



Trusted Key PKI Cryptographic Module

Part No: Trusted-Key-PKI-X15

Firmware Version No: V1.0.11

User Guide

Document Version: V1.0

Date: April 6th, 2021

International Copyright© Mobile-ID Technologies And Services Joint Stock Company (Mobile-ID™). All rights reserved. This document is the property of Mobile-ID™. and as such may only be distributed, partly or in full, in lieu of a non-disclosure agreement (NDA). Permission to copy and implement the material contained herein is granted subject to the conditions of the aforementioned NDA and that any copy must bear this legend in full, that any derivative work must bear a notice that it is a Mobile-ID™. copyright document jointly published by the copyright holders, and that none of the copyright holders shall have any responsibility or liability whatsoever to any other party arising from the use or publication of the material contained herein.

Document Revisions

Version	Date	Description	Author
1.0	20210406	First submission	KHANHPX

Contents

Document Revisions	2
Contents	1
1. Software Developer's Agreement	1
2. Runtime Installation	2
2.1. Supported Platform	2
2.2. Preparing for installing Trusted Key PKI.....	2
2.3. Installing Trusted Key PKI Runtime.....	2
2.4. Uninstalling Trusted Key PKI Runtime	4
3. Trusted Key PKI Token Manager	7
3.1. Prerequisite	7
3.2. Overview.....	7
3.2.1. Interface without USB token insertion	7
3.2.2. Interface with USB token insertion.....	7
3.2.3. Interface Buttons.....	8
3.3. Login	8
3.4. Certificate Management	9
3.4.1. Viewing Certificate Information.....	9
3.4.2. Importing	10
3.4.2.1. Importing PFX Certificate	10
3.4.2.2. Importing P7B Certificate	11
3.4.3. Exporting.....	12
3.4.4. Deletion	13
3.5. Changing Token Name	13
3.6. Changing User PIN	14
3.7. Unblocking (Admin Version Only)	16
3.8. Initializing (Admin Version Only)	17
3.9. Changing SO PIN (Admin Version Only).....	18
4. Windows PIN Management	20
4.1. Overview.....	20
4.2. Mobile-ID Minidriver PIN Management for Windows	20
4.2.1. Changing a User PIN	20
4.2.1.1. Changing a User PIN with Windows 2000, XP or Server 2003	20
4.2.1.2. Changing a User PIN with Windows Vista, 2008 and Windows 7	21
4.2.2. Unblocking Mobile-ID Minidriver	22
4.2.2.1. Example Unblock Procedure	22
4.2.2.2. Unblocking a Smart Card with Windows 2000, XP or Server 2003	23
4.2.2.3. Unblocking a Smart Card with Windows Vista, 2008 and Windows 7	23
4.2.2.3.1. Enabling Unblock Card with Windows Vista, 2008 and Windows 7	24
4.2.2.3.2. Unblocking a Smart Card with Windows Vista, 2008 and Windows 7	26
4.2.2.4. Administrator Tools for Card Unblock.....	26
5. Appendix: Terms and Abbreviation.....	28

1. Software Developer's Agreement

All Products of Mobile-ID Technologies And Services Joint Stock Company (Mobile-ID™) 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.

- 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.
- 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 Mobile-ID™ provided enhancement or upgrade to the Product.
- Warranty – Mobile-ID™ 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.
- Breach of Warranty – In the event of breach of this warranty, Mobile-ID™'s sole obligation is to replace or repair, at the discretion of Mobile-ID™, any Product free of charge. Any replaced Product becomes the property of Mobile-ID™. Warranty claims must be made in writing to Mobile-ID™ 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 Mobile-ID™. Any Products that you return to Mobile-ID™, or a Mobile-ID™ 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.
- Limitation of Mobile-ID™'s Liability – Mobile-ID™'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 Mobile-ID™ 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 Mobile-ID™ has been advised of the possibility of damages, or for any claim by you based on any third-party claim.
- 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.

2. Runtime Installation

2.1. Supported Platform

Windows platform:

- Windows 2000
- Windows XP x86/x64
- Windows 2003 x86/x64
- Windows Vista x86/x64
- Windows 2008 x86/x64
- Windows 7 x86/x64

Linux

macOS

2.2. Preparing for installing Trusted Key PKI

Before installing Trusted Key PKI 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)
- Trusted Key PKI available

2.3. Installing Trusted Key PKI Runtime

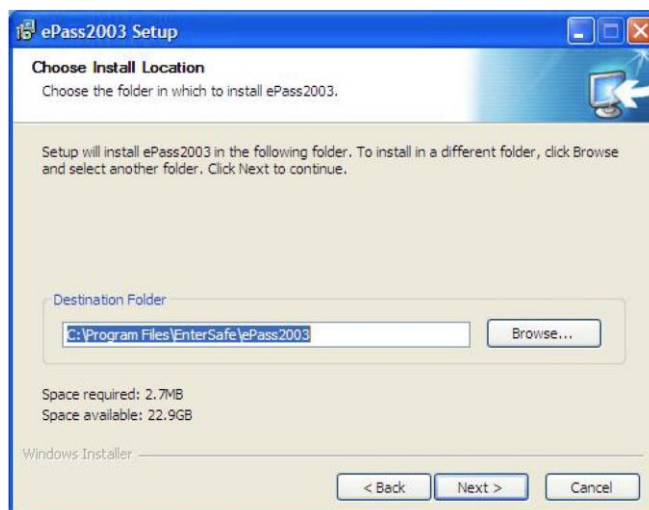
- Before you can use the Trusted Key PKI, you must install the Runtime library, execute TrustedKeyPKI-Setup.exe. The following select language interface appears:



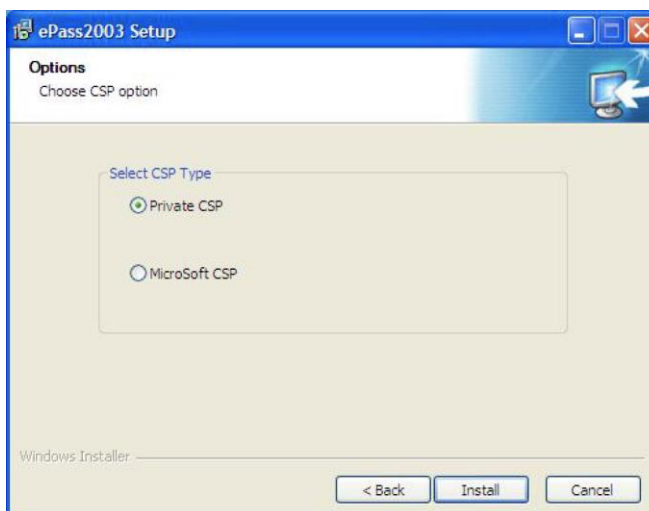
- After select language, click 'OK', the following welcome interface appears:



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



- Click "Next", the following choose CSP interface appears:



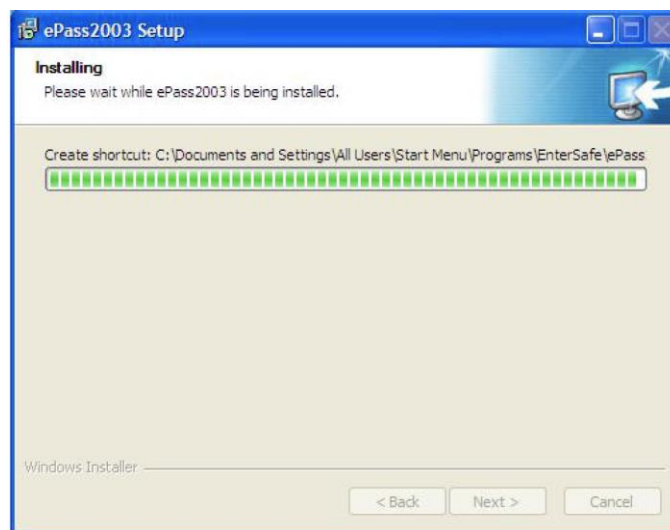
Note: Trusted Key PKI supports Private CSP and Microsoft CSP

For older windows systems such as Windows 2000/XP, users must install patch KB909520 to enable the option "Microsoft CSP"

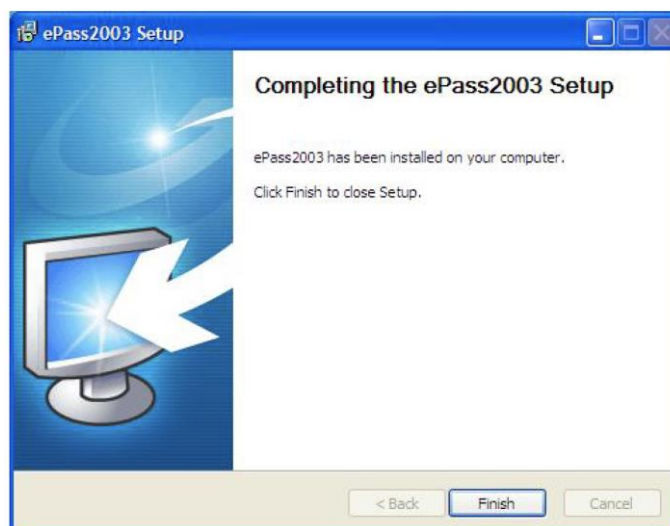
Private CSP is provided by Mobile-ID™, the CSP name "Trusted Key PKI Token CSP v1.0"

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.

