

# BioPass3000

---

## User's Guide

*Version 1.0*

Feitian Technologies Co., Ltd. ("Feitian" for short) will do their best to keep the content of this document as accurate as possible. But Feitian will not take the responsibilities for any direct or indirect loss that may be caused by this document. The content of this document will be amended along with the updating of the product without notification.

Revision History:

Date	Version	Description
December 2006	1.0	1st Edition

## Feitian Technologies Co., Ltd.

### 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.

**CE Attestation of Conformity**

The equipment complies with the principal protection requirement of the EMC Directive (Directive 89/336/EEC relating to electromagnetic compatibility) based on a voluntary test.

This attestation applies only to the particular sample of the product and its technical documentation provided for testing and certification. The detailed test results and all standards used as well as the operation mode are listed in

Test report No.: 70407310011

Test standards: EN 55022/1998 EN 55024/1998

After preparation of the necessary technical documentation as well as the conformity declaration the CE marking as shown below can be affixed on the equipment as stipulated in Article 10.1 of the Directive. Other relevant Directives have to be observed.

**FCC certificate of approval**

This Device is in conformance with Part 15 of the FCC Rules and Regulations for Information Technology Equipment.

**USB**

This equipment is USB based.

**WEEE**

Dispose in separate collection.



# Contents

<b>1 Using BioPass3000 Manager .....</b>	<b>1</b>
1.1 Prerequisite .....	2
1.2 Overview .....	2
1.2.1 Interface Before Connecting the Token .....	2
1.2.2 Interface After Connecting the Token .....	3
1.2.3 Buttons .....	4
1.3 Fingerprint Management .....	4
1.3.1 Verifying Fingerprint .....	5
1.3.2 Registering Fingerprint .....	8
1.3.3 Updating Fingerprint .....	11
1.3.4 Deleting Fingerprint .....	14
1.3.5 Exit .....	15
1.3.6 Considerations .....	16
1.4 Login .....	16
1.5 Certificate Management .....	18
1.5.1 Viewing Certificate Information .....	18
1.5.2 Importing .....	20
1.5.3 Deleting .....	22
1.6 Options .....	24
1.7 Changing Token Name .....	25
<b>2 Fingerprint Tour .....</b>	<b>27</b>
2.1 Interface .....	28
2.2 Usage .....	28
2.3 An Introduction to Fingerprint Images .....	29
2.3.1 Applicable Fingerprint Images .....	29
2.3.2 Inapplicable Fingerprint Images .....	30
<b>3 Using the Token with the Software .....</b>	<b>33</b>
3.1 How to Connect the Token to the Computer .....	33
3.2 Product View .....	33
3.3 How to Hold the Token .....	34
3.4 How to Slide the Finger .....	35
3.5 Usage Examples .....	36
<b>Appendix 1 Frequently Asked Questions .....</b>	<b>38</b>
<b>Appendix 2 Terms and Abbreviations .....</b>	<b>39</b>

# 1 Using BioPass3000 Manager

This chapter introduces the following topics:

- Prerequisite
- Overview
- Fingerprint Management
- Login
- Certificate Management
- System Options
- Changing Token Name

## 1.1 Prerequisite

You must correctly install BioPass3000 product software (the middleware and the hardware driver) on your computer before using the GUI manager of BioPass3000, because BioPass3000 Manager is middleware based and needs access to the token.

The PKI initialization should be performed upon BioPass3000 before it can be used. By default, initialization has been performed before shipment.

## 1.2 Overview

### 1.2.1 Interface Before Connecting the Token

The shortcut for the Manager could be found under “Start” → “Programs” → “EnterSafe” → “BioPass3000”. Click the shortcut to start the Manager. The following window appears:

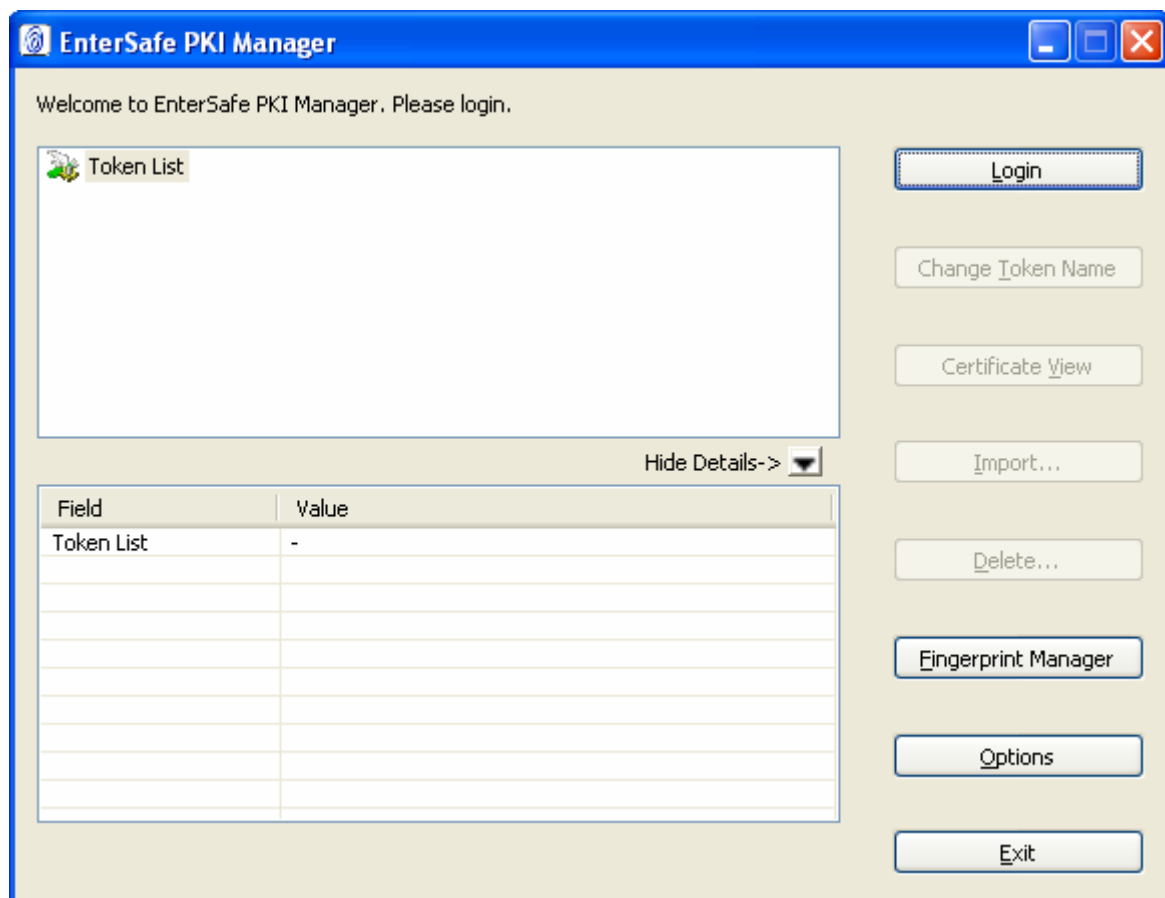


Fig. 1.1 Interface Before Connecting the Token



## 1.2.2 Interface After Connecting the Token

After a token named, for example, "BioPass3000", is connected to a USB port on your computer, the Manager will recognize the basic information of the token automatically. The interface looks like the following:

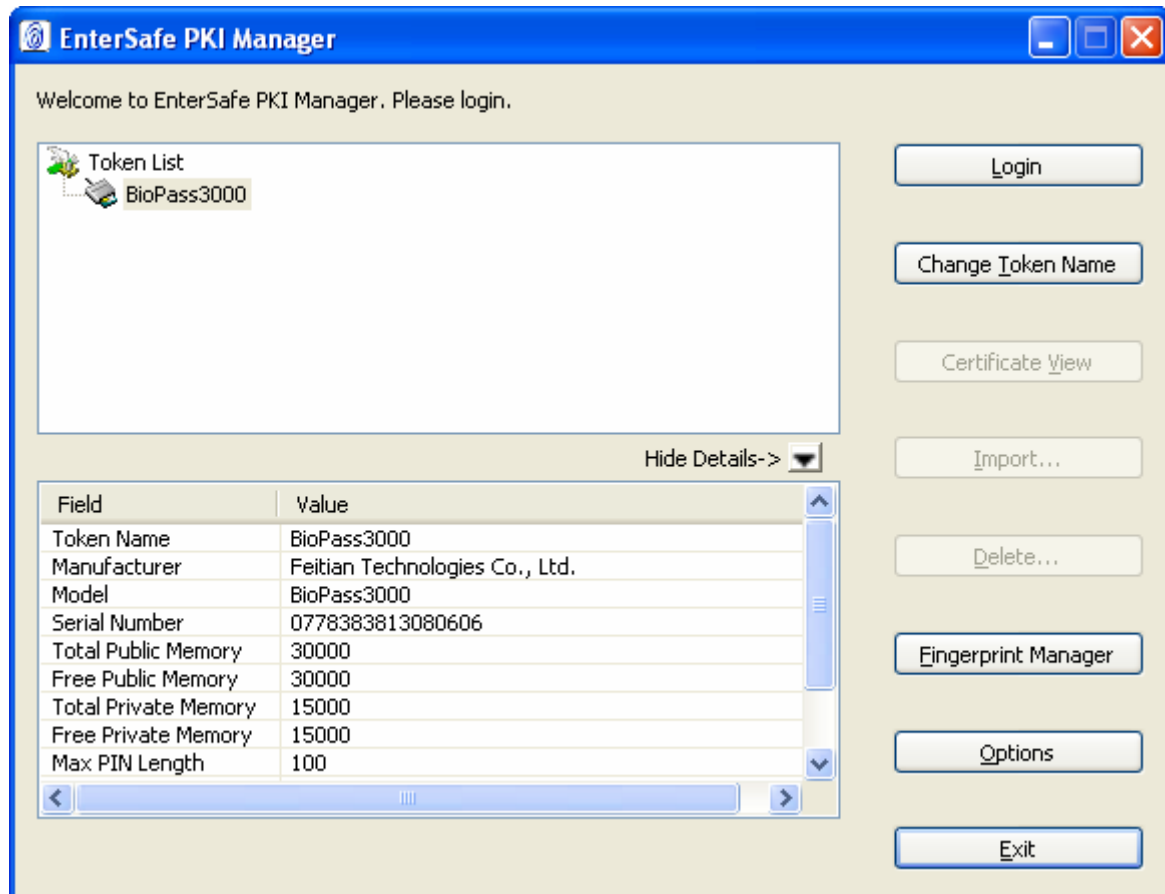


Fig. 1.2 Interface After Connecting the Token

If the token cannot be recognized correctly, the interface looks like the following appears. You may need to perform a PKI initialization on the token first.

