



# **ASECard Crypto for Windows**

## **Integration Guide**

**Release 2.0**



# 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

<b>PREFACE .....</b>	<b>2</b>
<b>WHO SHOULD READ THIS MANUAL .....</b>	<b>2</b>
<b>PREREQUISITES .....</b>	<b>2</b>
<b>CHAPTER 1 - STEP-BY-STEP INSTRUCTIONS FOR SMART CARD LOGON ADMINISTRATION. ....</b>	<b>3</b>
<b>1. INSTALLING AN ASEDRIIVE IIIIE SMART CARD READER.....</b>	<b>3</b>
<b>2. INSTALLING THE ASECARD CRYPTO TOOLKIT.....</b>	<b>3</b>
<b>3. DEFAULT CARD PERSONALIZATION PARAMETERS .....</b>	<b>5</b>
<b>4. USING THE ASECARD CRYPTO ADMIN TOOL .....</b>	<b>6</b>
<b>5. CHANGING OR UNBLOCKING THE USER PIN .....</b>	<b>11</b>
CHANGING THE USER PIN .....	11
UNBLOCKING A BLOCKED USER PIN.....	11
<b>6. THE ASECARD CRYPTO USER TOOL .....</b>	<b>14</b>
<b>7. CHANGING THE USER PIN USING THE ASECARD CRYPTO USER TOOL.....</b>	<b>15</b>
<b>8. SMART CARD USER/LOGON CERTIFICATE ENROLLMENT.....</b>	<b>16</b>
<b>9. LOGGING ON WITH AN ASECARD CRYPTO FOR WINDOWS 2000 SMART CARD .....</b>	<b>21</b>
<b>10. POLICY SETTINGS FOR SMART CARD REMOVAL BEHAVIOR .....</b>	<b>22</b>
<b>11. LOCKING &amp; UNLOCKING A PC UPON CARD REMOVAL.....</b>	<b>23</b>
<b>APPENDIX A.....</b>	<b>24</b>
<b>A. SETTING UP A SMART CARD ENROLLMENT STATION .....</b>	<b>24</b>
<b>B. DETERMINING THE CERTIFICATE TYPES TO BE ISSUED.....</b>	<b>25</b>
SETTING UP THE SMART CARD CERTIFICATE ENROLLMENT STATION .....	27



## Preface

ASECard Crypto for Windows is a set of utilities and middleware which, coupled with an ASECard Crypto for Windows card, provide support for Microsoft Windows 2000/2003 smart card services such as Interactive Logon, secure e-mail, VPN, etc.

## 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 logon and support in their organization.

This Manual assumes that you are familiar with:

- General use of computers
- Microsoft Windows 2000 and/or XP
- Microsoft Windows 2000 Server and/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:

- *Active Directory* installed on the 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 *Appendix A*)

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

<http://www.microsoft.com/windows2000/techinfo/planning/security/casetupsteps.asp> and <http://www.microsoft.com/windows2000/techinfo/planning/default.asp>

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



## Chapter 1 - Step-by-Step Instructions for Smart Card Logon Administration.

### 1. Installing an ASEDrive IIIe Smart Card Reader

Installing your ASEDrive IIIe is an easy procedure. Please follow the instructions below:

- 1 Download and save on your PC the latest driver installation utility from:  
<http://www.asedrive.com/downloads>
- 2 Make sure that the ASEDrive IIIe reader **is not** connected to your PC.
- 3 Run the installation utility.
- 4 Follow the instructions on the screen.
- 5 Your ASEDrive IIIe is ready for use.

### 2. Installing the ASECard Crypto Toolkit

In order to support the issuance of smart card certificates and storing them on ASECard Crypto for Windows 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.

**When installing the ASECard Crypto CSP, you have the choice of 2 installation packages:**

- A. **ASECard Crypto Toolkit – Admin:** installs the ASECard Crypto CSP middleware and the ASECard Crypto Admin Tool.
- B. **ASECard Crypto Toolkit – User :** Installs the ASECard Crypto CSP middleware and the ASECard Crypto User Tool.

You will need the ASECard Crypto Admin Tool if you would like to change the default card personalization, re-personalize cards, change User, Unblock, or Admin PINS, and manage other card properties.

The ASECard Crypto User Tool provides the end user with the facility to change the User PIN and view basic details about his card.

**Note:** 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.



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

Go ahead now and locate the installation files and install the selected package. You can only install one of the packages on a specific PC – either the **Admin** or **User** packages.



### 3. Default Card Personalization Parameters

The ASECARD Crypto smart cards provided with the *ASECARD Crypto for Windows* package are personalized at the factory and are ready for smart card enrollment.

The factory personalization is based on the default *ASEDefault* personalization profile (more on *profiles*, in the following text).

The main parameters of the *ASEDefault* profile are:

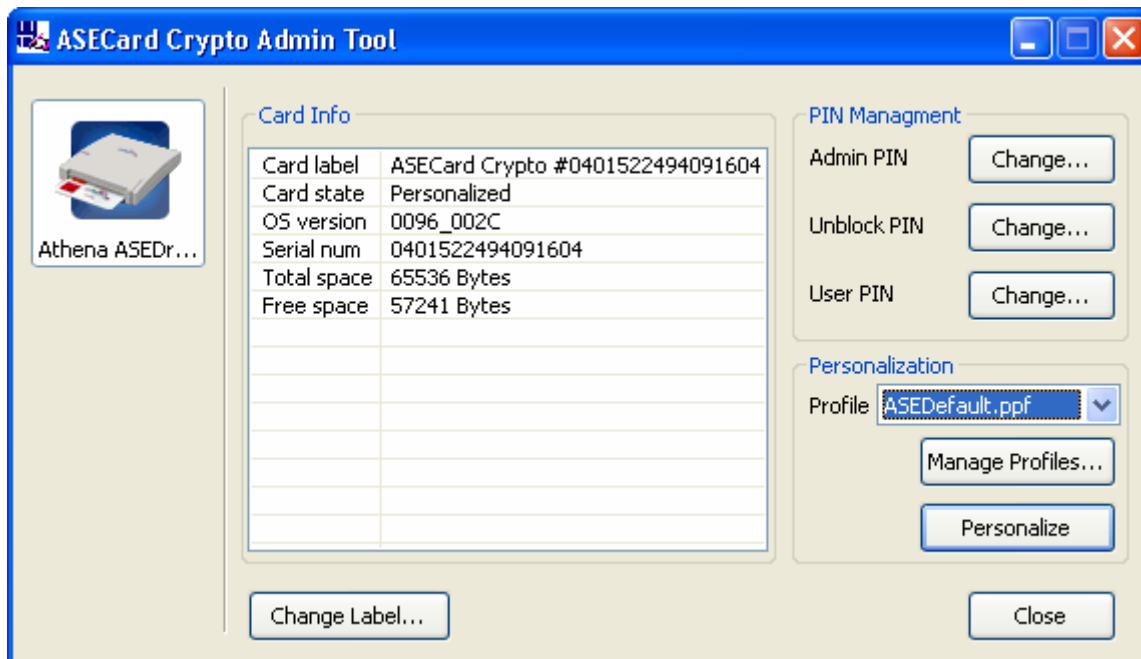
Parameter	Default Value	Changing Requires Re-Personalization
<b>Administrator PIN</b>	ASECARD+	NO
<b>User PIN</b>	11111111	NO
<b>Unblock PIN</b>	00000000	NO
<b>User must change PIN (at first use)</b>	YES	YES
<b>Reserve space for PKI</b>	NONE	YES
<b>Min User PIN length</b>	4 Characters	YES
<b>Max User PIN length</b>	10 Characters	YES
<b>Max User PIN verify attempts</b>	10 Attempts	YES
<b>Max unblocks of User PIN</b>	3 Attempts	YES
<b>Min Unblock PIN length</b>	4 Characters	YES
<b>Max Unblock PIN length</b>	10 Characters	YES
<b>Max Unblock PIN verify attempts</b>	3 Attempts	YES
<b>PIN Complexity Rules</b>	None	YES
<b>Default Card Label</b>	Card Serial Number + Product Name	NO

If these default personalization parameters suit you needs, you may jump to [Chapter 8](#) and start smart card enrollment now.

