



ASECard Crypto for Windows

User Guide

For version 4.1
June, 2007

WWW.ATHENA-SCS.COM

LICENSE

ATHENA SMARTCARD SOLUTIONS INC.

SOFTWARE LICENSE AGREEMENT

READ THIS AGREEMENT CAREFULLY BEFORE CONTINUING WITH THE INSTALLATION OF THE ASECARD CRYPTO TOOLKIT AND UTILITIES.

ALL ORDERS AND USE OF PRODUCTS OF ATHENA SMARTCARD SOLUTIONS INC. OR ANY OF ITS AFFILIATES, ALL OF WHICH ARE HENCEFORTH REFERRED TO AS **ATHENA** INCLUDING, WITHOUT LIMITATION, SOFTWARE, DOCUMENTATION, CD-ROMs, AND ASECARDS, ARE AND SHALL BE SUBJECT TO THE TERMS AND CONDITIONS SET FORTH IN THIS AGREEMENT. BY OPENING THE SEALED PACKAGE CONTAINING THE PRODUCTS, AND/OR BY INSTALLING THE SOFTWARE (as defined hereunder) IN YOUR COMPUTER AND/OR BY USING THE SOFTWARE OR ANY OF ATHENA'S PRODUCTS, YOU ARE ACCEPTING THIS AGREEMENT AND AGREEING TO BE BOUND BY ITS TERMS. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, YOU SHOULD PROMPTLY (WITHIN 7 DAYS FROM THE DATE YOU RECEIVED THIS PACKAGE) RETURN THE DEVELOPER'S KIT AND THE DEVELOPER'S GUIDE TO ATHENA, UNOPENED. YOUR MONEY WILL BE REFUNDED.

- 1. Title & Ownership.** THIS IS A LICENSE AGREEMENT AND NOT AN AGREEMENT FOR SALE. Athena hereby grants you, and you hereby accept, a personal, non-transferable, non-exclusive license ("**License**") to use (and the right to resell only as explicitly provided herein) Athena's product(s) ordered or obtained by you, upon the terms set forth herein. The software component of Athena's product(s), including any revisions, corrections, modifications, enhancements and/or upgrades thereto ("**Software**") and Developer's Guides and any other documentation or user guide related to the Software, shall remain Athena's property. All intellectual property rights (including, without limitation, copyrights, trade secrets, trademarks, etc.) evidenced by or embodied in and/or attached/connected/related to the Software, the User Guides and any other documentation are and shall be owned solely by Athena. Nothing in this Agreement constitutes a waiver of Athena's intellectual property rights under any law.
- 2. License.** You are granted a limited License to use the Software in executable form only, and only according to the terms of this Agreement: (1) you may install the Software and use it on computers located in your place of business; (2) Should the Product obtained by you contain special utilities, you may use the said utilities in the fashion described in the User Guide and only to that extent you may merge and link the utilities into your application(s); however, any portion of the software merged into another application shall be deemed as derivative work and will continue to be subject to the terms of this agreement.
- 3. Prohibited Uses.** Except as permitted in Sections 2 and 3 above, you agree not to (1) use, modify, merge or sub-license the Software or any other of Athena's product(s) except as expressly authorized in this Agreement; and (2) sell, license (or sub-license), lease, assign, transfer, pledge, or share your rights under this License with/to anyone else; and (3) modify, disassemble, decompile, reverse engineer, revise or enhance the Software or attempt to discover the Software's source code; and (4) place the Software onto a server so that it is accessible via a public network; and (5) use any back-up or archival copies of the Software (or allow someone else to use such copies) for any purpose other than to replace an original copy if it is destroyed or becomes defective. If you are a member of the European Union, this agreement does not affect your rights under any legislation implementing the EC Council Directive on the Legal Protection of Computer Programs. If you seek any information within the meaning of that Directive you should initially approach Athena.
- 4. Limited Warranty.** Athena warrants, for a period of twelve (12) months after the date of delivery to you, (the "**Warranty Period**"), the following: (1) that the Software, when and as delivered to you, will perform in substantial compliance with the User's Guide, provided that it is used on the computer hardware and with the operating system for which it was designed; and (2) that the *ASEDrives* and *ASECards* are substantially free from significant defects in materials and workmanship.
- 5. Warranty Disclaimer.** ATHENA DOES NOT GUARANTEE THAT ANY OF ITS PRODUCT(S) WILL MEET YOUR REQUIREMENTS OR THAT IT'S OPERATION WILL BE UNINTERRUPTED OR ERROR-FREE. TO THE EXTENT ALLOWED BY LAW, ATHENA EXPRESSLY DISCLAIMS ALL EXPRESS WARRANTIES NOT STATED HERE AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
- 6. Limitation of Remedies.** In the event of a breach of this warranty, Athena's sole obligation is to replace or repair, at Athena's option, any of its products or component thereof that does not meet the foregoing limited warranty, free of charge. Warranty claims must be made in writing during the Warranty Period and within seven (7) days of the observation of the defect accompanied by evidence satisfactory to Athena. All Products should be returned to the Athena distributor from which they were purchased (if not purchased directly from Athena) and shall be shipped by the returning party with freight and insurance paid. The product or component thereof must be returned with a copy of your receipt.

7. **Exclusion of Consequential Damages.** The parties acknowledge that the Software and Athena's product(s) are inherently complex and may not be completely free of errors. ATHENA SHALL NOT BE LIABLE (WHETHER UNDER CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE) TO YOU, YOUR DISTRIBUTORS, THE USERS OF YOUR SOFTWARE PROGRAM OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE (INCLUDING INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES), INCLUDING, WITHOUT LIMITATION, ANY LOSS OR DAMAGE TO BUSINESS EARNINGS, LOST PROFITS OR GOODWILL AND LOST OR DAMAGED DATA OR DOCUMENTATION, SUFFERED BY ANY PERSON, ARISING FROM AND/OR RELATED WITH AND/OR CONNECTED TO ANY USE OF THE SOFTWARE, AND/OR ANY OF ATHENA'S PRODUCT(S) AND/OR YOUR SOFTWARE PROGRAM, EVEN IF ATHENA IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
9. **Limitation of Liability.** IN THE EVENT THAT, NOTWITHSTANDING THE TERMS OF THIS AGREEMENT, ATHENA IS FOUND LIABLE FOR DAMAGES BASED ON ANY DEFECT OR NONCONFORMITY OF ITS PRODUCT(S), ITS TOTAL LIABILITY FOR EACH DEFECTIVE PRODUCT SHALL NOT EXCEED THE PRICE PAID TO ATHENA FOR SUCH DEFECTIVE PRODUCT.
10. **Termination.** Failure to comply with the terms of this Agreement shall terminate your license and this Agreement. Upon termination of this License Agreement by Athena: (1) the License granted to you in this Agreement shall expire and you, upon termination, shall discontinue all further use of the Licensed Software and other Licensed product(s); and (2) you shall promptly return to Athena all tangible property representing Athena's intellectual property rights and all copies thereof and/or shall erase/delete any such information held by it in electronic form. Sections 1, 4, 5, 6, 7, 8, 9, 10 and 11 shall survive any termination of this Agreement.
11. **Governing Law & Jurisdiction.** This Agreement is governed only by the laws of Japan, and only the courts in Japan shall have jurisdiction in any conflict or dispute arising out of this Agreement.
12. **Export control and Government Regulations.** **You agree that the product will not be shipped, transferred, or exported to any country or used in any manner prohibited by law. The Athena products are subject to additional export control law applicable to you or in your jurisdiction, including, without limitation, the United States. You warrant that you will comply in all respects with the export and re-export restriction applicable to the Athena products and will otherwise comply with any United States law and regulations in effect from time to time.**
13. **Miscellaneous.** **This Agreement represents the complete agreement covering this License and may be amended only by a written agreement executed by both parties. If any provision of this Agreement is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable.**

By accepting this document you confirm the following statement:

I HAVE READ AND UNDERSTOOD THIS LICENSE AGREEMENT AND AGREE TO BE BOUND BY ALL OF THE TERMS.



Table of Contents

PREFACE	2
WHO SHOULD READ THIS MANUAL	2
PREREQUISITES	2
STEP-BY-STEP INSTRUCTIONS FOR INSTALLING AND USING THE ASECARD CRYPTO TOOLKIT	3
1. INSTALLING THE ASECARD CRYPTO TOOLKIT	3
INSTALLING THE TOOLKIT TO SUPPORT PIN CARDS	3
INSTALLING THE TOOLKIT TO SUPPORT BIO CARDS	5
2. DEFAULT CARD PERSONALIZATION PARAMETERS	8
3. USING THE ASECARD PERSONALIZATION TOOL FOR PIN CARDS	10
4. USING THE ASECARD PERSONALIZATION TOOL FOR BIO CARDS	18
4.1 PERSONALIZING A BIO CARD	26
5. CHANGING OR UNBLOCKING THE USER PIN	31
6. BIOMETRIC ENROLLMENT	34
7. THE ASECARD MANAGER TOOL	35
8. ASECARD MANAGER OPTIONS	40
9. SMART CARD USER/LOGON CERTIFICATE ENROLLMENT	48
10. LOGGING ON WITH AN ASECARD CRYPTO PIN SMART CARD	53
11. LOGGING ON WITH AN ASECARD CRYPTO BIO ENABLED SMART CARD	54
12. POLICY SETTINGS FOR SMART CARD REMOVAL BEHAVIOR	55
13. LOCKING & UNLOCKING A PC UPON CARD REMOVAL	57
14. ADVANCED INSTALLATION OPTIONS	58



Preface

ASECard Crypto is a set of utilities and middleware which, coupled with an ASECard Crypto card, provide support for Microsoft Windows smart card services such as Interactive Logon, secure e-mail, VPN, and support for most smart card aware third party applications using CAPI and/or PKCS#11 middleware standards.

ASECard Crypto Cards are factory programmed to support PIN only or Fingerprint Biometrics and/or PIN. In this Manual, cards that support PIN only are referred to as "**PIN Cards**" and cards that support both PIN and Bio are referred to as "**Bio Cards**".

Who Should Read This Manual

This manual is intended for IT managers, System Administrators, and software engineers who are in charge of implementing smart card support in their organization.

This Manual assumes that you are familiar with:

- General use of computers
- Microsoft Windows 2000, XP, Vista
- Microsoft Windows 2000 Server or Server 2003
- Active Directory and Microsoft Certificate Authority

Prerequisites

The prerequisites for setting up Smart Card Logon on a Windows 2000/2003 Server are:

- *Domain Controller* installed on a Windows 2000/2003 domain server.
- A *Microsoft CA* configured with the Enterprise Policy Module.
- *Smart Card Enrollment Station* configured with Smartcard User or Smartcard Logon policies (See the separate document titled **Windows Server Smart Card Integration Guide**)

For detailed instructions on installing and configuring a *Microsoft CA* and *Active Directory*, please refer to Microsoft documentation.

Once you complete installation of *Domain Controller* and your *CA* is configured with a *Smart Card Enrollment Station*, proceed to the next section for step-by-step instructions.

Step-by-Step Instructions for Installing and Using the ASECard Crypto Toolkit

1. Installing the ASECard Crypto Toolkit

ASECard Crypto Toolkit 4.0 can be installed on the following operating systems:

- Windows 2000 / Windows 2000 Server
- Windows Server 2003 and 2003 x64
- Windows XP and XP x64
- Windows Vista and Vista x64

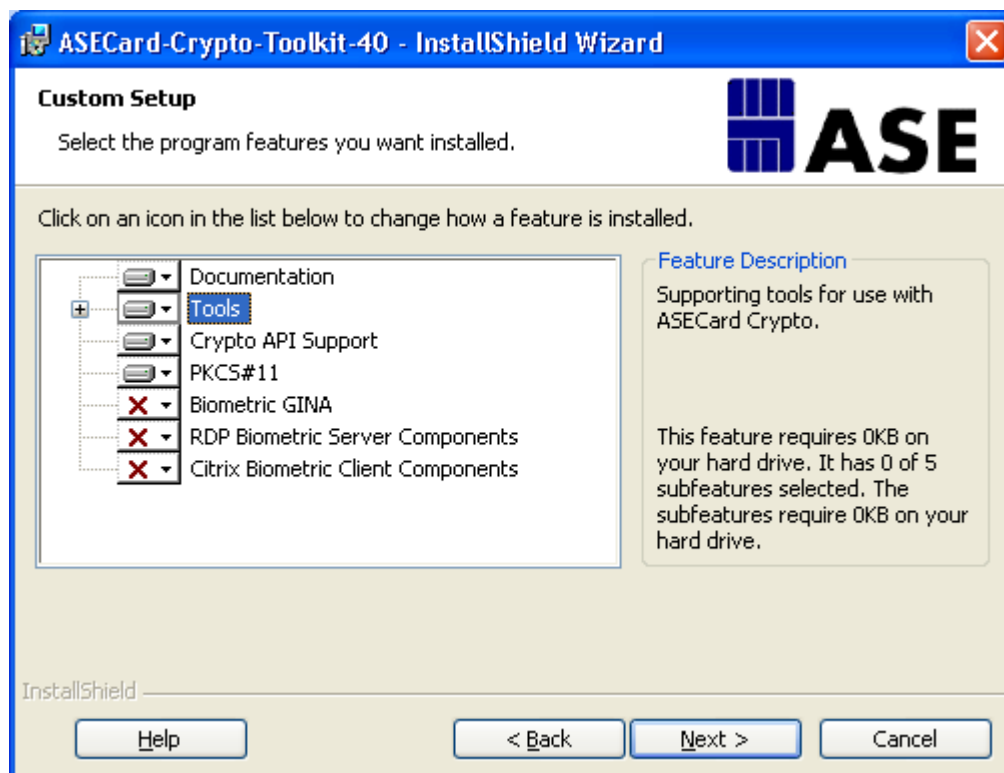
The ASECard Crypto Toolkit 4.0 supports both x86 and x64 bit operating systems and the latest version/service packs of each operating system. To install on x86 operating systems, run the setup.exe installation program or use the ASECard-Crypto-Toolkit-40.msi installer. To install on x64 operating systems, run the setupx64.exe installation program or use the ASECard-Crypto-Toolkit-40x64.msi installer. The msi installer allows installing the toolkit to domain users using Group Policy; it has various flag options that allow controlling the toolkit installation and the toolkit components to be installed on each machine. See the chapter Advanced Installations Options at the end of this manual for a list of the installer flags and their usage.

In order to support the issuance of smart card certificates and storing them on ASECard Crypto smart cards, the ASECard Crypto CSP middleware component must be installed on a smart card enrollment station PC. You also have to install the ASECard Crypto CSP on each end-user PC that will be enabled for smart card logon.

Installing the Toolkit to support PIN Cards

When installing the ASECard Crypto Toolkit to support PIN Cards, you have the choice of 2 installation methods:

- A. ASECard Crypto Toolkit – Typical:** Installs the ASECard Crypto CSP and PKCS#11 middleware, the ASECard Personalization Tool and the ASECard Manager. It does not install software components that are required in order to support biometric logon either locally or in Terminal Services and Citrix environments.
- B. ASECard Crypto Toolkit – Custom:** Allows selection of specific items. For example, you may not want to install the documentation or various tools on each end-user's PC. For PIN cards, you do not have to install the Biometric GINA, the Biometric RDP and Citrix support.



You will need to install the ASECard Personalization Tool in order to personalize, re-personalize cards, change User or Admin PINS, Enroll fingerprints and manage other card properties. The cards you purchased may be personalized or non-personalized, in which case you will have to personalize them before use.

Important!: If you have a previously installed version of ASECard Crypto Toolkit or CSP, please remove it using the **ADD or Remove Program** windows Control Panel utility, before proceeding with the new installation. You may be requested to restart your PC after removing the CSP. In such a case, if you are upgrading from any version lower than 3.99, you **MUST** restart your PC before installing version 4.xx of the Toolkit. In such case, make sure that your PC is configured for Username/Password login as you will not be able to login with a smart card after restart and until you install a new version of the Toolkit. If you are upgrading from version 3.99 or higher, **DO NOT** restart the PC after removing the previous version. Following the un-install, run the installer for version 4.xx and then restart the PC.

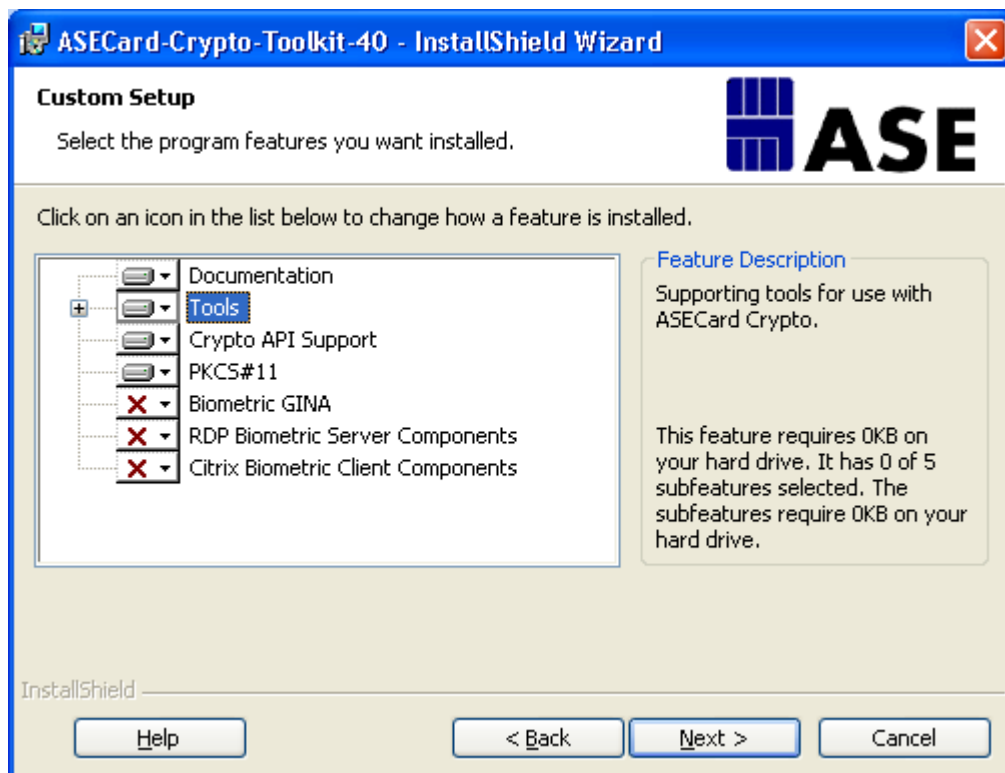
Please note that Administrator rights on the Local Machine are required in order to install the Toolkit.