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



- After install process finish, the following interface appears:



- Click "Finish" to finish the installation.

2.4. Uninstalling Trusted Key PKI Runtime

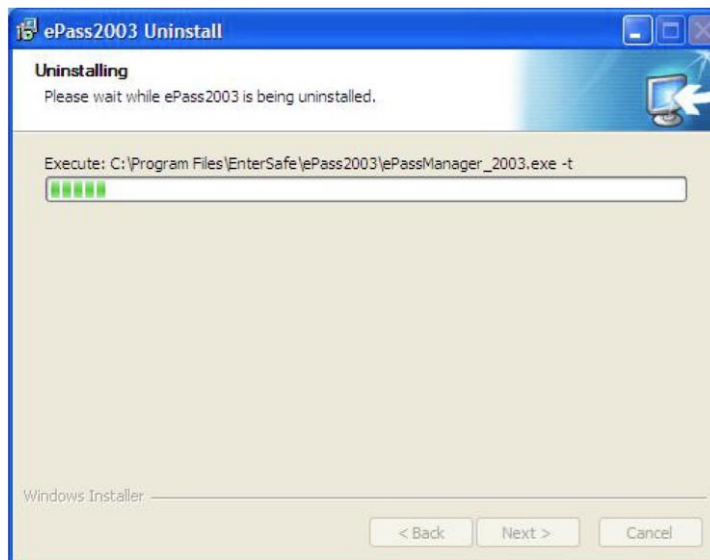
After install the Trusted Key PKI Runtime, you can uninstall it through following methods:

- Use "Add or Remove Programs" to uninstall: Open "Start" menu → Select "Control Panel", double click "Add or Remote Programs", choose "Trusted Key PKI (Remove only)" in the "Currently installed programs" list, then click "Change/Remove".
- Uninstall it from start menu: Open "Start" menu → "All Programs" → "Mobile-ID" → "Trusted Key PKI" → "Uninstall Trusted Key PKI Token Manager"

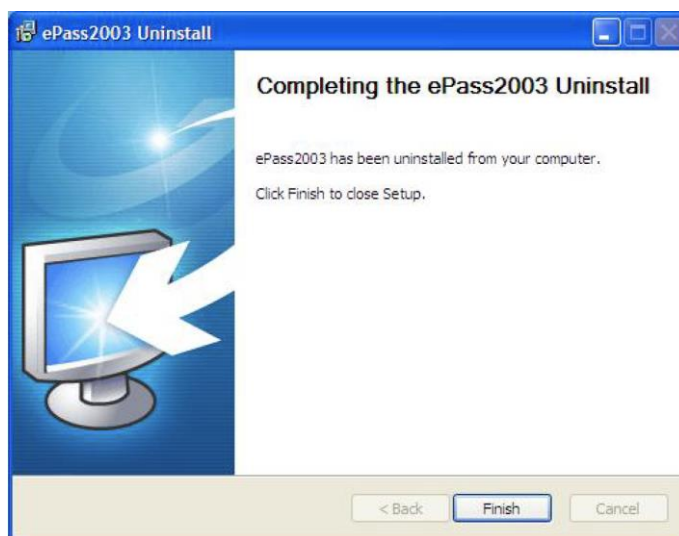
Both of above two methods can launch the Uninstall Wizard of Trusted Key PKI, see following interface:



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



After uninstall process finish, the following interface appears:



Click "Finish" to close uninstall wizard, now Trusted Key PKI has been uninstalled from your computer.

3. Trusted Key PKI Token Manager

3.1. Prerequisite

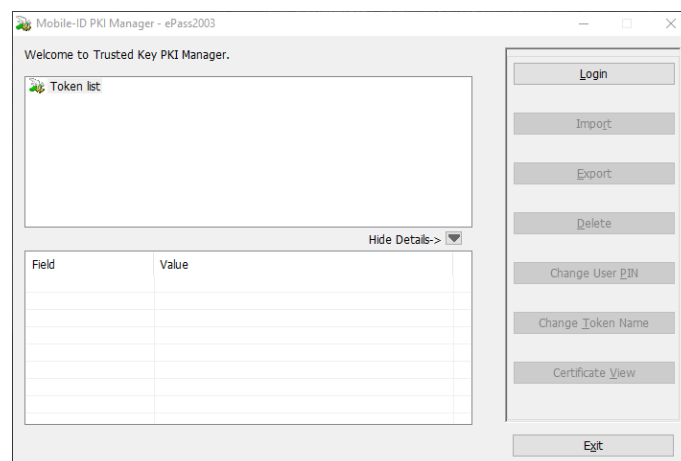
Because the Manager is based on the middleware of Trusted Key PKI and it needs to access the token, you must have installed Trusted Key PKI product on your computer before using the Manager.

The token must be PKI initialized before use

3.2. Overview

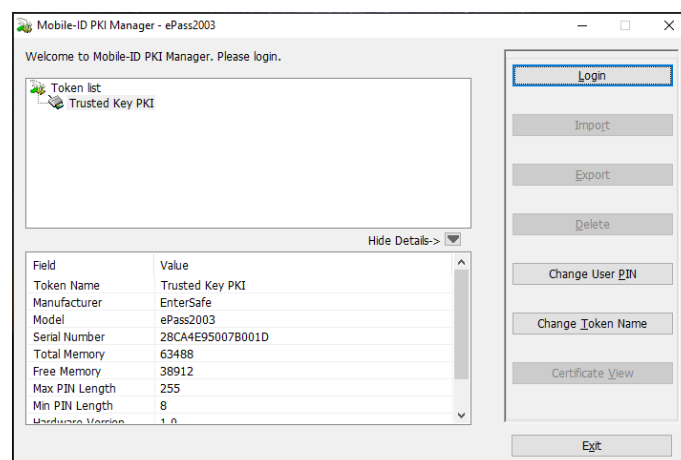
3.2.1. Interface without USB token insertion

You can find the shortcut for the Manager by clicking Start → All Programs → Mobile-ID → Trusted Key PKI Token Manager. Click the shortcut to start the Manager. The following interface appears:



3.2.2. Interface with USB token insertion

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



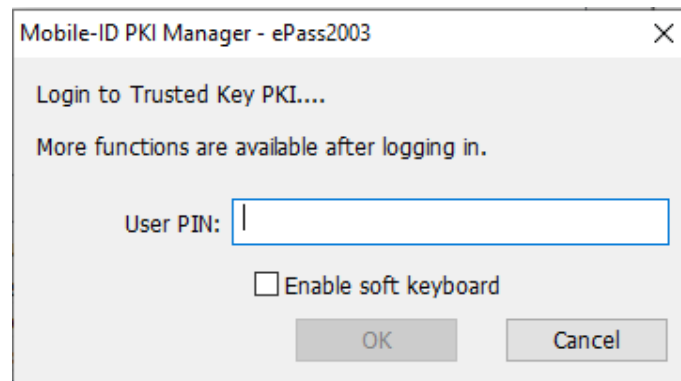
Note: The total private memory space and the free private memory space refer to the PIN protected spaces. Since the private key is extremely sensitive and it is managed by the COS, it doesn't show the total private memory space and the free private memory space.