**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, Unblock PIN, Admin PIN, or Card Label will not result in loss of credentials. See more details in the following chapter.



The **ASECard Crypto Admin Tool** window will now 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.

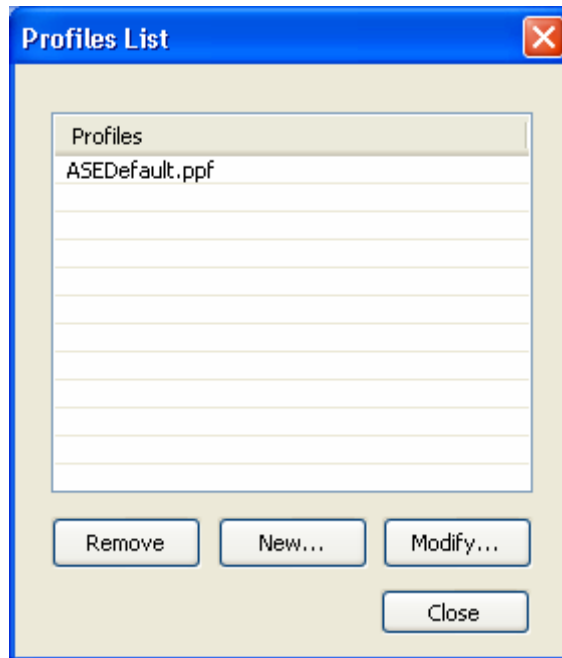


If a valid card is inserted, the **PIN Management**, **Change Label...**, and **Personalize** buttons become active.

- As mentioned in [Chapter 3](#), changing the Admin, Unblock, and User PINs and also setting a new Card Label will not erase credentials which are stored on the card. You may change the PINs and label by clicking the relevant buttons in the Admin Tool window.
- If you need to re-personalize a card and you are familiar with the available personalization profiles:
  - Select the required *Personalization Profile* from the *Profile* pop-up list.
  - Click the **Personalize** button.
  - When prompted, enter the **Admin** PIN. ('ASECARD+' is the default).
  - Wait for the "Success" message.

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

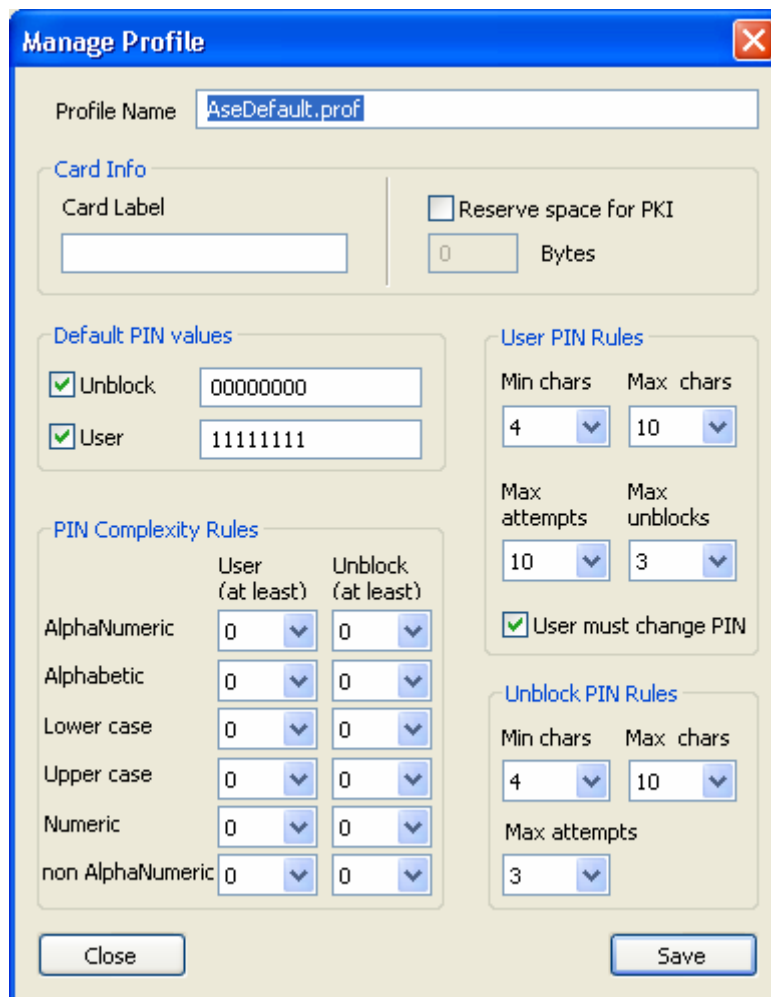
The **Profile List** window appears:



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. Each of the parameters is described below.



The screenshot shows the 'Manage Profile' dialog box with the following settings:

- Profile Name:** AseDefault.prof
- Card Info:**
  - Card Label: (empty text box)
  - Reserve space for PKI:  (unchecked)
  - 0 Bytes
- Default PIN values:**
  - Unlock:  (checked), 00000000
  - User:  (checked), 11111111
- PIN Complexity Rules:**

	User (at least)	Unlock (at least)
AlphaNumeric	0	0
Alphabetic	0	0
Lower case	0	0
Upper case	0	0
Numeric	0	0
non AlphaNumeric	0	0
- User PIN Rules:**
  - Min chars: 4, Max chars: 10
  - Max attempts: 10, Max unblocks: 3
  - User must change PIN:  (checked)
- Unlock PIN Rules:**
  - Min chars: 4, Max chars: 10
  - Max attempts: 3

Buttons: Close, Save

### 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 “Card Name + Card serial number”.

**Reserve space for PKI** - Unlike some other cards, ASECard Crypto does not require the Administrator to allocate space for public and private objects. The underlying 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.



### Default PIN Values

**Unblock/User** - You may select the check boxes and enter default values for User and/or Unblock PINs. These values will be applied to each card which will be personalized using this profile.

However, your security policy may require you to enter different User and/or Unblock PINs for each card issued. In such case, leave either or both check boxes unchecked and you will be automatically prompted to enter the User and/or Unblock PINs during the personalization process.

### User 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 Unlocks** - The number of successful User PIN unlocks allowed before the User PIN is blocked.

**User must change PIN** – If selected, the user will be prompted to change the User PIN at the first use of the card, following personalization. Normally, this will be during the Certificate Enrollment process.

### Unblock PIN Rules

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

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

### Pin Complexity Rules

Enable you to apply complexity rules to the User and/or Unblock PINs, 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 are finished with the 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.
- You may manage profiles without having a card inserted.

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

## 5. Changing or Unblocking the User PIN

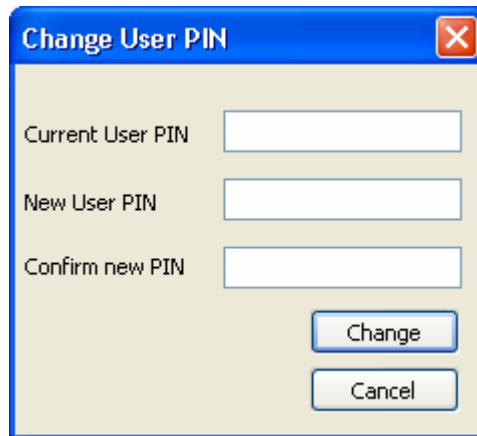
As mentioned in *Chapter 4*, it is possible to change the User, Admin, and Unblock PINS without re-personalizing the card. Follow the instructions below to change each PIN.

