EnterSafe

Shuttle User Guide

Ver.1.0

www.EnterSafe.com

EnterSafe will do their best to keep the content of this document as accurate as possible. But EnterSafe 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.

Editing History:

Date	Version	Edition
Jan 15th, 2009	1.0	1st Edition

Software Developer's Agreement

IMPORTANT - READ CAREFULLY: This Software Developer's Agreement (SDA) is a legal agreement between you (either an individual or a single entity) and EnterSafe Corporation for the software that accompanies this SDA, which includes computer software and may include associated media, printed materials, "online" or electronic documentation, and Internet-based services ("Software").YOU AGREE TO BE BOUND BY THE TERMS OF THIS SDA BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE. IF YOU DO NOT AGREE, DO NOT INSTALL, COPY, OR USE THE SOFTWARE; YOU MAY RETURN IT TO YOUR PLACE OF PURCHASE FOR A FULL REFUND, IF APPLICABLE..

1. GRANT OF LICENSE. EnterSafe grants you the rights described in this SDA provided that you comply with all terms and conditions of this SDA.
1.1 EnterSafe grants you a limited, nonexclusive license to use the Software, and to make and use copies of the Software, for the purposes of designing, developing and testing your software applications.
1.2 EnterSafe grants you to merge and link the Software with other programs for the sole purpose of protecting those programs in accordance with the usage described in the Developer's Guide.
1.3 You may make archival copies of the Software. If EnterSafe makes a request via public announcement or press release to stop using the copies of the Software, you will comply immediately with this request.

2. LIMITATIONS ON REVERSE ENGINEERING, DECOMPILATION, AND DISASSEMBLY. You may revise, reverse engineer, decompile, disassemble, enhanced or otherwise modified the Software, except only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.
3. NO RENTAL OR COMMERCIAL HOSTING. You may not rent, lease, lend or provide commercial hosting services with the Software.

4. LIMITATION OF LIABILITY AND REMEDIES. Notwithstanding any damages that you might incur for any reason whatsoever (including, without limitation, all damages referenced herein and all direct or general damages in contract or anything else), the entire liability of EnterSafe and any of its suppliers under any provision of this SDA and your exclusive remedy hereunder shall be limited to the greater of the actual damages you incur in reasonable reliance on the Software up to the amount actually paid by you for the Software.

5. DISCLAIMER OF WARRANTIES. To the maximum extent permitted by applicable law, EnterSafe and its suppliers provide the Software and support services (if any) AS IS AND WITH ALL FAULTS, and hereby disclaim all other warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the Software and the provision of or failure to provide support or other services, information, software, and related content through the Software or otherwise arising out of the use of the Software. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NON-INFRINGEMENT WITH REGARD TO THE SOFTWARE.

6. RESERVATION OF RIGHTS AND OWNERSHIP. EnterSafe reserves all rights not expressly granted to you in this SDA. The Software is protected by copyright and other intellectual property laws and treaties. EnterSafe own the title, copyright, and other intellectual property rights in the Software.

7. TERMINATION. This SDA is effective until terminated. Upon any violation of any of the provisions of this SDA, rights to use the Software shall automatically terminate and the Software must be returned to EnterSafe or all copies of the Software destroyed. You may also terminate this SDA at any time by destroying all copies of the Software in your possession or control. The provisions of paragraphs 2, 3, 4, 5 and 6 will survive any termination of this SDA.

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 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.

Technical Terms and Abbreviations

Terms	Explanation
PKCS#11Interface	Software programming interface which is presented by RSA (www.rsasecurity.com). It maps cryptographic devices into a type of universal logical model, i.e. Cryptographic Token, for the usage of system's upper applications. This design could achieve the device independent and resource sharing.
CryptoAPI interface (CAPI for short)	Cryptographic operation interface presented by Microsoft. It provides device independent or software implemented cryptographic algorithms' encapsulation, which is easy to use for developers to design their own PKI applications, including data encryption, certificate verification and digital signature, under Windows® platform.
Token	General name of all cryptographic devices, such as smartcards, devices having passwords and certificates storage functionalities etc.
USB Token	Cryptographic devices with USB port. Portable and easy to use.
ePass2001	Portable cryptographic device integrates smartcard and USB port, which is released by Feitian. It inherits the advantages of smartcard device and also portable. Supporting PKI applications.
ePass3003	The same as ePass2001, but functions is better than ePass2001's.
ePass3003Auto	The same as ePass3003, but it haves flash stored of window's library.

Catalog

Chapter 1 Shuttle Introduction

Shuttle is a new generation platform independent data security products framework.
It mainly provides hardware supports to upper layer of PKI applications. The certificates, key pairs and other classified information are all stored in ePassToken. Shuttle provides standard PKCS#11 and CryptoAPI programming interfaces to support standard PKI applications. It is easy to be redeveloped by ISVs (Independent Software Vendors) for their end users.

