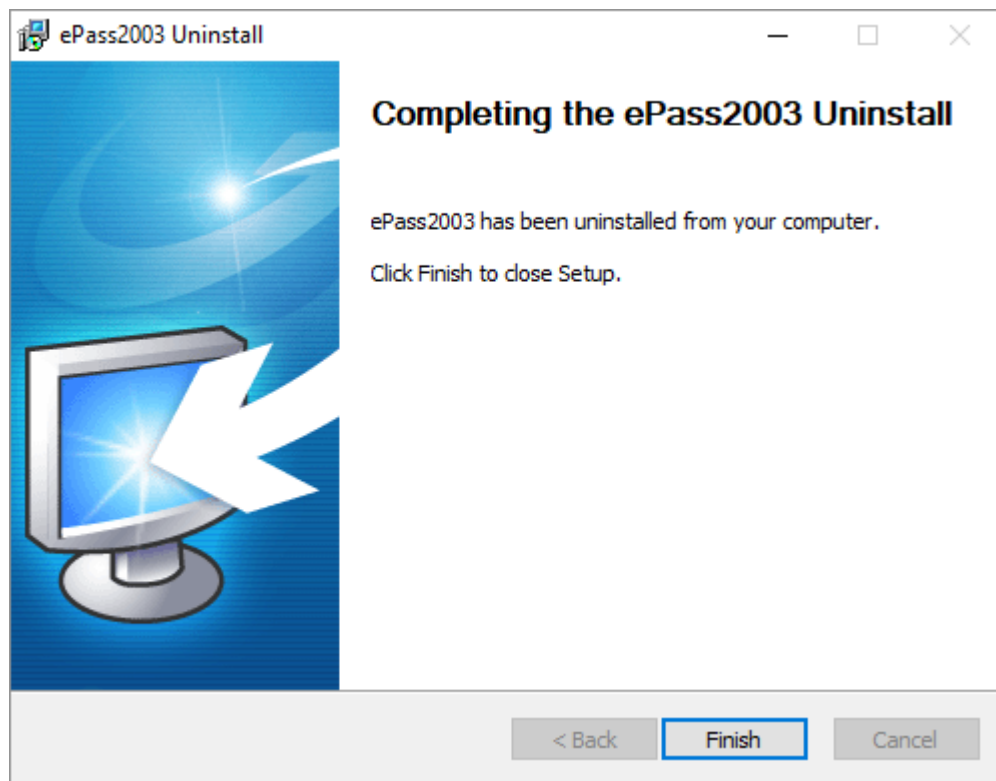


Figure 9 uninstall completed

4. Click "Finish" to close uninstall wizard, now ePass2003 has been already uninstalled from your computer.

Chapter 2 ePass2003 Token Manager

2.1 Prerequisite

Because the Manager is based on the middleware of ePass2003 and it needs to access the token, you must have installed ePass2003 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 -> Feitian -> ePass2003. Click the shortcut to start the Manager. The following interface appears:

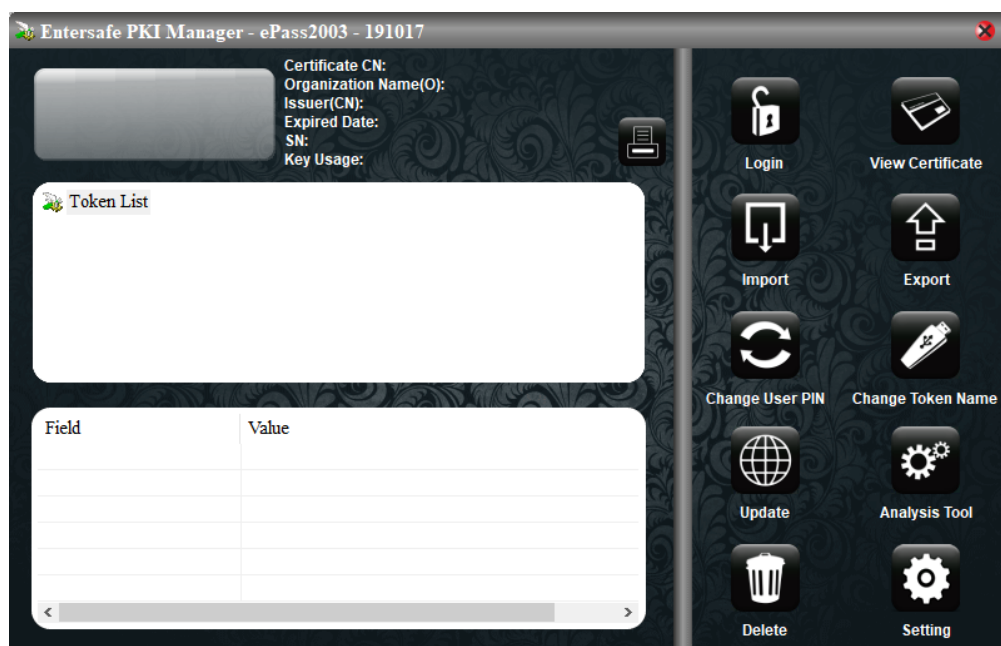


Figure 10 USB Key Not Inserted

2.2.2 Interface with USB Key Insertion

Connect ePass2003 to a USB port on your computer. The Manager will recognize it immediately as follows:



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:

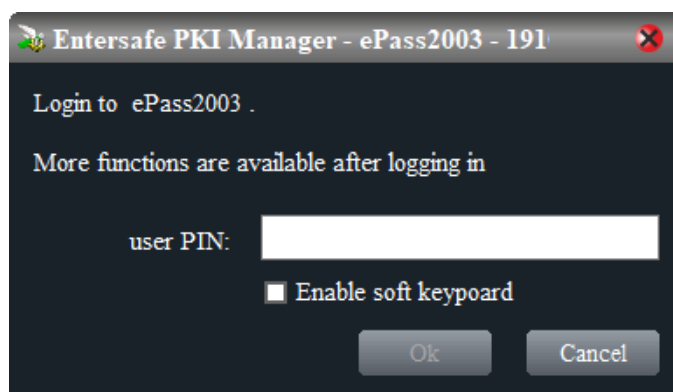


Figure 12 Login dialog box

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.

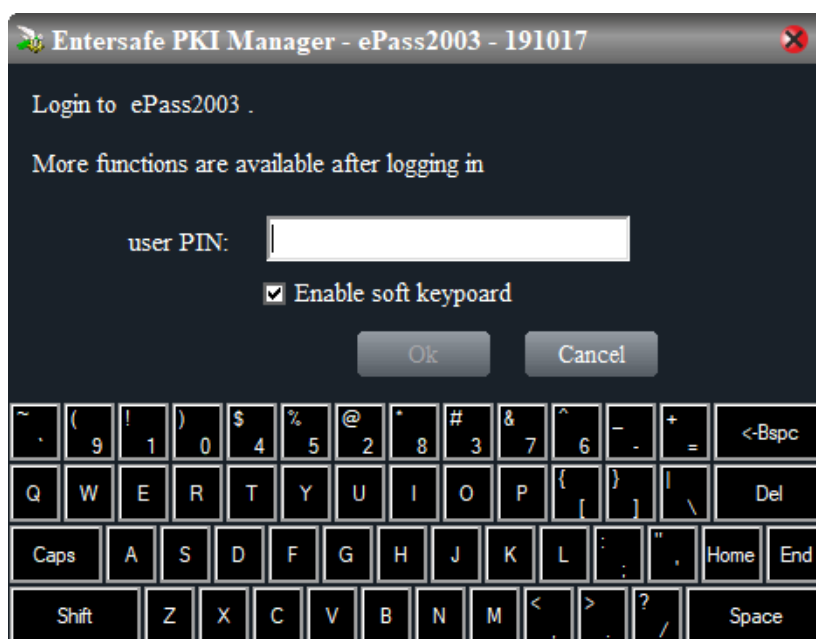


Figure 13 Soft Keyboard

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.