Installing the Toolkit to support BIO Cards

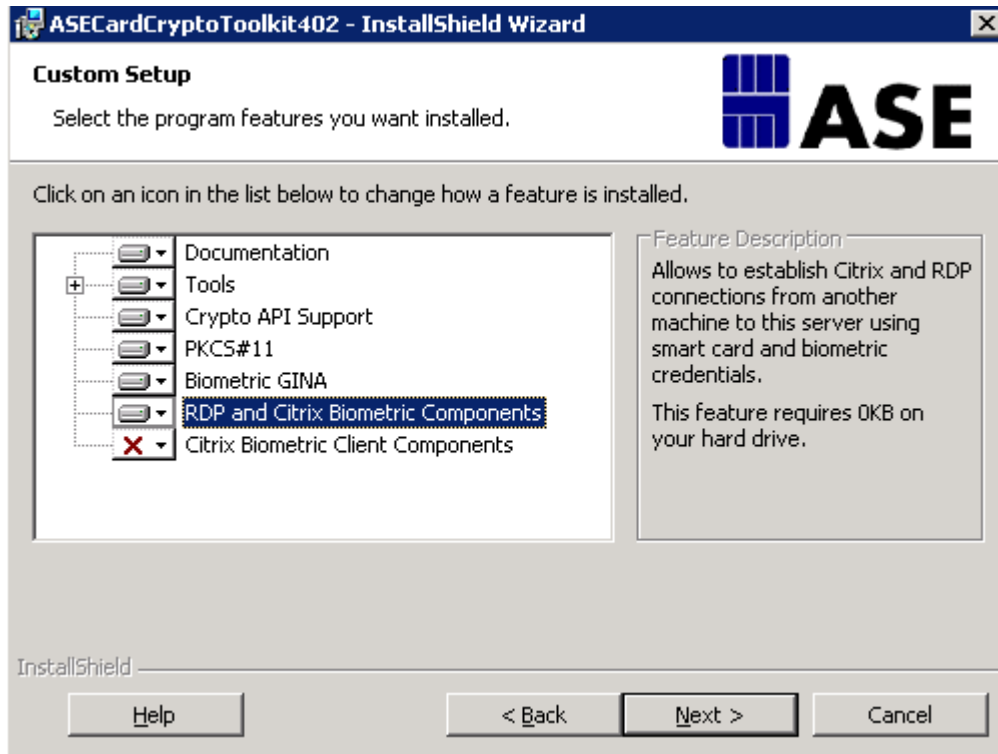
When installing the ASECard Crypto Toolkit to support BIO Cards, you must choose the Custom installation option:

ASECard Crypto Toolkit – Custom: This option allows the selection items that will be installed. For example, you may not want to install the documentation and/or various Tools on each end-user’s PC. For **BIO** cards you may need to select one of the following features:

- a. **Biometric GINA** – Selecting the Biometric GINA will replace the default Microsoft GINA that supports only Username/Password and/or PIN Smart Card logon, with a new dialog window that will allow you to logon with Fingerprint verification and/or PIN. Installing the GINA will require a restart of the PC. With the current version of the Toolkit, this option is not available on Windows Vista
- b. **RDP Biometric Server Components** – If you plan to logon to remote PCs, you must install this component on the PC that will act as server for the RDP session.
- c. **Citrix Biometric Client Components** - If you plan to use **BIO** cards in the Citrix environment, you will have to install this component on the Client PC



When installing the Toolkit on a Server 2000/2003 you will be presented with the following custom setup options:



You will need to install the ASECard Personalization Tool in order to personalize, re-personalize cards, change User or Admin PINS, Enroll fingerprints and manage other card properties. The cards you purchased may be personalized or non-personalized, in which case you will have to personalize them before use.

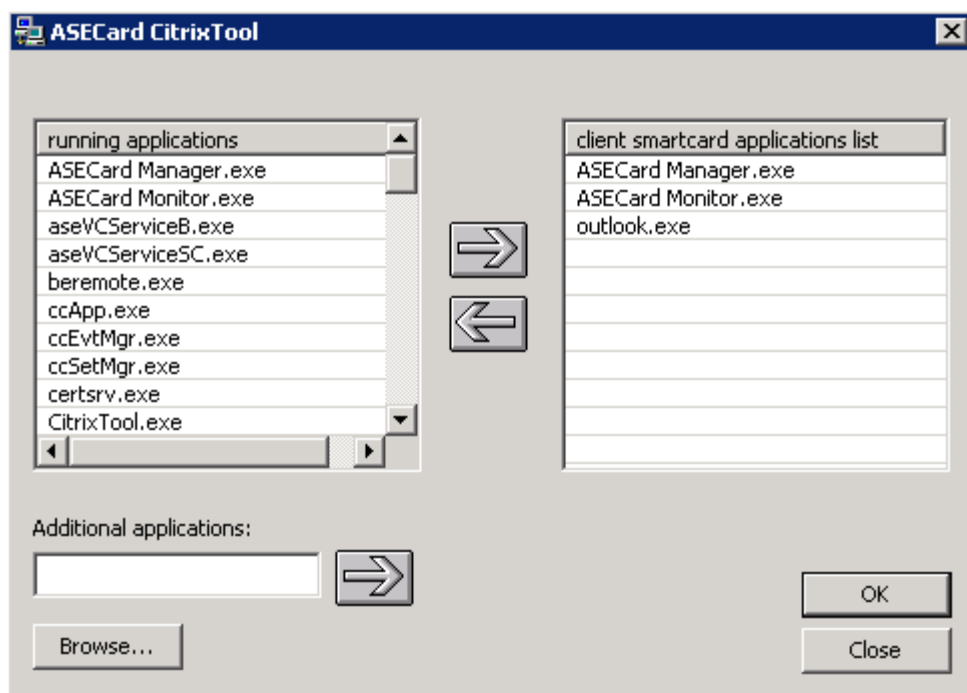
Important!: If you have a previously installed version of ASECard Crypto Toolkit or CSP, please remove it using the **ADD or Remove Program** windows Control Panel utility, before proceeding with the new installation. You may be requested to restart your PC after removing the CSP. In such a case, if you are upgrading from any version lower than 3.99, you **MUST** restart your PC before installing version 4.xx of the Toolkit. In such case, make sure that your PC is configured for Username/Password login as you will not be able to login with a smart card after restart and until you install a new version of the Toolkit. If you are upgrading from version 3.99 or higher, **DO NOT** restart the PC after removing the previous version. Following the un-install, run the installer for version 4.xx and then restart the PC.

Please note that Administrator rights on the Local Machine are required in order to install the Toolkit.

Installing the ASECard Crypto Toolkit in Citrix and Windows Terminal Server environment

If you plan to use a **Bio Card** in Citrix or Terminal Server environment, you must install the Toolkit on both the client and server side.

When installing the Toolkit on a Server 2000/2003 the ASECard Citrix Tool will be installed. You must use this tool to specify which applications to publish for smart card use, instead of the Citrix SCCONFIG tool supplied by Citrix, in all cases when you install the Citrix Server and Client components.



Install the Toolkit before proceeding to chapter 2.



2. Default Card Personalization Parameters

The ASECard Crypto smart cards require personalization before being enrolled for smart card certificates. If you are not sure if the card is personalized, you will be able to view this info in the Personalization or ASECard Manager Tools.

The ASECard Personalization Tool is supplied with the *ASEDefault* personalization profile.

The main parameters of the *ASEDefault* profile are:

Parameter	AseDefault Value	Changing Requires Re-Personalization
Profile Name	ASEDefault.ppf	NO
Card Label	" ASECard" + Card Serial Number	NO
PKI Quota (reserved memory)	0 Bytes	YES
Change PIN at first use	No	YES
(PIN) Stays valid for ... Min	Not set	YES
(PIN) Expires after ... Days	Not set	YES
Remember last x PINs	X=1	YES
Generate ANSI X9.31 RSA key pairs	No	YES
User PIN	11111111	NO
Verification type	PIN	YES
Min User PIN length	4 Characters	YES
Max User PIN length	10 Characters	YES
Max User PIN verify attempts	10 Attempts	YES
Max unblocks of User PIN	Unlimited	YES
Maximum fingers to enroll	Not set	YES
Image Quality	Not set	YES
False acceptance rate	Not set	YES
PIN Complexity Rules	None	YES
Admin PIN Value	00000000	NO



Min Unblock PIN length	4 Characters	YES
Max Unblock PIN length	10 Characters	YES
Max Unblock PIN verify attempts	3 Attempts	YES
PIN Complexity Rules	None	YES

Note: Some of the parameters above can only be changed through re-personalization of the card which results in the loss of the credentials saved on the card. Changing the User PIN, User Fingerprint, Admin PIN, or Card Label will not result in loss of credentials. See more details in the following chapter.

3. Using the ASECard Personalization Tool for PIN Cards (see Chapter 4 for personalizing Bio Cards)

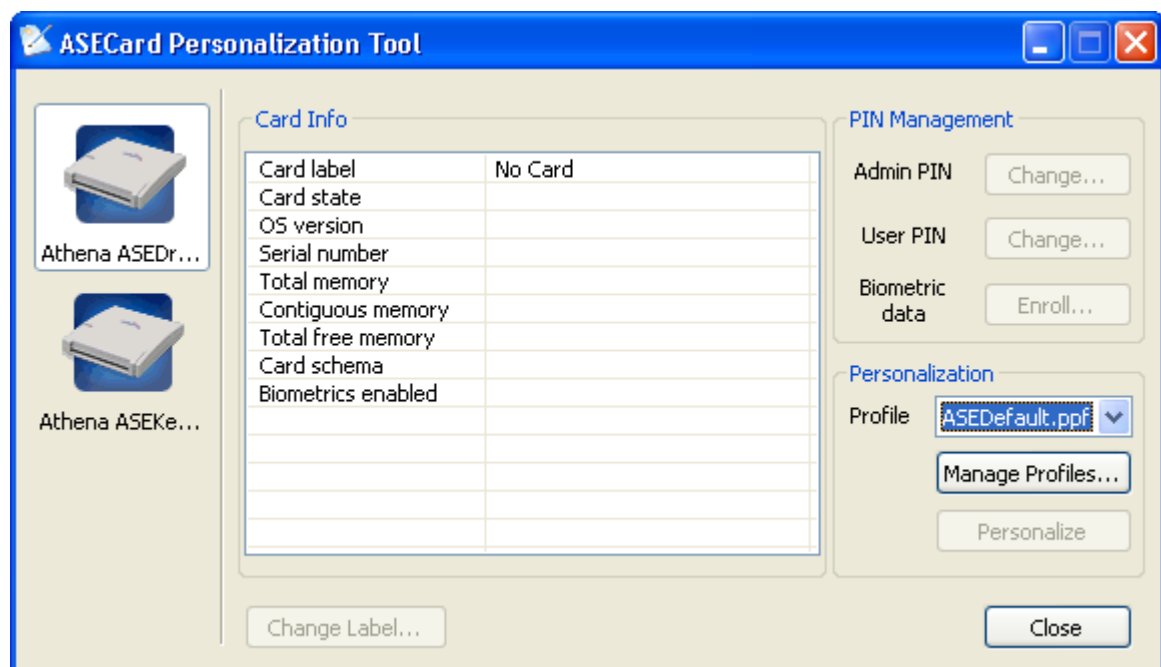
The ASECard **Personalization Tool** is an easy to use tool that provides the Administrator with full control over the card security policy and various card parameters. The tool can be used in order to:

- View card details such as *Serial Number, Free Space, etc.*
- Change the User and Admin PINs and set a Card Label without invalidating the credentials stored on the card.
- Viewing, editing and creating new *Personalization Profiles*.
- Personalizing and re-personalizing cards.

To start the **ASECard Personalization Tool**:

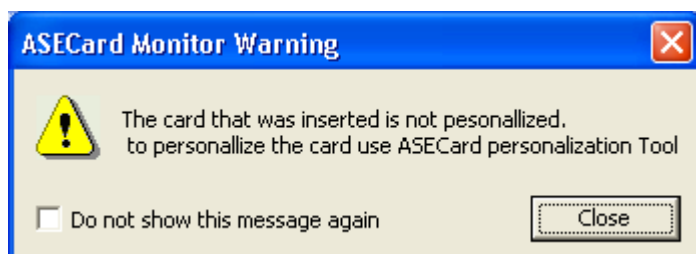
Click **Start ->Programs->ASECard Crypto Toolkit ->ASECard Personalization Tool**

The **ASECard Personalization Tool** window appears:

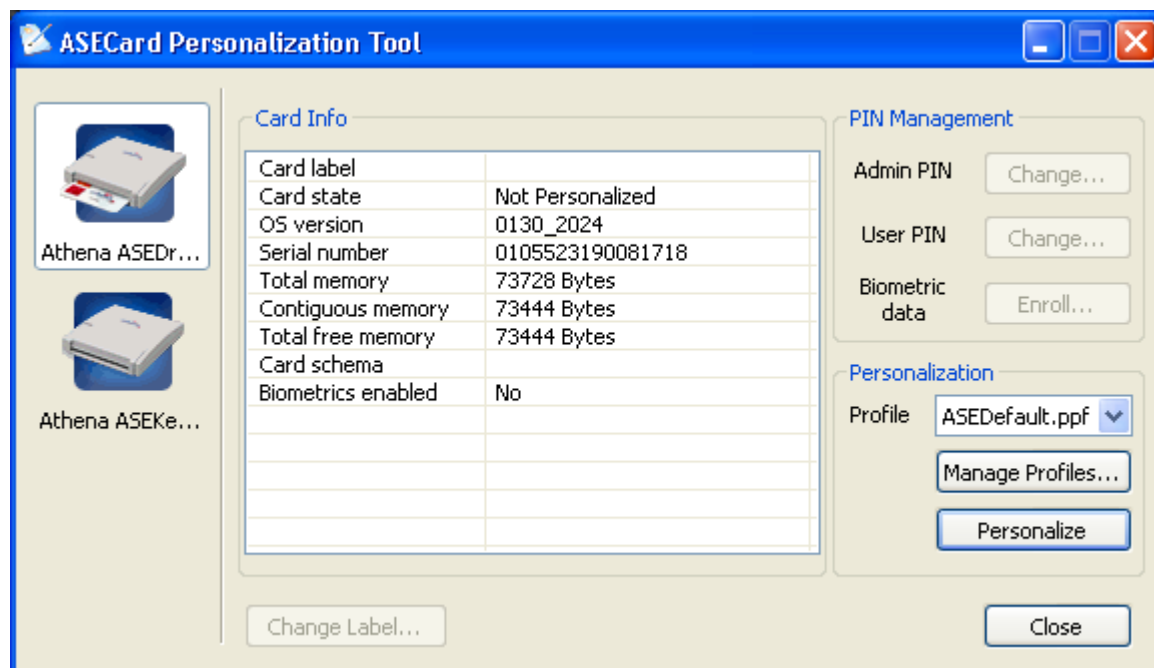


- Insert an ASECard Crypto smart card into an installed smart card reader in order to start working with the **ASECard Personalization Tool**.

The **ASECard Monitor**, which is a background task that monitors smart card events, will identify that the card inserted is not personalized and will show the following warning. You may choose not to show this alert in the future.



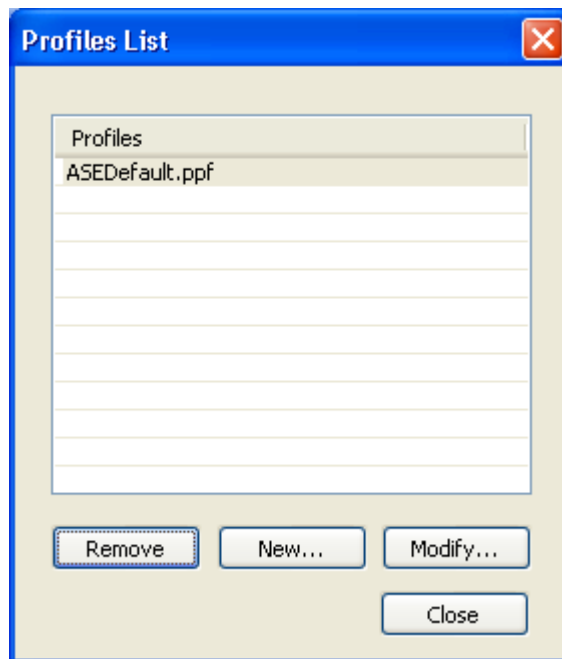
Next, the **ASECard Personalization Tool** window will show the inserted card details while the smart card reader picture, on the left side of the window, will indicate that a card is inserted.



- In order to personalize a card:
 - Select the required *Personalization Profile* from the *Profile* pop-up list.
 - Click the **Personalize** button.
 - Note: If you are re-personalizing a previously personalized card, you will be prompted to enter the **Admin** PIN. ('00000000' is the value indicated in the default profile).
 - Wait for the "Success" message.

- If you would like to review, add, remove, or edit any personalization profile, click the **Manage Profiles...** button.

The **Profile List** window appears:



You may now **select** the *ASEDefault.ppf* profile and click **Modify...** to modify or review the personalization parameters or click **New...** to create a new profile. Clicking **Remove** will delete the selected profile.