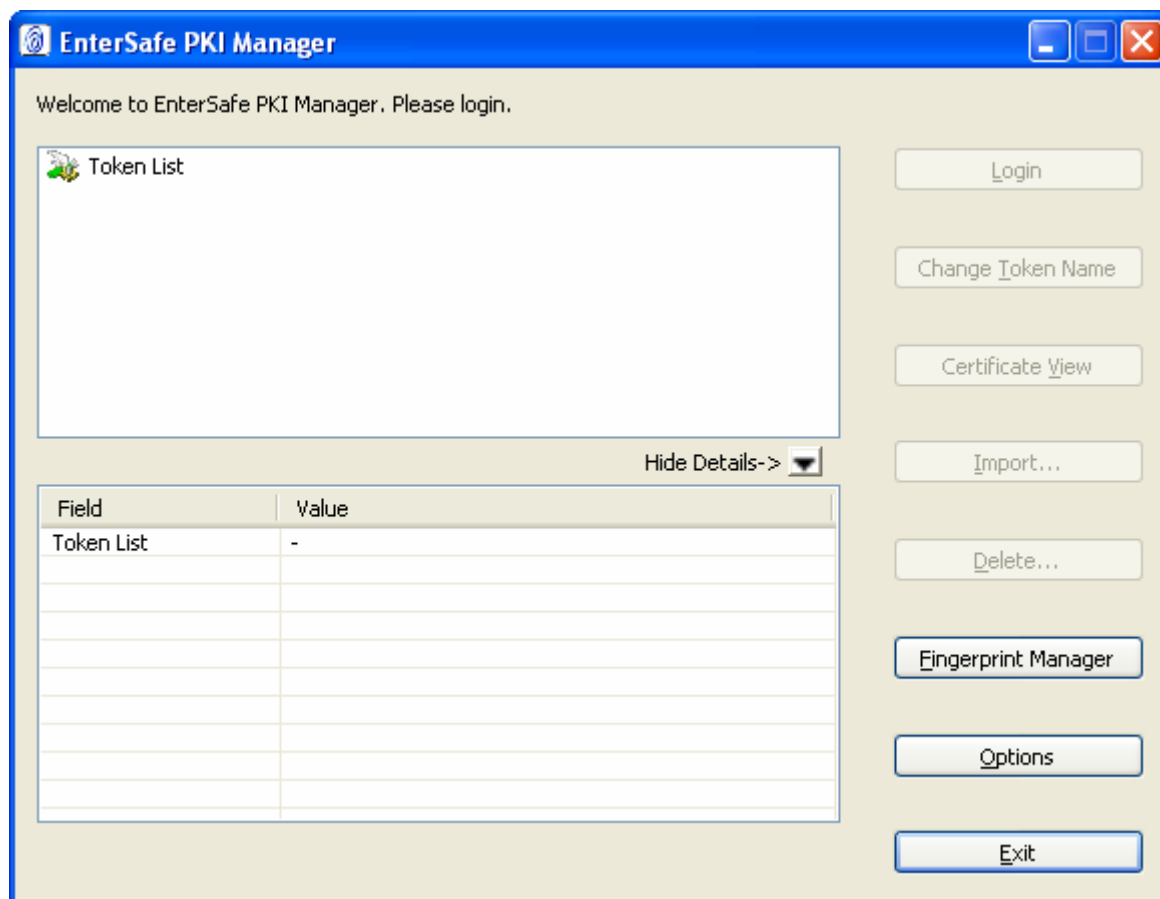


Fig. 1.3 Interface When a Unknown Token Connected

### 1.2.3 Buttons

The buttons on the main interface of the Manager include: "Login", "Change Token Name", "Certificate View", "Import", "Delete", "Fingerprint Manager", "Options" and "Exit".

## 1.3 Fingerprint Management

Click "Fingerprint Manager" button to open Fingerprint Manager widow. On the window, there are five buttons: "Verify", "Register", "Update", "Delete", and "Exit". When you place your mouse over each button, the functional description will be displayed in the text box at the bottom of this window. See the following.



Fig. 1.4 Fingerprint Manager Window

### 1.3.1 Verifying Fingerprint

You must register at least one fingerprint before verifying the fingerprint. The verification procedure is described as follows:

1. Click "Verify" button on Fingerprint Manager window. Verify Fingerprint window appears.

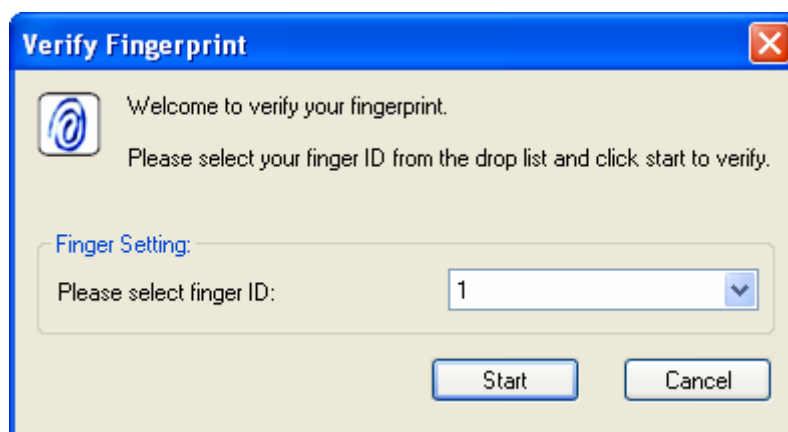


Fig. 1.5 Verify Fingerprint Window

If you have not registered any fingerprint yet, a message will be displayed to tell you that you

must register a fingerprint first.



Fig. 1.6 Fingerprint Registration Prompt

2. You are required to select a finger ID from the drop down list in Finger Setting panel, then click "Start" button. When Verify Fingerprint dialog box appears, you can scan your fingerprint.

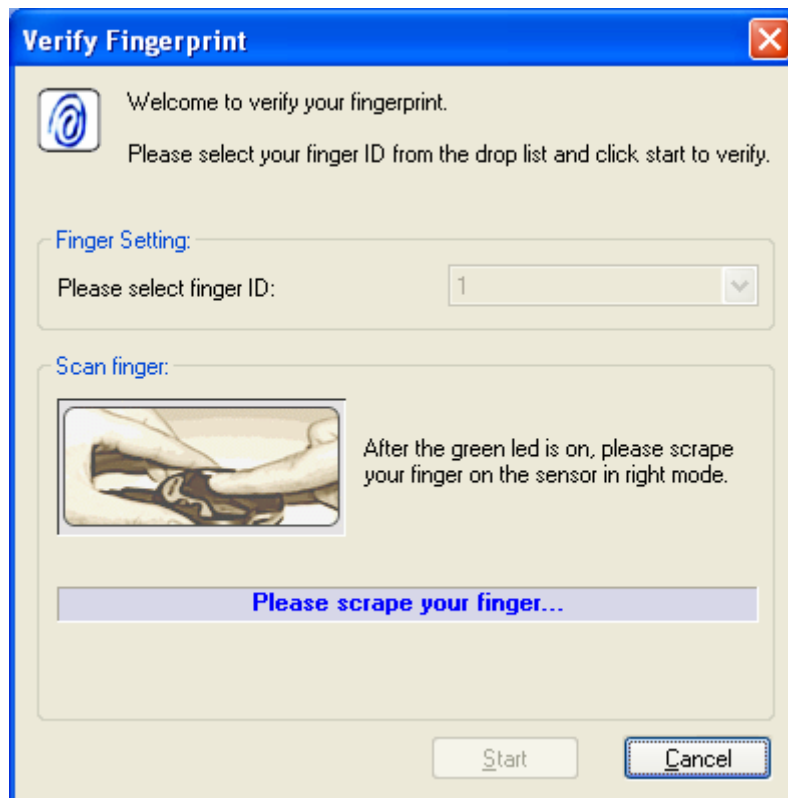


Fig. 1.7 Verify Fingerprint dialog box

Note: When you click "Start", the fingerprint indicator (green) of BioPass3000 will be switched on, indicating the state waiting for you to scan your fingerprint. After scanning finished, the indicator (green) will be switched off. The indicator (red) will be switched on.

3. If you have scanned a correct fingerprint, the dialog box like the following will be displayed. Click "OK" to login the token.



Fig. 1.8 Verification Success window

### 1.3.2 Registering Fingerprint

You must have verified your fingerprint or verified initial password before you can register a new fingerprint. The registration procedure is described as follows:

1. Click "Register" button on Fingerprint Manager window. If it's the first time you register a fingerprint, the fingerprint template does not contain any fingerprint, and an Initial Password Input dialog box will be displayed. By default, the initial password is 1234. You must input correct initial password to continue. After a fingerprint is registered successfully, the initial password will be invalidated.

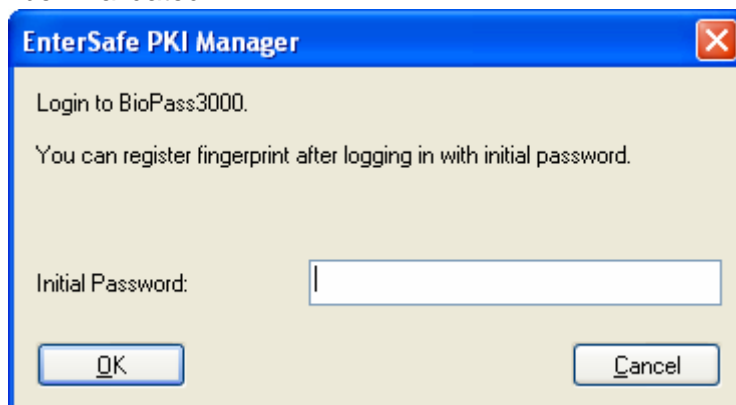


Fig. 1.9 Initial Password Input dialog box

After entering a correct initial password, click “OK” to open Register Fingerprint window.

If it's not the first time you register a fingerprint, clicking “Register” will bring you to Register Fingerprint window directly.