Chapter 2 EnterSafe PKI Manager

The interface and operating method of EnterSafe PKI Manager are similar under different system platforms so as to provide more convenience to users. Furthermore, ePass2001, ePass3003 and ePass3003Auto share the same Manager.
There are two versions of EnterSafe PKI Manager: administrator edition and end user edition. Administrator edition provides more functions, such as “Initialize Token”, “Unblock Token” and “Change SO PIN”.
To let you know how to use the administrator edition of EnterSafe PKI Manager with ePass2001 product under Linux system, this chapter will explain the following functions(This document describes with RedHat 9.0):

- Initialize Token (Only applicable for administrator edition)
- Unblock Token (Only applicable for administrator edition)
- Change SO PIN(Only applicable for administrator edition)
- Login (Verify user PIN)
- View Token and Slot Information
- Change User PIN
- Change Token Name
- Manage Token Data

2.1 Precondition

Because EnterSafe PKI Manager is based on Shuttle middleware and will access hardware token, before using EnterSafe PKI Manager, please confirm the Shuttle library have been installed properly.

2.2 Profile

2.2.1 Interface without Token plugged in

Run EnterSafe PKI Manager, system will display the interface like figure 2-1:

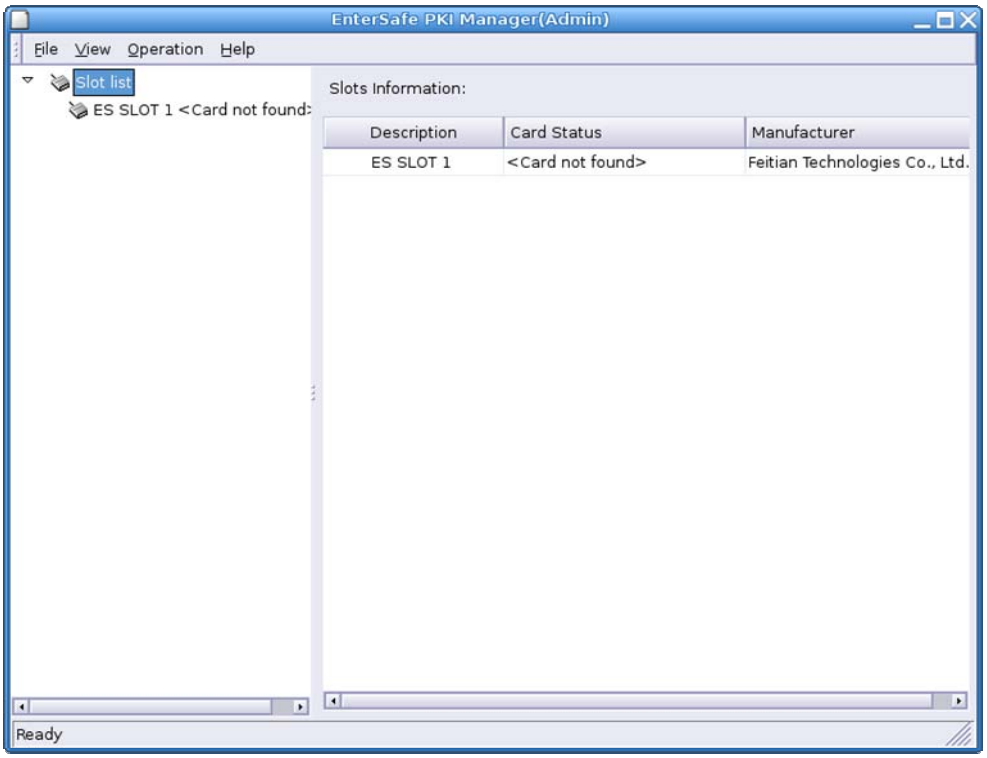

Figure 2-1 Interface without Token plugged in

Left column lists all the supported slots. Right column briefs the basic information of these slots.

2.2.2 Interface with Token plugged in

Plugging an USB token named “ePass Token” in USB port of the computer, the EnterSafe PKI Manager will recognize the basic information of the token and display the interface like figure2-2：