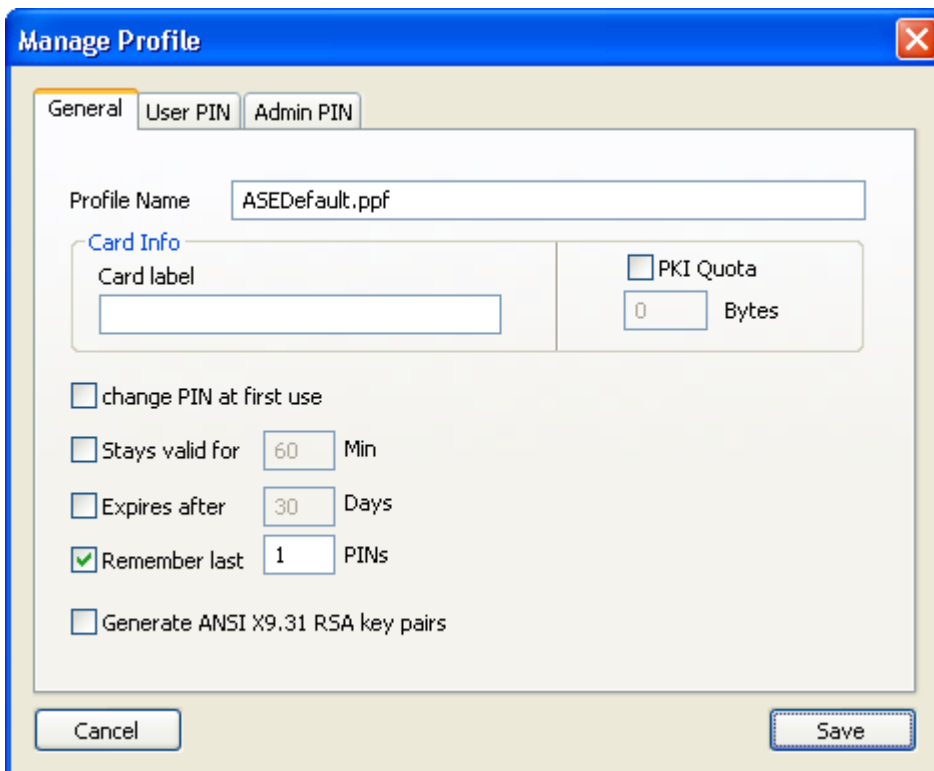
Clicking **Modify...** or **New...** will launch the **Manage Profile** window.

Notes:

- The *ASEDefault.ppf* profile cannot be deleted. It can only be saved under a different name.
- Profiles are saved under the currently logged-on user directory. They are not visible from other accounts, unless they are manually copied there.

The **Manage Profile** window is where you set the security policy and relevant parameters for cards that you plan to personalize. There are 3 separate tabs – **General**, **User PIN**, and **Admin PIN** and each is described below.

I. General Tab



Profile Name – Lets you set a name for a new profile or modify an existing profile name.

Card Info

Card Label – The Card Label is used in order to help you identify the cards you personalize. The label has no effect on any of the Windows smart card services. It is equivalent to the *PKCS#11 Token Label*. If not set by you, the label will automatically default to the “ASECard + Card serial number”.

PKI Quota- ASECard Crypto does not require the Administrator to allocate space for public and private objects. The ASEPCOS card operating system manages this memory dynamically. However, if you would still like to allocate a specific memory size only for PKI, you may select this option and enter the memory size in Bytes. You will need a minimum of 20KByte for normal operation, so avoid allocating less memory.

Change PIN at first use– The user will be prompted the change the **User PIN** at the next use of the card. Aside from changing the PIN, no other PIN protected smart card enabled action will be allowed until the PIN is changed to a new value. The PIN may be changed during the Windows Logon procedure (not supported in Windows Vista).

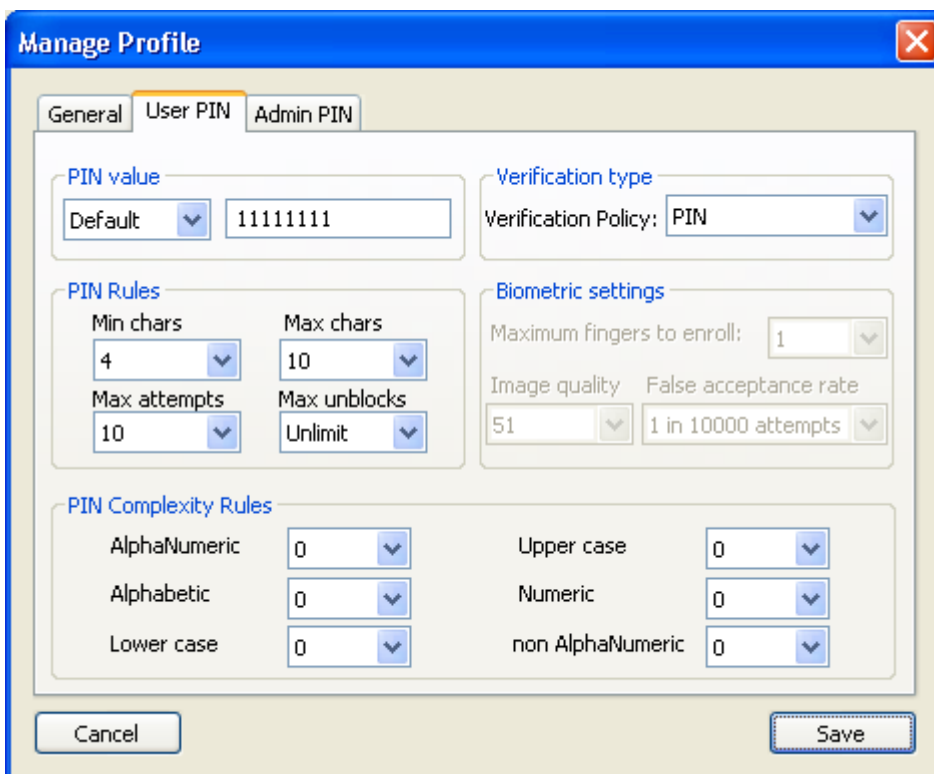
Stays valid for X Minutes– sets the duration in which a verified **User PIN** stays valid. Once X minutes pass, the user will be asked to verify the PIN again.

Expires after X Days – Force the user to change his PIN every X days.

Remember last X PINs – Enforces a policy whereby a new PIN cannot be equal to one of the last X PIN values (up to 16 last values can be stored on the card. For security reasons, only a HASH of the old PIN is stored).

Generate ANSI X.9.31 RSA Key Pairs – forces the card to generate keys according to the specified format.

II. User PIN Tab for PIN Cards



The screenshot shows the 'Manage Profile' dialog box with the 'User PIN' tab selected. The settings are as follows:

- PIN value:** Default (dropdown), 11111111 (text field)
- Verification type:** Verification Policy: PIN (dropdown)
- PIN Rules:**
 - Min chars: 4 (dropdown)
 - Max chars: 10 (dropdown)
 - Max attempts: 10 (dropdown)
 - Max unblocks: Unlimit (dropdown)
- Biometric settings:**
 - Maximum fingers to enroll: 1 (dropdown)
 - Image quality: 51 (dropdown)
 - False acceptance rate: 1 in 10000 attempts (dropdown)
- PIN Complexity Rules:**
 - AlphaNumeric: 0 (dropdown)
 - Alphabetic: 0 (dropdown)
 - Lower case: 0 (dropdown)
 - Upper case: 0 (dropdown)
 - Numeric: 0 (dropdown)
 - non AlphaNumeric: 0 (dropdown)

Buttons: Cancel, Save

Verification type

Verification policy – select PIN for PIN cards (for Bio Cards, see next chapter).

PIN Value

You may select from the pop-up menu, 3 methods to set PINs during personalization:

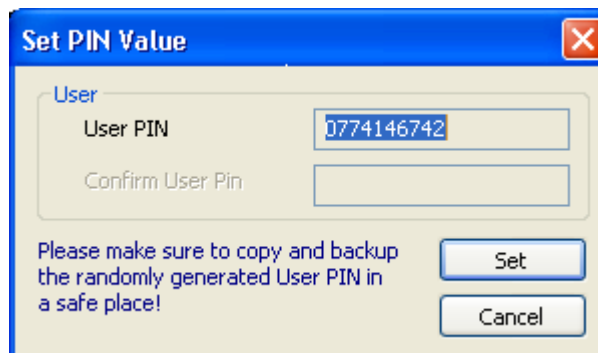
- **Manual** - you will be automatically prompted to enter the **User PIN** during the personalization process of each card.

- **Default** – Each card will be personalized with the default **User PIN** as specified in the Profile.
- **Random** - A random PIN will be generated during the personalization of the card and will be presented to you. You must copy this PIN and save it in a safe place.

Note: If you choose **Random** PIN generation, you must copy the PIN value from the screen and save it in a safe place. There is no way to recover a **Random** PIN, aside from noting it down.

Random PINs are generated according to the PIN complexity rules as set below.

For example, when choosing a **Random User PIN** value, the following dialog will appear during personalization of the card.



Make sure to match the choice of PIN generation options, to your organization security policy.

PIN Rules

Min and Max chars - sets the required length of the **User** PIN.

Max Attempts – The number of unsuccessful consecutive verification attempts, before the **User** PIN is blocked.

Max Unblocks - The number of successful **User** PIN unblocks allowed during the life of a card. Reaching the maximum number will require re-personalization of the card.

Pin Complexity Rules

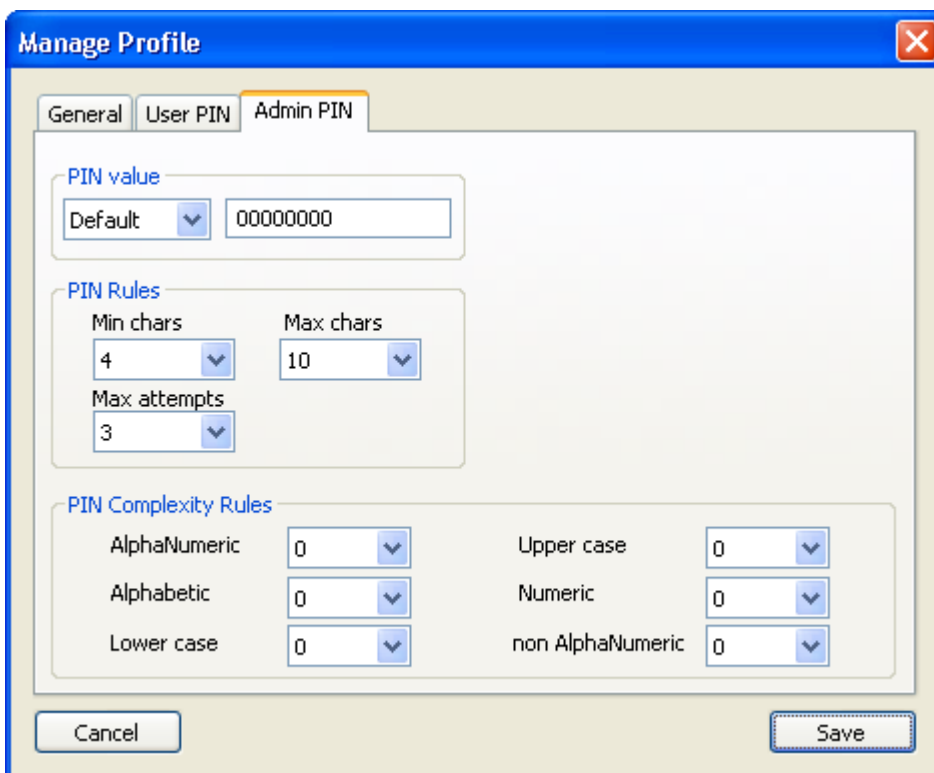
Enable you to apply complexity rules to the **User PIN**, according to your organization security policy.

- You may change any of the parameters in the **Manage Profile** window to suit your security policy. Once you have finished editing, you may save the profile under the same

name, replacing the previously saved profile or save it under a different name (recommended). If you click **Cancel**, any changes made to the current profile will be lost.

Once you decide to use a specific profile for card personalization, select it from the Profile pop-up list in the main **Personalization Tool** window and click **Personalize**.

III. ADMIN PIN Tab

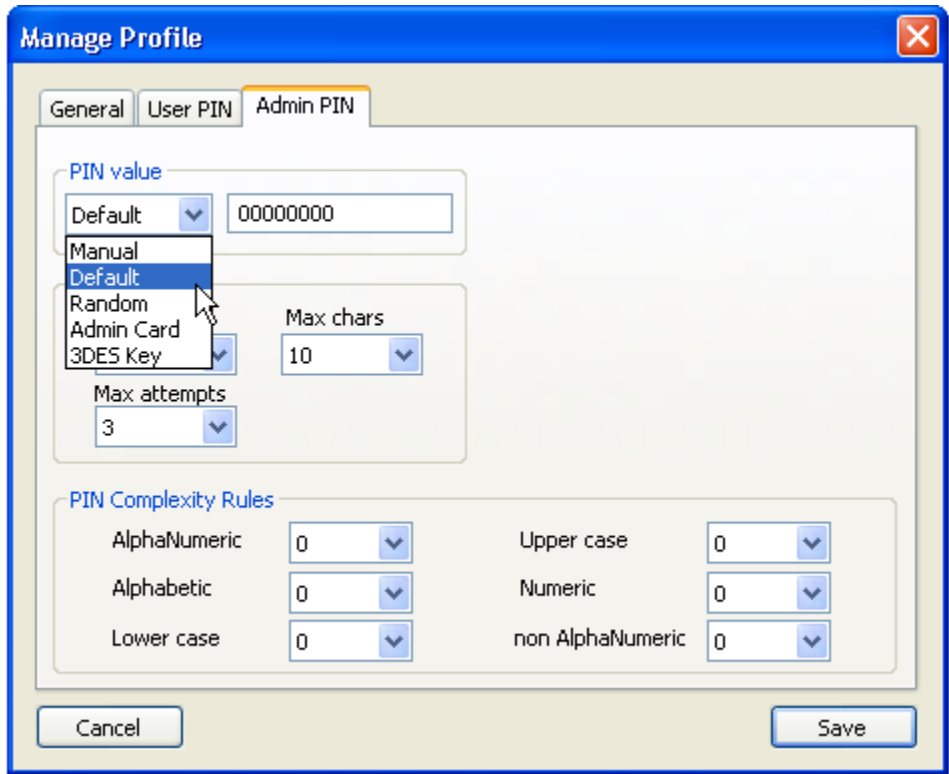


Using the **Admin PIN** tab is similar to the **User PIN** tab. There are 2 main differences:

a. Setting the **Max attempts** on the Admin PIN has important consequences since once the Admin PIN is blocked, the card cannot be used any more.

Warning: Once the Admin PIN is blocked, the card can be still be used but any action requiring the Admin PIN such as User PIN Unlock and Personalization will fail.

b. The **Admin PIN** value can also be set to **Admin Card**. **Admin Card** is a powerful tool for secure card personalization and PIN unlock which is provided separately from this Toolkit. Please contact Athena or your Athena reseller for more details regarding this feature.



4. Using the ASECard Personalization Tool for Bio Cards (see Chapter 3 for personalizing PIN Cards)

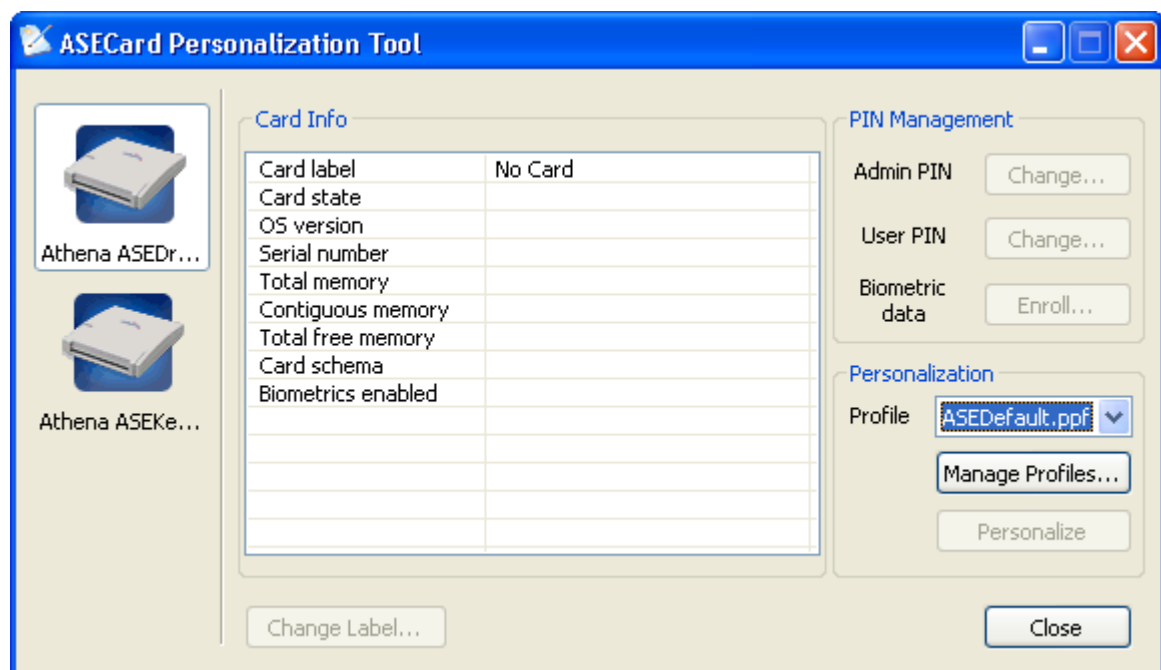
The ASECard **Personalization Tool** is an easy to use tool that provides the Administrator with full control over the card security policy and various card parameters. The tool can be used in order to:

- View card details such as Serial Number, Free Space, etc.
- Change the User and Admin PINs, Enroll biometric data and set a Card Label without invalidating the credentials stored on the card.
- Viewing, editing and creating new *Personalization Profiles*.
- Personalizing and re-personalizing cards.