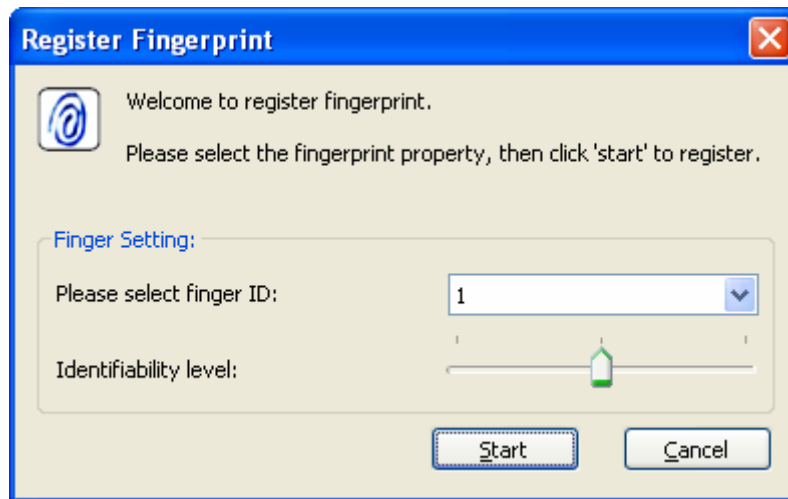


Fig. 1.10 Register Fingerprint window

2. You are required to select an unused finger ID from the dropdown list in Finger Setting panel, and specify a fingerprint matching level for Identifiability level. The level can be high, medium, or low. The verification is more strict at higher level. The default level is medium.

Then, click “Start” button. Register Fingerprint dialog box appears, asking you to scan your fingerprint.



Fig. 1.11 Register Fingerprint dialog box

3. To register your fingerprint, you must successfully scan your finger 3 times. You must not use different fingers in the process. After that, a registration success dialog box will appear. Click "OK" to complete registration.



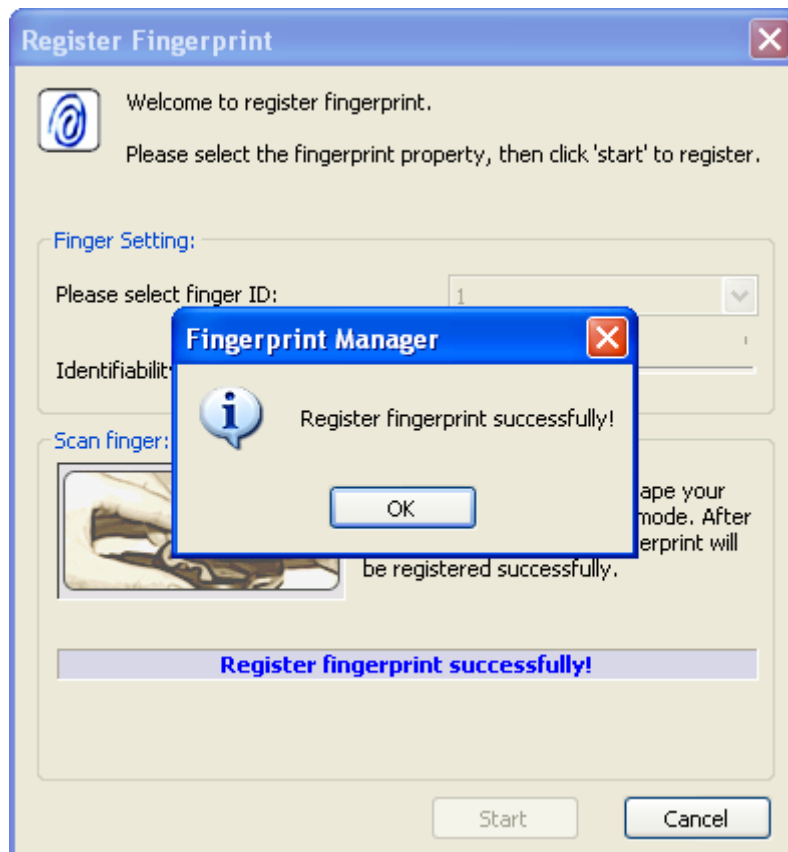


Fig. 1.12 Registration Success window

You can register up to 8 fingerprints in the same way.

Tip: To avoid failing to use the token due to unexpected situation, such as the breaking the skin of your registered finger, we recommend you register more than one fingerprint with both from your hands.

### 1.3.3 Updating Fingerprint

You can also modify registered fingerprints with BioPass3000 Manager. You must have registered at least one fingerprint and passed the fingerprint verification or initial password verification before you can update a fingerprint. This procedure is described as follows:

1. Click "Update" on Fingerprint Management window. Update Fingerprint window appears.

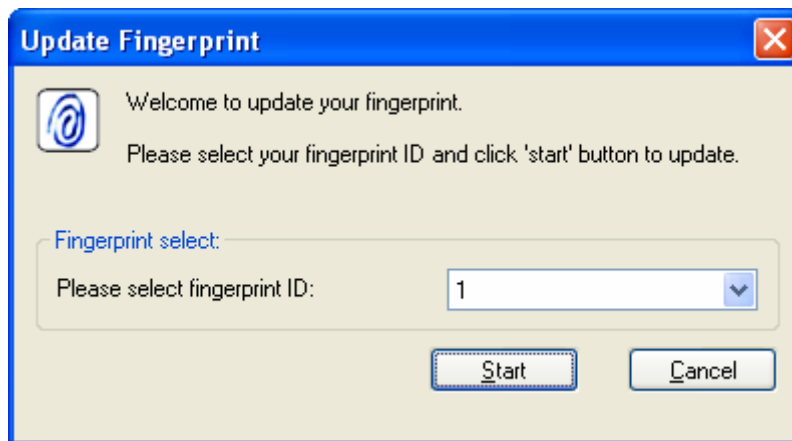


Fig. 1.13 Update Fingerprint window

If you have not registered any fingerprint yet, a message will be displayed prompting you to register a fingerprint first.



Fig. 1.14 Fingerprint Registration Prompt

2. You are required to select a fingerprint ID which you want to update from the dropdown list in Fingerprint select panel, and click "Start". Then Update Fingerprint dialog box appears asking you to scan your fingerprint.

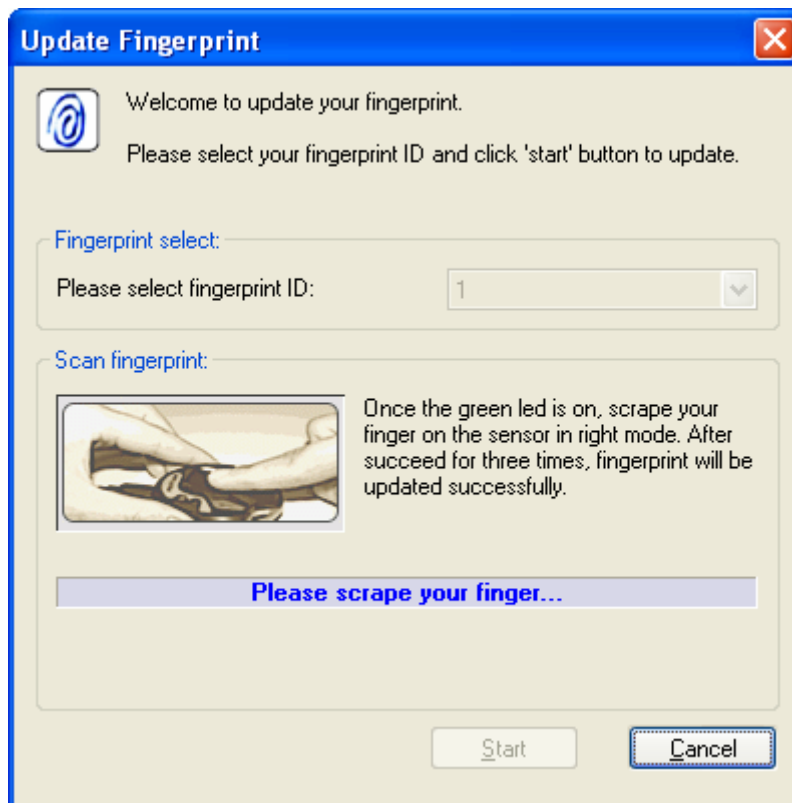


Fig. 1.15 Update Fingerprint dialog box

3. To update a fingerprint, you must successfully scan your fingerprint 3 times. You must not use different fingers in the process. After that, click "OK" in updating success dialog box to complete fingerprint update.

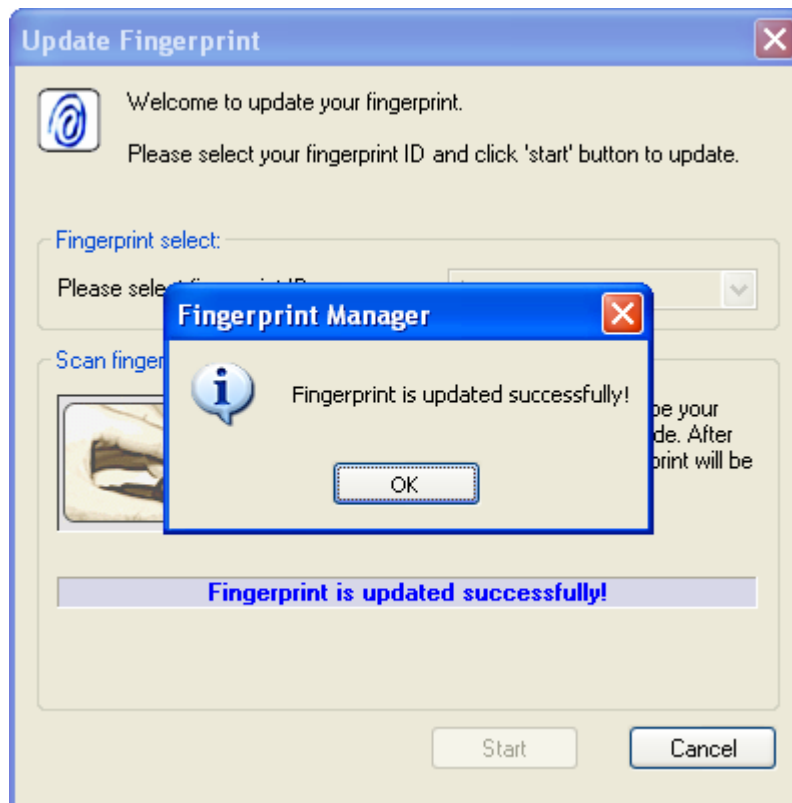


Fig. 1.16 Updating Success dialog box

### 1.3.4 Deleting Fingerprint

You can also delete registered fingerprints. But you must pass the fingerprint verification or initial password verification before you can delete a fingerprint. This procedure is described as follows:

1. Click “Delete” button on Fingerprint Manager window. Delete fingerprint window appears.

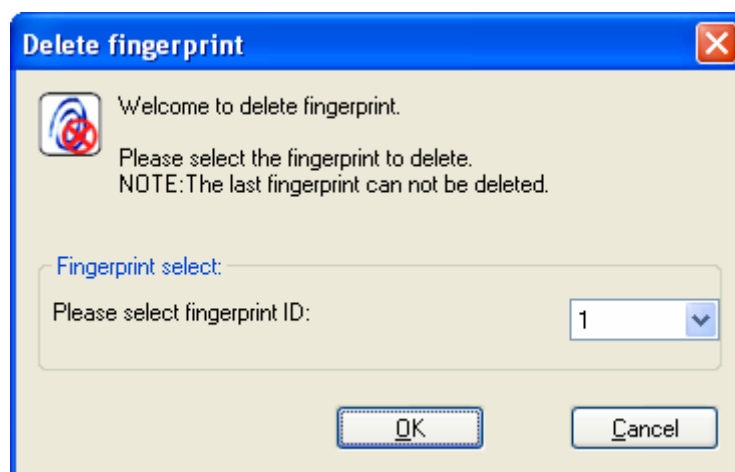


Fig. 1.17 Delete Fingerprint window

2. You are required to select a fingerprint ID which you want to delete from the dropdown list in Fingerprint select panel and click "OK". Then Deletion success dialog box appears.

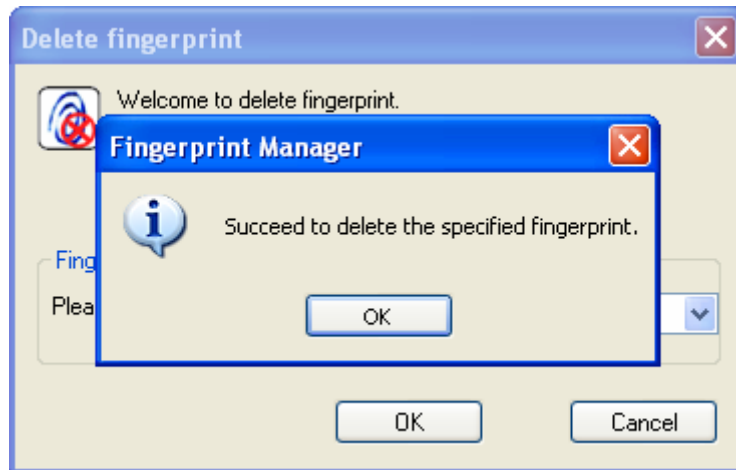


Fig. 1.18 Deletion Success dialog box

3. Click "OK" to complete deletion.

Note: You must keep at least one fingerprint in the token. If there is only one fingerprint on the token, the Manager will prompt you that deletion is not allowed.

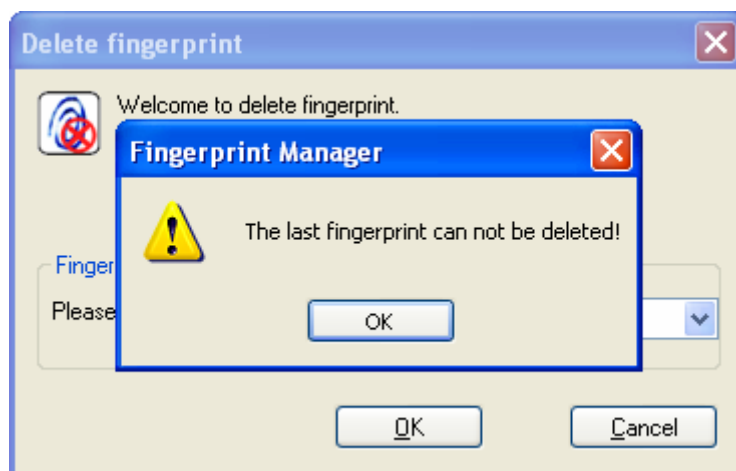


Fig. 1.19 No Deleting Prompt

### 1.3.5 Exit

Click "Exit" button on Fingerprint Management window to exit, and return to the main window.

### 1.3.6 Considerations

- BioPass3000 supports both forward and backward fingerprint scanning. You may scan your fingerprint in the way you preferred. But you should know that if you use forward acquisition when registering a fingerprint, you must scan your fingerprint forward when verifying your fingerprint, and vice versa. Otherwise, you will not be able to pass through the verification.
- Tip: We recommend that you scan your fingerprint in the same direction, so as to avoid forgetting the scan direction and fail to be recognized.
- You should not scan your fingerprint too quick or too slow. The optimal speed for a scan is half a second. You can check your scanning speed with the learning tool. If the speed is inappropriate, you cannot get a “good” image on the screen. If the image is clear and covers the whole display area, you should keep up your speed and the way you scan your fingerprint later.
- Do not register with a wet, grease stained, or scared finger. Otherwise, the verification will be likely to fail.

## 1.4 Login

1. Click “Login” on the main window of the Manager. Then scan fingerprint dialog box appears.

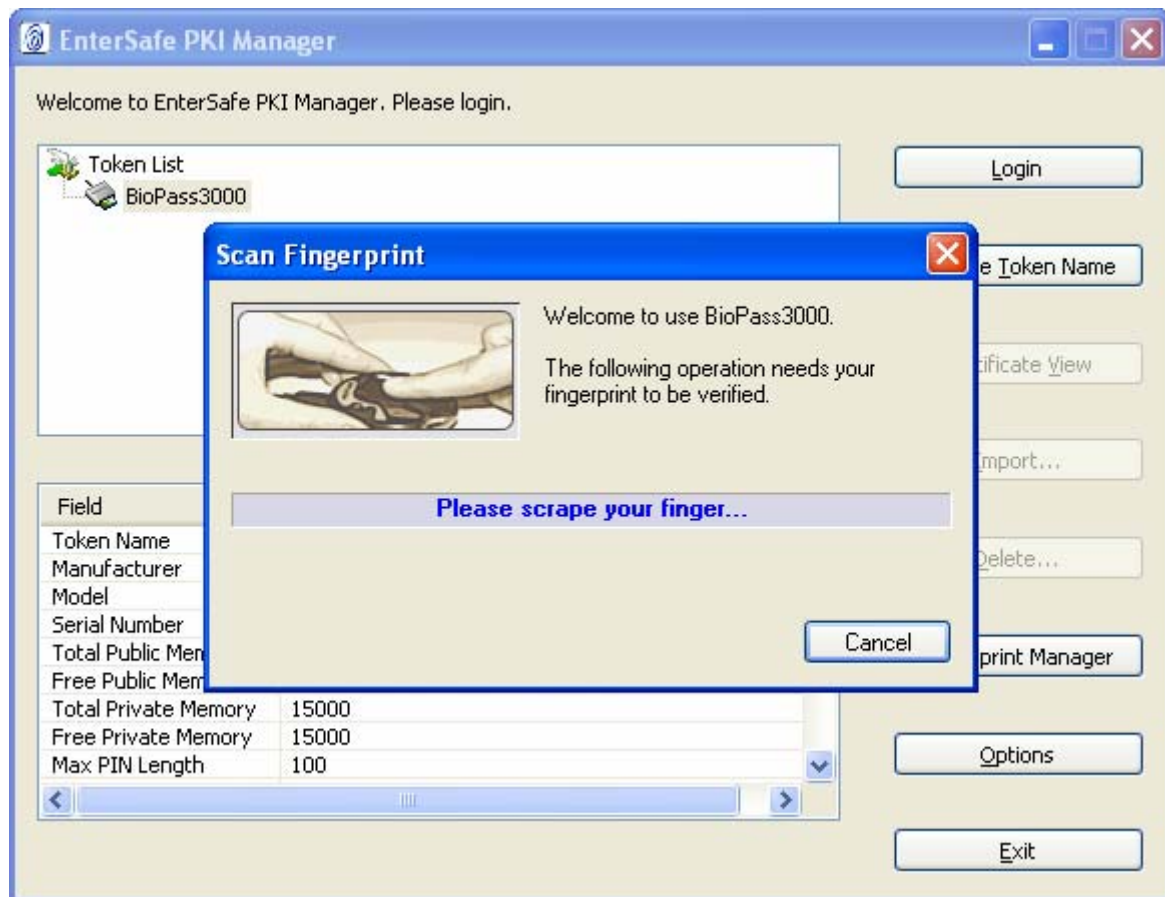


Fig. 1.20 Login and Scan Fingerprint

If you have not registered a fingerprint yet, you are required to use an initial password to log in. By clicking "Login" button, an Initial Password Verification dialog box appears.

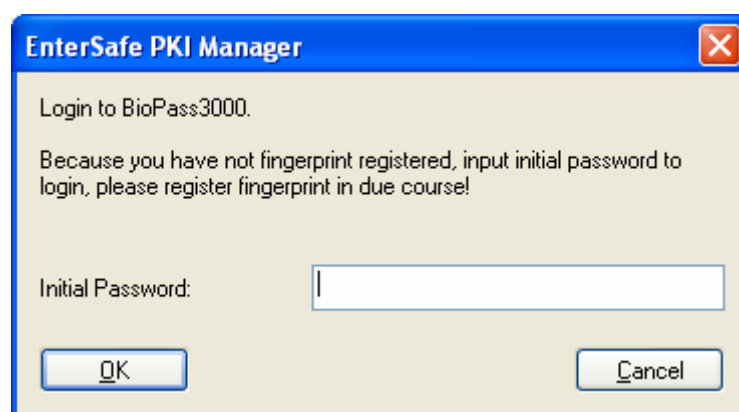


Fig. 1.21 Initial Password Login

- After you have successfully verified fingerprint or initial password, the following window appears. The token list is displayed on the top. You can click to select an item from the tree view. The attribute values of that item you selected will be displayed at the bottom. You can

click “Hide Details” to hide the attributes. After login, you can not only view the public data, but also the private data on the token. And “Login” button changes to “Logout” button. You can click “Logout” to safely exit.