Figure 14 Logged In

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

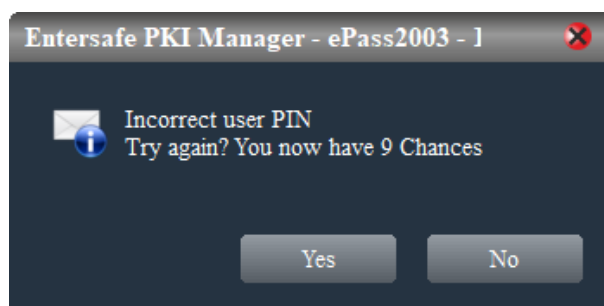


Figure 15 Incorrect PIN Prompt

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.



Figure 16 Viewing Certificate Information

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

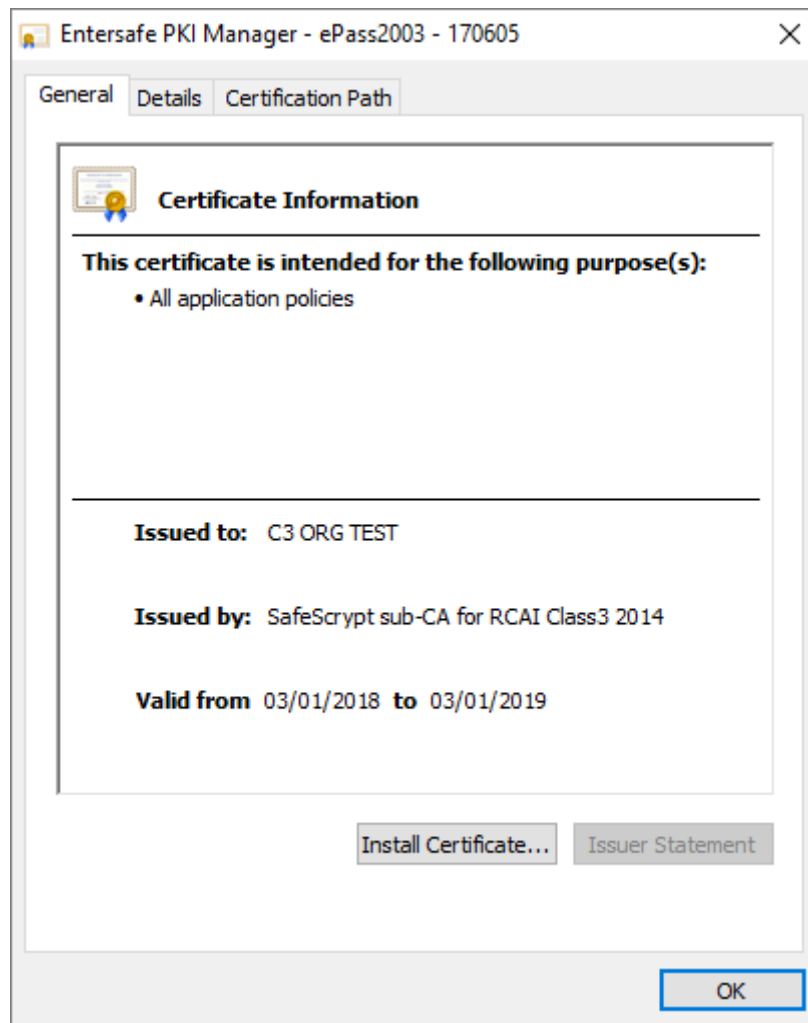


Figure 17 Certificate Information

You can view the information of your interest.

2.4.2 Importing

Currently, ePass2003 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.



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 ePass2003 token. Click OK.

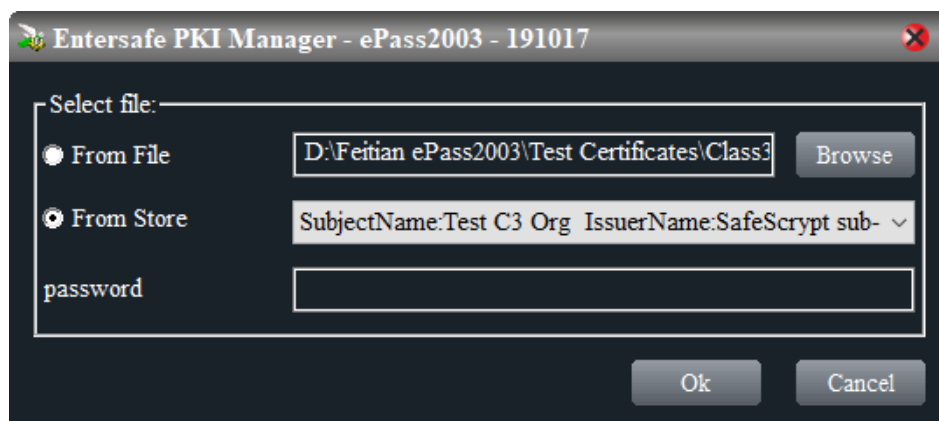


Figure 19 Certificate Import

2.4.3 Exporting

You can export a certificate from ePass2003 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.