### Changing the User PIN

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

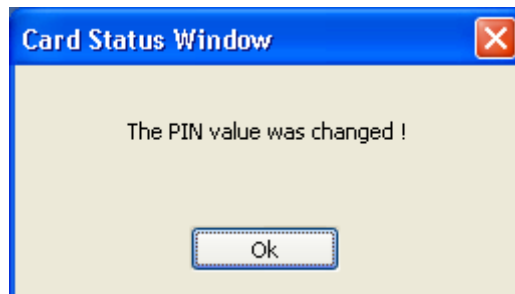
The **Change User PIN** window will appear, prompting you to enter your new PIN.

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



The image shows a dialog box titled "Change User PIN" with a close button (X) in the top right corner. It contains three text input fields labeled "Current User PIN", "New User PIN", and "Confirm new PIN". Below the fields are two buttons: "Change" and "Cancel".

When completed, the following dialog will appear:

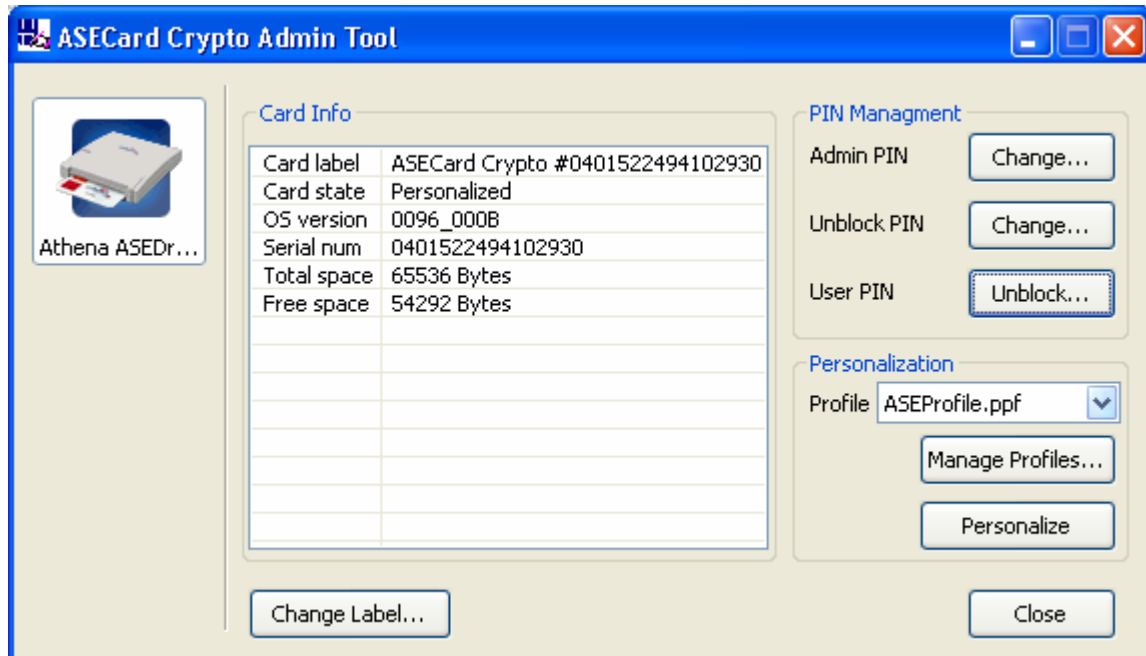


The image shows a dialog box titled "Card Status Window" with a close button (X) in the top right corner. It contains a single line of text: "The PIN value was changed !". Below the text is an "Ok" button.

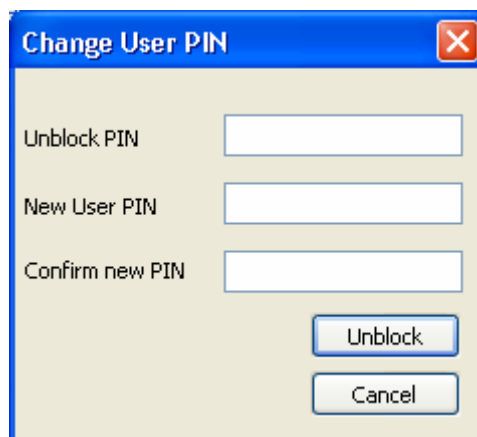
### Unblocking a blocked User PIN

When the User PIN is entered with a wrong value for more times than the Max Attempts parameter which was set during the card personalization (the default is 10 attempts), the User PIN becomes blocked and can only be unblocked using the **Admin Tool**.

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



Clicking the **Unblock...** button will open the **Change User PIN** dialog:



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

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

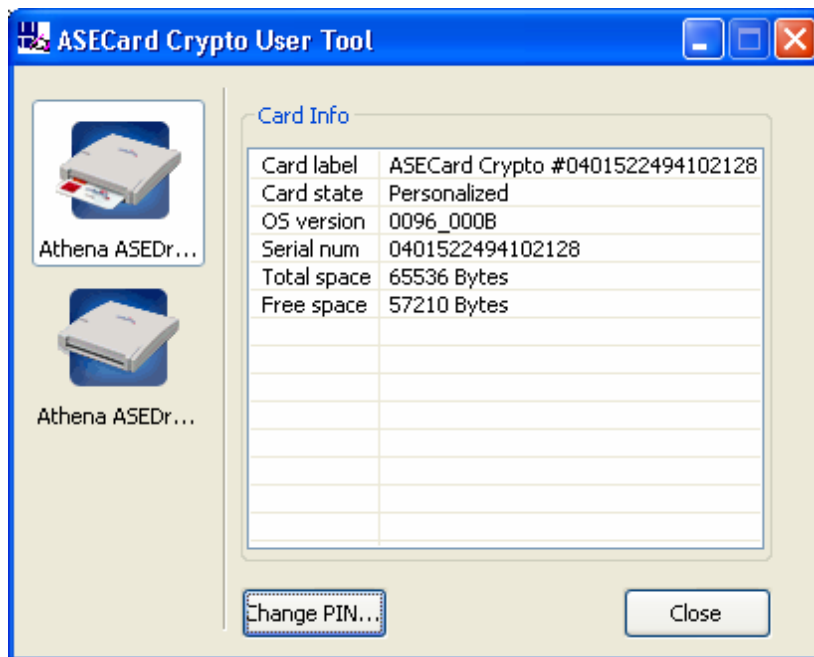


**Note:** After 2 additional (unsuccessful) attempts (or as set in the Max Attempts parameter of the Unblock PIN in the profile used to personalize the card), the card will be blocked. In order to continue and use the card, you will have to personalize it and lose all credentials stored on the card.

## 6. The ASECard Crypto User Tool

As mentioned in [Chapter 2](#), the **ASECard Crypto User Tool** has to be installed on each PC where Smart Card Logon will be enabled.