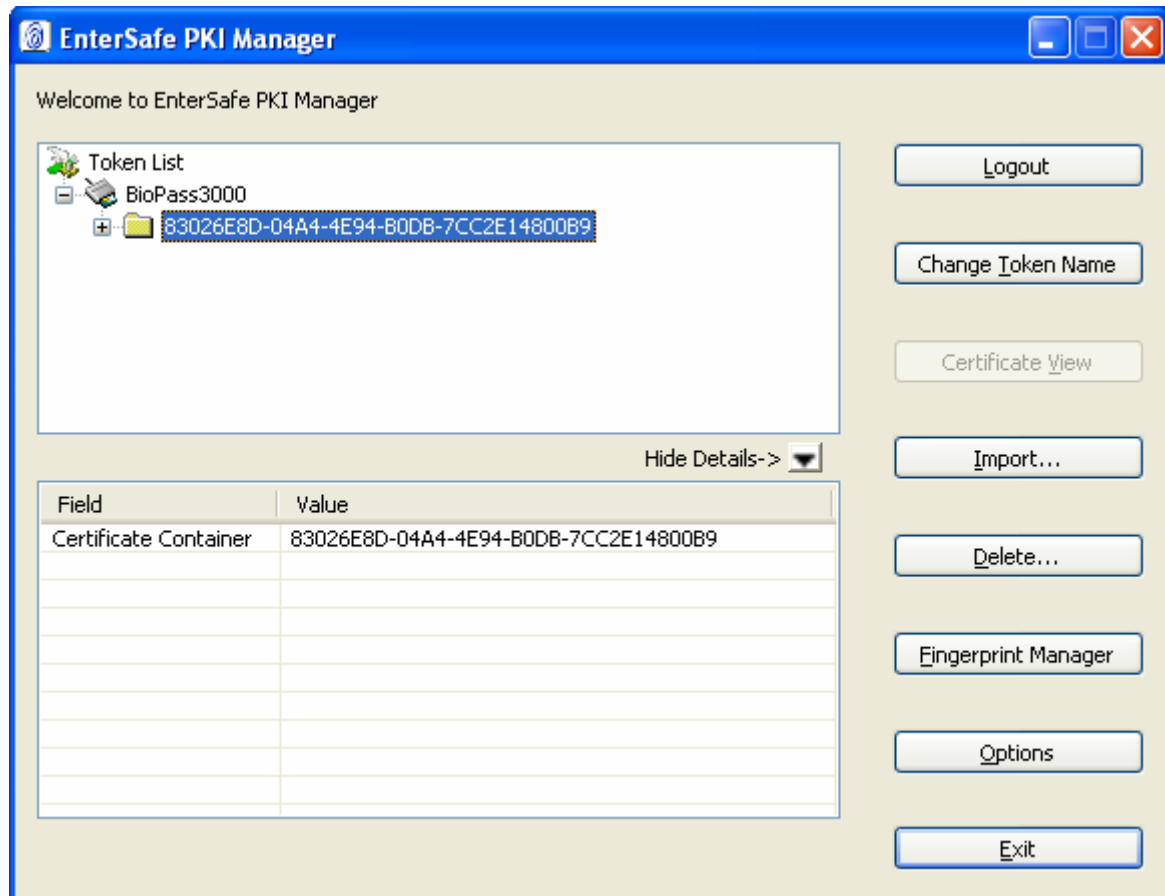


Fig. 1.22 The Interface After Login

## 1.5 Certificate Management

Once you have logged into BioPass3000 Manager, you can perform the operations, such as viewing certificate information, importing, and deleting.

### 1.5.1 Viewing Certificate Information

1. Click “+” sign on the left of any container (folder icon) or double-click the icon to display its contents in token list. Similarly, click “+” sign on the left of a certificate or double-click the certificate icon to display a public and private key-pair. At this step, “Certificate View” button is enabled.



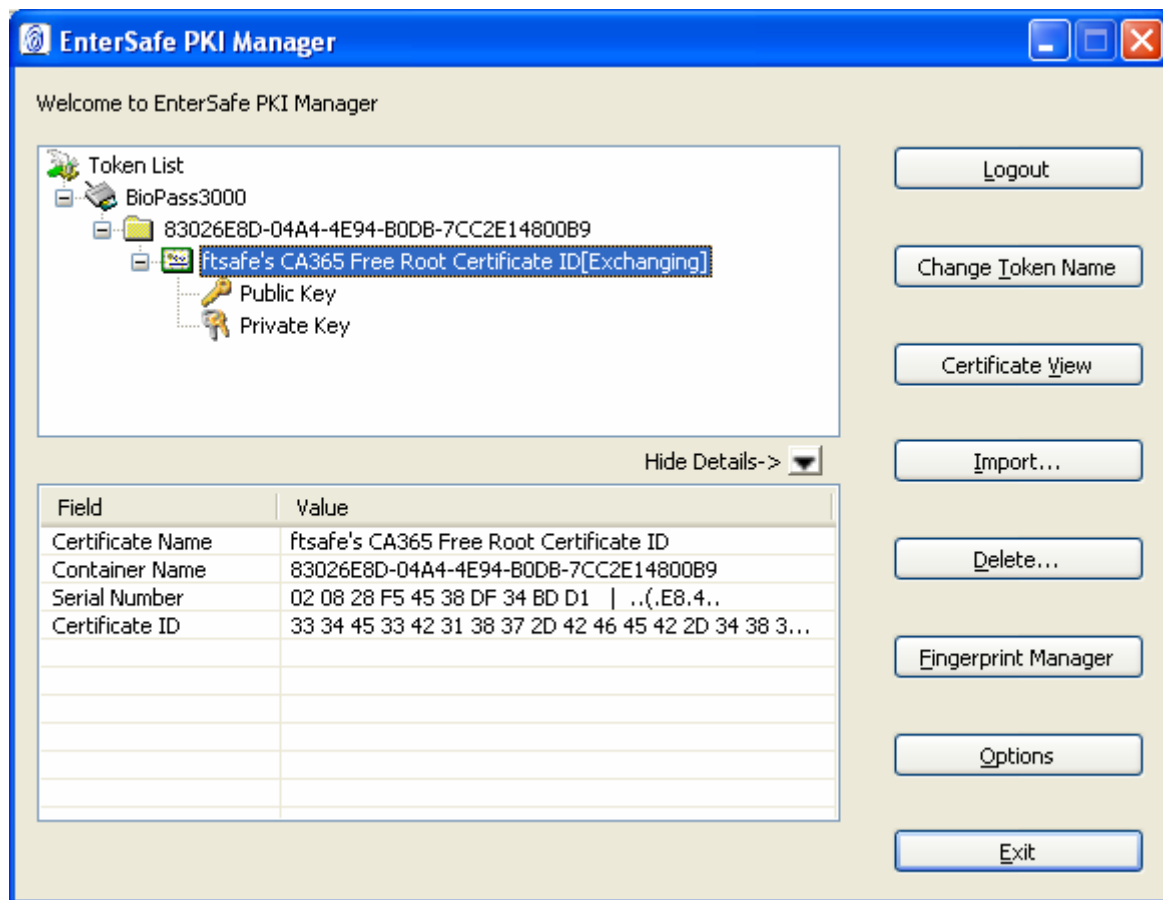


Fig. 1.23 Certificate View

- Click "Certificate View" button. Then Certificate View dialog box appears. You can click "General", "Details" or "Certification Path" to view certificate information.

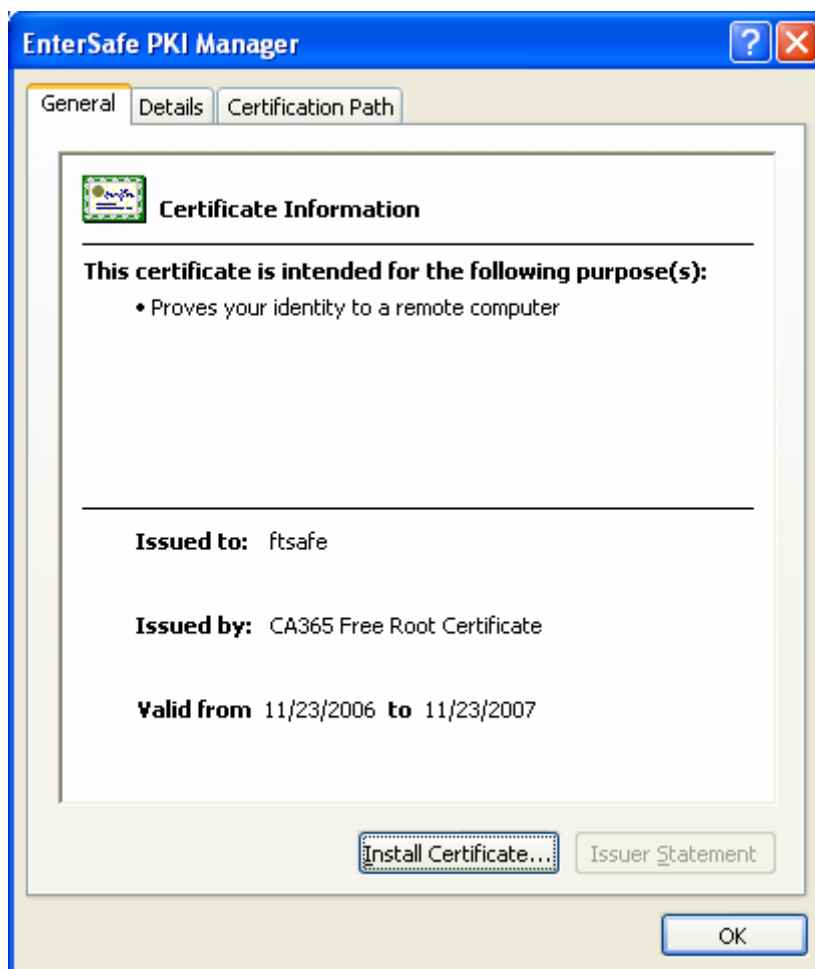


Fig. 1.24 Certificate View dialog box

## 1.5.2 Importing

Currently, the certificate types supported by BioPass3000 are P12, PFX, P7B and CER. P12 and PFX certificates contain a public and private key-pair. P7B and CER certificates do not contain a public and private key-pair. PFX and CER certificates are used to illustrate how to import a certificate.

### 1.5.2.1 Importing a PFX Certificate

Click “Import” button in the main window of the Manager. The following window appears. Click “Browse” button, and choose the path for the PFX certificate you want to import. If the certificate requires a password, enter the password in “File Password” field. You may need to create a container to store the imported certificate, or you can use an existing container. As a certificate contains a public and private key-pair, it can be used for exchanging or signing. After specify a

PFX purpose for the certificate, please click “OK” to import the certificate.