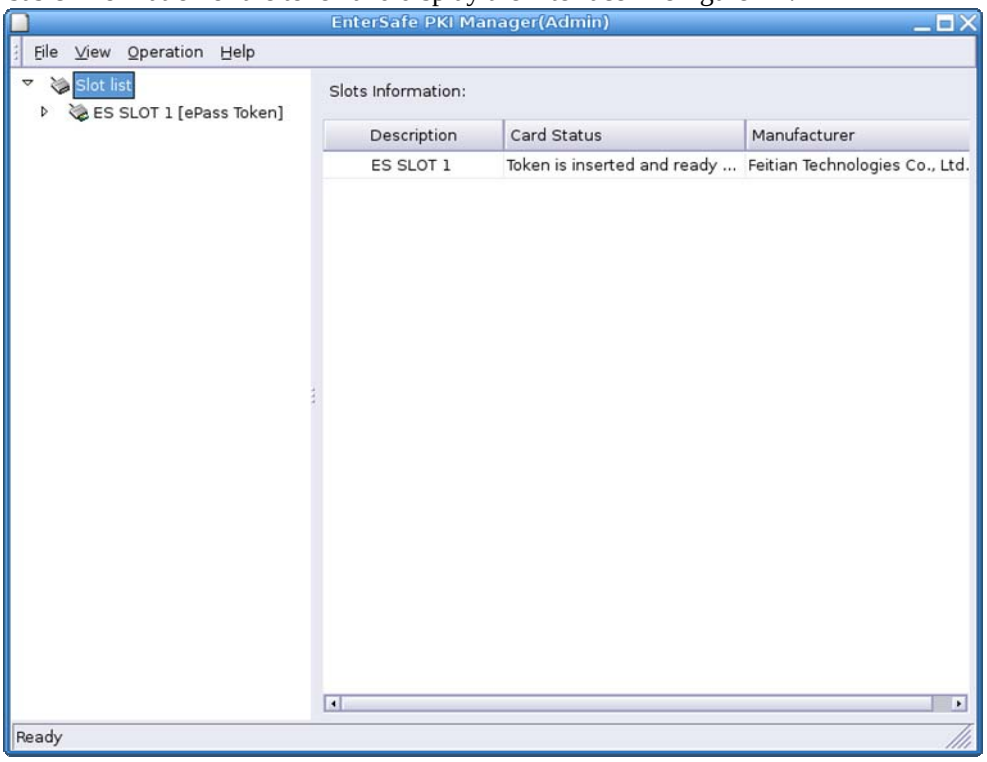

Figure2-2 Interface with Token plugged in

2.2.3 Menu of EnterSafe PKI Manager

Like figure 2-3:

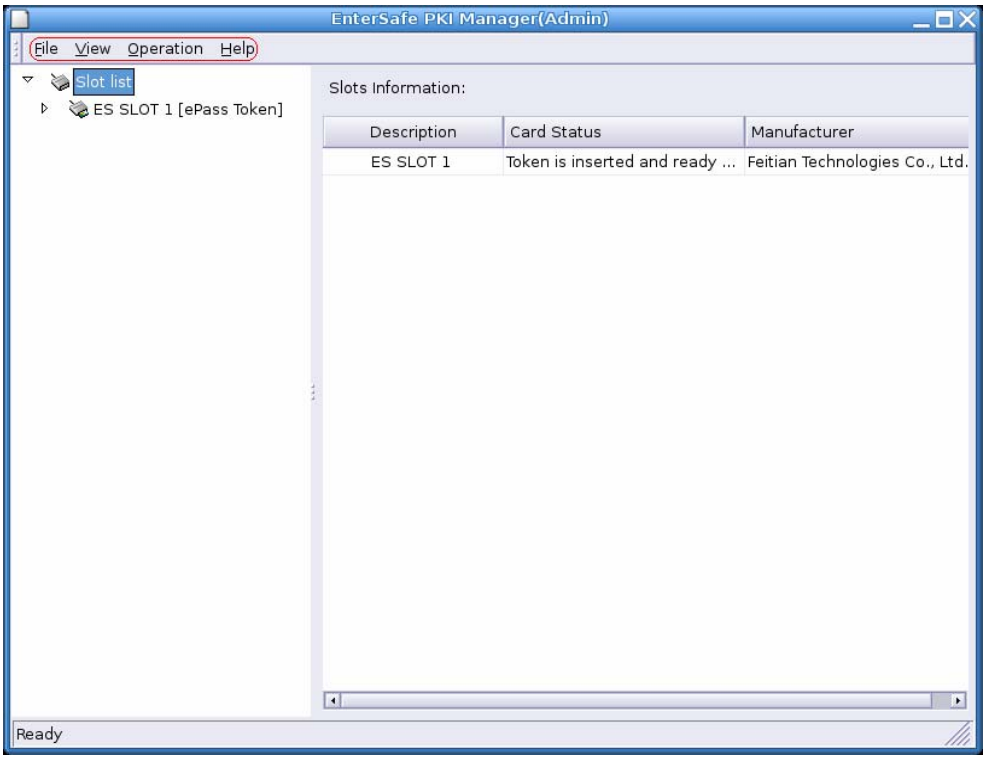

Figure2-3 menu of the Manager

The main menu includes: File (exit the Manager and select a language), View (Check information of the slot), Operation (Operations about the slot) and Help (Version Information).

2.2.4 “Operation” Menu

Detailed options refers to figure 2-4：

Figure 2-4 Options in “Operation” Menu

Drop down menu lists the applicable options.

2.2.5 “View” Menu

Detailed options refers to figure 2-5：

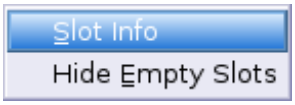

Figure 2-5 Options in “View” Menu

2.2.6 Right-Click Menu in Slot Tree

Right-click on any slot listed in left-side slot tree, system will prompt the menu shown in figure 2-6：

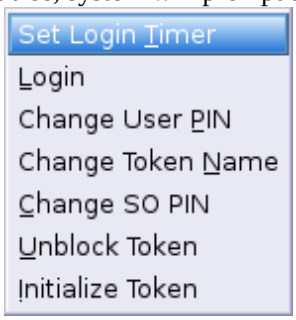

Figure 2-6 Right-Click Menu in Slot Tree

Operations includes “Set Login Timer”, “Login”, “Change User PIN”, “Change Token Name”, “Change SO PIN”, “Unblock Token” and “Initialize Token”.