The **ASECard Crypto User Tool**, is accessed from **Start ->Programs->ASECard Crypto Toolkit -->ASECard Crypto User Tool**



**The** ASECard Crypto User Tool displays the inserted card information and enables changing of the User PIN.

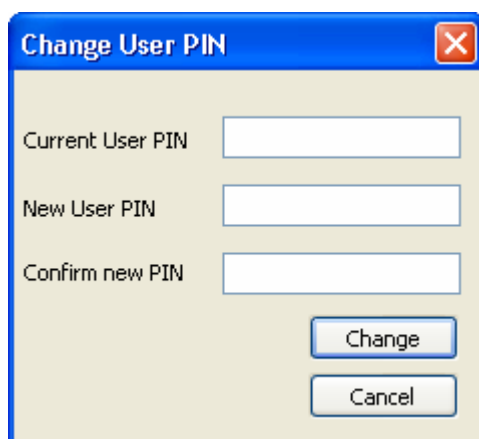
## 7. Changing the User PIN using the ASECard Crypto User Tool

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

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

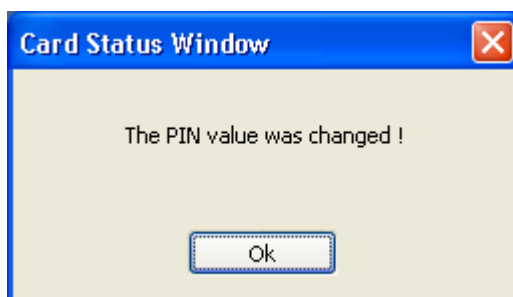
The **Change User PIN** window will appear, prompting you to enter your new PIN.

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



The image shows a Windows-style dialog box titled "Change User PIN". It has a blue title bar with a close button (X) in the top right corner. The main area is light beige and contains three text input fields stacked vertically. The first field is labeled "Current User PIN", the second "New User PIN", and the third "Confirm new PIN". Below the input fields are two buttons: "Change" and "Cancel".

When completed, the following dialog will appear:



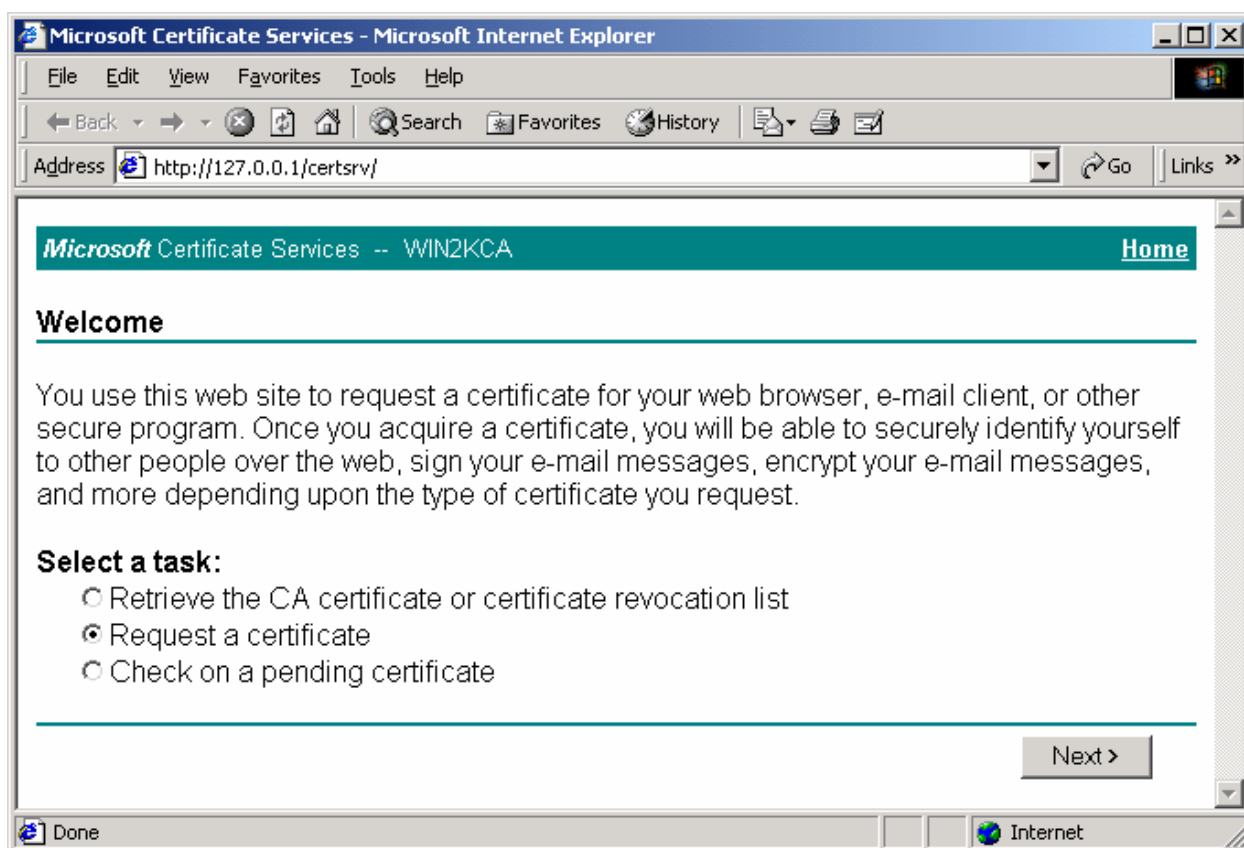
The image shows a Windows-style dialog box titled "Card Status Window". It has a blue title bar with a close button (X) in the top right corner. The main area is light beige and contains a single line of text: "The PIN value was changed !". Below the text is a single "Ok" button.

**Please note:** If the Maximum Attempts number is reached (default max attempts is 10), you will block the card and you will no longer be able to communicate with it. In order to have access to the card again, you will have to unblock the card using an **Admin Tool**.

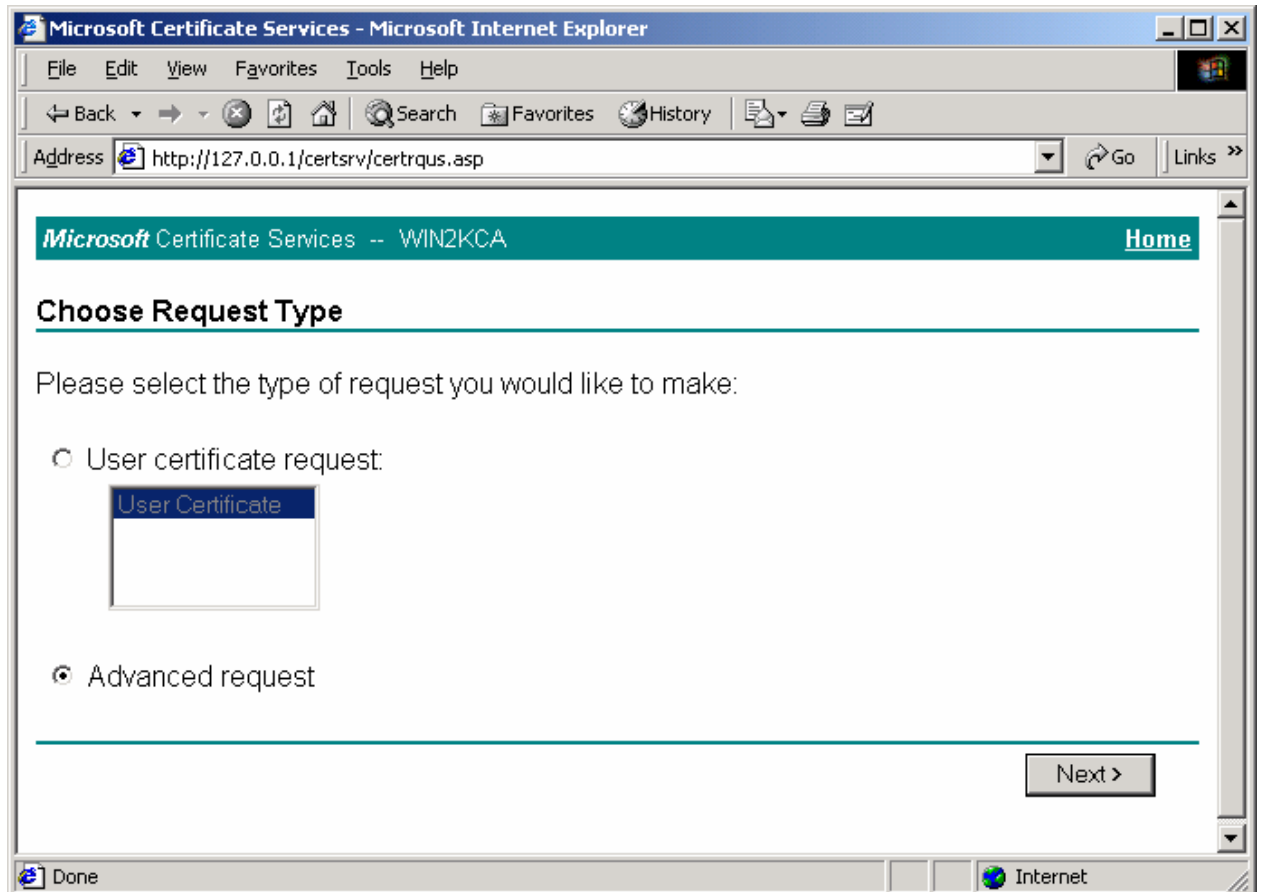
## 8. Smart Card User/Logon Certificate Enrollment