3.2.3. Interface Buttons

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

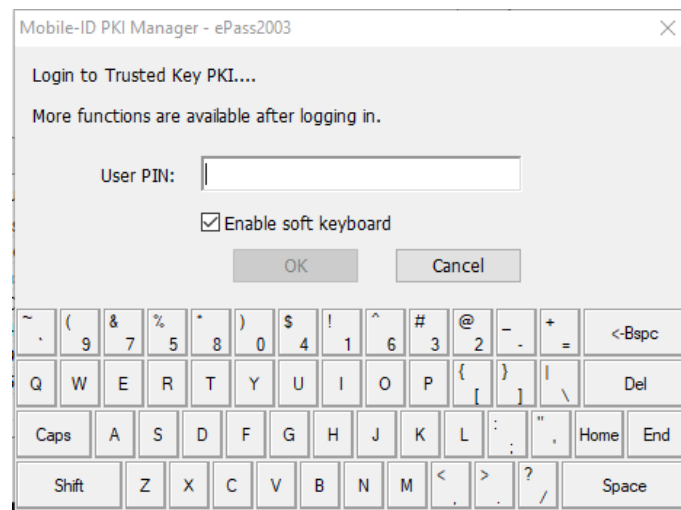
3.3. Login

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



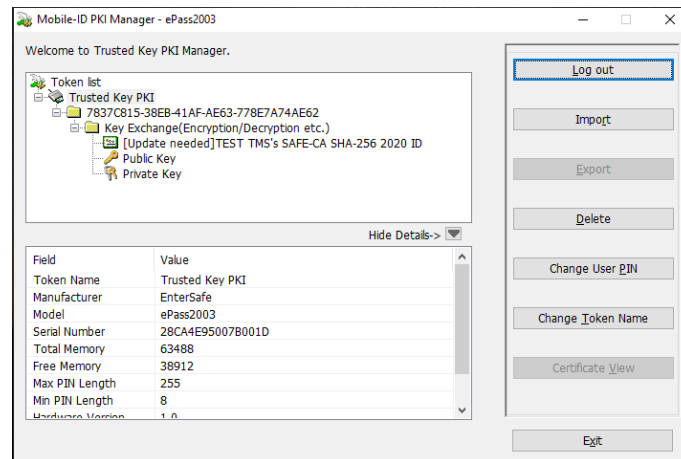
Note: When the PIN input dialog is displayed, the Manager will start the safe desktop. In this status, only the box is highlighted. Except input in the box, most of other operations are disabled.

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

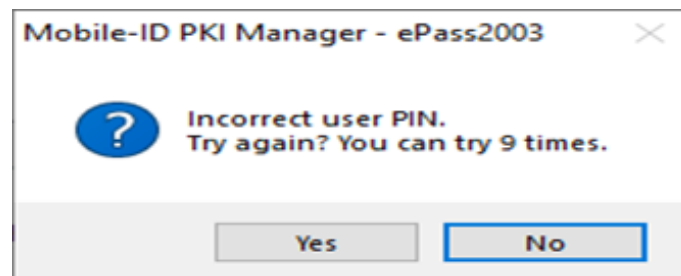


Note: The physical keyboard is disabled when you are using the soft keyboard.

After you enter a proper PIN and click OK, the interface as shown in Figure 5 above. 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.



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



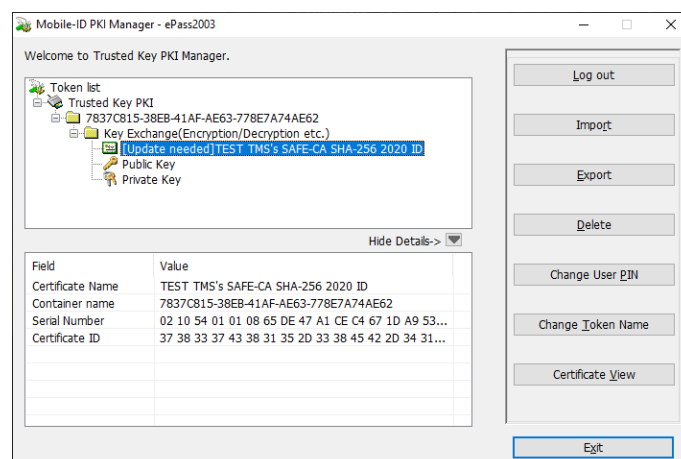
Note: There is a limit on the number of incorrect PIN inputs. If this number reaches 9, the token will be locked. You cannot perform any operations with it in this case.

3.4. Certificate Management

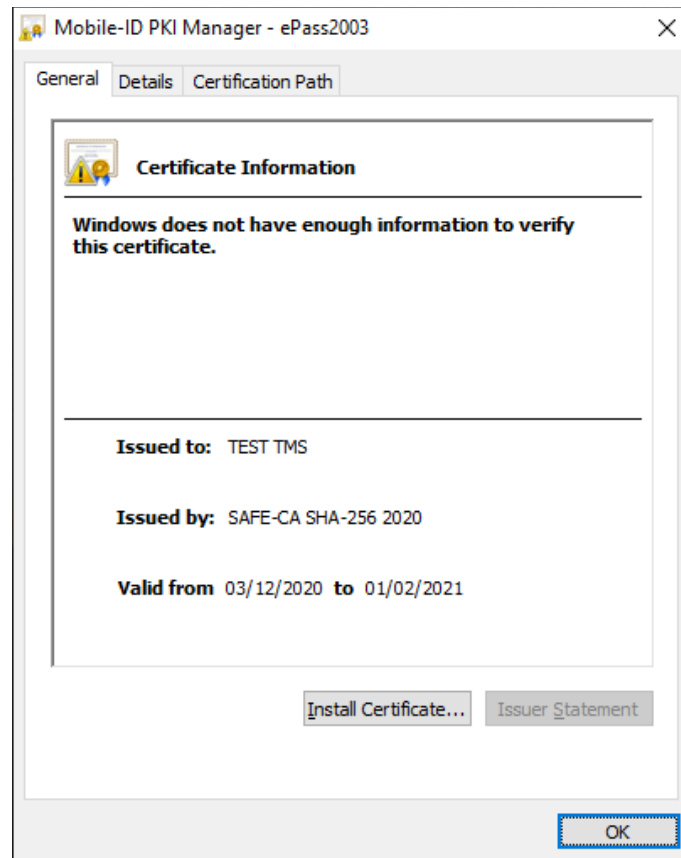
After you have logged into the Manager, you can view certificate information, import a certificate, delete a certificate etc.

3.4.1. Viewing Certificate Information

- 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.



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



You can view the information of your interest.

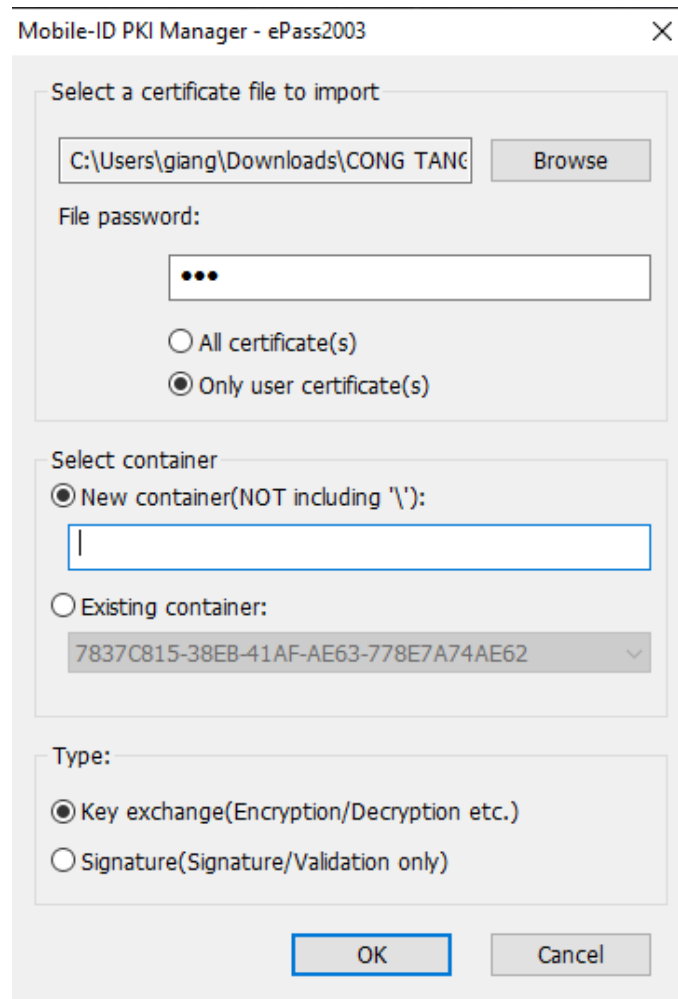
3.4.2. Importing

Currently, Trusted Key PKI supports the following certificate types: P12, PFX, P7B, CRT and CER. The P12 and PFX types contain a key pair (a public key and a private key), while the P7B, CRT and CER types do not. The PFX and CER types are used as examples below.