2.2.7 Information Displayed After Plug in Token

Click on any slot, its information and related possible operations will be displayed in right hand side, like figure 2-7：

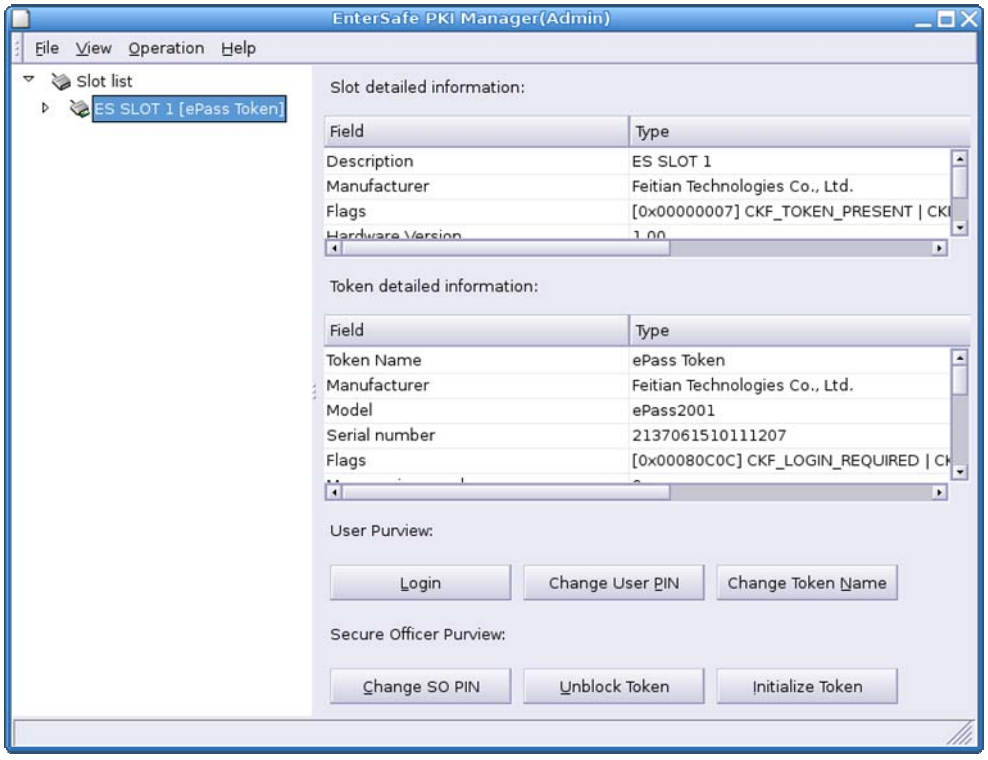

Figure 2-7 Information Displayed After Plug in Token

Information displayed in right includes the slot status, token detailed information and all of the possible operation buttons. Buttons which are currently not applicable will be disabled.

2.2.8 Information Displayed When No Token is Plugged in

Click any empty slot, the information displayed looks like figure 2-8:

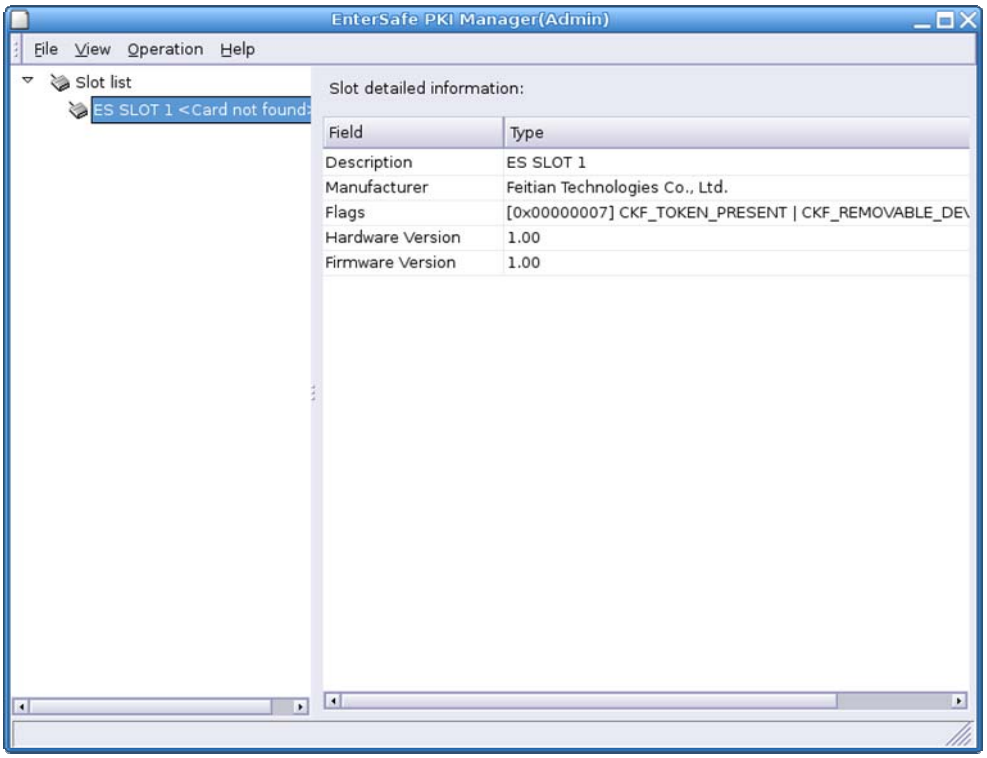

Figure 2-8 Information Displayed When No Token is Plugged in

Shuttle supports multiple tokens. Choose any token, user could process operations demonstrated in figure 2-4, figure 2-6 and figure 2-7.

2.3 Check Slot List Information

Click left hand side of the slot list or select "View→Slot info", system will display the slot's information like figure 2-1.