If you chose to use the **ASECard Crypto** cards without change, or if you completed editing the card parameters or re-personalizing it, you are now ready to enroll a user for **Smart Card Logon** or **Smart Card User** certificates:

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

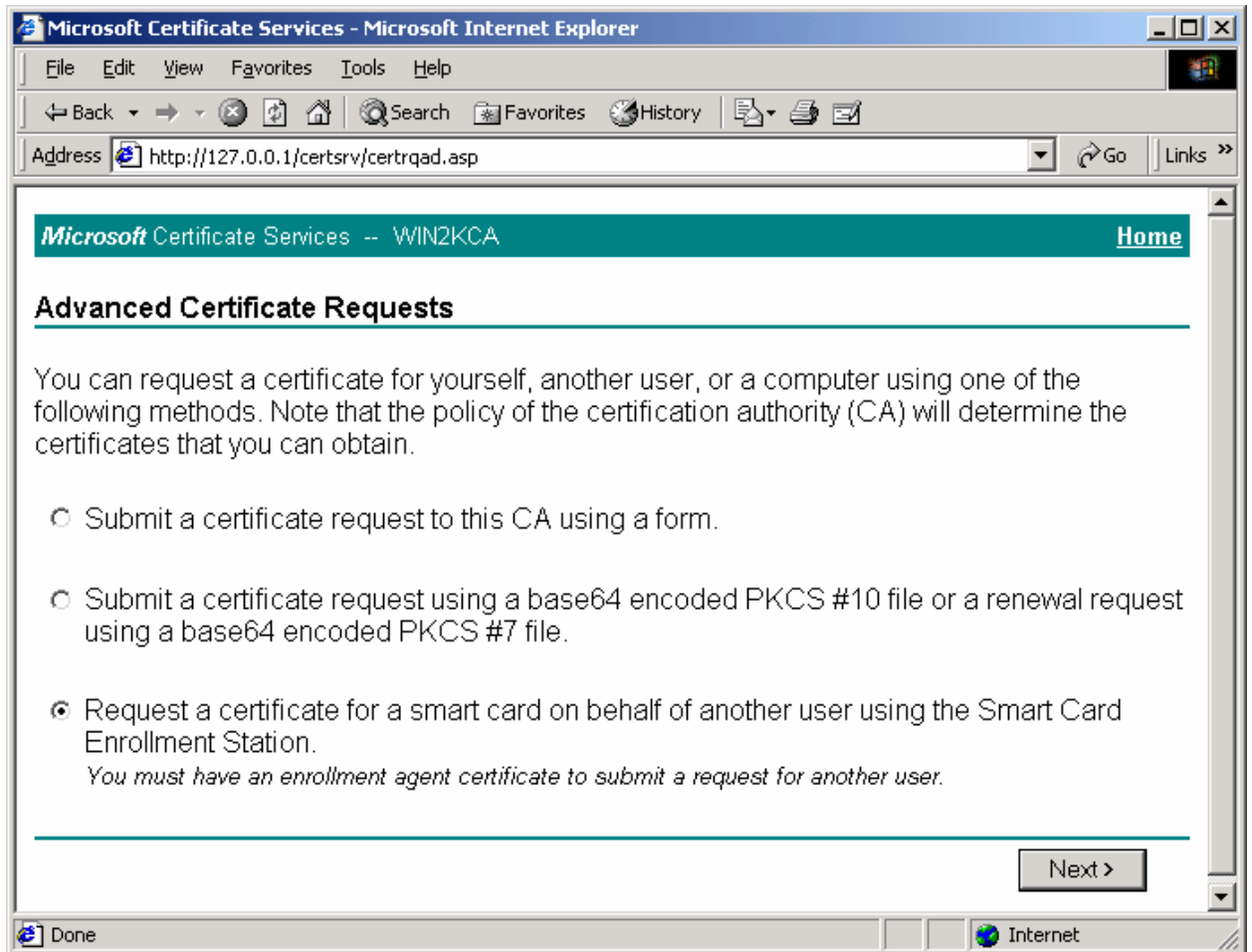


The **Choose Request Type** window will appear.



Select **Advanced request** radio button, and click **Next**.

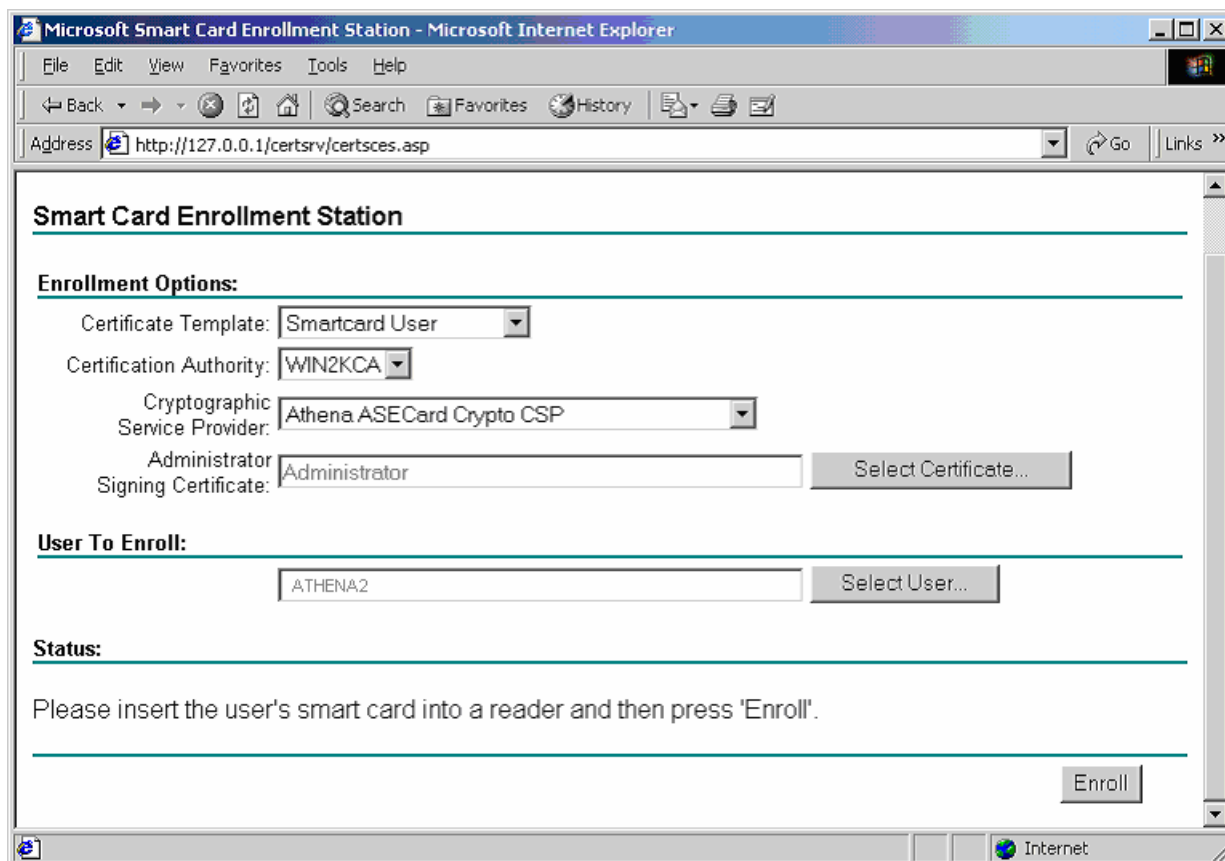
The **Advanced Certificate Requests** will appear.