To start the **ASECard Personalization Tool**:

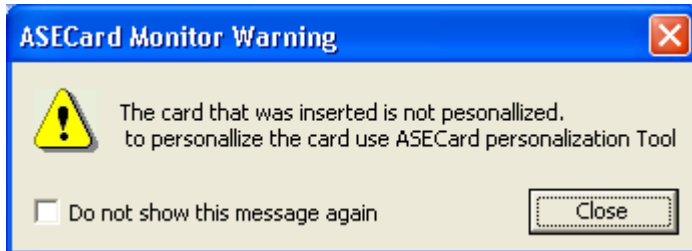
Click **Start ->Programs->ASECard Crypto Toolkit ->ASECard Personalization Tool**

The **ASECard Personalization Tool** window appears:

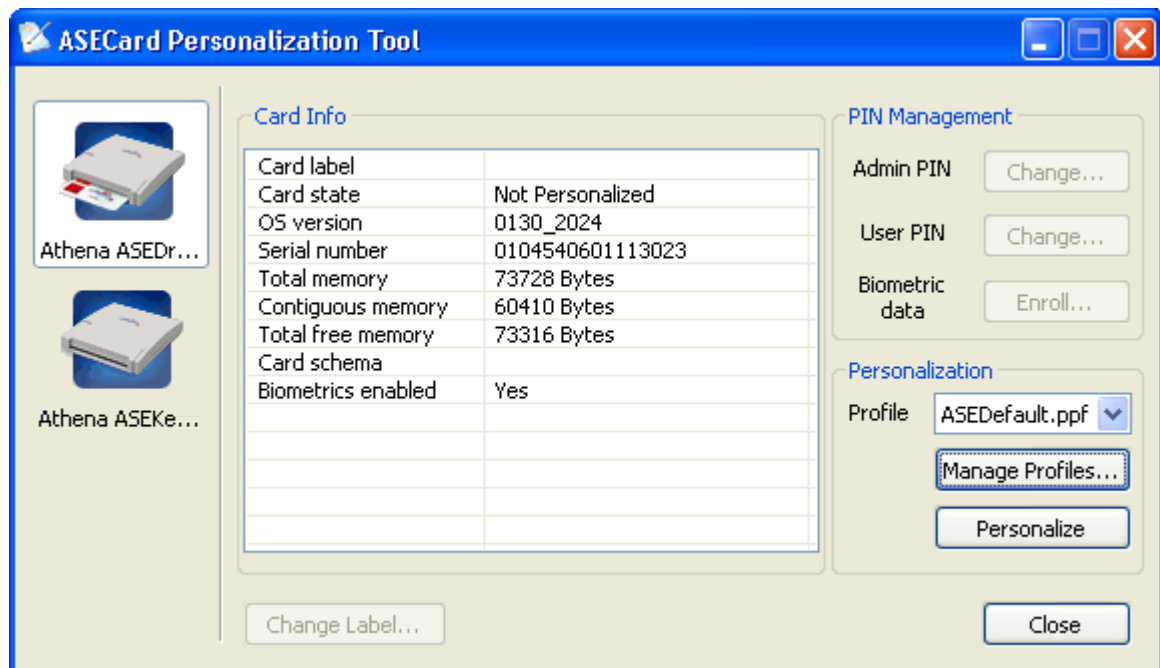


- Insert an ASECard Crypto smart card into an installed smart card reader in order to start working with the **ASECard Personalization Tool**.

The **ASECard Monitor**, which is a background task that monitors smart card events, will identify that the card inserted is not personalized and will show the following warning. You may choose not to show this alert in the future.



Next, the **ASECard Personalization Tool** window will show the inserted card details while the smart card reader picture, on the left side of the window, will indicate that a card is inserted.

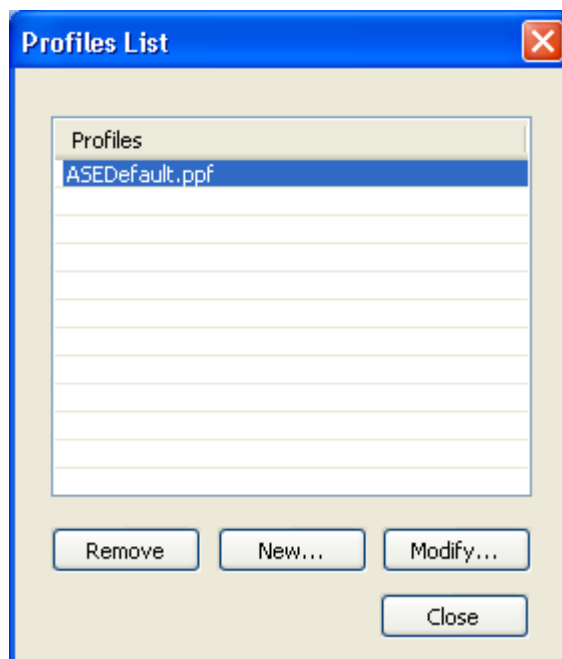


Note: If the **Biometrics enabled** label of the card does not show "Yes", the card cannot be used for Biometrics. Biometric cards are factory programmed to support Biometrics.

- In order to personalize a **Bio Card**:
 - Select the required *Personalization Profile* from the *Profile* pop-up list and make sure that the Verification Type (see below) is set to **Biometric**.
 - Click the **Personalize** button.
 - **Note:** If you are re-personalizing a previously personalized card, you will be prompted to enter the **Admin** PIN. ('00000000' is the default).

- You will be asked to enroll fingerprints (see below).
- Wait for the "Success" message.
- If you would like to review, add, remove, or edit any personalization profile, click the **Manage Profiles...** button.

The **Profile List** window appears:

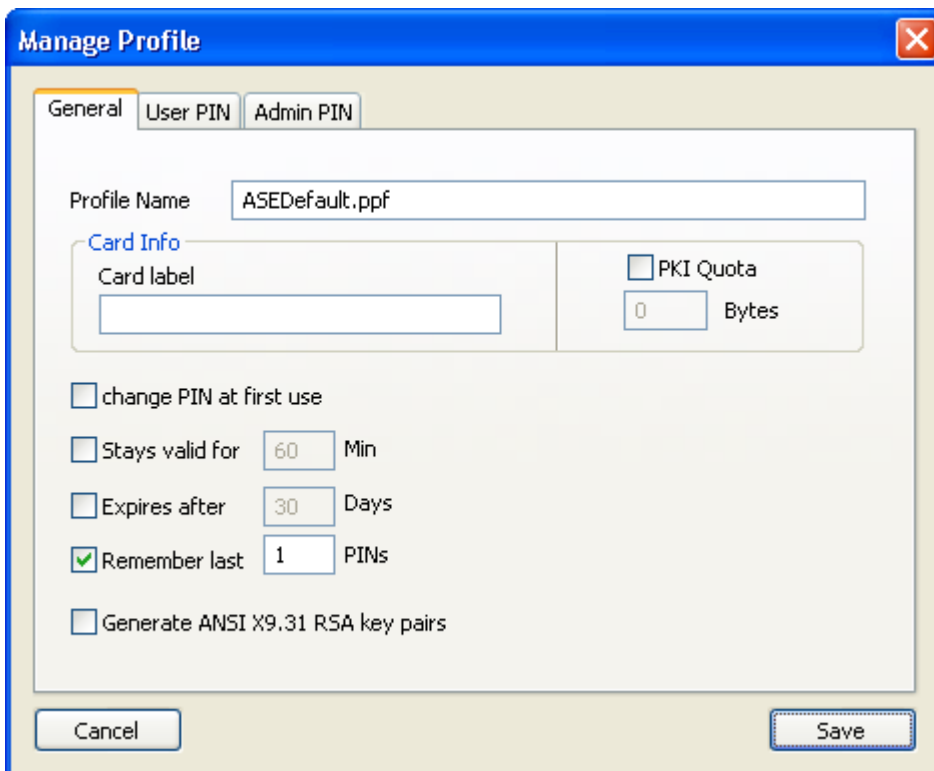


You may now **select** the *ASEDefault.ppf* profile and click **Modify...** to modify or review the personalization parameters or click **New...** to create a new profile. Clicking **Remove** will delete the selected profile.

Clicking **Modify...** or **New...** will launch the **Manage Profile** window.

The **Manage Profile** window is where you set the security policy and relevant parameters for cards that you plan to personalize. There are 3 separate tabs – **General**, **User PIN**, and **Admin PIN** and each is described below.

I. General Tab



The screenshot shows the 'Manage Profile' dialog box with the 'General' tab selected. The 'Profile Name' field contains 'ASEDefault.ppf'. Under the 'Card Info' section, there is a 'Card label' text box, a 'PKI Quota' checkbox (unchecked) with a value of '0' and the unit 'Bytes'. Below this are several checkboxes: 'change PIN at first use' (unchecked), 'Stays valid for' (unchecked) with a value of '60' and unit 'Min', 'Expires after' (unchecked) with a value of '30' and unit 'Days', 'Remember last' (checked) with a value of '1' and unit 'PINs', and 'Generate ANSI X9.31 RSA key pairs' (unchecked). At the bottom are 'Cancel' and 'Save' buttons.

Profile Name – Lets you set a name for a new profile or modify an existing profile name.

Card Info

Card Label – The Card Label is used in order to help you identify the cards you personalize. The label has no effect on any of the Windows smart card services. It is equivalent to the *PKCS#11 Token Label*. If not set by you, the label will automatically default to the "ASECard + Card serial number".

PKI Quota- ASECard Crypto does not require the Administrator to allocate space for public and private objects. The ASEPCOS card operating system manages this memory dynamically. However, if you would still like to allocate a specific memory size only for PKI, you may select this option and enter the memory size in Bytes. You will need a minimum of 20KByte for normal operation, so avoid allocating less memory.

Change PIN at first use– The user will be prompted the change the **User PIN** at the next use of the card. Aside from changing the PIN, no other PIN protected smart card enabled action will be allowed until the PIN is changed to a new value. The PIN may be changed during the Windows Logon procedure (not supported in Windows Vista).

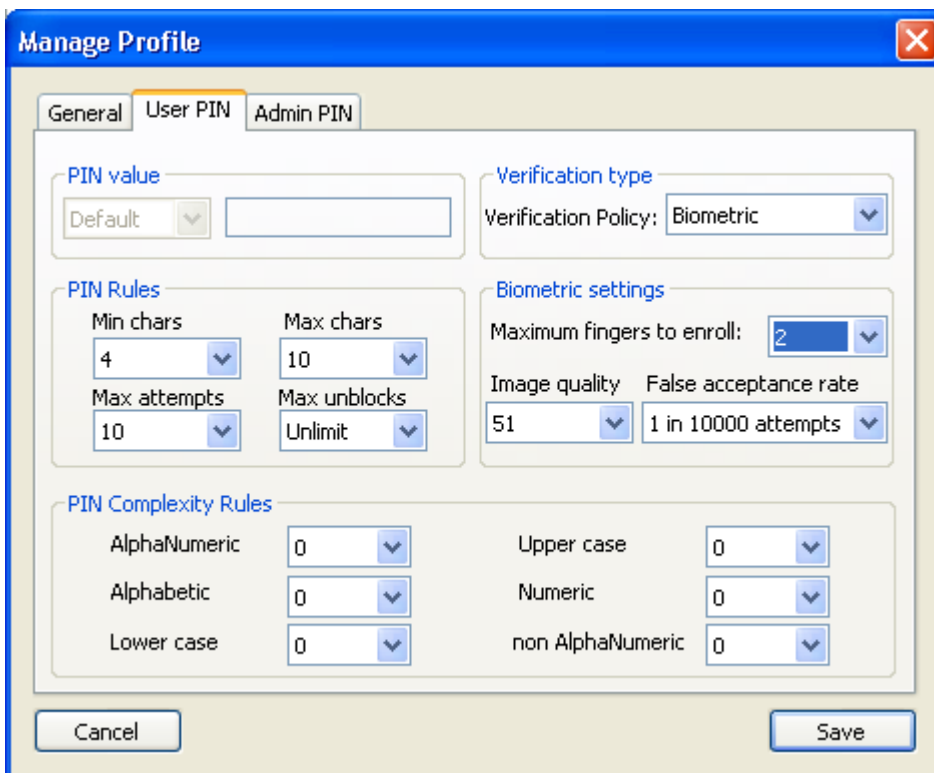
Stays valid for X Minutes– sets the duration in which a verified **User PIN** stays valid. Once X minutes elapsed, the user will be asked to verify the PIN again.

Expires after X Days – Force the user to change her PIN every X days.

Remember last X PINs – Enforces a policy whereby a new PIN cannot be equal to one of the last X PIN values (up to 16 last values can be stored on the card. For security reasons, only a HASH of the old PIN is stored).

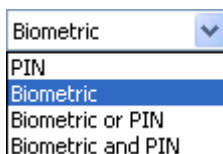
Generate ANSI X.9.31 RSA Key Pairs – forces the card to generate keys according to the specified format.

II. User PIN Tab for Bio Cards



Verification type

Verification policy – you may select from the following choices:





PIN – Only PIN verification will be supported. (Same as a **PIN Card**)

Biometric – Only fingerprint verification will be supported by the card.

Biometric or PIN – Either a PIN or a fingerprint matching may be used for verification.

Biometric and PIN - Both a PIN and a fingerprint verification must be used , allowing for true 3 factor authentication.

Biometric settings

Maximum fingers to enroll - you may choose to enroll between 1 to 10 fingers for each card. While your actual selection will be subject to your organizations security policy, it is recommended that a minimum of 2 fingers, one from each hand, will be enrolled in order to provide a fallback in cases where a finger is injured or not read properly by the biometric sensor.

Image quality – Sets the minimum threshold for image capture quality below which enrollment of the fingerprint will not be attempted. This setting can be different for each finger enrolled.

False Acceptance Rate (FAR) – The measure of the likelihood that the biometric system will incorrectly accept an access attempt by an unauthorized user. The FAR is stated as the ratio of the number of false acceptances divided by the number of identification attempts.

PIN Rules

Min and Max chars - sets the required length of the **User PIN**.

Max Attempts – The number of unsuccessful verification attempts, before the **User PIN** is blocked.

Max Unblocks - The number of successful **User PIN** unblocks allowed before the **User PIN** is blocked.

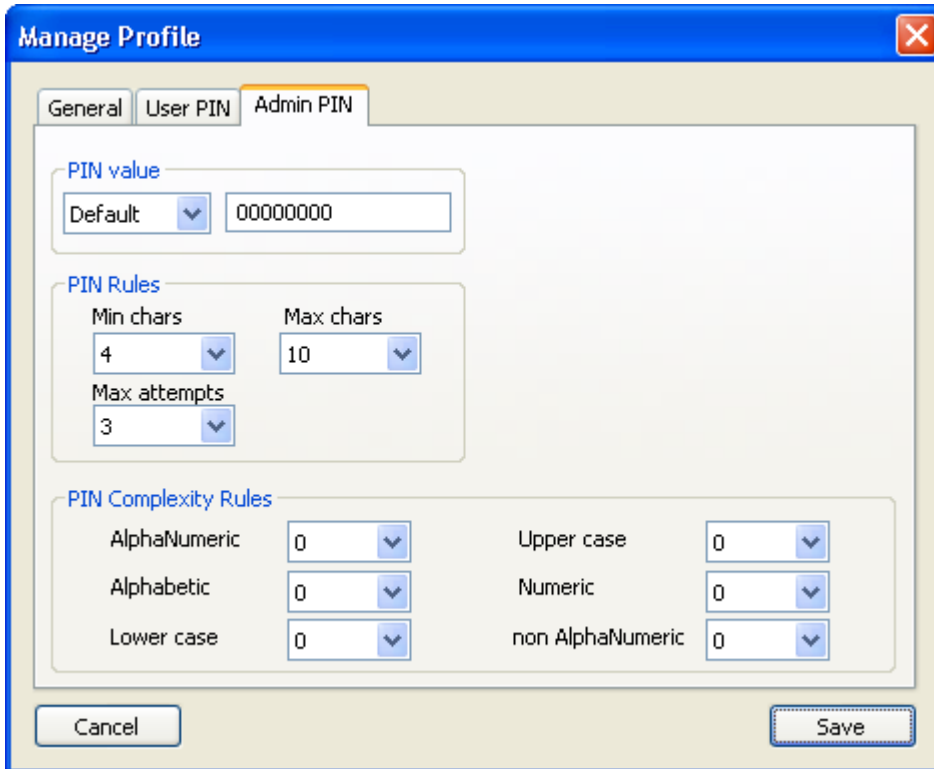
Pin Complexity Rules

Enable you to apply complexity rules to the **User PIN**, according to your organization security policy.

- You may change any of the parameters in the **Manage Profile** window to suit your security policy. Once you have finished editing, you may save the profile under the same name, replacing the previously saved profile or save it under a different name (recommended). If you click **Close**, any changes made to the current profile will be lost.

Once you decide to use a specific profile for card personalization, select it from the Profile pop-up list in the main **Personalization Tool** window and click **Personalize**.

III. ADMIN PIN Tab

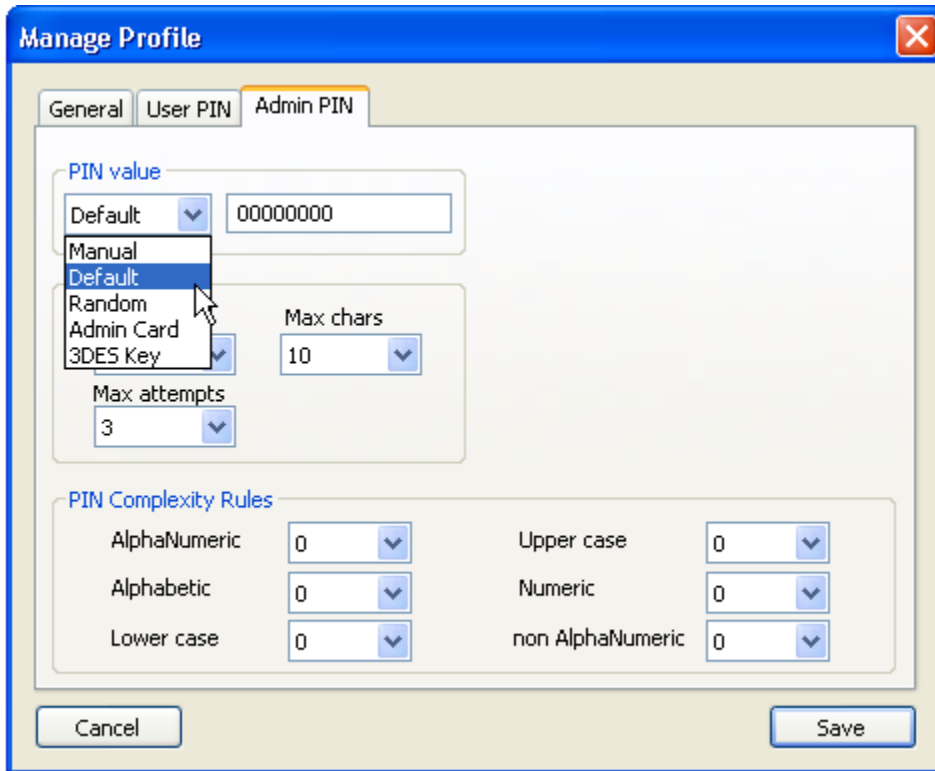


Using the **Admin PIN** tab is similar to the **User PIN** tab. There are 2 main differences:

a. Setting the **Max attempts** on the Admin PIN has important consequences since once the Admin PIN is blocked, the card cannot be used any more.

Warning: Once the Admin PIN is blocked, the card can be still be used but any action requiring the Admin PIN such as User PIN Unlock, Biometric Enrollment and Personalization will fail.

b. The **Admin PIN** value can also be set to **Admin Card**. **Admin Card** is a powerful tool for secure card personalization and PIN unlock which is provided separately from this Toolkit. Please contact Athena or your Athena reseller for more details regarding this feature.