3.4.2.1. Importing PFX Certificate

Click Import button in the main interface of the Manager. The following interface appears. Click Browse button to choose a PFX certificate to be imported. If necessary, enter a password below. You are allowed to create a container or select a container for the certificate. Since the PFX certificate consists of a public and a private key, it can be used for both exchanging and signing. You should specify a purpose for the certificate. Click OK.

Note: Two certificates for different purposes can be stored in a single container. When importing a certificate to an existing container, the existing certificate for the same purpose in the container will be replaced if applicable.



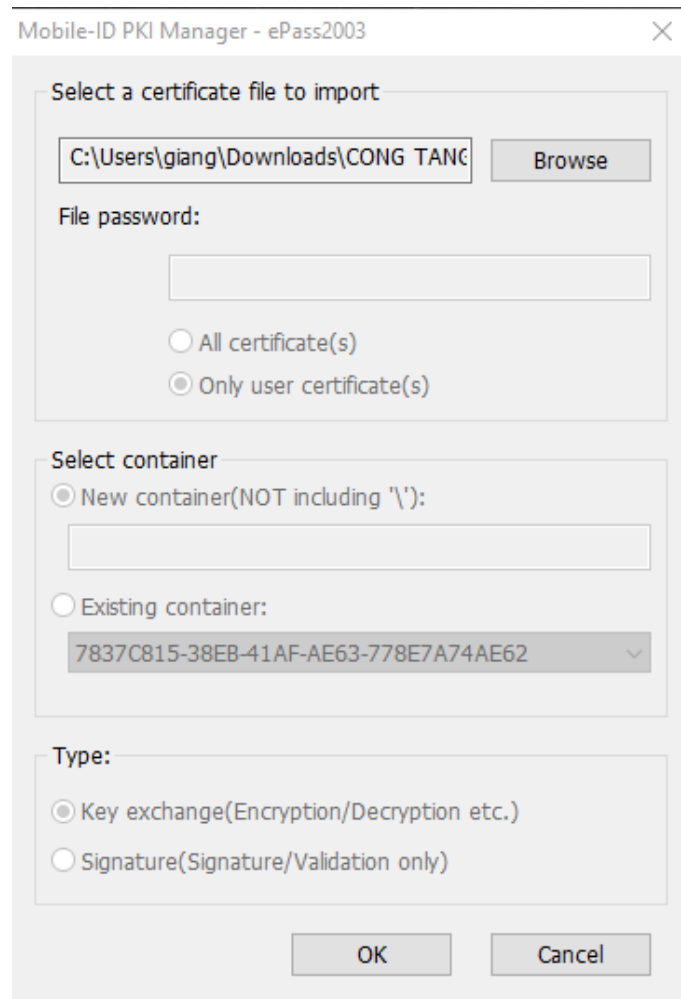
The screenshot shows a Windows-style dialog box titled "Mobile-ID PKI Manager - ePass2003". It contains three main sections: "Select a certificate file to import", "Select container", and "Type".

- Select a certificate file to import:** Includes a text field with the path "C:\Users\giang\Downloads\CONG TANC", a "Browse" button, a "File password:" label, a password input field with three dots, and two radio buttons: "All certificate(s)" and "Only user certificate(s)".
- Select container:** Includes two radio buttons: "New container(NOT including '\'):" and "Existing container:". The "New container" option is selected, and it has an empty text input field below it. The "Existing container" option has a dropdown menu showing the value "7837C815-38EB-41AF-AE63-778E7A74AE62".
- Type:** Includes two radio buttons: "Key exchange(Encryption/Decryption etc.)" and "Signature(Signature/Validation only)". The "Key exchange" option is selected.

At the bottom of the dialog are "OK" and "Cancel" buttons.

3.4.2.2. Importing P7B Certificate

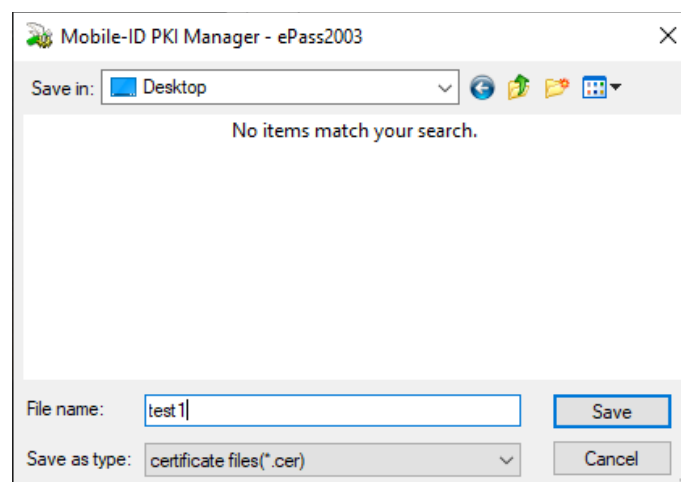
Click Import button in the main interface of the Manager. The following interface appears. Click Browse button to choose a P7B certificate to be imported. You must create a container to store the certificate. Since the P7B certificate does not contain a key-pair, it can only be used for exchanging. Click OK.



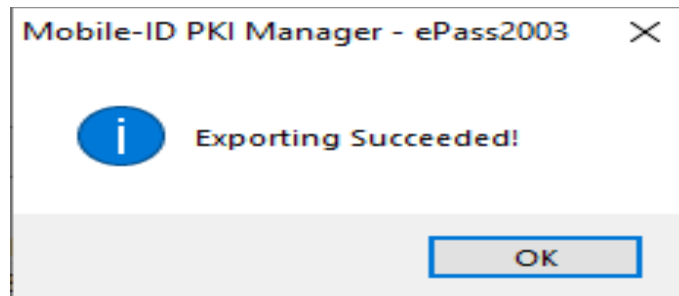
3.4.3. Exporting

You can export a certificate from the 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.



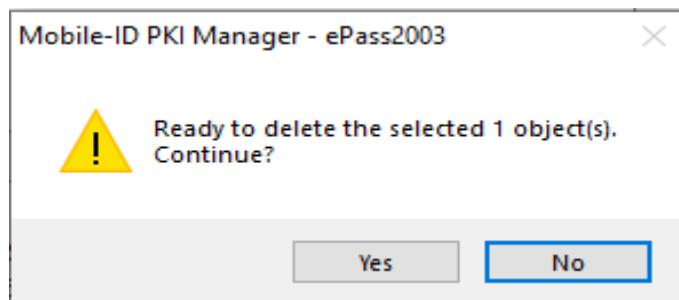
Click Save. If the operation has succeeded, the following message will appear:



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

3.4.4. 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:



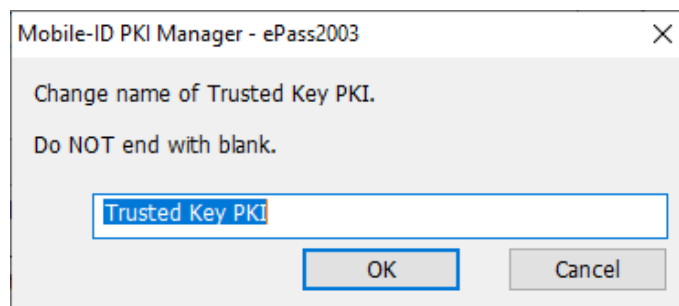
- Click Yes to delete the selected certificate if you do want.

By the way, you can delete the keys or container in Trusted Key PKI. If you select Trusted Key PKI and click Delete, all containers, certificates and keys in the token will be deleted.

3.5. Changing Token Name

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

- Click Change Token Name button. The following interface appears:

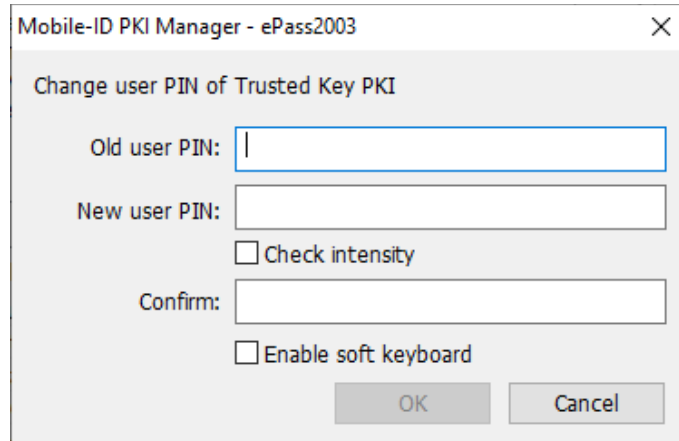


- Enter a name for the token and click OK.