Select **Request a certificate for smart card on behalf of another user using the Smart Card Enrollment Station**, click **Next**.

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 Enrollment Station** page will appear.



Select the following items from the drop-down menus:

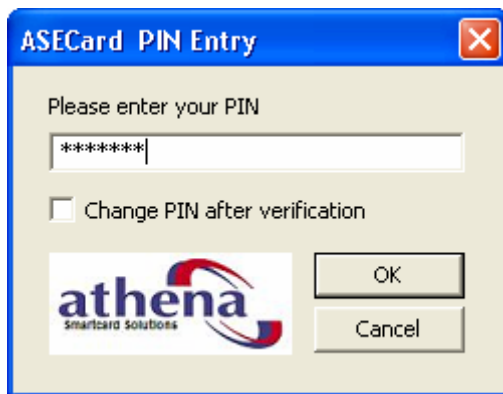
- **Smart Card Logon** or **Smart Card User** Certificate Template.
- The **Certification Authority**.
- The **Athena ASECard Crypto CSP**
- Click the **Select Certificate...** button and select **Administrator Signing Certificate** (select only one from the list) click **OK**.
- Click the **Select User...** 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** on the **Smart Card Enrollment Station** page.



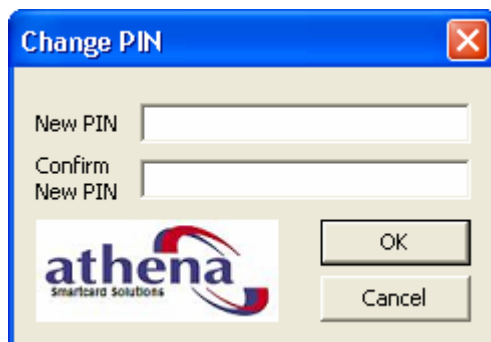
The **ASECard PIN Entry** window will appear.

Type in the PIN, and click **OK**. (The default User PIN for ASECard Crypto is '11111111').



Depending on whether "Change PIN at first use" policy was selected in the *Personalization Profile* which the card was personalized with (the default is YES, see [Chapter 3](#)), **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.

## 9. Logging on with an ASECard Crypto for Windows 2000 Smart Card

After enrolling a card in the smart card certificate enrollment station, as described in [chapter 8](#), 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.

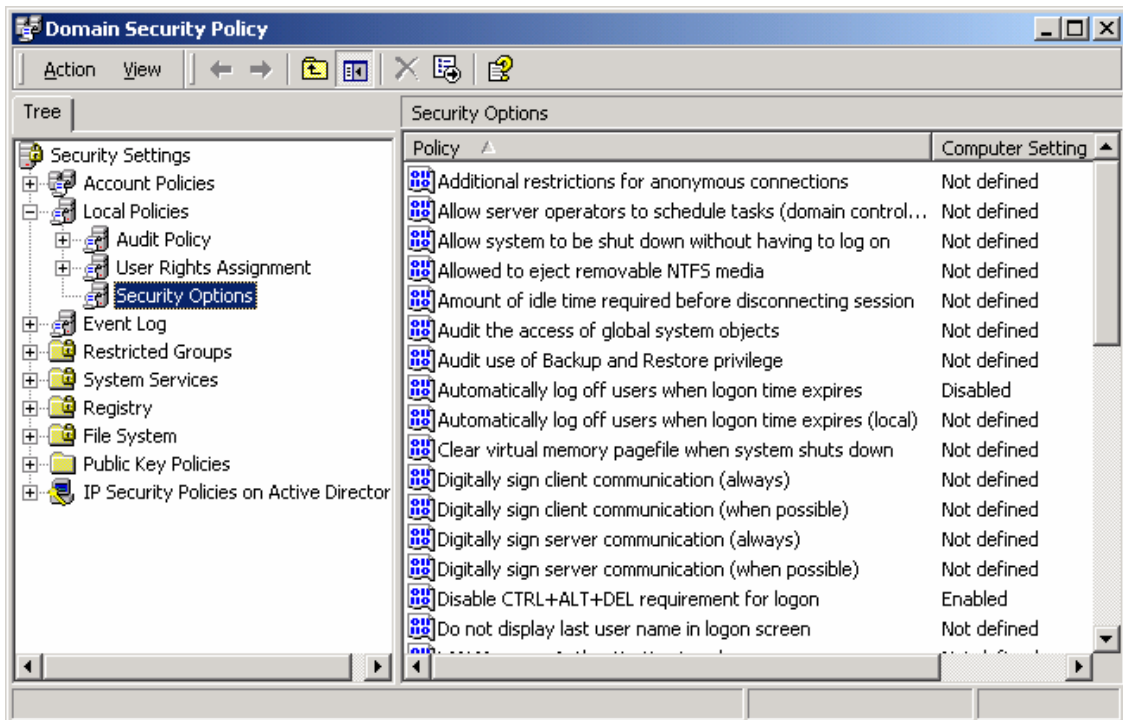


For smart card logon the user only needs to insert the smart card into the reader and when prompted, enter the User PIN, in order to logon to the PC and network.

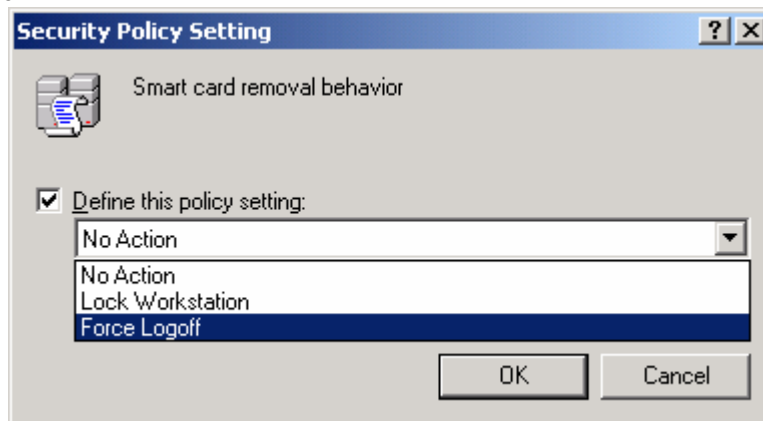
## 10. Policy Settings for Smart Card removal behavior

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.

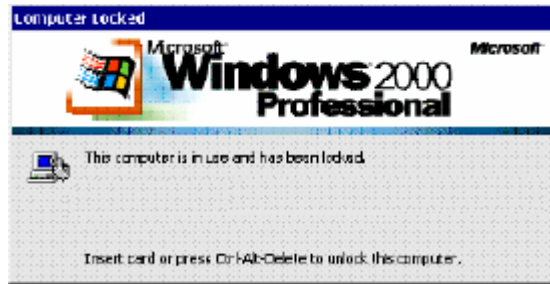


There are three options available. Choose one of the options and click OK to set smart card removal behavior for the Domain.