4.1 Personalizing a Bio Card

Personalizing a biometric card requires the following steps:

1. Installing a biometric smart card reader.
2. Running the ASECard Personalization Tool
3. Selecting (and modifying if required) a biometric profile (see Chapter 4, above).
4. Inserting a **Bio Card** into the smart card reader.
5. Clicking "**Personalize**"
6. If the card was personalized before, you will be asked to key-in the **Admin PIN** ("00000000" by default).
7. The Personalization tool will walk you through fingerprint enrollment as outlined below.

Fingerprint Enrollment

After clicking "**Personalize**" the ASECard Enroll dialog will pop-up and you will be prompted to select the first finger to enroll and click "**Enroll**".



The ASECard Enroll dialog will now indicate the current finger being enrolled by flashing a green dot above the enrolled finger.



You can select a biometric reader from the pull-down menu, in case you have more than one installed.

The "**Status**" window provides instructions throughout the enrollment process.

After placing the correct finger on the sensor, you will be asked to lift it and place it again for a total of 2 times. Make sure to completely remove the finger before placing it again on the sensor.

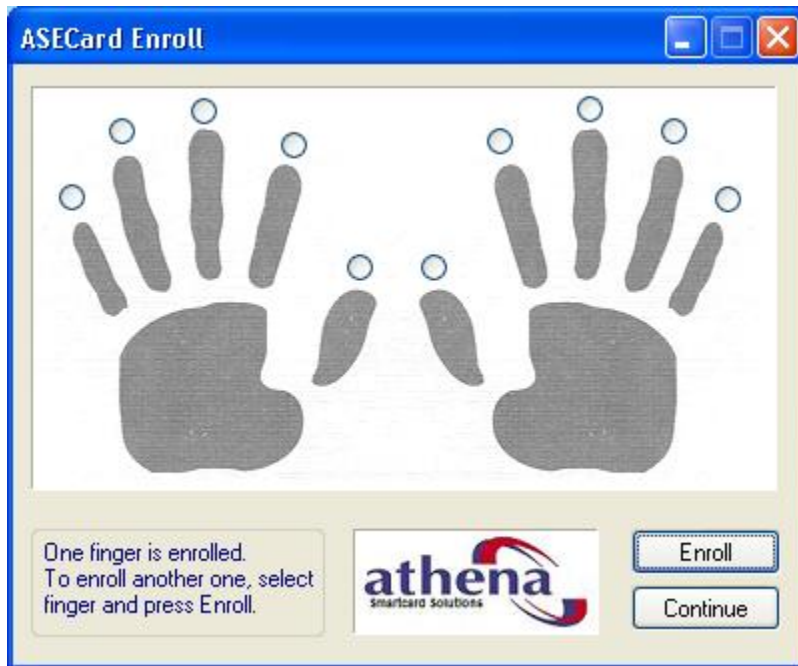


After placing the correct finger twice, you reach the verification stage for this fingerprint, as shown below:



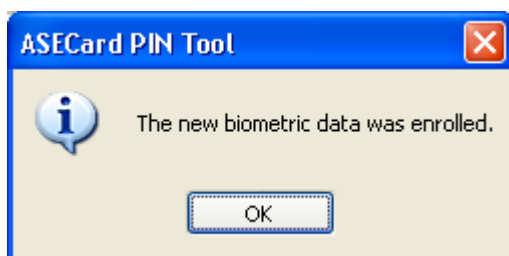


After successful verification of the first finger, you will be asked to select the next finger to enroll:

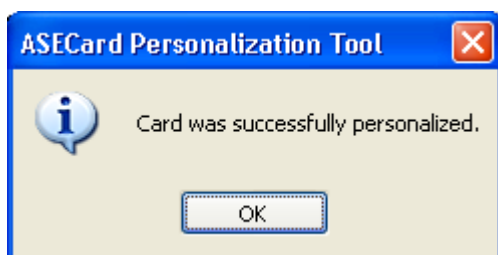


The process will continue until all fingers are enrolled, up to the number of fingers set in the Personalization Profile, as outlined in the beginning of this chapter. At any time, you may click "Continue" in order to skip the enrollment of one or more fingers. You will be able to continue finger enrollment using the Biometric Enrollment tool (see Chapter 6). In any case, the card will be regarded as "Personalized" even if no fingers are enrolled. From this point and on, Biometric Enrollment or re-personalization of the card will require the **Admin PIN** or **Admin Card**.

If you completed the finger enrollment successfully, the following message appears:



Followed by:



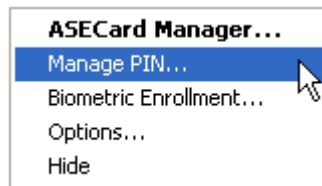
5. Changing or Unblocking the User PIN

As mentioned previously, it is possible to change the **User** and **Admin PINs** without re-personalizing the card. There are several ways to access the Change/Unblock PIN tools.

5.1 Changing the User PIN from the PIN Tool in the System Tray

The End User may change the **User PIN** of her card at any time by following this procedure:

Right-clicking the **ASECard Monitor** icon  in the System Tray and selecting the **Manage PIN...** menu

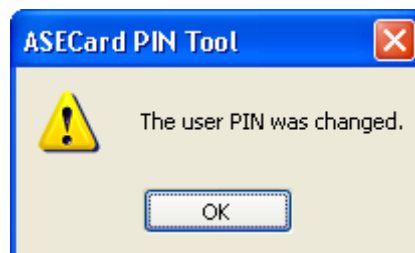


The **Change User PIN** window will appear, prompting the user to enter a new PIN.

(The default **User** PIN on the card is: '1111111')



When completed, the following dialog will appear:



Please note: If the user enters a wrong PIN several times until the Maximum Attempts number is reached (default max attempts is 10), he/she will block the card and will no longer be able to communicate with it. In order to have access to the card again, the User PIN will have to be unblocked using the **Admin** PIN.

5.2 Changing the User PIN from the PIN Tool in the Card Manager

Click **Start > All Programs > ASECard Crypto Toolkit 4.x > ASECard Manager Tool** and Select **Manage PIN...** from the **PIN** menu

5.3 Changing the User PIN from the Personalization Tool

Click **Start > All Programs > ASECard Crypto Toolkit 4.x > ASECard Personalization Tool** and click on the **User PIN Change...** button in the **Personalization Tool** window.

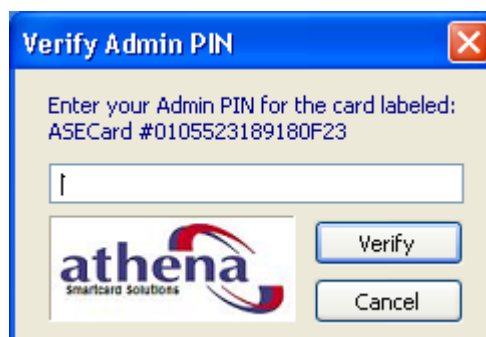
Continue and change the PIN as described in section 4.1 above.

Note: The User PIN can also be changed during normal operation of the card, whenever the User is presented with a Verify PIN dialog box. She simply has to choose the *Change PIN after verification* Tick Box and she will be prompted to change the PIN after successful verification of the current PIN.

5.4 Unblocking a blocked User PIN

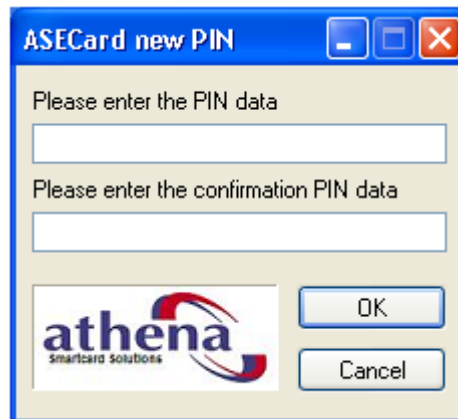
When a user enters a wrong PIN value several times until the Max Attempts parameter which was set during the card personalization (the default is 10 attempts) is reached, the **User** PIN becomes blocked and can only be unblocked using the **Admin** PIN.

Selecting the **PIN Tool** from the System Tray or the **ASECard Manager** menu will bring up the following dialog:



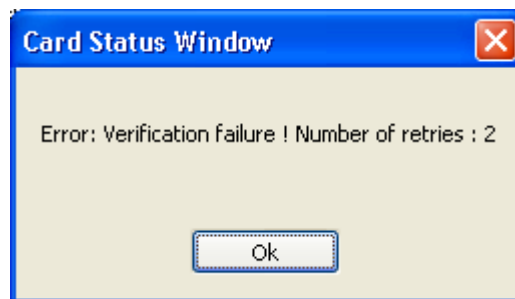
The Administrator will now have to enter the **Admin** PIN.

Please note that you will be presented with a different dialog if you are using an Admin Card or other method of Unblocking.



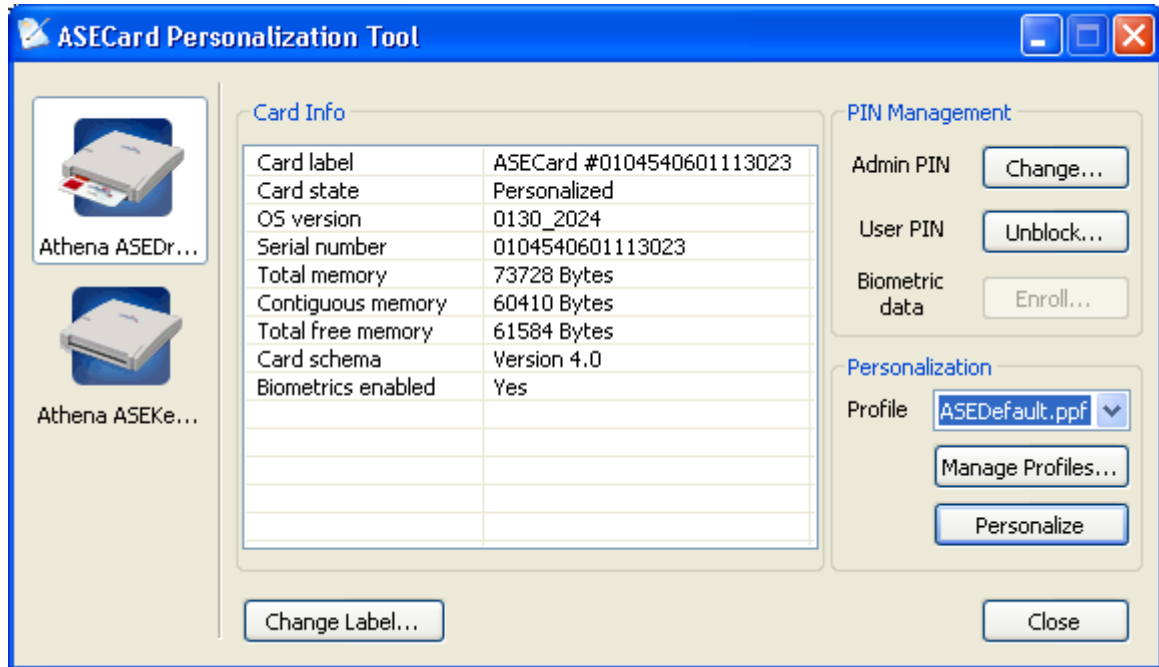
The Administrator will now have to enter and confirm a new value for the **User** PIN.

If the **Admin** PIN which was entered was wrong, the following message will appear:



Note: After 2 additional (unsuccessful) attempts (or as set in the Max Attempts parameter of the Admin PIN in the profile used to personalize the card), the card will be blocked. Once blocked, the card **cannot** be used or re-personalized.


When a **User PIN** is blocked, the **User PIN** button in the *Pin Management* area of the **ASECard Personalization Tool** will change from **Change...** to **Unblock...** as shown in the picture below:

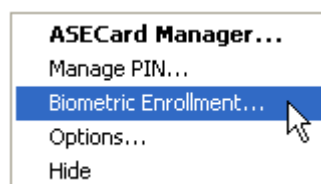


Clicking the **Unblock...** button will open the **Change User PIN** dialog as explained above.

6. Biometric Enrollment

Enrolling fingerprints is the **Bio Card** equivalent of Changing a PIN in a PIN Card. One of the main differences is that you must enter an **Administrator PIN** before enrollment. You can select to enroll fingerprints from the Personalization tool, from the ASECard Manager tool or from the **ASECard Monitor** as outlined below:

Right-clicking the **ASECard Monitor** icon  in the System Tray and selecting the **Biometric Enrollment...** menu

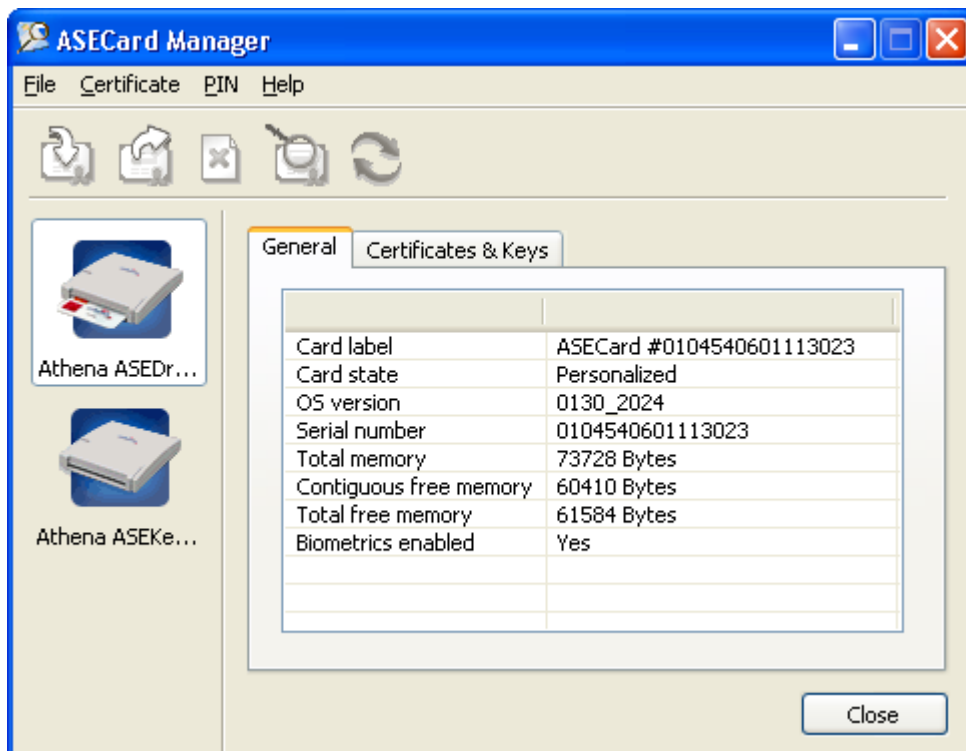


The process of Biometric Enrollment is described in section 4.1 above.

7. The ASECard Manager Tool

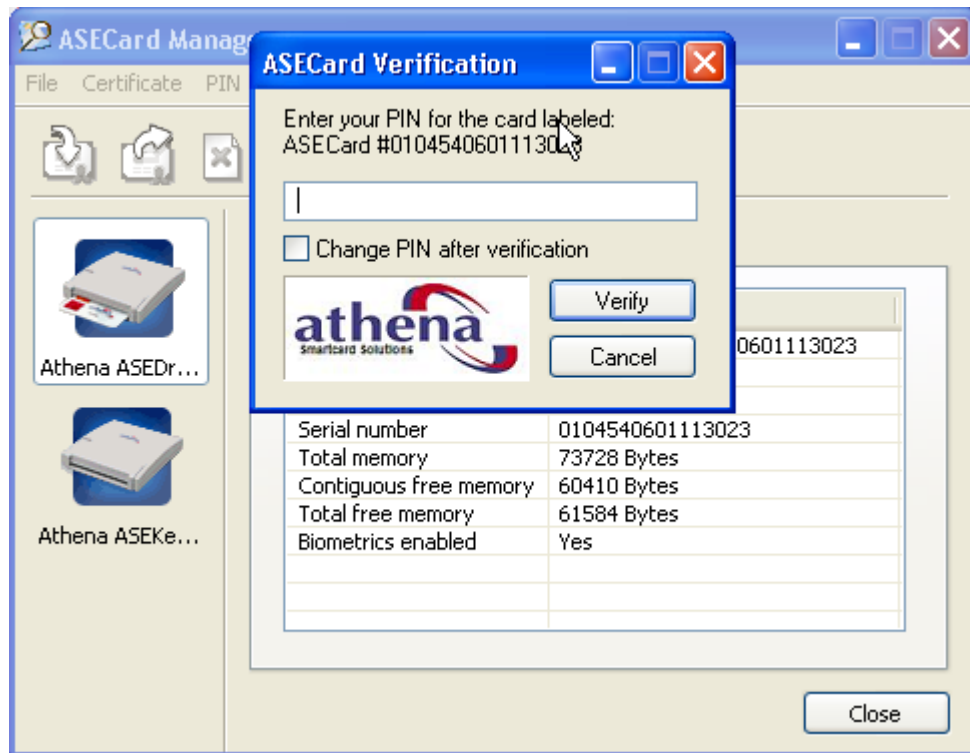
The **ASECard Manager Tool** may be installed on the end-User PCs or just on the Administrator workstation, as set in the Installation options described in Chapter 1.

The **ASECard Manager Tool** is accessed from **Start ->Programs->ASECard Crypto Toolkit ->ASECard Manager Tool** or by double-clicking its System Tray icon.



The **ASECard Manager** Tool displays the inserted card information and enables managing of the User PIN and viewing details about certificates and keys stored on the card.

Clicking on the Certificates & Keys tab will display information and enable managing of certificates, following verification of the User PIN and/or Fingerprint verification.