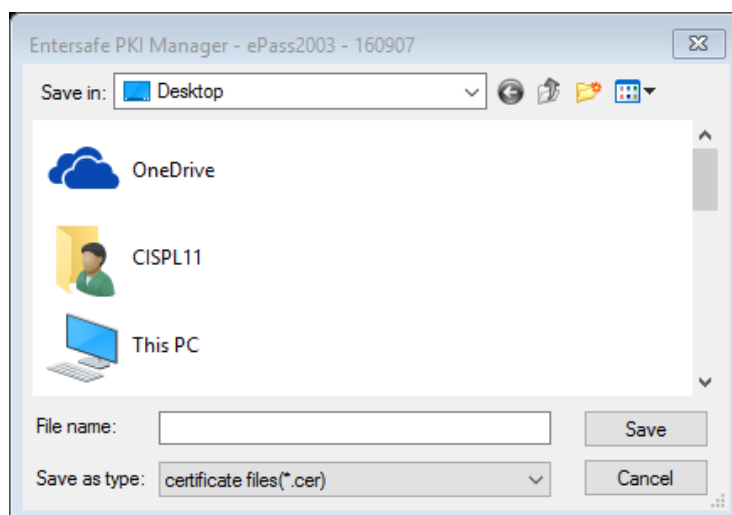


Figure 20 Certificate Export Path

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

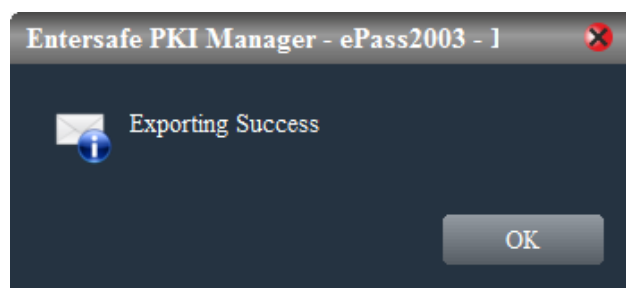


Figure 21 Successful Export

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:

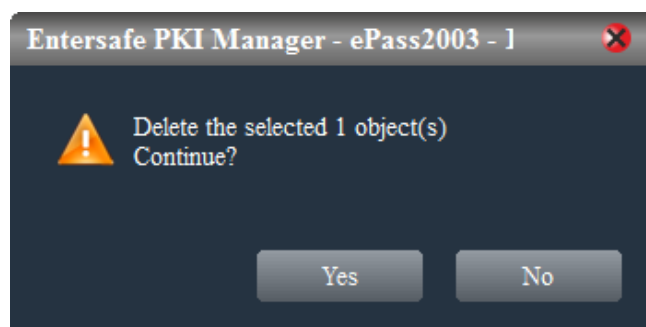



Figure 22 Deleting Certificate

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

2.4.5 Single Sign On (SSO):

ePass2003 has introduced a new feature Single Sign On (SSO).

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

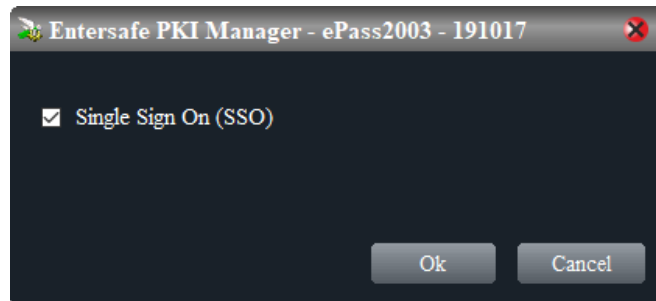


Figure 23 Enabling SSO

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  the main interface of the Token Manager and then click on Analysis. The following interface appears:

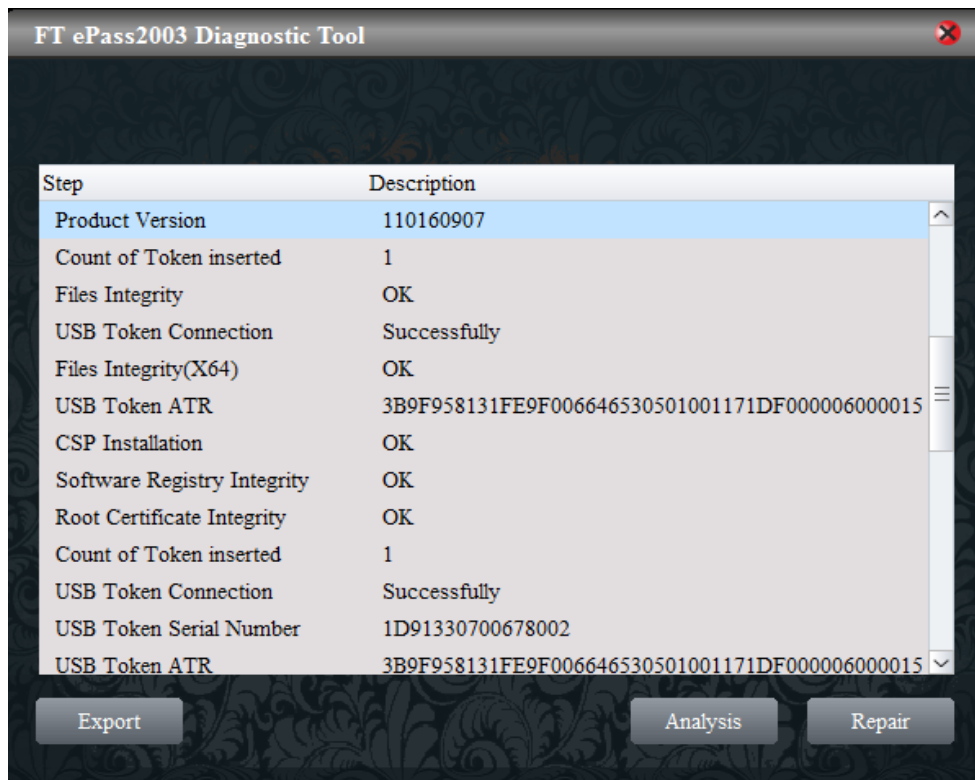


Figure 24 Running Analysis Tool

After Clicking on Repair button, following Interface appears:

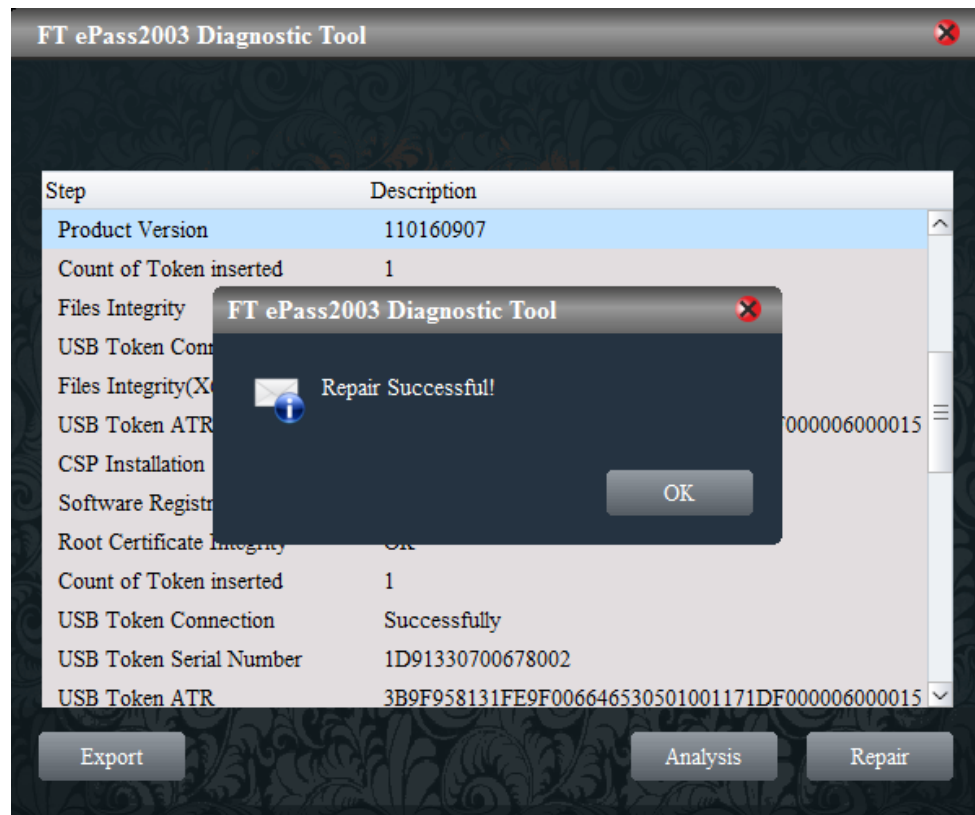


Figure 25 Running Repair Tool

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:

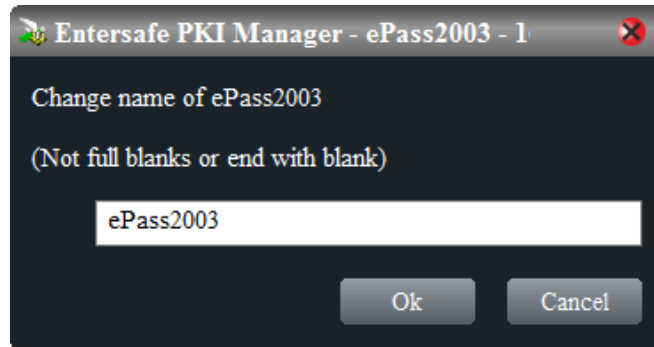


Figure 26 Changing Token Name

2. 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.