**Note:** The Domain policy can be disabled in which case the choice can be made by the individual user on a local basis from workstation to workstation

## 11. Locking & Unlocking a PC upon card removal

If you have the appropriate account privileges, you can lock a Windows 2000 computer simply by removing the card from the reader. The following window is displayed:



### To unlock a Windows 2000 computer:

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



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

**Note:** In Windows 2000, the computer does not lock by default when you remove your smart card from the reader. Use the Microsoft Management Console (see previous chapter) to change this feature.



## Appendix A

### A. Setting up a Smart Card Enrollment Station

A smart card enrollment station is included as part of the enterprise CA service available with Windows 2000 Server and Windows 2000 Advanced Server. This enrollment station supports the issuance of smart cards from a central location. Like the enterprise CA, the smart card enrollment station uses certificate templates to determine what information to include in a certificate such as intended usage. The default install of an enterprise CA does not enable the smart card certificate templates for issuance; instead, a CA administrator must enable these templates for issuance by an enterprise CA.

For smart card there are two certificate templates of interest: Smart Card Logon and Smart Card User. The Smart Card Logon certificate and Smart Card User certificates are very similar except the Smart Card Logon certificate cannot be used for secure email while the Smart Card User certificate can. Both certificate types have specific extended key usage properties that are used to determine the intended purpose of the certificate. For example, only these two certificate types can be used to log on interactively to a domain because each contains an extension specifying smart card logon.

In order to issue a smart card certificate, a smart card enrollment station must exist somewhere in the corporation to perform enroll-on-behalf operations. This requirement is necessary because, by default, domain users cannot enroll for smart card certificates issued by the Windows 2000 enterprise CA service. Access to the smart card certificates is restricted to domain administrators unless the access permissions on a template has been modified by a domain administrator to allow other user groups the ability to enroll. This is required to prevent an attack where a user leaves his or her workstation without logging off or locking it and someone uses the active logon session to enroll for a smart card certificate as the (unaware) user.

To operate the Windows 2000 smart card enrollment station, someone within the corporation must be authorized to be an enrollment agent. To support this role, the enterprise CA can issue an Enrollment Agent certificate for the explicit purpose of enroll-on-behalf operations. This certificate is the most powerful of all certificates because an employee with an Enrollment Agent certificate has the ability to enroll for smart card certificates for any domain user, including Administrator. It is therefore recommended that the default access permissions on the Enrollment Agent certificate template be set to allow only select employees the ability to enroll for one. In addition, it may be desirable to disable issuance of this certificate type at the CA except when specifically needed or to take the CA offline. By default, the access permissions for the Enrollment Agent certificate are set to domain administrators.

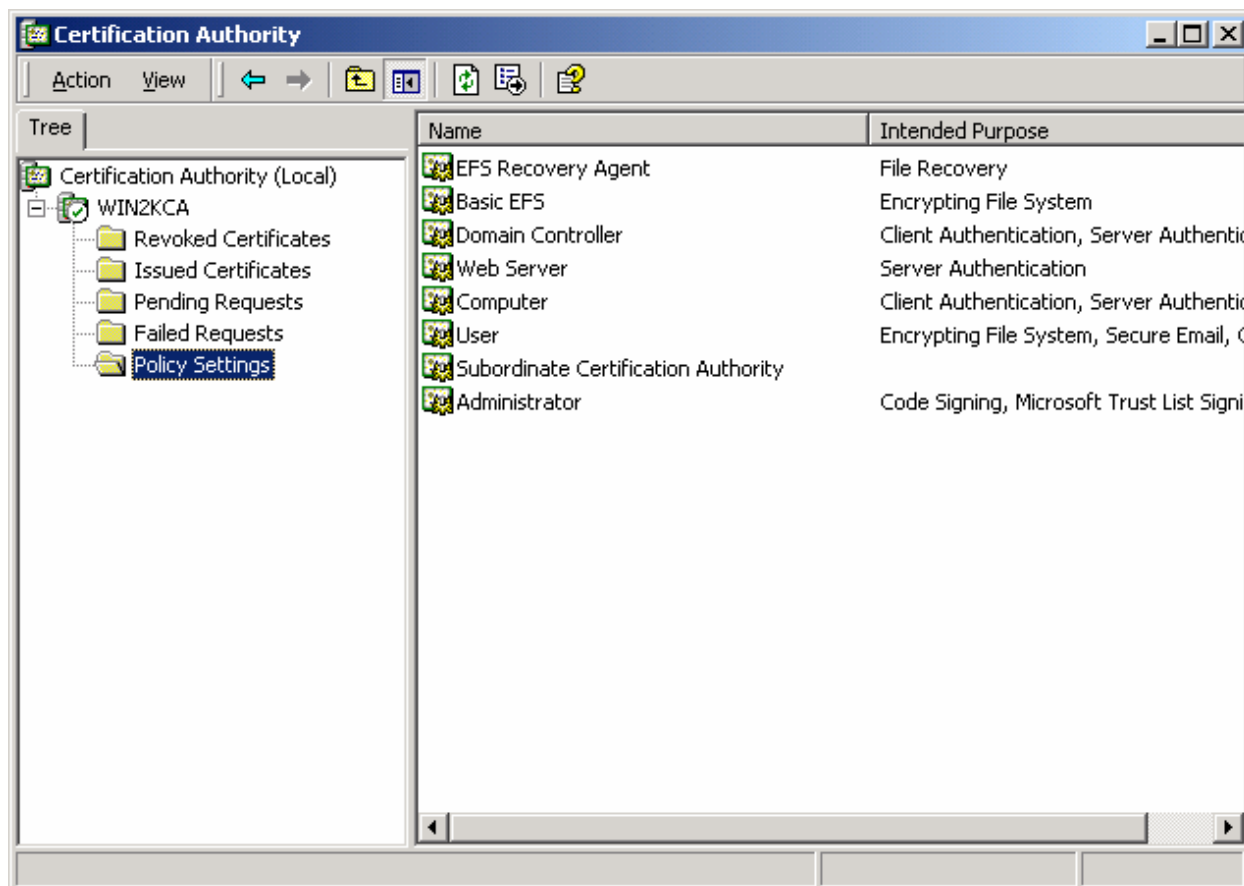
## B. Determining the certificate types to be issued

In order to issue Smart Card based certificates, the issuing of **Enrollment Agent** and **Smart Card User** (authorize the use of smart card based certificates for network logon and email signing/encryption) and/or Logon (for network logon only) certificates must be enabled in the CA Policy Settings module.

Log on to the CA Computer as **Administrator**.

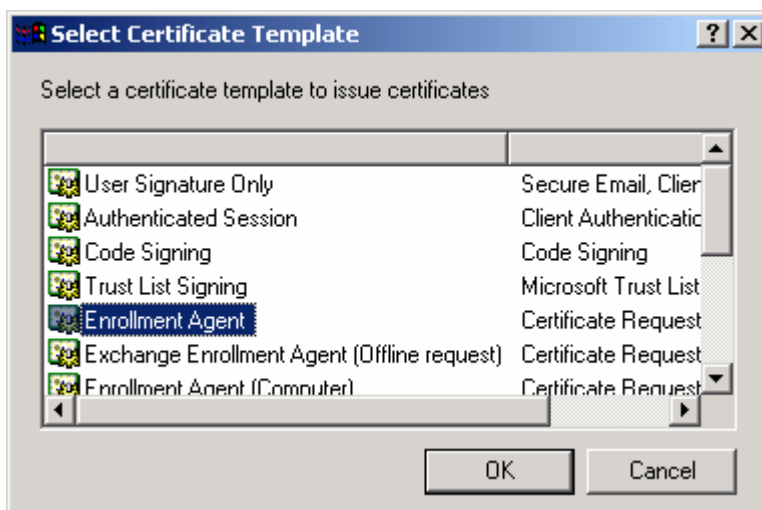
Click **Start > Programs > Administrative Tools > Certification Authority**

In the **Certification Authority** window, Expand the 'CA Name' and click **Policy Settings**.