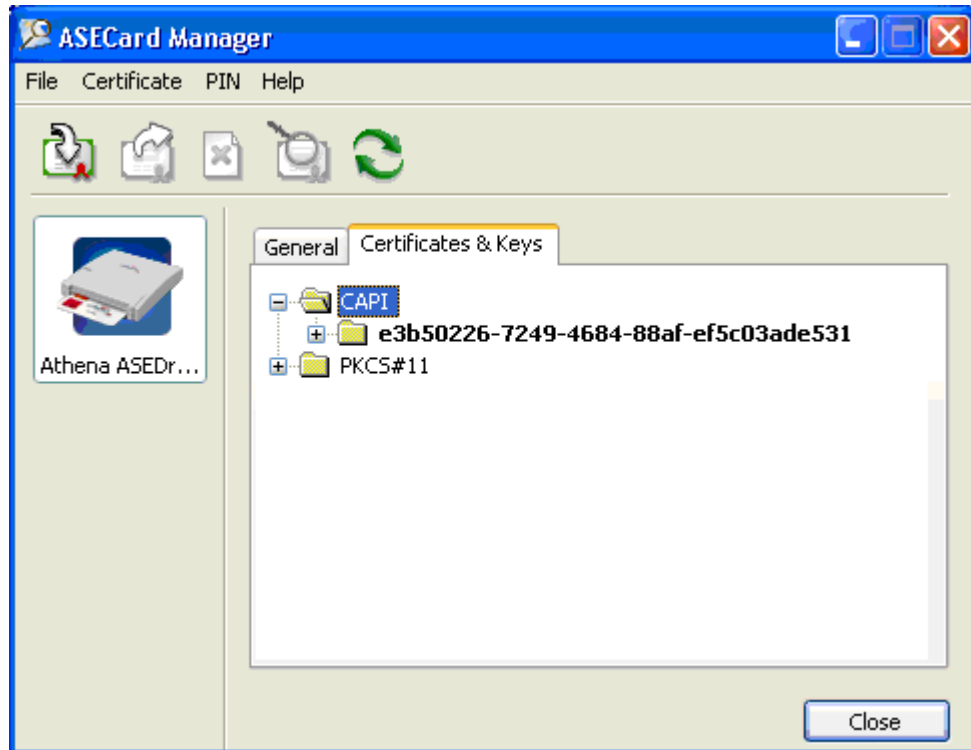
The ASECard Manager window opens and displays 2 main areas:

CAPI – This is the area of the card dedicated for saving certificates and keys according to Microsoft CAPI specifications. Microsoft Windows Smartcard Logon and Smartcard User certificates are stored in this area of the card, for example.

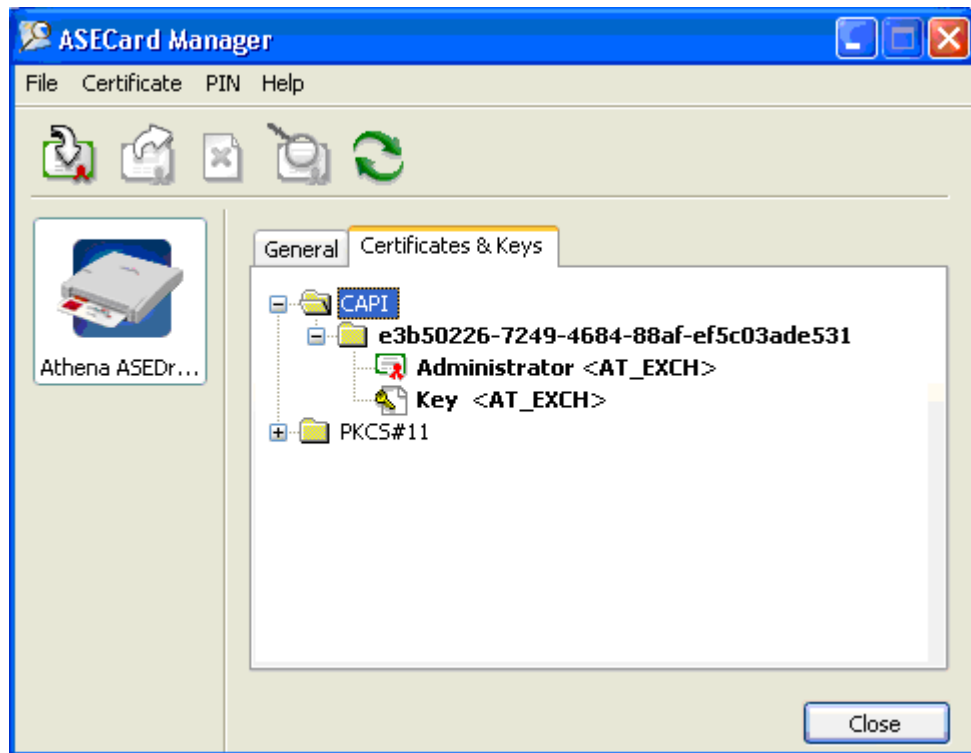
PKCS#11 – Storage area for certificates, keys, and objects that conform to the PKCS#11 specifications. PGP, Mozilla/Netscape generated certificates and keys are stored here.

Note: Containers (certificates and keys) which are created in the **CAPI** area of the card are also accessible through the **PKCS#11** API (used by applications such as PGP, Netscape/Mozilla/Firefox, etc.) however containers created in the **PKCS#11** area are not accessible through **CAPI**.

Clicking once on the CAPI folder or "+" sign will open the folder to reveal its content. If a Windows Logon or Smartcard User certificate was already downloaded to the card, the CAPI folder will display the container name associated with the certificate.




Clicking the container label or "+" sign will further open the folder to reveal the certificate and key stored. In the example shown below, a certificate was issued to the user "Administrator" and a private key is associated with this certificate and stored on the card.



You may now use the drop down menus, Toolbar Icons, or right-click menu to perform the following operations on the card:

- **Importing certificates** – enables the importing of several types of certificates, including .cer certificates that include only the certificate itself without the private key, and .P12 and .pfx files that include both the certificate and the private key associated with it.
- **Exporting certificates** – enables exporting of a certificate using the .cer format.
- **Deleting objects**- most objects can be deleted, unless they are part of a CAPI Default Container. Parts of a Default Container can be deleted only after designating another container as Default.
- **Viewing certificate information** – Double clicking on the certificate opens the Microsoft Certificate viewer tool
- **Refreshing the display**

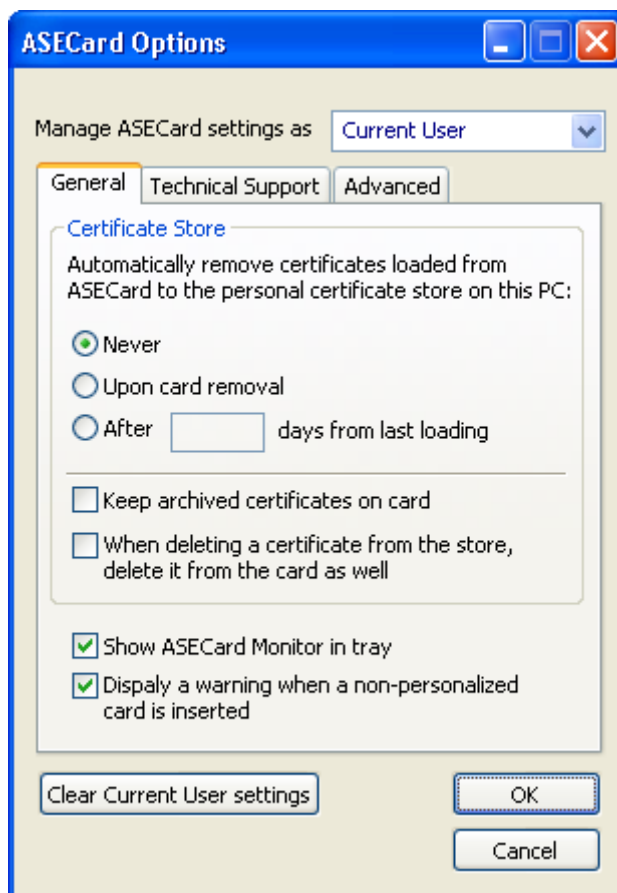
8. ASECard Manager Options...

Selecting the **Options...** menu from the **File** menu of the **ASECard Manager** (or right-clicking the **ASECard Monitor** icon  in the System Tray) opens the **ASECard Options** dialog.

Options are set either for the computer's "Current User" or for the "Local Machine" in which case the options set will become the default settings for each user, unless there is a specific setting for that user.

The **ASECard Options** window has 3 tabs:

I. General – provides access to Certificate settings and ASECard Monitor display options.



Certificate Store options

Whenever a card is inserted into a reader, the **ASECard Toolkit** automatically loads the certificates found on the card to the certificate store of the currently logged-on user. Normally, User Certificates are loaded to the **Personal** certificate store, and other certificates, such as CA certificates are stored in the **Trusted Root CA** and **Intermediate CA** stores.

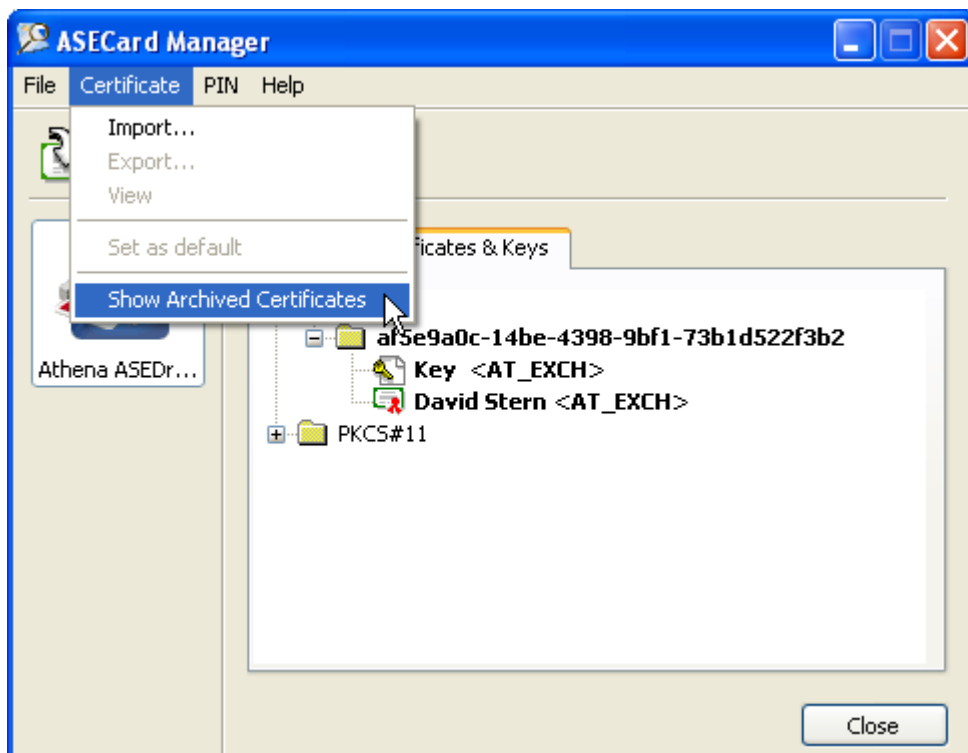
By default, when a card is removed, the certificates that were loaded when the card was inserted are not removed from the **Personal** Certificate Store. You can change this setting in the **Options** dialog:

<input checked="" type="radio"/> Never	Certificates loaded from the card, will not be removed when the card is removed from the reader. This is the default behavior.
<input type="radio"/> Upon card removal	Certificates that were loaded when the card was inserted will be removed when the card is removed. Note - this only applies to certificates loaded to the Personal store.
<input type="radio"/> After <input type="text" value=""/> days from last loading	Certificates that were loaded from a card will be removed from the Personal certificate store X days after the card was last introduced to the reader.

Archiving Certificates

Whenever a certificate is renewed Microsoft Windows marks the certificate with the "archived" status. In such case, it is also possible to archive the certificate on the card.

In order to view archived certificates on the card Select "Show Archived Certificates" from the Certificate menu of the ASECard Manager.



In order to view archived certificates in the Microsoft Windows Certificate Store, run the MMC – Certificates snap-in, select 'Certificates – current user' and make sure it is highlighted, and then View->Options, and click the 'Archived certificates' check box. The certificates will then appear and the 'status' field will show if the certificate is archived.


<input type="checkbox"/> Keep archived certificates on card	Whenever Microsoft archives a card based certificate, archive on the card as well.
---	--

Deleting Certificates

By default, when certificates are deleted from the Windows Certificate Store, they are not deleted from the card. The following option enables deleting of certificates from the card in such case.

<input type="checkbox"/> When deleting a certificate from the store, delete it from the card as well	<p>Will delete the certificates from the card if the card is in the reader when the certificates are deleted from the PC certificate store. Removal of certificates requires entering the User PIN code.</p> <p>Important Note: Do not use this option if you are issuing certificates "On behalf" of another user. When doing so, Microsoft Windows removes the certificate from the store and it will also be removed from the card.</p>
--	---

Other options

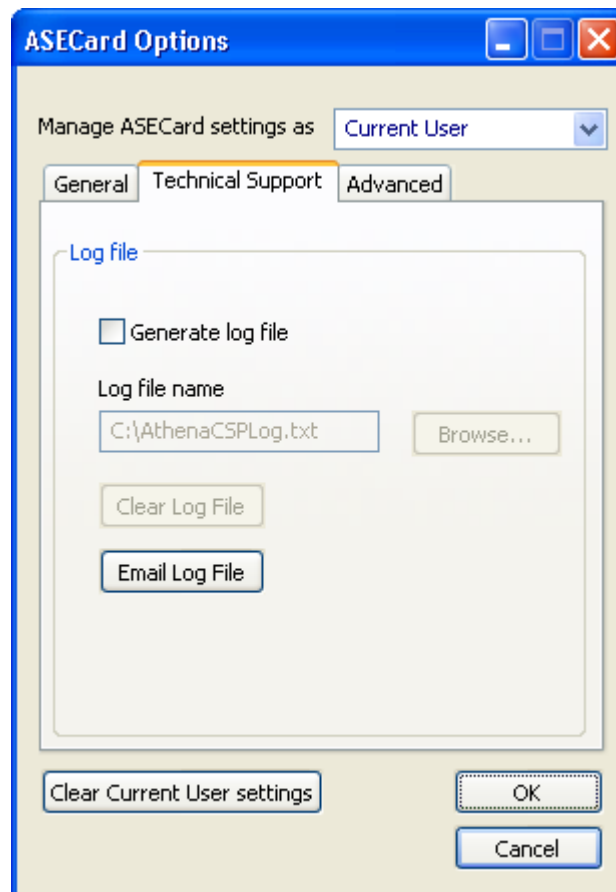
<input checked="" type="checkbox"/> Show ASECard Monitor in tray	Will toggle between showing and hiding the ASECard Monitor icon  in the System Tray.
--	---

<input checked="" type="checkbox"/> Display a warning when a non-personalized card is inserted	Will toggle between showing and hiding the "non-personalized card" warning.
--	---

<input type="button" value="Clear Current User settings"/>	Will restore the settings for the Current User to those of the Local Machine.
--	---

When selecting the "Manage ASECard Settings" for the **Local Machine**, the above mentioned button will change to Force Local Machine settings and the settings will override all other user settings.

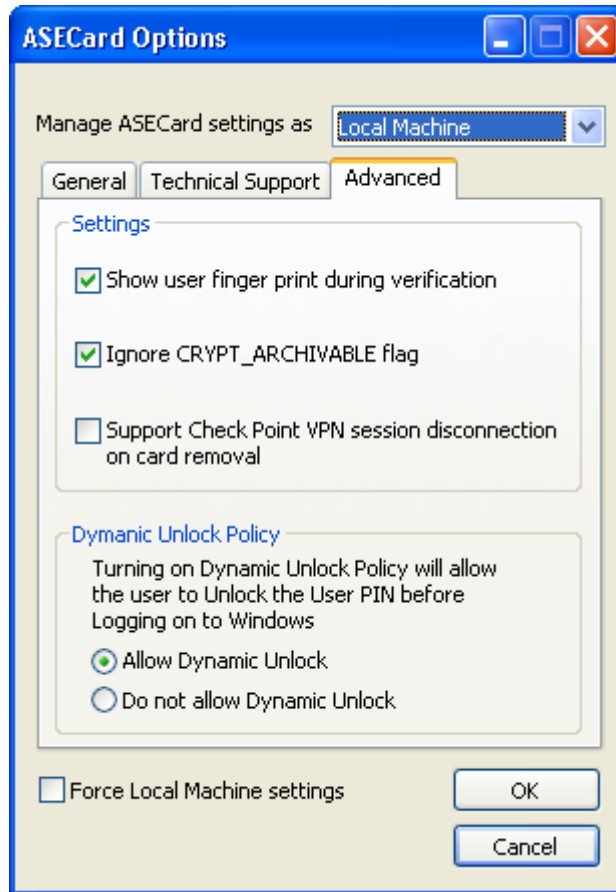
II. Technical Support – enables generating, clearing and e-mailing log files.



<input checked="" type="checkbox"/> Generate log file	Will generate a log file of the ASECard Crypto Toolkit events in the designated location.
<input type="button" value="Clear Log File"/>	Clears the log file, if exists.
<input type="button" value="Email Log File"/>	Attempts to open the e-mail client and attach the generated log file so that it can be sent to Athena's technical support department.

Note: Log files should be created only if instructed so by a technical support representative. After creating the log file, remove the check mark from the check box.

III. Advanced – enables unlock of cards without logon to Windows, provides support for Checkpoint firewall “disconnect session upon card removal” option and sets other features.



Settings

<input checked="" type="checkbox"/> Show user finger print during verification	You can choose to display a “dummy” fingerprint figure or the real fingerprint image captured. Please note that when using biometric readers that utilize Match-on-Reader only a “dummy” fingerprint image can be displayed.
<input checked="" type="checkbox"/> Ignor CRYPT_ARCHIVABLE flag	Clear this flag if you need to generate keys that can be archived.
<input type="checkbox"/> Support Check Point VPN session disconnection on card removal	Disconnects Checkpoint VPN session when a card is removed.

Dynamic Unlock Policy

One of the "Catch-22" situations with Windows Smart Card Logon is the fact that if one inadvertently locks the User PIN (after too many failed attempts) she cannot logon to Windows in order to use the PIN tools that will allow her to unblock the PIN.