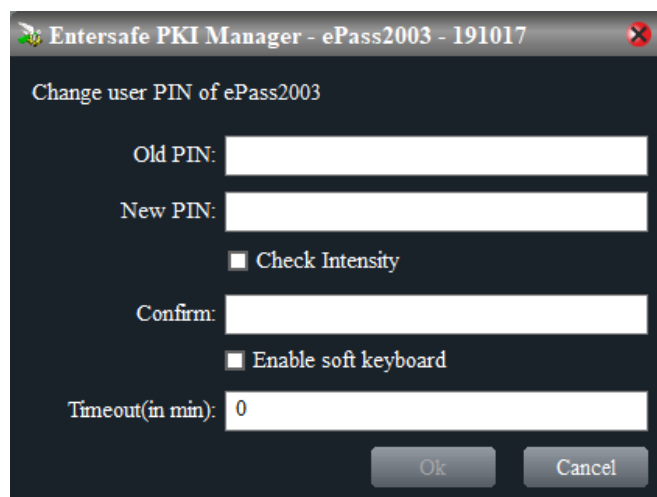


Figure 27 Changing User PIN

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

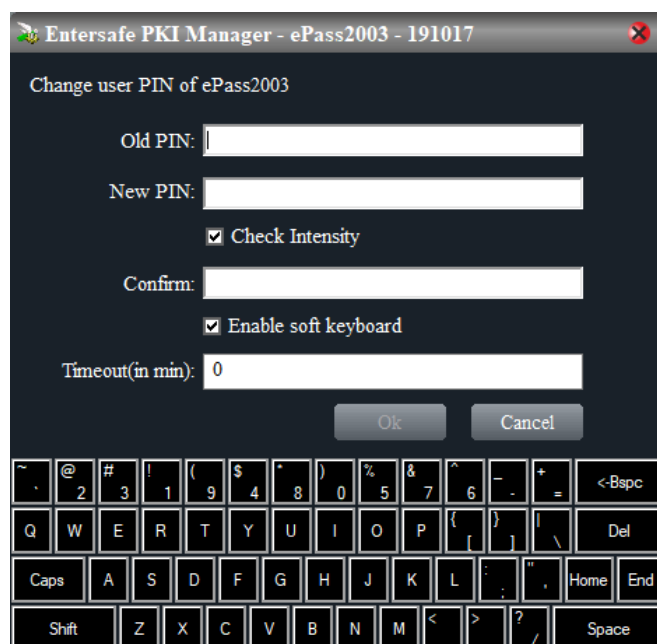


Figure 28 Soft Keyboard Input

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

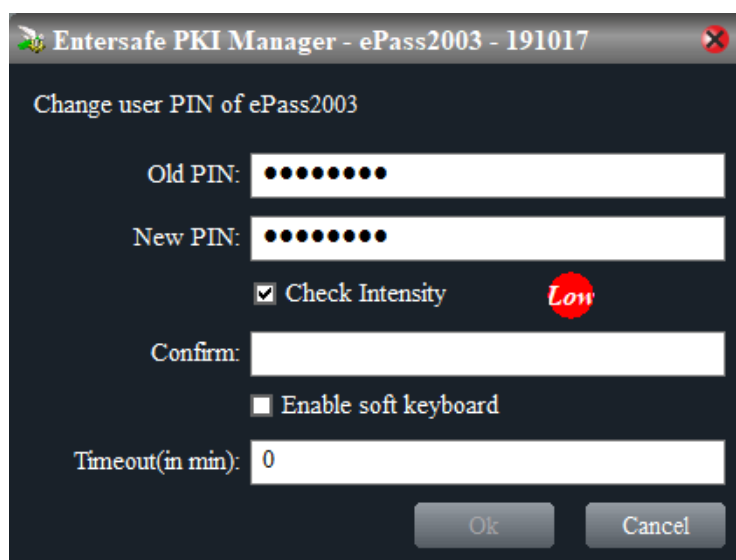


Figure 29 Low Strength

If the strength is higher, the following interface appears:

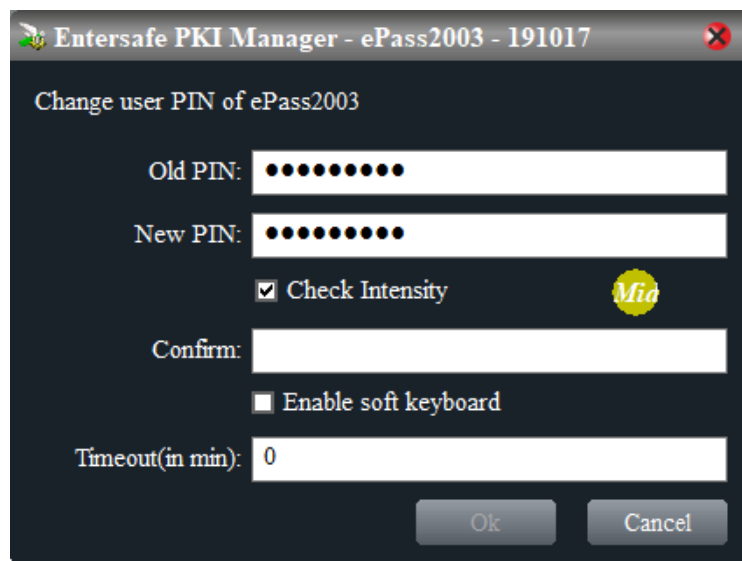


Figure 30 Medium Strength

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

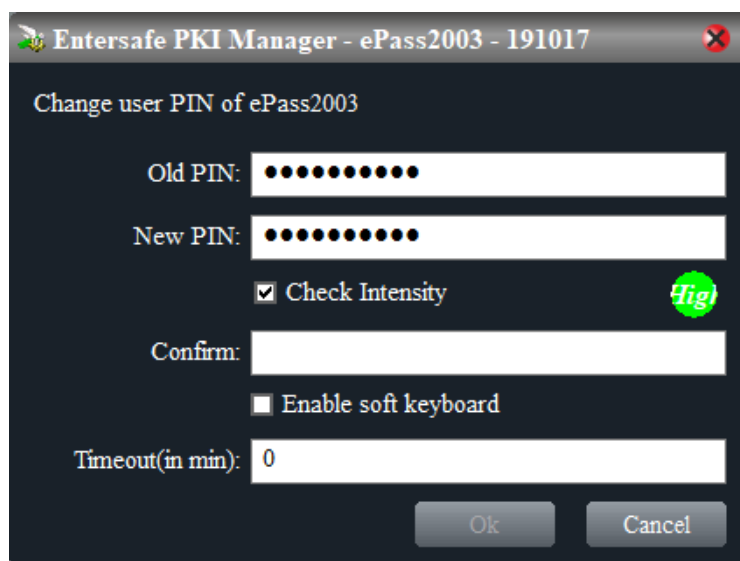


Figure 31 High Strength

By clicking OK, the following interface may appear:

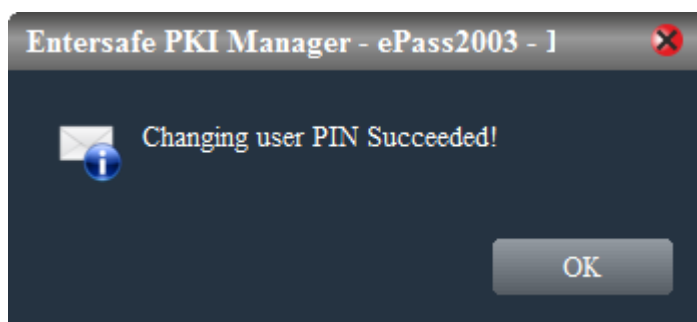


Figure 32 PIN Changed

Chapter 3 Unlock/Rest User Pin

Please download the Remote Unblock Client from below :

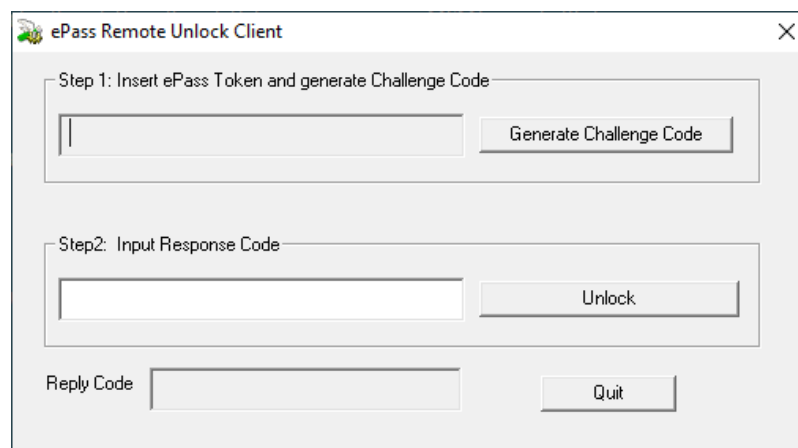
<https://taxpro.co.in/DSC/TokenDrivers/RemoteUnblockClient.zip>

Make sure latest ePass2003 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.



Extract the downloaded Remote Unblock Client.

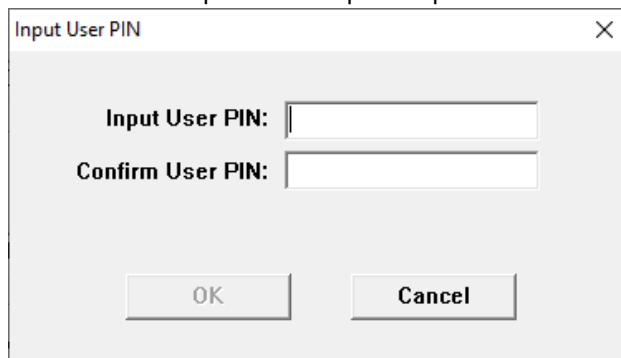
Now, open the RemoteUnblockClient.exe dialog Box showing as below.



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

If you get Reply Code SNjçCert 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 tokenunlock@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.

A dialog box titled "Input User PIN" with a close button (X) in the top right corner. It contains two text input fields. The first field is labeled "Input User PIN:" and the second field is labeled "Confirm User PIN:". Below the input fields are two buttons: "OK" and "Cancel".

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.

Appendix: Terms and Abbreviations

Entry	Description
ePass2003	A smart card based token with FIPS proved for PKI applications, introduced by Feitian Technologies. It is designed for PKI application systems.
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 Provider.
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.