**Note:** One container can only contain two certificates for different purposes (exchange or sign). If you import a certificate to an existed container for the same purpose as the existed certificate, the manager will prompt you to replace the existed certificate.

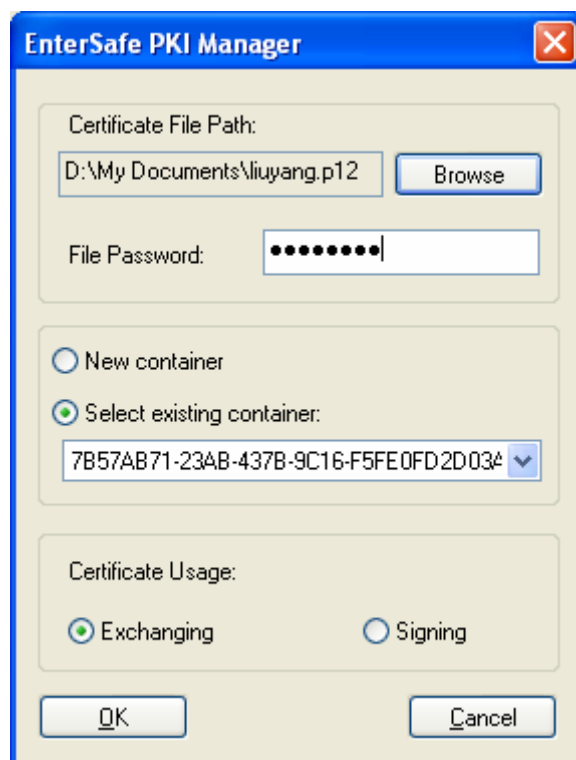


Fig. 1.25 Importing a PFX Certificate

### 1.5.2.2 Importing a CER Certificate

Click “Import” button in the main window of the Manager. The following window appears. Click “Browse” button, and choose the path for the CER certificate you want to import. If the certificate requires a password, enter the password in “File Password” field. You may need to create a container to store the imported certificate, or you can use an existing container. Since a CER certificate does not contain a public and private key-pair, it only can be used for exchanging; you cannot select any option in Certificate Usage area. Then click “OK” to import the certificate.

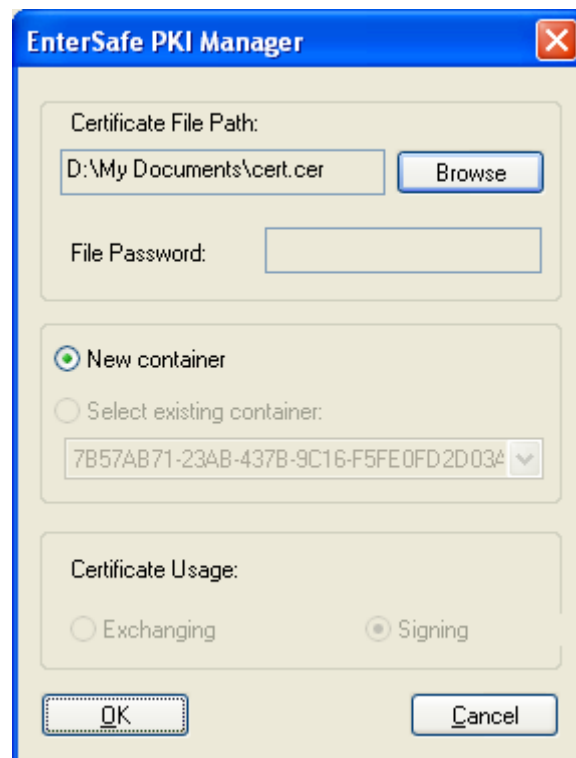


Fig. 1.26 Importing a CER Certificate

### 1.5.3 Deleting

1. Select a certificate you want to delete from the tree view in the main window. Click "Delete" button. The following dialog box appears.

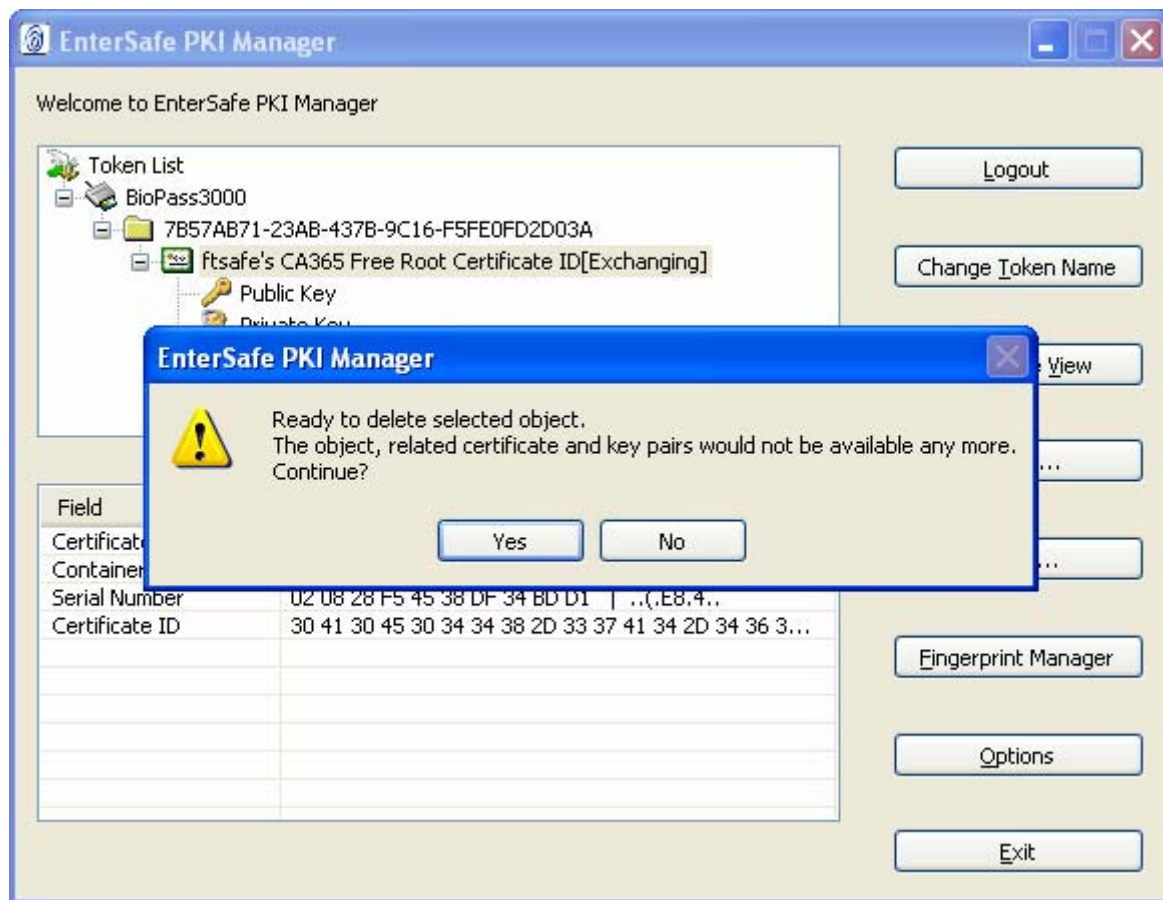


Fig. 1.27 Deleting a Certificate

- Click "Yes" to confirm the deleting operation. The post-deletion interface will look like the following:

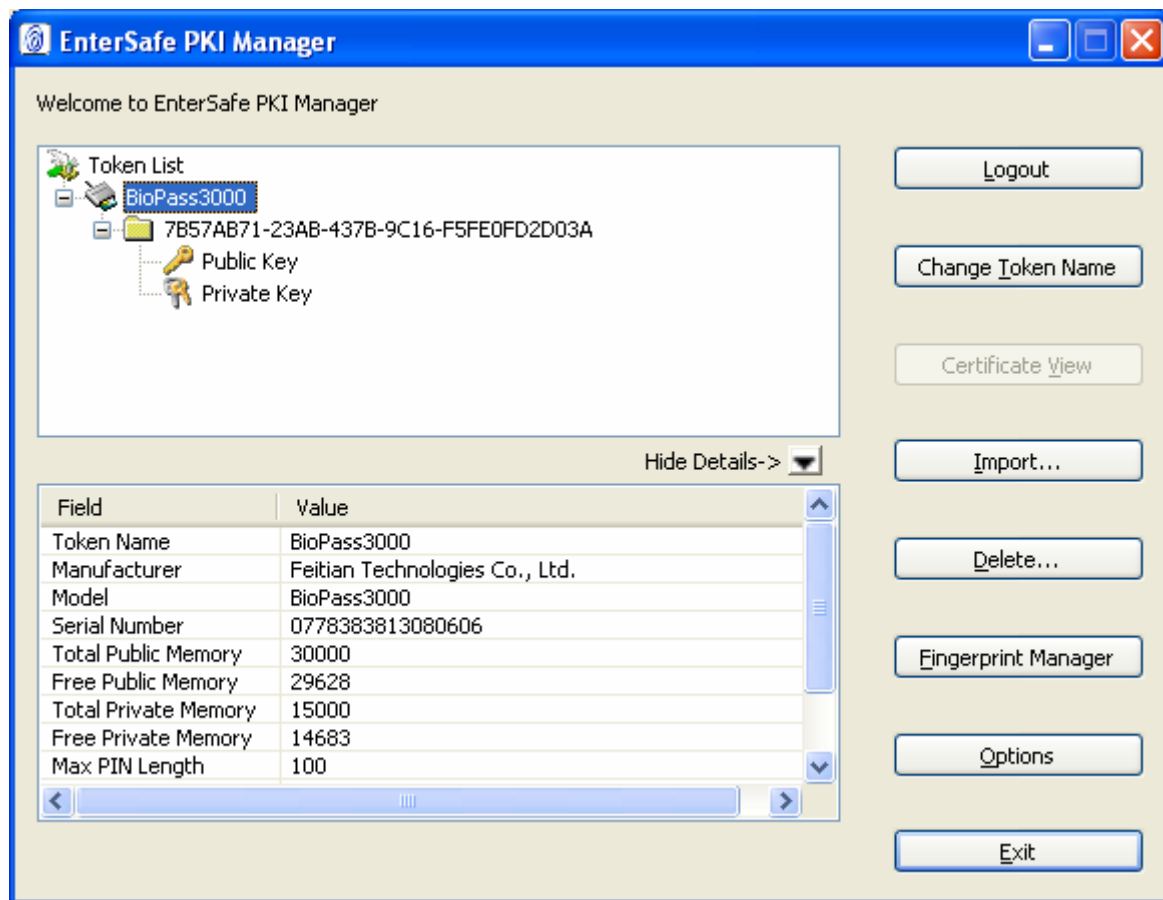


Fig. 1.28 Post-deletion Interface

You can delete any key or container on the token in the same way, simply by clicking the key or container in the tree view and clicking “Delete”. If you click a token name, for example, “BioPass3000” in the tree view and click “Delete” button, you will delete all containers and certificates and keys inside the token.