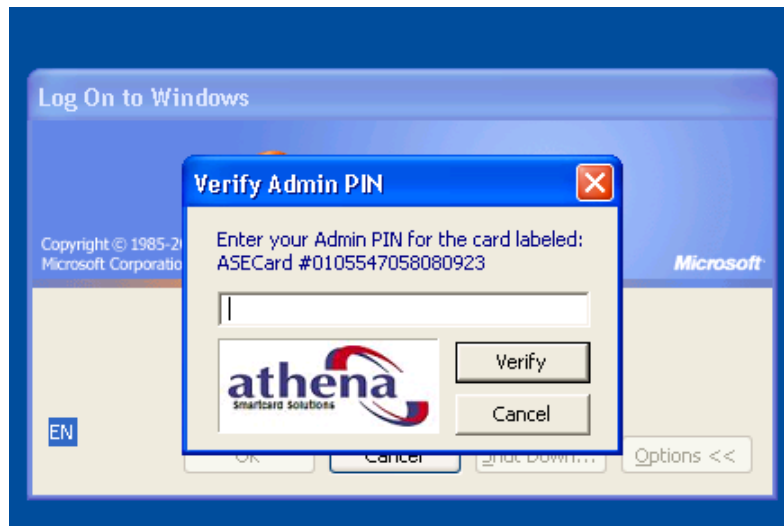
ASECard Crypto Toolkit provides a unique tool that displays a PIN Unlock dialog whenever a locked card is inserted to a reader during a Windows Logon attempt.

<input checked="" type="radio"/> Do not allow Dynamic Unlock	Does not show the PIN Unlock dialog whenever an attempt is made to use a locked User PIN.
<input type="radio"/> Allow Dynamic Unlock	Shows the PIN Unlock dialog whenever an attempt is made to use a locked User PIN.

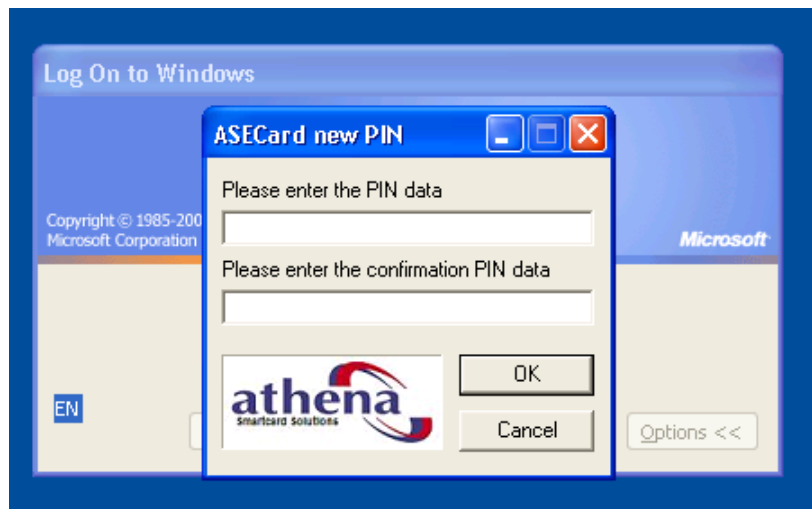
When an attempt is made to logon to Windows with a locked card and the Dynamic Unlock option is allowed, the following Dialog will be displayed.



Click OK in order to continue the Unlock PIN process.



You are prompted to enter the Admin PIN. Enter the correct Admin PIN and click Verify to continue.



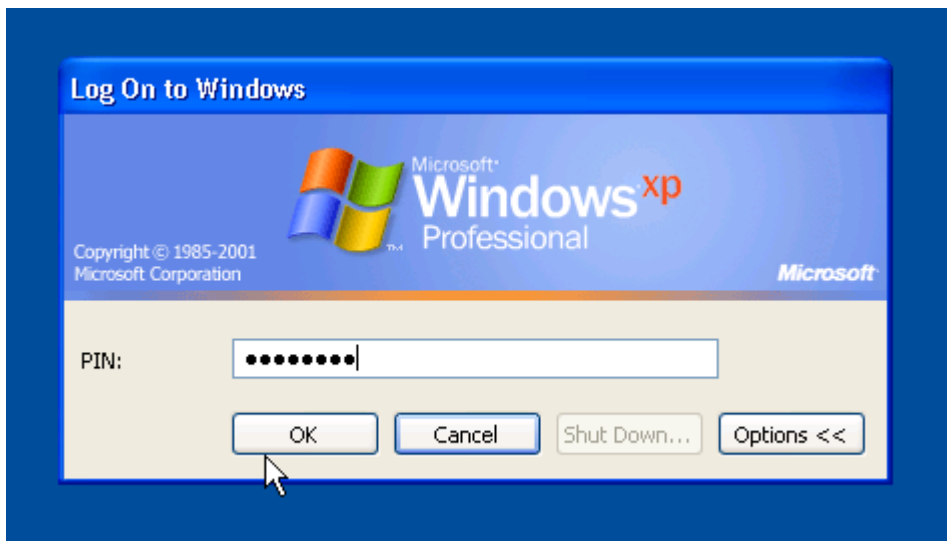
You are prompted to enter and confirm a new User PIN. Click OK to continue.

After clicking OK, Windows will display an error. This is actually a “delayed” message, and should be disregarded.



Click OK, and then remove and insert the card.

The new PIN can now be entered and Windows will log you in.

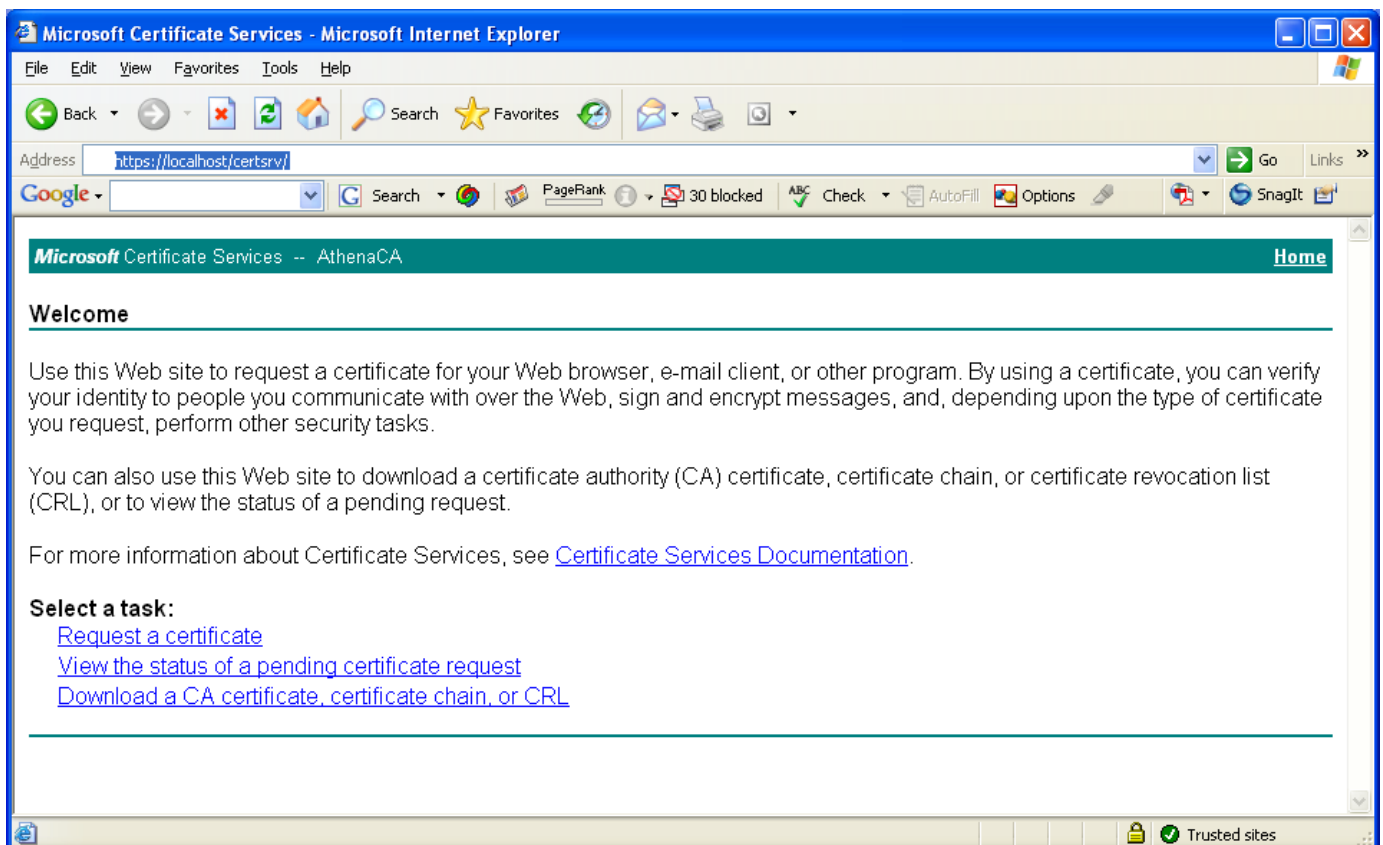


Note: Dynamic Unlock is not supported in Windows Vista

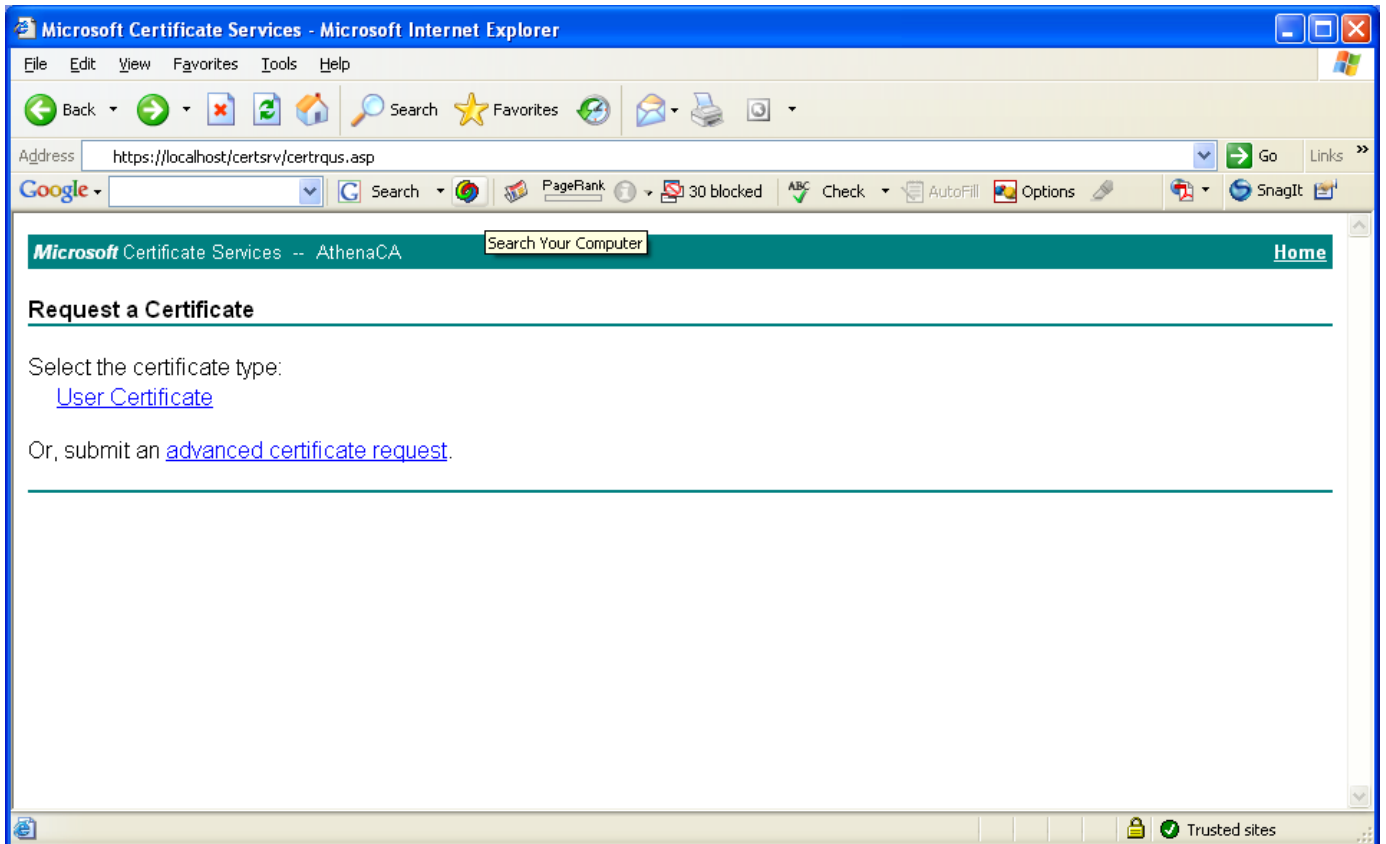
9. Smart Card User/Logon Certificate Enrollment

Following personalization of the **ASECard Crypto** cards, you are now ready to enroll a user for **Smart Card Logon** or **Smart Card User** certificates. This chapter assumes that you have already set up a Smart Card Enrollment Station as outlined in a separate document.

- 1 Type `http://<host>/certsrv` into the **Address** field of Microsoft Internet Explorer and press **Enter**.
- 2 The **Microsoft Certificate Services** Welcome page will appear. Click on **Request a certificate**.

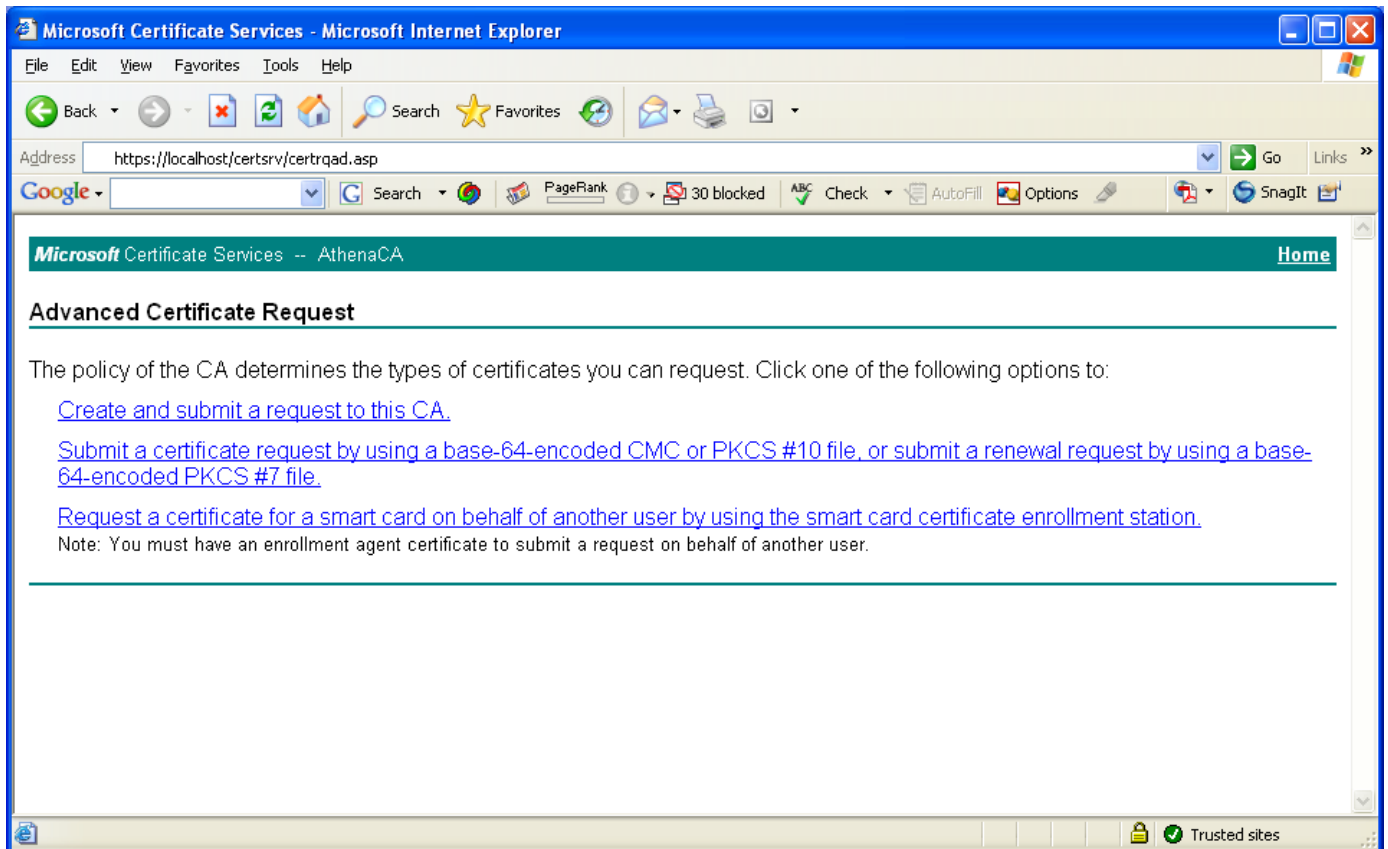


The **Request a Certificate** page will appear



Click on the **advanced certificate request** link.

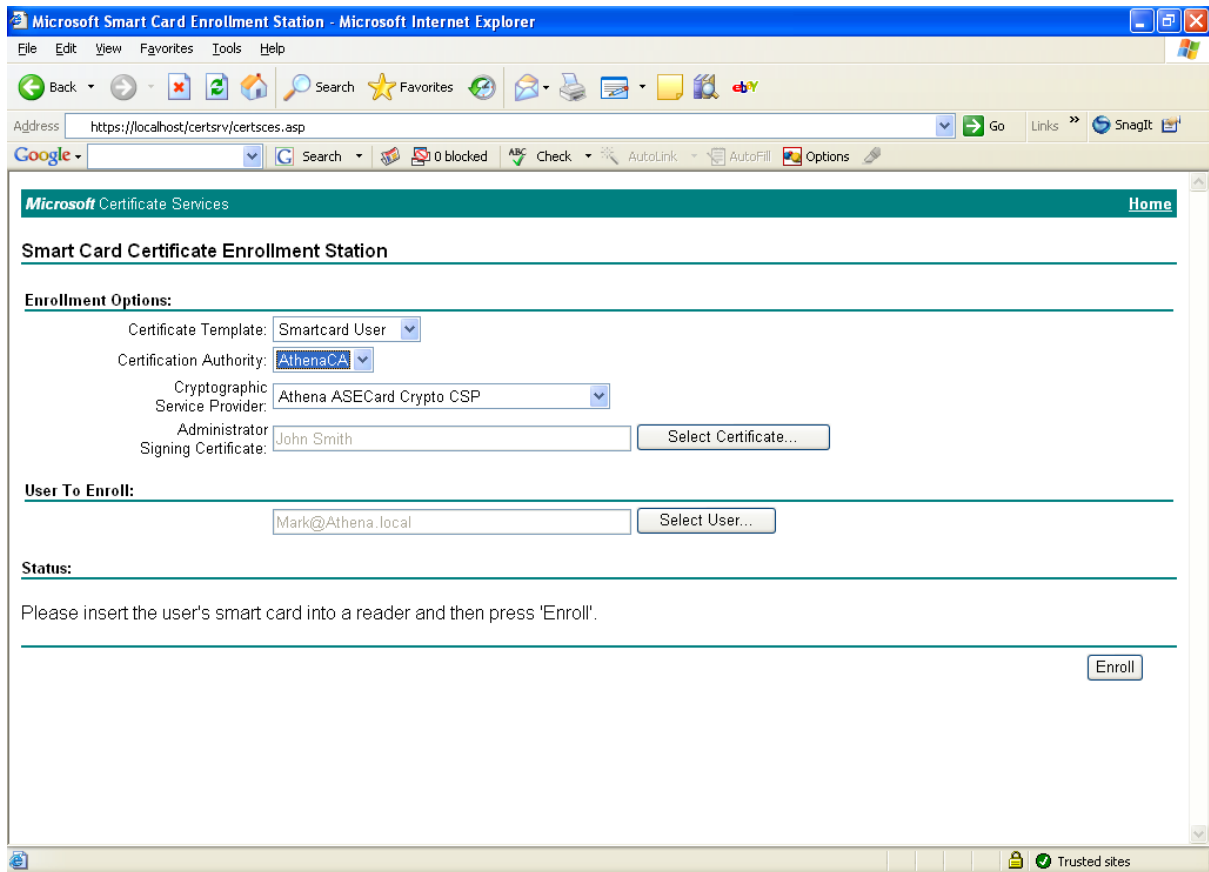
The **Advanced Certificate Request** page will appear



Click on the **Request a certificate for a smart card on behalf of another user using the smart card enrollment station** link.