2.4 Check Token Information

Click left hand side of the slot list. The related information will be displayed in the right hand side. If a token is plugged in and it will display the token's detailed information like figure 2-7. If slot is empty, the information about the slot will be displayed like figure 2-8.

2.5 Login

Before login, user could only view public information of the token. Private information could only be retrieved after user login with the correct PIN number. Click on "Login", system will prompt the Token login dialog box like figure 2-9:

Figure2-9 Login Dialog

After inputted correct user PIN, click "OK" to login the PKI Manager.

2.6 Change User PIN

The initial user PIN of the token is “1234”, and you are recommended to change user PIN. By clicking “Change User PIN”. System will prompt the dialog box like figure 2-10:

Figure2-10 Change User PIN Dialog

When changing the user PIN, user must input the old user PIN, input the new user PIN and confirm the new user PIN. Then click “OK” to process the operation.

2.7 Change Token Name

Generally, token is distinguished by their serial number. But the serial number is not significative and hard to be remembered. Token name could also be used to identify a token. It could be specified by user’s will.

Click “Change Token Name”, system will prompt the dialog like figure 2-11:

Figure 2-11Change Token Name Dialog

Input any name for the token and click “OK”, system will refresh and display the token’s new name.

2.8 Change SO PIN

The initial SO PIN of the token is “*rockey*”. User could change it by click “Change SO PIN”. System will prompt the dialog box like figure 2-12:

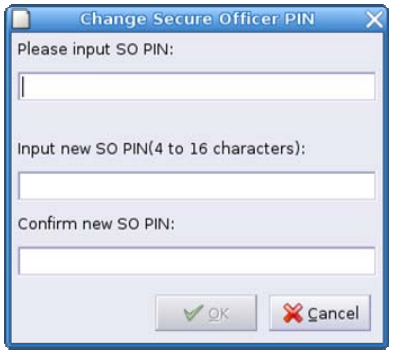

Figure 2-12 Change SO PIN Dialog

When changing the SO PIN, user must input the old SO PIN, input the new SO PIN and confirm the new SO PIN.

Then click “OK” to process the operation.

2.9 Unblock Token

When user failed to input the correct user PIN over a certain number, user PIN will be blocked. Even user input the correct user PIN again, token could not be accessed. Administrator must unblock the token by click “Unblock Token”. System will prompt the dialog box like Figure 2-13:

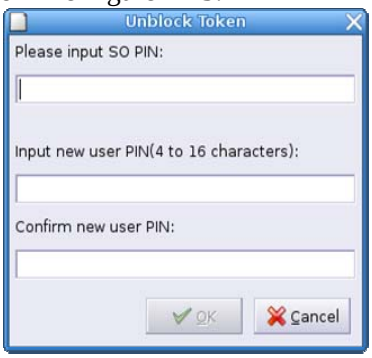

Figure 2-13 Unblock Token Dialog

To unblock the Token, SO PIN must be provided. The user PIN must be reset. After inputting and confirming the new user PIN, click “OK” to unblock the token. After unblocked the token, user could login with the new user PIN.

2.10 Initialize Token

This operation will clear all the information in the token and reset the token hardware into PKI operation hardware token.

WARNING: ALL the information in the token including PKI certificates, public and private keys and user data will be totally removed after you initialize the token.

Click “Initialize Token”, system will prompt the dialog like figure 2-14:

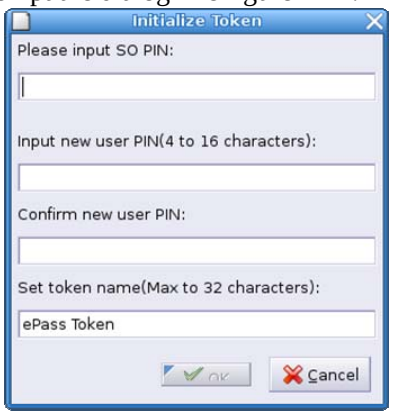

Figure 2-14 Initialize Token Dialog

Initializing token needs administrator input SO PIN. user PIN and the token name must be reset. All the data in the token will be erased. After successful initialization, system will refresh and change to token’s login state.

2.11 Data Management in Un-login State

In the left area of the PKI Manager, each token has a data management function. Click it in un-login state, system will display token’s public information and related possible operations in right hand side like figure 2-15:

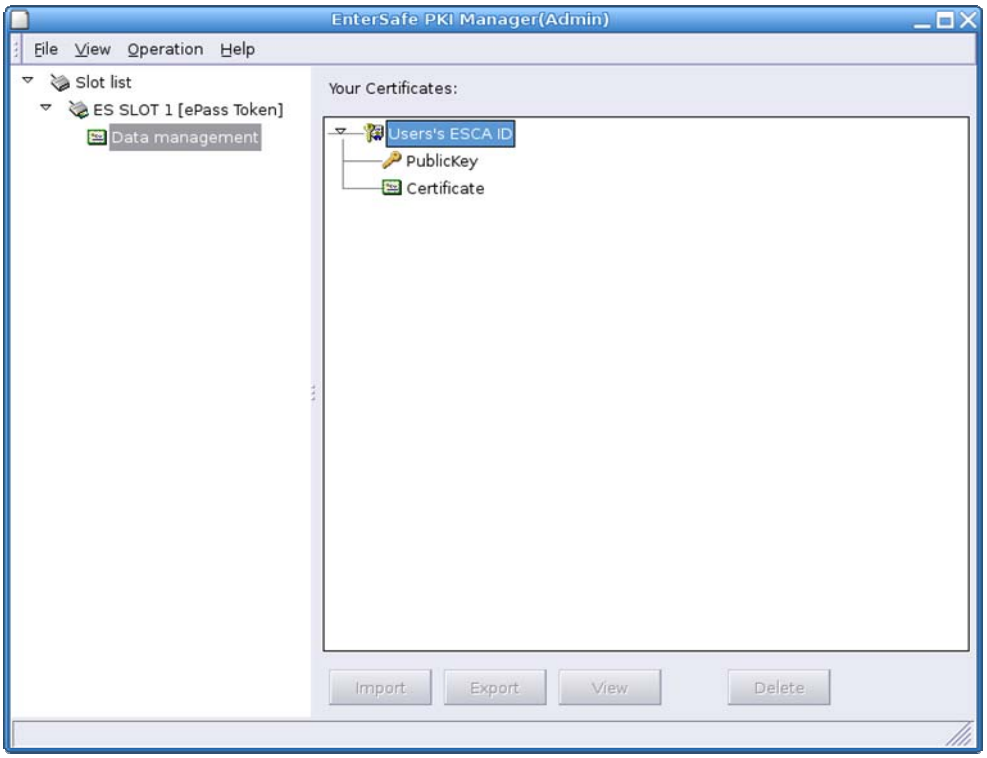

Figure 2-15 Data Management in Un-login State

2.12 Data Management in Login State

After user login the token, system interface looks like figure 2-16:

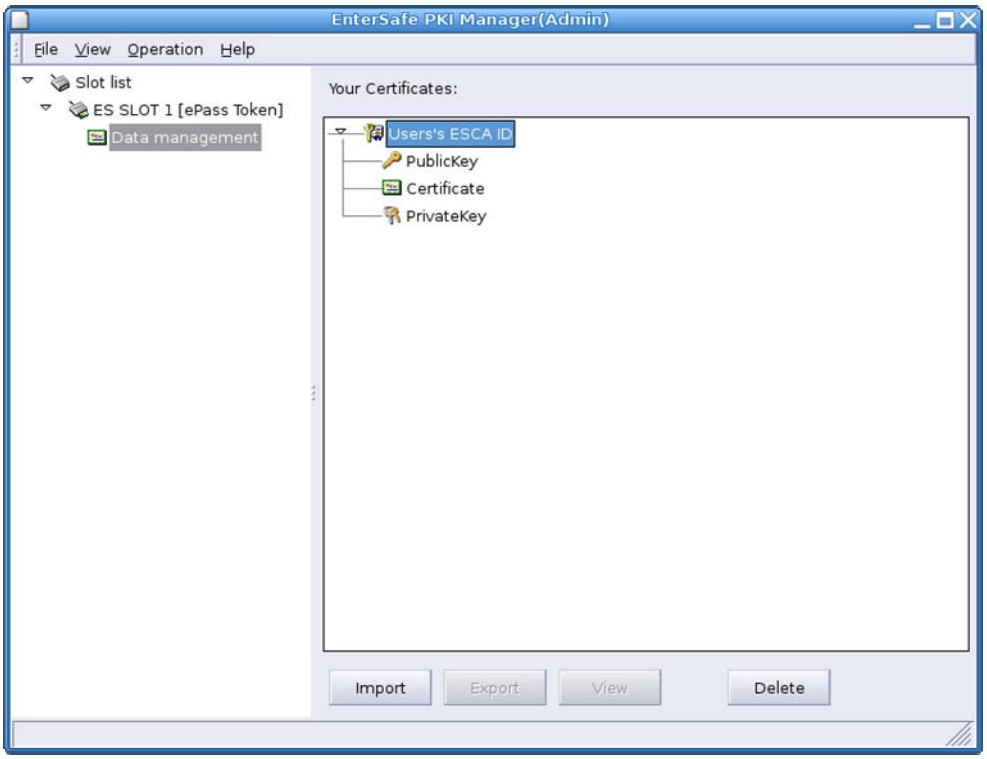

Figure 2-16 Data Management in Login State

After login, user could view both token's public information and private information. "Import" button will only be

enabled after user login. “Export” button will be enabled when a certificate is selected. “View” button is always enabled except for contain name. “Delete” button is always enabled when login.

After user login, “Login” button will be disabled, demonstrating the token has changed into login state, like figure 2-17:

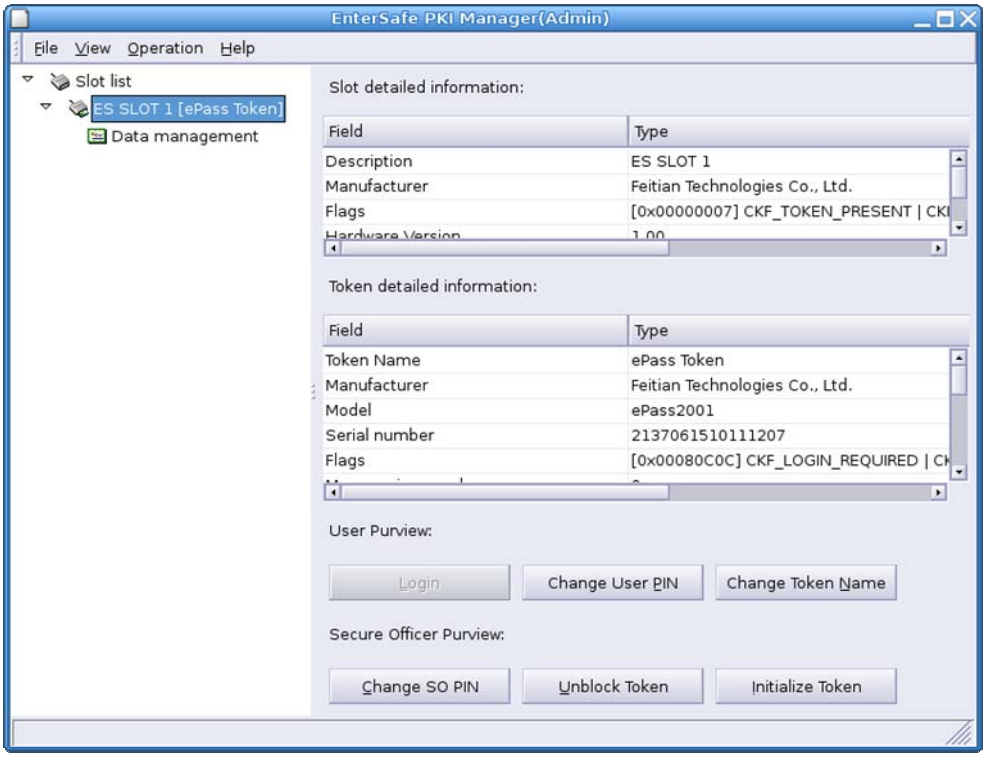

Figure 2-17

2.13 Import Certificate

When user wants to import P12，P7B，CER，PFX，CRT certificate into the token, click “Import”. System will prompt the dialog box like figure 2-18:

Figure 2-18 Import Certificate Dialog box 1

Only P12 and PFX certificate needs to confirm certificate password. Importing other types of certificate, system will disable the password gap. Click “…” button and choose the certificate that needs to be imported, confirm the correct certificate access password and click “OK”, system will import the certificate into the token and refresh automatically, like figure 2-19 and figure 2-20:

Figure 2-19 Import Certificate Dialog 2

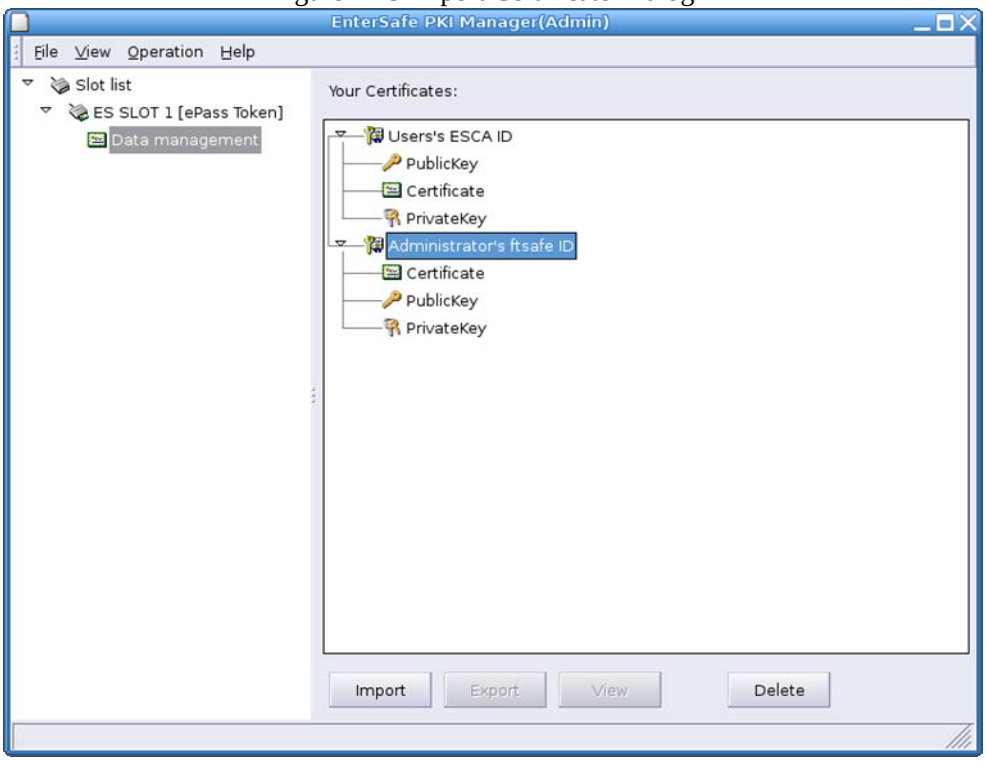

Figure 2-20 Data Management Interface after Certificate Imported

2.14 Export Certificate

When user wants to export a certificate, click on “Export” and the system will prompt the dialog like figure 2-21：