## 1.6 Options

Click “Options” button in the main window of the Manager. Then Settings window appears. You can set “Windows Domain Logon” and “Visit Website when token is inserted”.

If you choose “Support Windows domain logon by BioPass3000” option, you can use BioPass3000 to log in as a smart card. (Smartcard logon is supported by Windows2000, Windows XP and later Windows series systems)

If you choose “Visit a Website when token is inserted” option and input a website below, you

can visit the website automatically next time you connect the token to the computer.

Finally, click "OK" button.

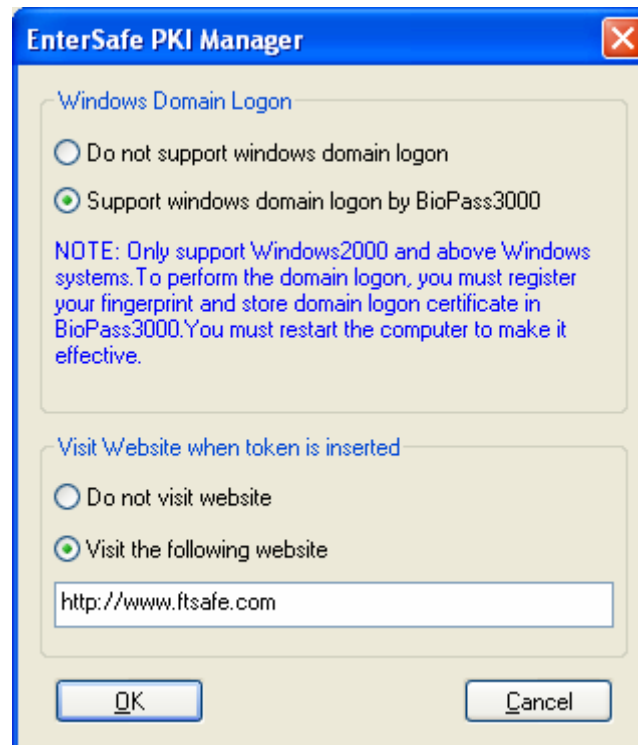


Fig. 1.29 Settings window

## 1.7 Changing Token Name

Generally, a token is identified by a serial number. But the serial number is not hard to be remembered. You can specify a customized name for the token for BioPass3000. To change a token name:

1. Click "Change Token Name" button in the main window of the Manager. A window looks like the following appears.

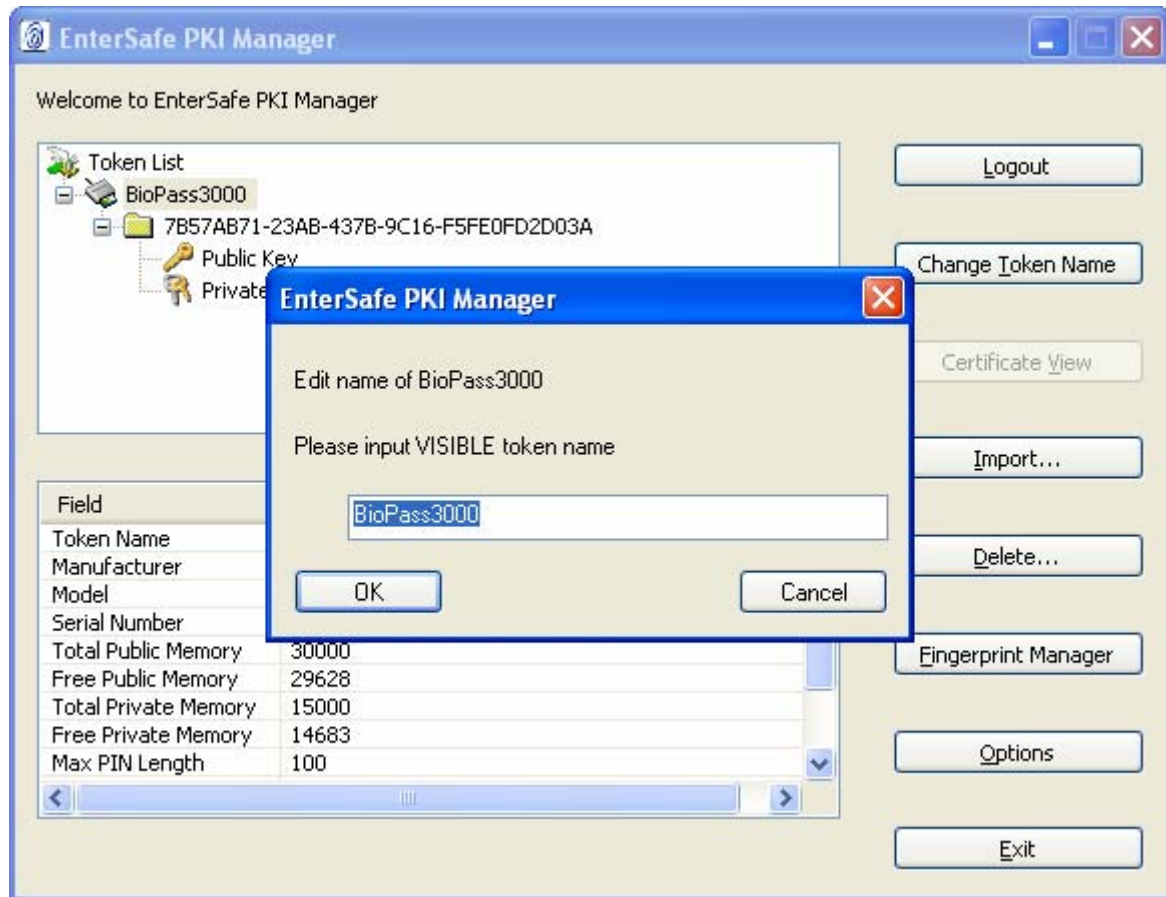


Fig. 1.30 Changing Token Name

2. Type a new name for the token in the text box, and click "OK".



## 2 Fingerprint Tour

This chapter introduces a tool, Fingerprint Tour ("Tour"), helping you learn how to input your fingerprint correctly. To start this tool, click "Start" → "Programs" → "EnterSafe" → "BioPass3000" → "Fingerprint Tour".

This chapter covers the following topics:

- Interface
- Usage
- An Introduction to Fingerprint Images

## 2.1 Interface

The main window of Tour is divided into 4 areas: Fingerprint Display Area, Control Area, Status Area, and Sample Area.

Area		Description
Fingerprint Display		Display scanned fingerprint image
Control	Scan	Click "Scan" to scan a fingerprint.
	Help	Click "Help" to get help.
	Exit	Click "Exit" to quit from the tour.
Status		Display current status.
Sample		Display common fingerprint sample images for comparison.

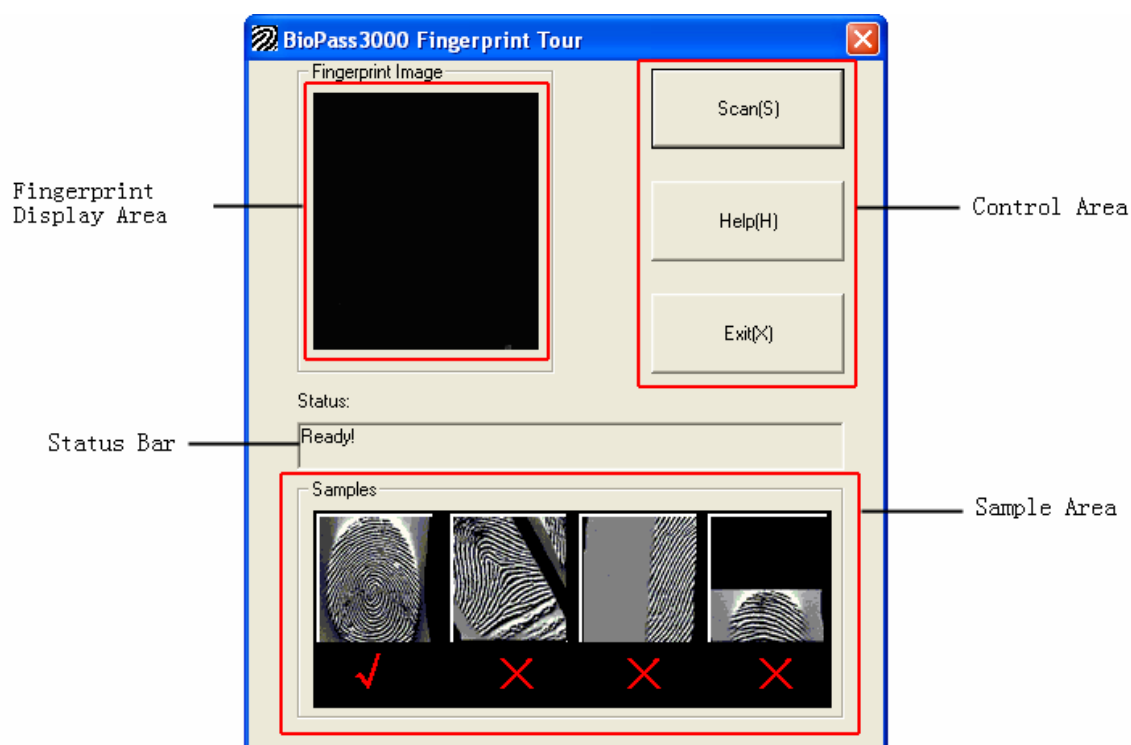


Fig. 2.1 Main window

## 2.2 Usage

After connected a BioPass3000 token, start the Fingerprint Tour. Click "Scan" button in Control Area, then wipe your finger through the grey sensor bar of the token. The Display Area will

render your fingerprint image. You can see whether your input is correct or not by comparing it with the sample images.