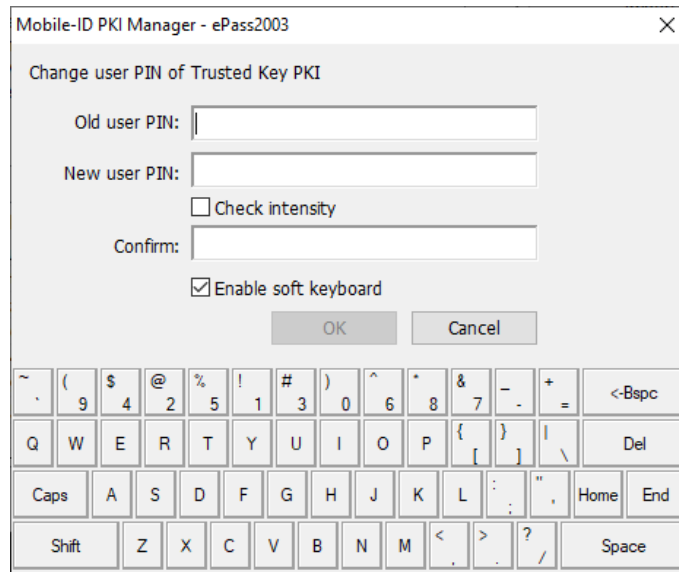
Note: At most a 32-character name can be provided.

3.6. 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.



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



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

Mobile-ID PKI Manager - ePass2003

Change user PIN of Trusted Key PKI

Old user PIN: [.....]

New user PIN: [.....]

☒ Check intensity **L**

Confirm: [.....]

☐ Enable soft keyboard

OK Cancel

If the strength is higher, the following interface appears:

Mobile-ID PKI Manager - ePass2003

Change user PIN of Trusted Key PKI

Old user PIN: [.....]

New user PIN: [.....]

☒ Check intensity **M**

Confirm: [.....]

☐ Enable soft keyboard

OK Cancel

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

Mobile-ID PKI Manager - ePass2003

Change user PIN of Trusted Key PKI

Old user PIN: [.....]

New user PIN: [.....]

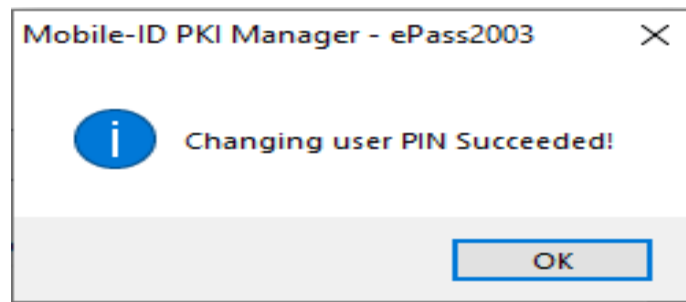
☒ Check intensity **H**

Confirm: [.....]

☐ Enable soft keyboard

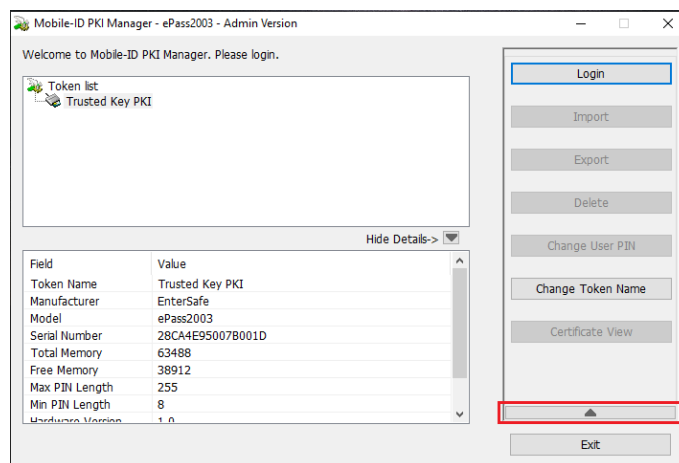
OK Cancel

By clicking OK, the following interface may appear:

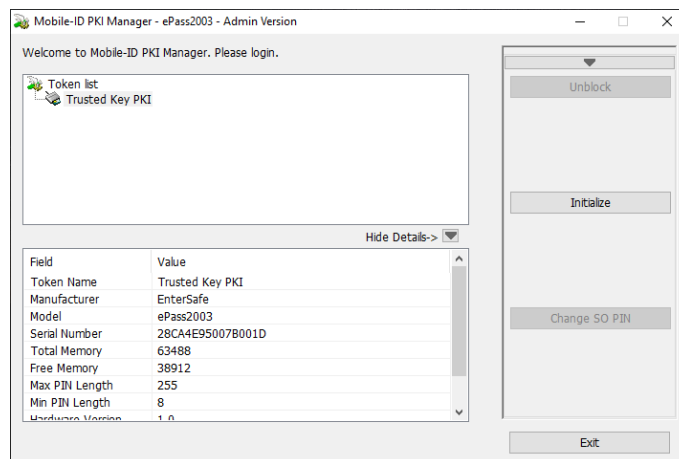


The above description is for the user version of Manager. The admin version incorporates some additional functions.

The main interface includes a triangle button for switching buttons.



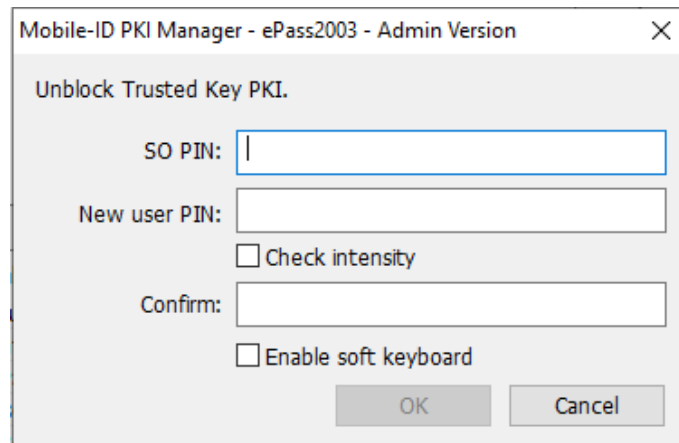
Click this button. The following interface appears:



3.7. Unblocking (Admin Version Only)

The Admin version can be used to unblock a token.

Click Unblock button in the main interface. The following interface appears:



Mobile-ID PKI Manager - ePass2003 - Admin Version

Unblock Trusted Key PKI.

SO PIN:

New user PIN:

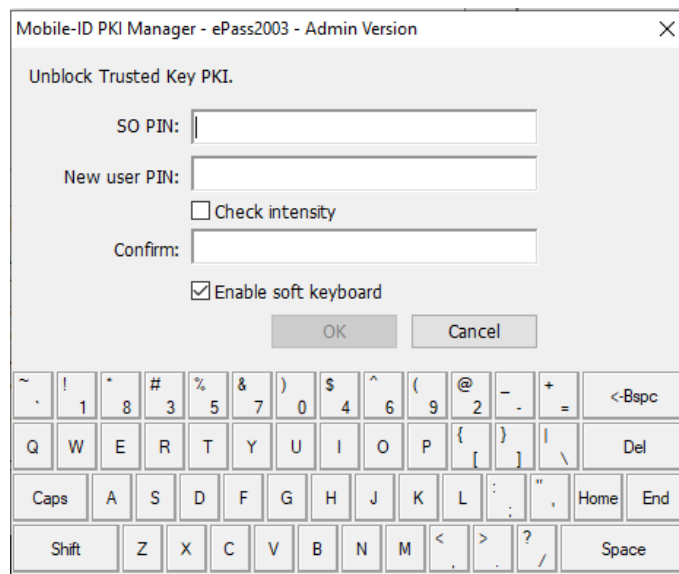
☐ Check intensity

Confirm:

☐ Enable soft keyboard

OK Cancel

You can use a soft keyboard to enter PINs. If you select Soft keyboard option, the following interface appears:



Mobile-ID PKI Manager - ePass2003 - Admin Version

Unblock Trusted Key PKI.