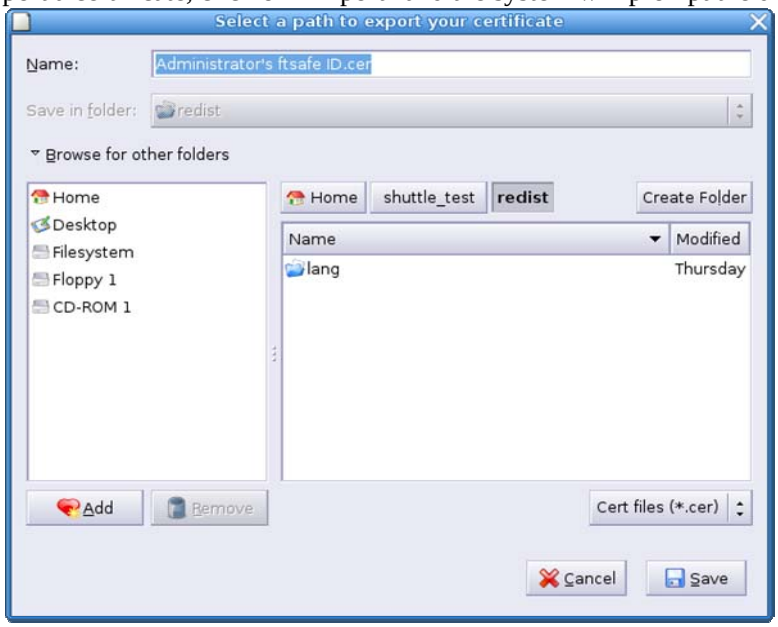

Figure 2-21 Certificate Export Dialog

Click “Browse for other folders” button and choose the directory. Then click “OK” to export the certificate.

2.15 View Data Information

When user wants to view detailed information of certificate, public key, private key and other data, user could select a special item and click “View”. System will prompt the dialog box like figure 2-22:

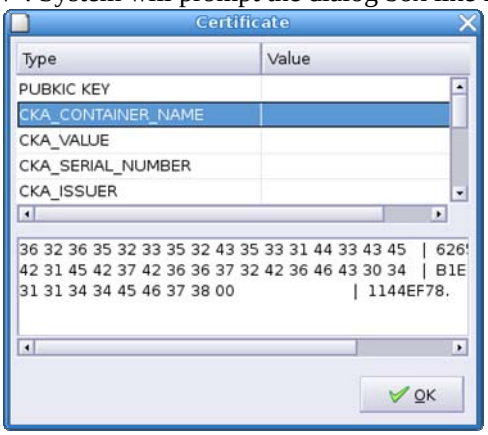

Figure 2-22 View Certificate Information Dialog

To view other data information (such as public key, private key or other data), system will prompt the dialog box like figure 2-23:

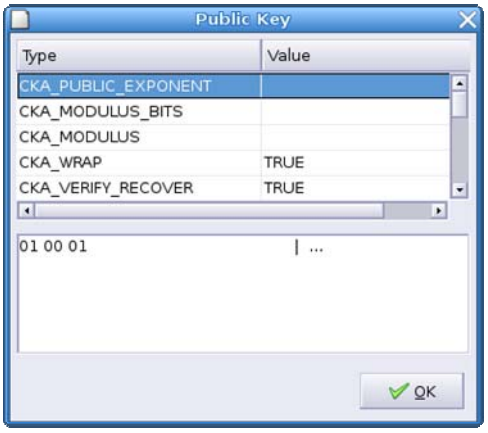

Figure 2-23 View Public Key Information Dialog

Click on any attribute button, its detailed information will be displayed in the bottom.

2.16 Delete Data

When user wants to delete data in the token, after login, select the information to delete and click on “Delete”. System will prompt the dialog box like figure 2-24:

Figure 2-24 Delete Data Dialog

Data can not be retrieved after the delete operation.

Chapter 3 ePass's Product

3.1 ePass2001

Features:

- On-board generation of RSA 512/1024-bits key pair
- Built-in support for RSA, DES and 3DES algorithms
- Full support for PKI applications, CSP and PKCS#11 interfaces available
- Standard support for Microsoft CAPI applications
- Support for X.509 v3 standard certificate format
- Seamless integration with Internet Explorer
- No hardware driver needed
- Random number generation performed in hardware
- Powerful Plug & Play connectivity to PKI applications
- Digital signature signed in hardware
- Support for multiple PKI applications
- Standard USB interface
- CE and FCC Conformity Certified
- Tamper evident hard plastic casing
- Multiple color options and third party branding available
- Support for Windows 98SE/Me/2000/XP/Server 2003/Vista linux

3.2 ePass3003

Features:

- On-board generation of RSA 512/1024/2048-bits key pair
- Built-in support for RSA, DES and 3DES algorithms
- Full support for PKI applications, CSP and PKCS#11 interfaces available
- Standard support for Microsoft CAPI applications
- Support for X.509 v3 standard certificate format
- Seamless integration with Internet Explorer
- No hardware driver needed
- Random number generation performed in hardware
- Powerful Plug & Play connectivity to PKI applications
- Digital signature signed in hardware
- Support for multiple PKI applications
- Standard USB interface
- CE and FCC Conformity Certified
- Tamper evident hard plastic casing
- Multiple color options and third party branding available

- Support for Windows 98SE/Me/2000/XP/Server 2003/Vista linux

3.2 ePass3003Auto

Features:
- The same as ePass3003
- ePass3003Auto have flash stored of window's library