## 2.3 An Introduction to Fingerprint Images

### 2.3.1 Applicable Fingerprint Images

For a high quality fingerprint image, the following requirements should be met:

- The fingerprint central point is located at the central area of the image
- The fingerprint image is centered without excursion
- The image is clear and has no noises
- The texture is clear and complete
- The image is close to the scan area
- High contrast

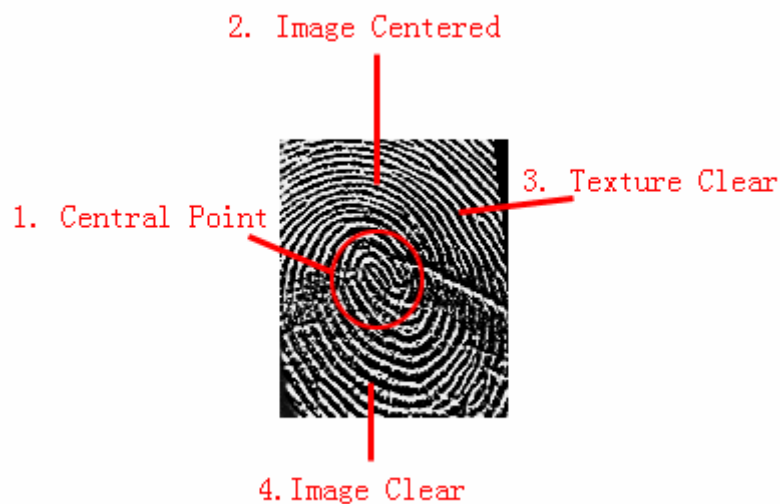


Fig. 2.2 Applicable Fingerprint Image

The following are two applicable fingerprint images:



Fig. 2.3 Example 1



Fig.2.4 Example 2

### 2.3.2 Inapplicable Fingerprint Images

As the fingerprint sensor of the product works by sensing the difference in temperature between the ridge and the valley, sometimes the quality of the fingerprint image is poor for some reasons. These reasons are:

1. The finger is somewhat wet. The image is dark with low contrast.



Fig. 2.5 Wet Finger

2. The skin of finger is broken or partly desquamative. Some part of the image is not clear.

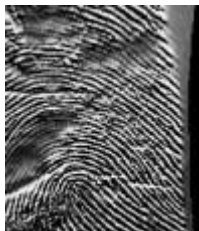


Fig. 2.6 Break or Partly Desquamative

3. The finger has a scar or scars. There are one or more imprints on the image.



Fig. 2.7 Scars

4. The finger is worn severely. Large area of the image is not clear. The image does not present a 3D look and feel.



Fig. 2.8 Worn

Incorrect input could lead to a recognition failure. You should avoid the following ways to scan your fingerprint:

5. The finger excurses (or nearly) out of the scan panel of the sensor when scanning.



Fig. 2.9 Excursive

6. The finger inclines greatly when scanning.



Fig. 2.10 Inclined

7. The finger slides too fast when scanning.



Fig. 2.11 Too Fast

8. The finger does not fully contact the sensor when scanning.



Fig. 2.12 Not Fully Contact Sensor

9. The fingerprint itself is damaged.



Fig. 2.13 Damaged Fingerprint

## 3 Using the Token with the Software

This chapter covers the following topics:

- How to Connect the Token to the Computer
- Product View
- How to Hold the Token
- How to Slide the Finger
- Usage Examples

### 3.1 How to Connect the Token to the Computer

Use USB wire (standard part) to connect the BioPass3000 token to the computer. The Mini USB port is connected to the token, while the standard USB port is connected to the computer. See the following figure.

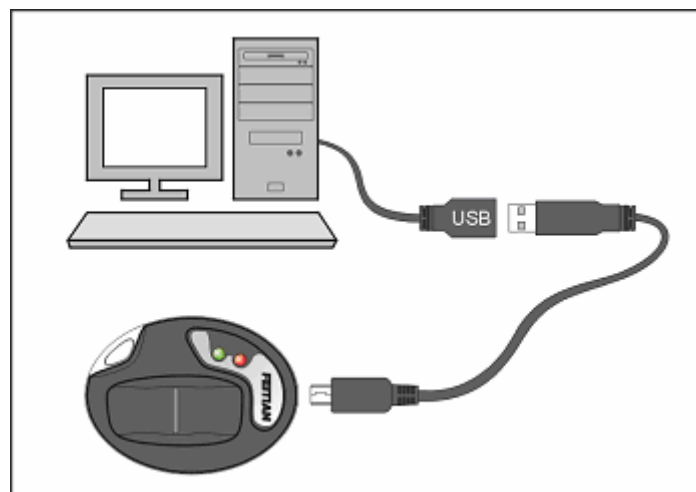


Fig. 3.1 Connection Method

### 3.2 Product View

The following is the product view.



Fig. 3.2 Product View

① Mini USB port

The BioPass3000 token is equipped with a Mini USB port, so that it is easy to connect the token to the computer. BioPass3000 token is a low power consumption product. It is powered through the USB port without the need of external power supply.

② ③ LED

The token has two LED indicators to show the token's working status.

Red	On	Idle
	Off	Processing
Green	On	Waiting for scanning
	Off	Scanning finished

④ Sensor

⑤ Key Hole

### 3.3 How to Hold the Token

You can hold the token in whatever way applicable to scan your finger. The following are two frequently used methods:





Fig. 3.3 Method 1



Fig. 3.4 Method 2

### 3.4 How to Slide the Finger

The finger should slide from one side to another side along the groove. The finger must fully contact the sensor.



Fig. 3.5 Sliding Example 1



Fig. 3.6 Sliding Example 2

Note: The sensor scans the fingerprint image through the temperature difference between the ridge and the valley. To generate a high quality image, the sensor tries to increase the temperature difference comparative to the finger by heating. You may feel somewhat hot when sliding your finger on the groove. Please take it easy, because the highest temperature of the sensor is merely 50°C and you could firmly slide your finger as quickly as possible, if applicable, when inputting your fingerprint.

## 3.5 Usage Examples

When the token is connected to the computer and Fingerprint Tour is opened, click “Scan” button. Then slide your finger on the sensor. After that, your fingerprint image is displayed in the fingerprint display area of Fingerprint Tour. You can learn whether your input is correct by comparing your fingerprint image with the samples. This process is introduced as follows.

1. Click “Scan” button. The green LED then will be turned on. The red LED then will be turned off.

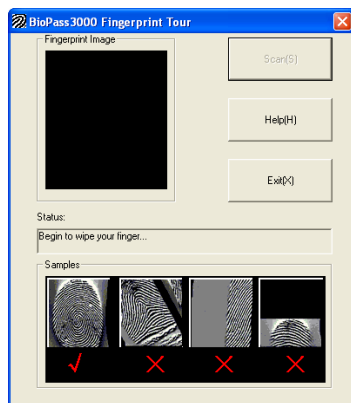


Fig. 3.7 Scanning Finger



Fig. 3.8 LEDs

You can wipe your finger here.

Note: If you click “Exit” after “Scan” without sliding your finger, the program will wait 10 seconds to quit. To avoid long time waiting, you can touch the sensor once before clicking “Exit”.

2. Before sliding the finger, please place your finger on one side of the groove without touching the sensor.



Fig. 3.9 Before Sliding Finger

Slide your finger gently along the groove in even and medium speed (0.5s).



Fig. 3.10 How to Slide

3. When done, the green LED then will be turned off and the red LED then will be turned on. The scanned image will be presented in the display area of Fingerprint Tour. Observing whether the scanned fingerprint is good or not, you can repeat exercising and trying to get qualified fingerprint images.



Fig.3.11 Scan Successful

# Appendix 1 Frequently Asked Questions

## 1. Why my token cannot be recognized by the system and New Hardware Found message appears?

In this case, it is likely caused by device driver is not installed or not installed properly. Please make sure that you have run BioPass3000-English.exe under redist directory in the SDK package before you use the BioPass3000 token for the first time. If this problem persists, please uninstall the driver and reinstall it after rebooting your system.

## 2. How to register my fingerprint?

Please refer to User's Guide Section 1.3.2.

## 3. What's the initial password? For what it is used?

When the token is used for any security purposes, such as requesting a certificate, signing etc., the user must be authenticated before using the device. For BioPass3000, the user must verify his/her fingerprint with registered fingerprint. However, the BioPass3000 contains no fingerprint when it is initially shipped from manufacturer. To facilitate the users and protect the token, we provide an initial password. You can take it as a user password to active your token, and then replace it your registered fingerprint. , such as certificate related operations and registering first fingerprint if you have not registered a fingerprint yet. The initial password can be acquired from your device distributor. Once you have registered a fingerprint, the initial password will be invalidated.

## 4. Why I can't register my fingerprint successfully, or pass the verification?

Refer to Section 2.3.2. Learn how to register and verify your fingerprint by reading Chapter 2 and 3.

## 5. Why I can't login with smart card?

Refer to The CAPI applications for BioPass3000 for smart card logon. To login with smart card, the following requirements must be met: a) Your computer has joined a domain; b) You have registered a fingerprint; c) There is at least a smart card logon certificate on the token; d) You have chosen the option to support smart card logon. Using the initial password for smart card logon is not supported currently.

## 6. Why I often have problems with token connection?

Check if your USB cable is firmly connected with the USB port or the Mini USB port. Bad connection could lead to the problem.

## Appendix 2 Terms and Abbreviations

Terms and Abbreviations	Description
BioPass3000	A portable USB device introduced by Feitian Technologies, which integrates a fingerprint sensor and recognition module, a smart card and a USB port. It employs fingerprint protection, instead of password protection.
Token	A general definition for cryptographic devices. It can be a smart card, or any devices that can store keys and certificates.
USB Token	A cryptographic device with a USB port. It is portable and easy to use. Herein, BioPass3000 is a token.
Initial Password	A password we provide when shipping for registering a first fingerprint, which is invalidated after the registration of the first fingerprint.
CryptoAPI (CAPI)	A cryptography interface developed by Microsoft Corporation, providing a cryptographic algorithm package that is independent from the device or software implementation, which facilitates the developer in making PKI applications for data encryption/decryption, authentication with digital certificates and encoded signature on the Windows platform.
PKCS#11	A programming interface developed by RSA Laboratories, which digests the cryptographic device as a general logic view (i.e. cryptographic token) providing for upper level applications. It provides device independency and resource sharing.