SO PIN:

New user PIN:

☐ Check intensity

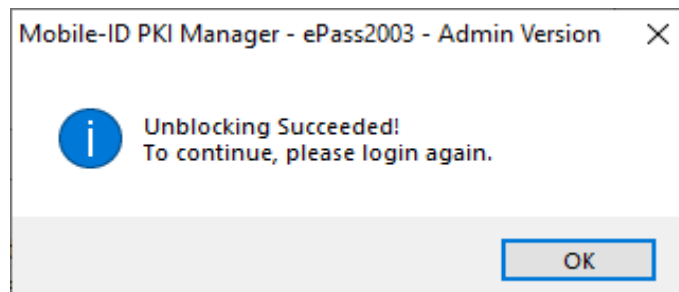
Confirm:

☒ Enable soft keyboard

OK Cancel

~	!	@	#	%	&)	\$	^	(@	-	+	<-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	

You can also select Check intensity option to get aware of the security strength of the PIN you have set. Enter a SO PIN and type and confirm a new PIN. Click OK. The following interface may appears:



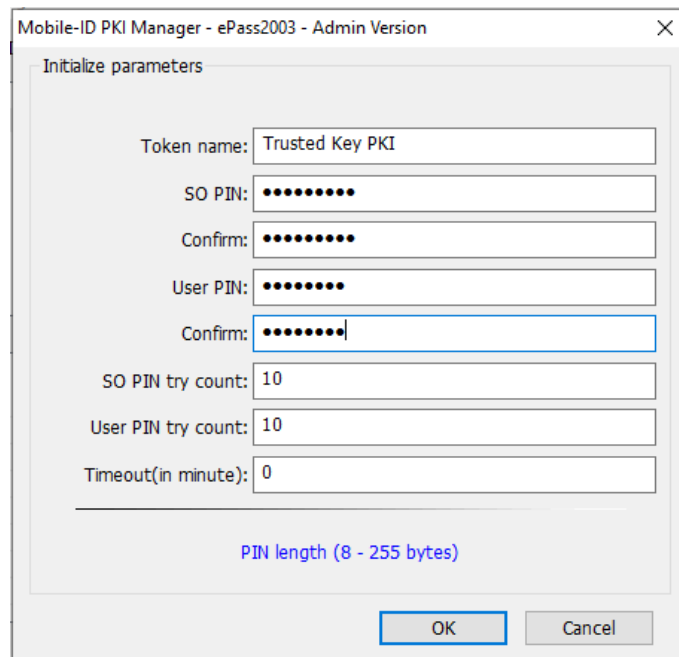
Mobile-ID PKI Manager - ePass2003 - Admin Version

i Unblocking Succeeded!
To continue, please login again.

OK

3.8. Initializing (Admin Version Only)

Click Initialize button in the main interface. The following interface appears:



Mobile-ID PKI Manager - ePass2003 - Admin Version

Initialize parameters

Token name: Trusted Key PKI

SO PIN:

Confirm:

User PIN:

Confirm:

SO PIN try count: 10

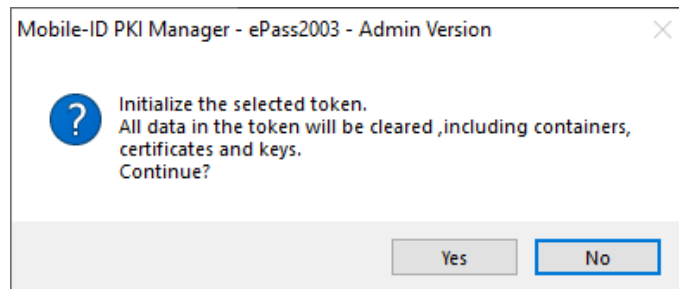
User PIN try count: 10

Timeout(in minute): 0

PIN length (8 - 255 bytes)

OK Cancel

After completing all parameters, click OK. The following prompt is displayed:

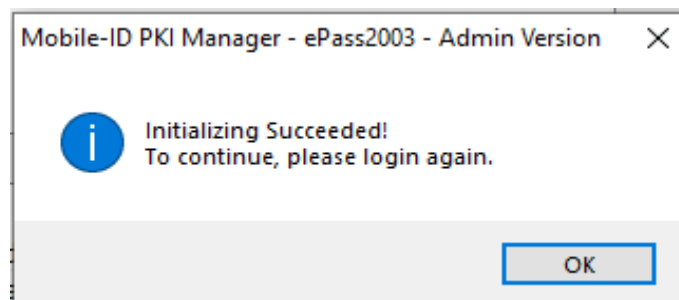


Mobile-ID PKI Manager - ePass2003 - Admin Version

Initialize the selected token.
All data in the token will be cleared, including containers, certificates and keys.
Continue?

Yes No

Click Yes to start initializing operation. If the operation is performed successfully, the following interface appears:



Mobile-ID PKI Manager - ePass2003 - Admin Version

Initializing Succeeded!
To continue, please login again.

OK

3.9. Changing SO PIN (Admin Version Only)

Click Change SO PIN in the main interface. The following interface appears:

Use a soft keyboard to avoid potential attacks. If you select Soft keyboard option, the following interface appears:

You can also select Check intensity option to get aware of the security strength of the SO PIN you have set. Enter the old SO PIN, a new SO PIN and confirm the new PIN. Click OK. If the operation is successful, the following interface appears:

4. Windows PIN Management

4.1. Overview

Mobile-ID Minidriver is a new smart card minidriver developed by Mobile-ID™ according to Microsoft Windows Smart Card Framework.

The new Windows smart card architecture leverages the fact that the cryptography required in common at the top is separate from the unique smart card hardware interfaces at the bottom. Windows now has a simple smart card interface layer, called smart card minidriver, which leverages common cryptographic components now included in the Windows platform.

The cryptography for smart cards has been implemented both in the legacy Cryptography API as well as the Cryptography API Next Generation (CNG) in Microsoft Windows Vista™ and 2008. The CSP implementation for CAPI is called the Microsoft Base Smart Card Cryptographic Service Provider, and the CNG implementation is called the Microsoft Smart Card Key Storage Provider. The Base CSP is not supported natively in those legacy Operating Systems, but it is available as Microsoft Windows Update # KB909520.

Base CSP and KSP provide the common software cryptographic portions, while the minidriver of a given smart card compliant with this architecture simply plugs in to provide access to the hardware and software of that particular smart card.

From an application developer perspective, the Base CSP, KSP and Minidriver interfaces provide a common way to access smart card features, regardless of the card type.

For users, the new architecture includes support for all preexistent smart card scenarios, and it also provides new tools for the management of the Personal Identification Number (PIN).

4.2. Mobile-ID Minidriver PIN Management for Windows

4.2.1. Changing a User PIN

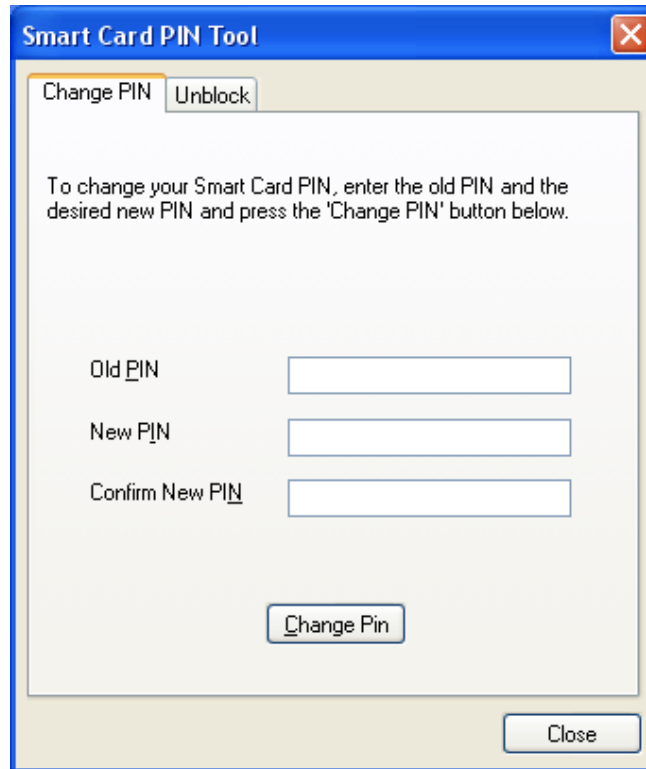
Generally, the User PIN is a password used to protect the data on the token. If a user operation (Windows logon, email signature, email encryption, VPN access, etc.) should access the Private Memory, the user will be asked for a User PIN.