The very first time you use the Smart Card Enrollment Station, a digitally signed Microsoft® ActiveX® control is downloaded from the Certification Authority server to the enrollment station computer. To use the enrollment station, select **Yes** from the Security Warning dialog box to install the control.

The **Smart Card Certificate Enrollment Station** page will appear



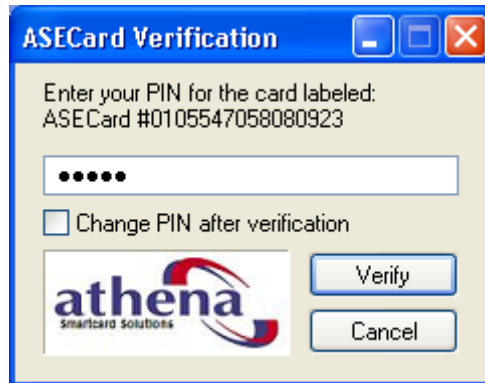
Select the following items from the drop-down menus:

- **Smartcard Logon** or **Smartcard User** Certificate Template.
- The **Certification Authority**.
- The **Athena ASECard Crypto CSP**
- Click the **Select Certificate...** button and select **Administrator Signing Certificate** (select only one from the list) click **OK**.
- Click the **Select User...** button and select the user name you would like to enroll and Click **OK**.
- Insert a personalized ASECard Crypto smart card into the smart card reader.

Click **Enroll** to start the enrollment process.

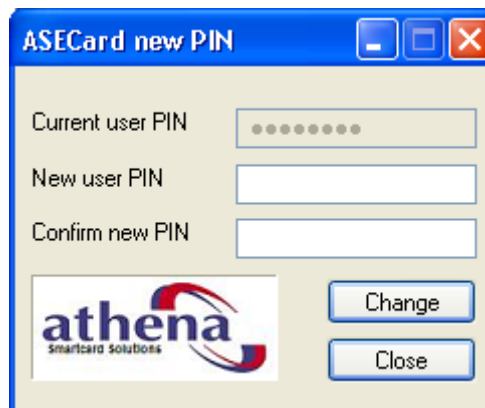
The **ASECard PIN Entry** or **Fingerprint Verification** dialog will appear.

Type in the PIN, and click **OK** (The default User PIN for ASECard Crypto is '1111111') or place a correct fingerprint on the sensor. In case of a PIN Card, the following dialog is used.



Depending on whether "Change PIN at first use" policy was selected in the *Personalization Profile* which the card was personalized with (the default is NO, see Chapter 2), **The ASECard PIN Entry** dialog may appear, requesting the user to enter and confirm a new User PIN.

The user may also mark the **Change PIN after verification** check box in order to be prompted for a PIN change. In both cases, the following dialog will appear.



Enter a **New** PIN and confirm it, and the enrollment will take place.

If successful, the *Smart Card Enrollment Station* informs you that the enrollment is completed. The smart card is now ready for use. You can either view the certificate by clicking **View Certificate** or re-start the process for a new user by clicking the **New User** button.

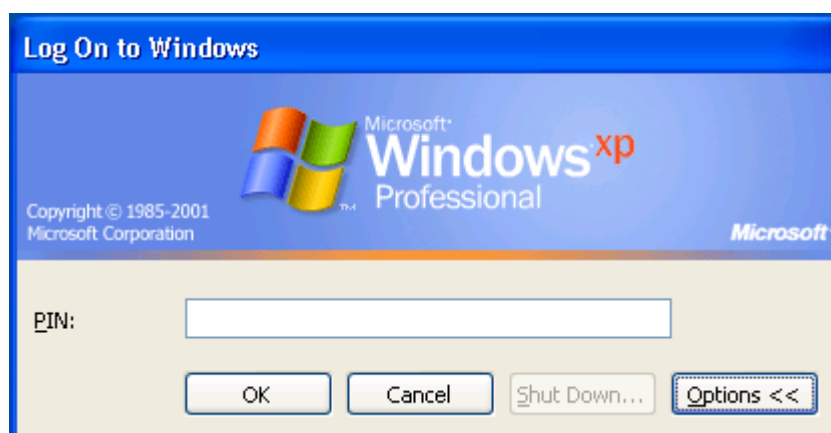
10. Logging on with an ASECard Crypto PIN Smart Card

After enrolling a card in the smart card certificate enrollment station, as described in Chapter 9 you will be able to logon to a Windows 2000 Server or Server 2003 using a smart card and a User PIN.

If the client PC has been properly configured with a smart card reader, the **Welcome to Windows** dialog box will display the figure of a smart card reader, in addition to the standard keyboard figure, as shown below.



For smart card logon the user only needs to insert the smart card into the reader and when prompted, enter the User PIN, in order to logon to the PC and network.



11. Logging on with an ASECard Crypto Bio Enabled Smart Card

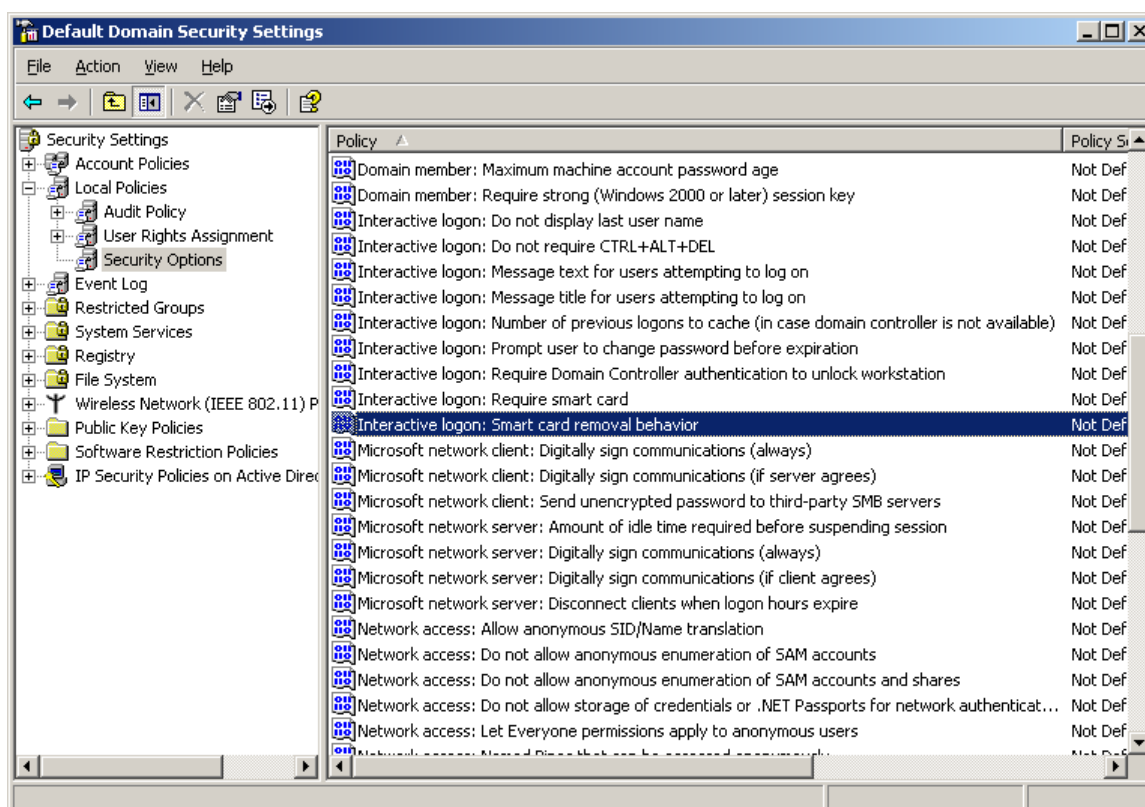
When trying to logon to Microsoft Windows with a biometric enabled ASECard Crypto card, the following dialog is presented. The user will then have to present a correct fingerprint in order to logon to her workstation.



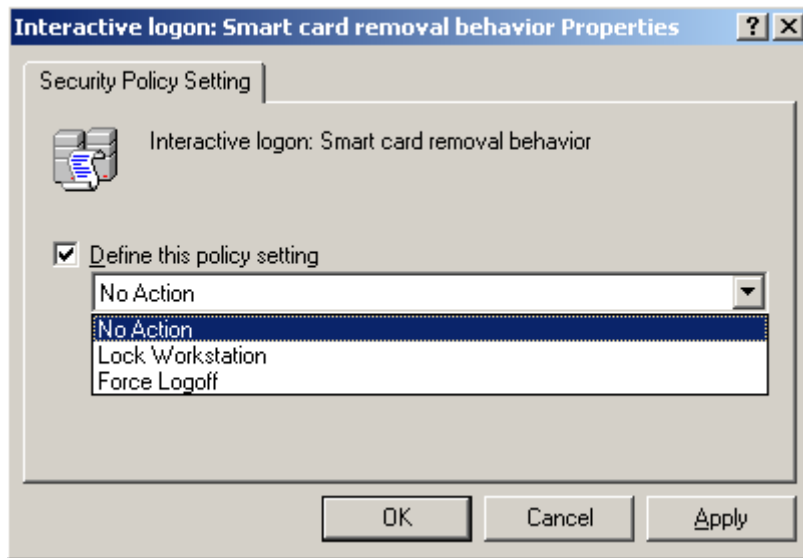
12. Policy Settings for Smart Card removal behavior

You can set different policies to define smart card removal behavior. Defining these require setting Domain Security Policies on the Domain Controller.

Click **Start > Settings > Control Panel >> Administrative Tools >> Domain Security Policy**, the following dialog box will appear.



Double-click on **Local policies**, and then on **Security options** and choose **smart card removal behavior** in the window on the right. Right-click on it and choose **Properties** which brings up the following dialog box.



There are three options available. Choose one of the options and click OK to set smart card removal behavior for the Domain.

Note: *If the Security Policy is not defined on the Domain the choice can be made by the individual user on a local basis from workstation to workstation*

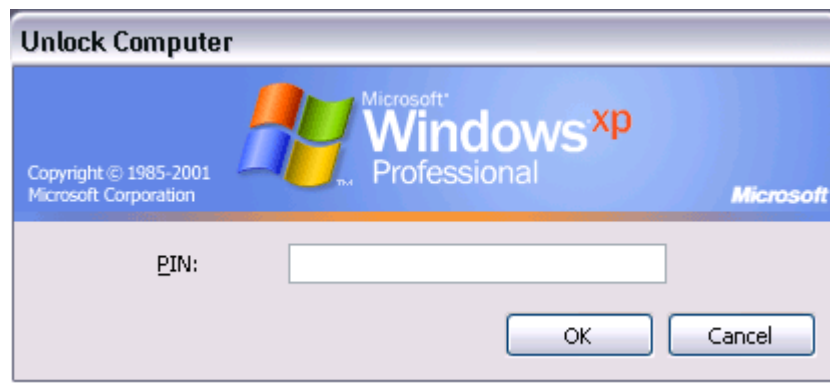
13. Locking & Unlocking a PC upon card removal

If set properly as described in Chapter 12, you can lock a Windows XP computer simply by removing the card from the reader. The following window is displayed:



To unlock a Windows XP computer:

Re-insert your smart card. The Unlock Computer dialog box opens.



Enter your User PIN and click **OK** to log back on.

Windows Vista Note: In Windows Vista, you may need to start the Smart Card Removal Policy service in order to activate the lock screen upon card removal option.

14. Advanced Installation Options

Command line Parameters

IBOOT

Default value: 0 - Reboot if needed post installing. For instance, when Gina support is installed. When set to 1 no reboot will take place post installation.

Command line:(Install Boot - Do not reboot post installing)
msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" IBOOT=1

UBOOT

Default value: 0 - Reboot post uninstalling.
When set to 1 no reboot will take place post uninstallation. This option gives the user an opportunity to install a new Toolkit before rebooting in order to have the Toolkit installed on the next boot to enable smart card logon.

Command line:(Uninstall Boot - Do not reboot post uninstalling)
msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" UBOOT=1

VERIFICATIONTYPE

Default value:None - RegKey verificationtype will not be installed if the parameter is not set

When it is set, regkey will be installed with the value which was set.

Command line:(Verification type - will be installed and set to 10 (hex))
msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" VERIFICATIONTYPE=10

INSTALLMANGEPIN

Default value:1

Optional parameter which defines if the ASECard Manage PIN will be installed. 0 - do not install 1 - install.

Command line:(Do not install ASECard Manage PIN).
msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" INSTALLMANGEPIN=0



INSTALLMONITOR

Default value:1

Optional parameter which defines if the ASECard Monitor will be installed. 0 - do not install 1 - install.

Command line:(Install ASECard Monitor).

msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" INSTALLMONITOR=1

INSTALLDOC

Default value:1

Run setup without installing documents

Command line:(Run setup without installation of documents).

msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" INSTALLDOC=0

INSTALLRDPSEVER

Default value:0

Run setup without installing the two services which enable RDP server support

Command line:(Run setup without installation of RDP server).

msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" INSTALLRDPSEVER=0

INSTALLGINA

Default value:0

When it is Set to 1, Gina components will be installed.

Command line:(Install Gina components).

msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" INSTALLGINA=1

INSCITRIXCLIENT

Default value:0

When it is set to 1, and Citrix client is installed, Citrix components will be installed.

Command line:(Install Citrix components).

msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" INSCITRIXCLIENT=1



DELCERTSTORE

Default value:0

When it is Set to 1, every time an ASECard Crypto certificated is deleted from the store, it is deleted from the card too.

Command line:(Set certificate to be deleted from the card if it was deleted from the root store).
msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" DELCERTSTORE=1

KEEPARVCERT

Default value:0

When it is set to 1, every time a certificate is marked as archived, it is marked as archived on the card too. Otherwise it is deleted from the card.

Command line:(Set certificate as archived).
msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" KEEPARVCERT=1

DELCARDCERT

Default value:1

For all values other than 0, every time a certificate is deleted from the card, it is deleted from the root store as well.

Command line:(Do not delete certificate from the store even if it was deleted from the card).
msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" DELCARDCERT=0

LOADROOT

Default value:0

Set registry entry for uploading root certificate to the root store if it exists on the smart card. By default it will not be loaded to the certificate store.

Command line:(Set load root to upload certificate to the root store).
msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" LOADROOT=1

CPSUPPORT

Default value:0

Set registry entry for supporting Check Point. By default Check Point is not supported.

Command line: (Set support for Check Point).
msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" CPSUPPORT=1



CERTPOLICY

Default value:NONE

Set registry entry for controlling the number of days certificates will be kept in the certificate store before being deleted.

By default it will be installed and set to empty string.

Command line: (Cert policy to 5 days).

msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" CERTPOLICY=5

SHOWICONTRY

Default value:1

Set registry entry to control the appearance of the Sys tray Icon.

By default it will be installed and set to 1.

Command line: (Do not show icon in tray).

msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" SHOWICONTRY=0

INSTALLCITRIXUTIL

Default value:1

Optional parameter which defines if Citrix util will be installed. 0 - do not install 1 - install.

Command line:(Do not install Citrix util).

msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" INSTALLCITRIXUTIL=0

INSTALLPERSO

Default value:1

Optional parameter which define if the Personalization Tool will be installed. 0 - do not install 1 - install.

Command line:(Do not install Personalization tool).

msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" INSTALLPERSO=0

INSTALLMANAGER

Default value:1

Optional parameter which defines if the ASECard Manager will be installed. 0 - do not install 1 - install.

Command line:(Do not install ASECard Manager).

msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" INSTALLMANAGER=0



INSTALLOPTIONS

Default value:1

Optional parameter which defines if ASECard Options will be installed. 0 - do not install 1 - install.

Command line:(Do not install ASECard Options).
msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" INSTALLOPTIONS=0

GINASUPPORT

Default value:1

Defines if Gina support will be installed or not. By default it is set to GINASUPPORT=1, with Gina support.

If no parameter is passed Gina support will be installed.

Command line: (Do not install Gina support):
msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" GINASUPPORT=0

ORIGBIOFINGERPRINT

Default value:1

Define if a real time image of the fingerprint will be displayed in the dialog or only a static image of a "dummy" fingerprint.

Command line: (Show real fingerprint image):
msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" ORIGBIOFINGERPRINT=1

ALLOWUNLOCK

Default value: 1 - Do not allow dynamic unlock.
When set to 2 dynamic unlock is allowed.

Command line:(Allow dynamic unlock)
msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" ALLOWUNLOCK =2

Combination of parameters

The parameters can be combined into a single command line:
Command line:(Do not install ASECard Options, install ASECard Manager and set Check Point support).

msiexec.exe /i "[PathToMsi]\ASECard Crypto Toolkit X.X.msi" INSTALLOPTIONS=0
INSTALLMANAGER=1 CPSUPPORT=1