Set the Security permissions for Enrollment Agent certificate, Smart Card Logon, and Smart Card user templates as follows:

1. On the **Action** menu, select **New > Certificate to Issue**.
2. Click the **Enrollment Agent** certificate template, and then click **OK**.



**For Smartcard Logon certificate template:**

1. On the **Action** menu, select **New > Certificate to Issue**.
2. Click the **Smartcard Logon** certificate template, and then click **OK**.

**For Smart Card User certificate template:**

1. On the **Action** menu, select **New > Certificate to Issue**.
2. Click the **Smartcard User** certificate template, and then click **OK**.



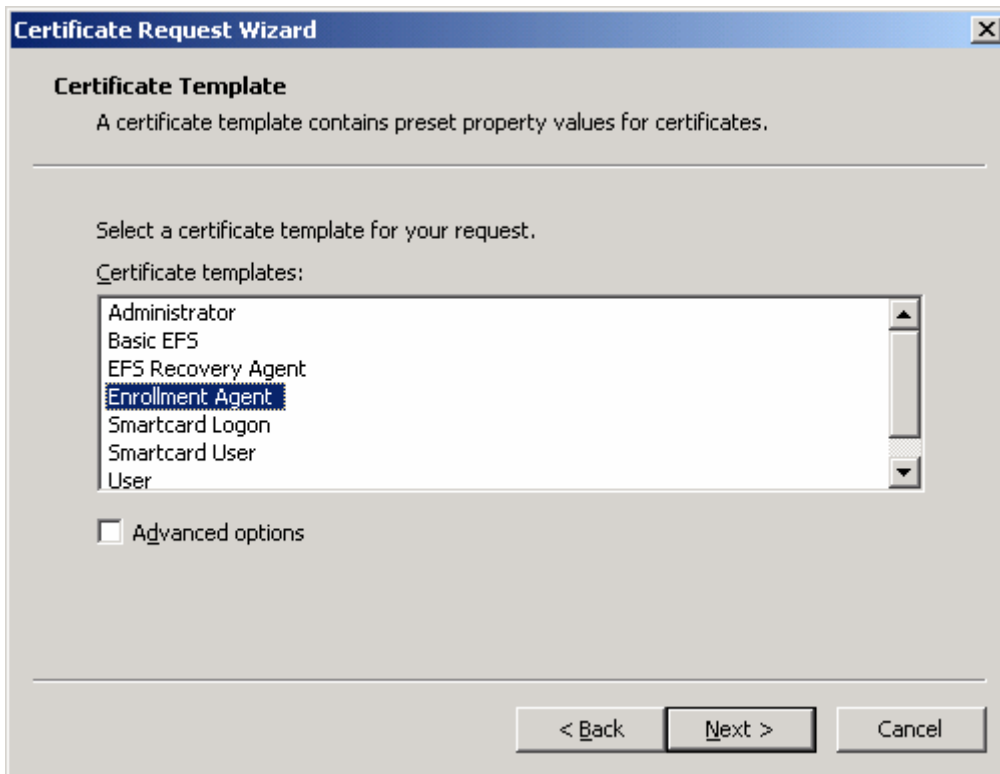
## Setting up the smart card certificate enrollment station

Smart Card Users may be enrolled on the CA Computer or on a separate enrollment station. In addition, it is possible to assign several enrollment agents.

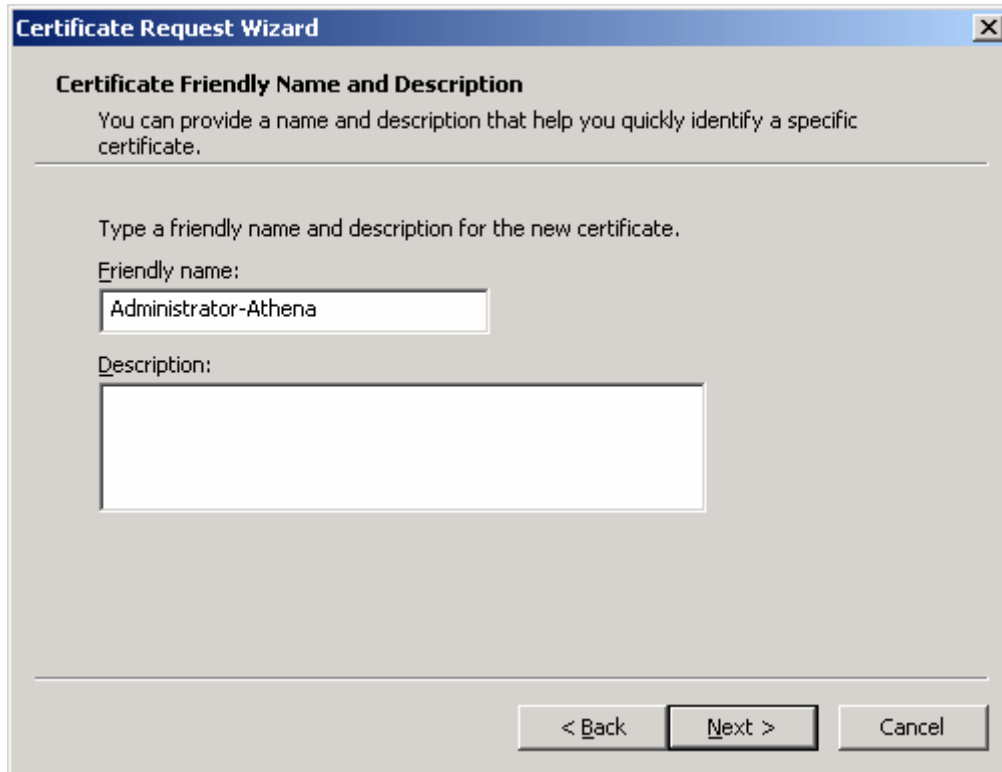
In order to start enrollment, an Enrollment Certificate must be issued first on the selected enrollment station PC.

- 1 Log on to the Enrollment Station computer as **Administrator**
- 2 Click **Start**, click **Run** and type **mmc** and click **OK**.
- 3 On the **Console** menu, click **Add/Remove Snap-in...**
- 4 Click **Add...** button.
- 5 In **Snap-in**, double-click **Certificates** (select "My User account" if prompted).
- 6 Click **Finish**.
- 7 Click **Close**.
- 8 Click **OK**.
- 9 Double-click **Certificates - Current User**.
- 10 In the console tree, click **Personal**.
- 11 On the **Action** menu, point to **All Tasks > Request New Certificate....**

- 12 In the Certificate Request wizard, click **Next** and select the **Enrollment Agent** and click **Next**.



- 13 Enter a friendly name and a description (optional) for the certificate and click **Next**.



**Certificate Request Wizard** [X]

**Certificate Friendly Name and Description**

You can provide a name and description that help you quickly identify a specific certificate.

---

Type a friendly name and description for the new certificate.

Friendly name:

Description:

---

< Back   Next >   Cancel

14 Review the certificate details and click **Finish**.



15 When prompted by the Certificate Request Wizard, click **Install Certificate**.



**Note:** In order to enroll smart card users, a smart card reader and the **ASECard Crypto Toolkit**, which includes **the ASECard Crypto CSP** and Utilities, must be installed on the enrollment station.