It is recommended that users should often change their PIN to better protect the data on the token. In order to allow users to change the value of their PIN, several interfaces are available to do so in Windows Vista/2008 and in legacy versions of Windows. Users can change the PIN as described below.

4.2.1.1. Changing a User PIN with Windows 2000, XP or Server 2003

Before changing a user PIN with Windows 2000, XP or 2003, users should download and install the update package # KB909520 to enable the Smart Card PIN Tool. After installing the update package, users can use the PIN Tool to change a User PIN as follows:

- Select the Option **Start/Run** and type **PinTool**. The following dialog box appears.



The image shows a Windows-style dialog box titled "Smart Card PIN Tool". It has two tabs: "Change PIN" (selected) and "Unblock". The "Change PIN" tab contains the following text: "To change your Smart Card PIN, enter the old PIN and the desired new PIN and press the 'Change PIN' button below." Below this text are three input fields labeled "Old PIN", "New PIN", and "Confirm New PIN". At the bottom of the dialog is a "Change Pin" button. In the bottom right corner of the dialog is a "Close" button.

- Input the Old PIN, the New PIN and then confirm the New PIN.
- Click Change Pin button to finish changing the User PIN.

Note: The Mobile-ID_Minidriver default PIN is 12345678.

4.2.1.2. Changing a User PIN with Windows Vista, 2008 and Windows 7

In Windows Vista, 2008 and Windows 7, users can change their smart card user PIN using the secure desktop.

The secure desktop is the most trusted context in the operating system. The most common use of the Secure Desktop is the User Log on to Windows. However, it is also used for other secure operations with user credentials, such as password changes and now smart card PIN management.

To change the PIN of the smart card in Windows Vista, perform operations as follows:

- Press **Ctrl+Alt+Delete** to access the Secure Desktop screen.
- Select the **Change a Password** option.
- Attach Mobile-ID Minidriver to a USB Port of the computer.
- Select the smart card user tile.
- Enter the old PIN, the new PIN and confirm the new PIN in the appropriate fields. As shown in following image:



4.2.2. Unblocking Mobile-ID Minidriver

Private data stored on Mobile-ID Minidriver is protected by the User PIN. The PIN code retry number is limited by hardware. Once the preset maximum retry number is exceeded, Mobile-ID Minidriver Token will be blocked. Once the card is blocked, it can no longer be used even you have the correct User PIN. The only way to restore it is by using the **Unblock Card** procedure.

Note: The Mobile-ID Minidriver default maximum number of wrong PIN attempts is 10.

4.2.2.1. Example Unblock Procedure

The smart card unblock functionality require the use of an Administrative key that the regular end user should not have direct access to. The user will require support from a Security Officer to complete this operation.

To protect the confidentiality of the Admin Key, the Unblock Card procedure does not require the end user to present the Admin key directly. Instead, a challenge-response mechanism is used:

- The user retrieves a **Challenge** from the card.
- The user communicates the **Challenge** to the IT Admin/Helpdesk.
- IT Admin/Helpdesk combine the **Challenge** (8 bytes) and the user's **Admin Key** (24 bytes) using the Triple DES algorithm to calculate the unique **Response** (8 bytes) to the challenge.
- IT Admin/Helpdesk communicates the **Response** to the end user.
- The end user enters the **Response** value and defines a new value for the **User PIN**, which will be established once the Card Unblock has completed.
- The smart card confirms that the **Response** provided is correct, by comparing the value entered by the user with one generated within the card using the **Challenge** generated by the card and the Admin Key stored in the card. If both values match, the card unblock is successful, the new user PIN is established and the PIN attempt counter is reset.

It is important to note that, like the Verify PIN procedure, the Unblock Card procedure is protected by a **maximum number of unsuccessful unblock attempts**. Once the maximum number of unsuccessful unblock attempts is reached the card will be permanently blocked even to an administrator, and all data stored in the card becomes permanently inaccessible. For this reason it is important to perform the unblock procedure with great care.

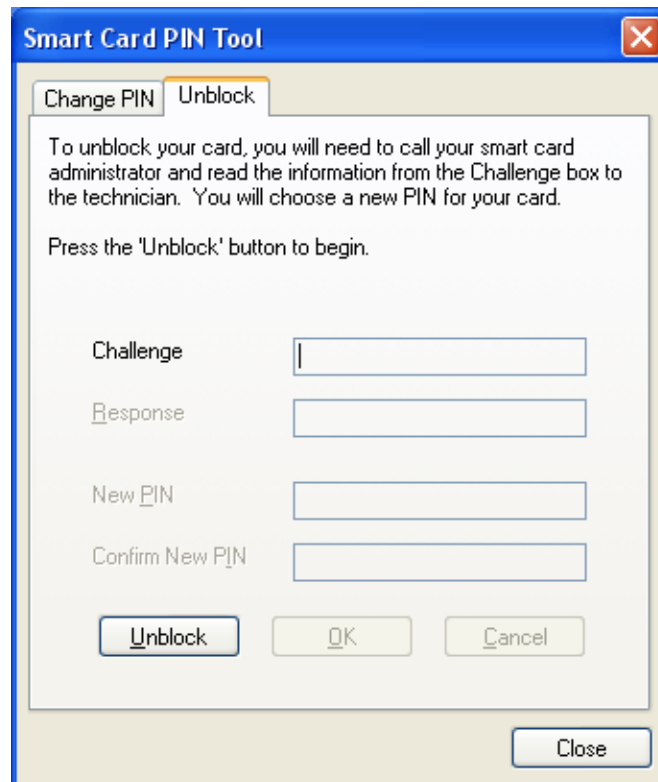
Like the Change PIN procedure, the process and tools used to unblock a Smart Card in Windows Vista/2008 and the legacy versions of Windows operating systems are different.

4.2.2.2. Unblocking a Smart Card with Windows 2000, XP or Server 2003

For Windows 2000, XP, and Server 2003 and later, the Smart Card PIN Tool used for changing the value of the User PIN can also be used to unblock the card.

Note that in order to use the PIN Tool the user must have access to a machine that is to be logged on. The user cannot logon using smart card credentials because the card has already been blocked. Accordingly, if the user's organization security policy introduces a smart card logon mechanism, the user will have to access another already logged machine in order to gain access to the PIN Tool to perform the Card Unblock procedure.

The PIN Tool provides the following dialog box to unblock the card:



The image shows a Windows-style dialog box titled "Smart Card PIN Tool". It has two tabs: "Change PIN" and "Unblock", with "Unblock" currently selected. The dialog contains the following text: "To unblock your card, you will need to call your smart card administrator and read the information from the Challenge box to the technician. You will choose a new PIN for your card. Press the 'Unblock' button to begin." Below this text are four input fields: "Challenge", "Response", "New PIN", and "Confirm New PIN". At the bottom of the dialog are three buttons: "Unblock", "OK", and "Cancel". A "Close" button is located at the bottom right of the dialog frame.

With the blocked Token attached to the USB port, when the user clicks on the **Unblock** button, the Smart Card will return the 16 digits of **Challenge**, and will enable the **Response**, **New PIN** and **Confirm New PIN** fields to allow the user to enter the corresponding values according to the process previously described.

Once the user clicks the **OK** button, the **Response** and **New PIN** values will be transmitted to the card to complete the card unblock procedure.

4.2.2.3. Unblocking a Smart Card with Windows Vista, 2008 and Windows 7

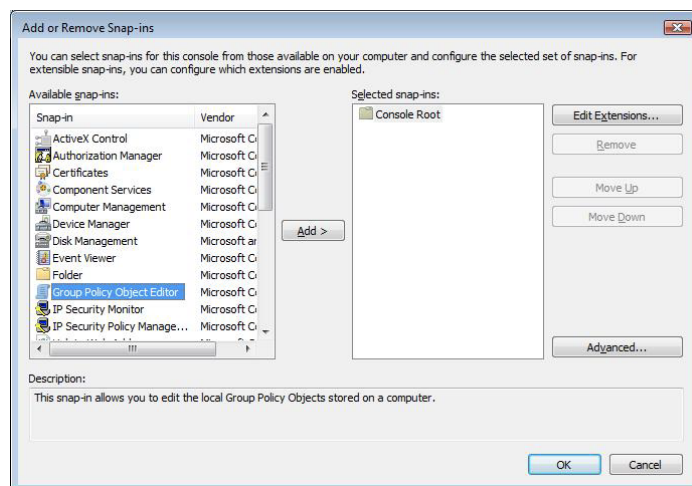
Smart Card Unblock is integrated into the Windows Vista, 2008 and Windows 7 Secure Desktop. However, it is not configured by default and must be explicitly enabled with Group Policy. When this feature is enabled, the user is presented with the Smart Card Unblock screen when logon is attempted using a blocked smart card.

Note: Smart card unblock requires that smart cards are assigned an administrator key before they are provided to users, and that the IT infrastructure includes a secure way to store and access these keys when a user needs assistance.

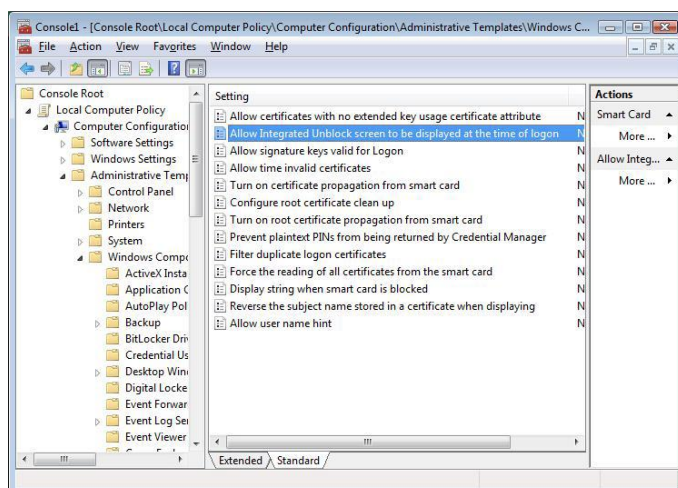
4.2.2.3.1. Enabling Unblock Card with Windows Vista, 2008 and Windows 7

The Unblock Card function in the secure desktop user interface is not enabled by default for Windows Vista, 2008 and Windows 7. To enable unblock in the secure desktop user interface, an administrator can use the Group Policy Object Editor snap-in in the Microsoft Management Console (MMC).

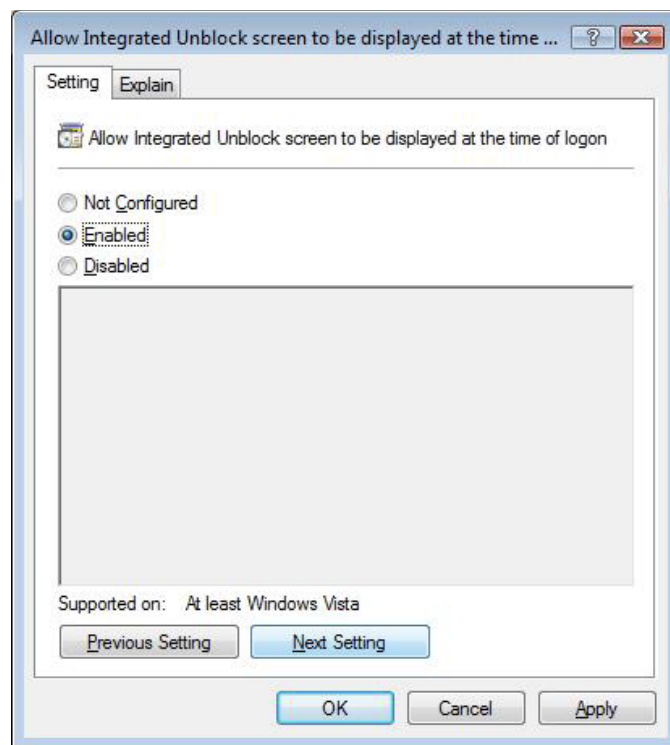
- Click **Start** button, type **MMC** in the Start Search field and then press **Enter**.
- When prompted to run Command Prompt as an administrator, click **Allow**. This will open the **Microsoft Management Console** dialog.
- In the **Console 1** dialog, click on the **File** menu and select **Add/Remove Snap-in**.
- In the **Add or Remove Snap-ins** dialog box, select **Group Policy Object Editor** in the **Available Snap-ins** pane on the left side, and then click **Add**, as shown in following image:



- You can either enable unblock for the local computer only, or for all computers in the domain.
 - o To enable unblock on the local machine (only), you must be an administrator on the local computer. Select **Local Computer** in the **Group Policy Object** control. Click **Finish** to close the **Select Group Policy** dialog.
 - o To enable unblock on all machines in the domain, you must be a Domain Administrator logged on to a Domain Controller and select **Default Domain Policy** in the **Group Policy Object** control. In the **Select Group Policy Object** dialog box, click **Finish**.
- Click **OK** in the **Add or Remove Snap-ins** dialog box to close it.
- Click on the **Local Computer Policy** node in the left side pane, then click on **Computer configuration—>Administrative Templates—>Windows Components—> Smart Card**. And then double-Click **Allow Integrated Unblock screen to be displayed at time of logon** in the **Setting** list, as shown in following image:

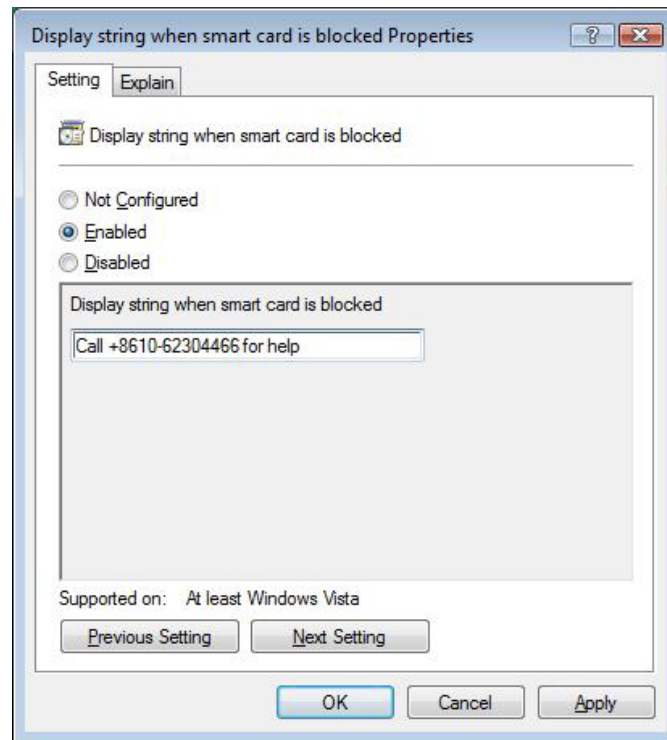


- Select the **Enabled** option button, and then click **OK**, as shown in following image:



At this point, the Smart Card Unblock screen can also be configured via Group Policy to display a custom string. This string can be used to provide a deployment-specific phone number for users to call to obtain the response to the smart card administrator challenge. You can set the custom string as follows:

- Back in the **Console 1** dialog, select the **Local Computer Policy** —> **Computer Configuration** —> **Administrative Templates** —> **Windows Components** —> **Smart Card**, and double-click on **Display string when smart card is blocked** on the right side pane.
- Select the **Enabled** option button and type the string to display on the Unblock screen in the **Display string when smart card is blocked** text box, and then press **OK**, as shown in following image:



4.2.2.3.2. Unblocking a Smart Card with Windows Vista, 2008 and Windows 7

Same as for the Change PIN function, the Smart Card Unblock is integrated into the Windows Vista, 2008 and Windows 7 **Secure Desktop**. However, it is not configured by default and must be explicitly enabled via Group Policy as 2.2.3.1 described. When this feature is enabled, the user is presented with the Smart Card Unblock screen when login is attempted using a blocked smart card,, as shown in following image:



4.2.2.4. Administrator Tools for Card Unblock

The Smart Card Unblock procedure requires the administrator to be able to calculate the **Response** to a **Challenge** provided by the smart card of any end users that he/she is responsible for. This in turn means that the administrator shall:

- Know or somehow have access to, the administrative key values for all smart cards in use.
- Have access to a Triple DES tool to calculate the Response based on the Challenge and the administrative key of a given user's smart card.

None of the Windows operating systems provide any means for administrators to handle the secure back-end storage of the user's smart cards Administrative keys, nor do they provide a back-end tool to calculate the response to a challenge.

These features will be commonly provided by any commercial Base CSP compliant Card Management System (CMS), including Microsoft's Identity Lifecycle Manager (ILM).

5. Appendix: Terms and Abbreviation

Entry	Description
Trusted Key PKI	A smart card based token with FIPS proved for PKI applications, introduced by Mobile-ID Technologies And Services Joint Stock Company. 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.