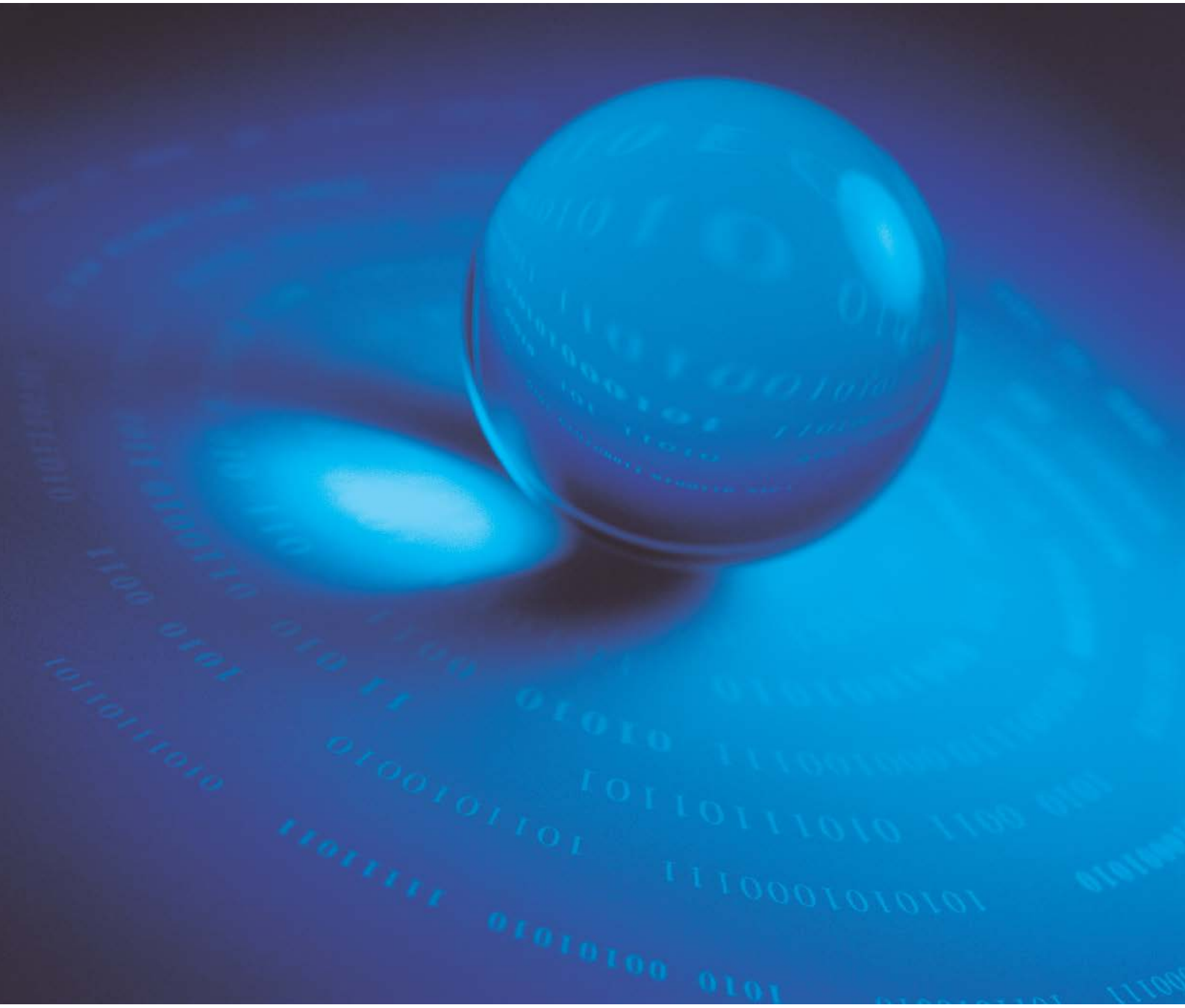
EnterSafe Minidriver PIN Management for Windows

V1.1



http://www.EnterSafe.com

EnterSafe will do their best to keep the content of this document as accurate as possible. But EnterSafe will not take the responsibilities for any direct or indirect loss that may be caused by this document. The content of this document will be amended along with the updating of the product without notification.

Revision History:

Date	Version	Description
January 2008	1.0	1st Edition
June 2011	1.1	2nd Edition

EnterSafe

SOFTWARE DEVELOPER'S AGREEMENT

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

1. GRANT OF LICENSE. EnterSafe grants you the rights described in this SDA provided that you comply with all terms and conditions of this SDA.

1.1 EnterSafe grants you a limited, nonexclusive license to use the Software, and to make and use copies of the Software, for the purposes of designing, developing and testing your software applications.

1.2 EnterSafe grants you to merge and link the Software with other programs for the sole purpose of protecting those programs in accordance with the usage described in the Developer's Guide. You may make archival copies of the Software.

2. LIMITATIONS ON REVERSE ENGINEERING, DECOMPILATION, AND DISASSEMBLY. You may revise, reverse engineer, decompile, disassemble, enhanced or otherwise modified the Software, except only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

3. NO RENTAL OR COMMERCIAL HOSTING. You may not rent, lease, lend or provide commercial hosting services with the Software.

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

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

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

7. TERMINATION. This SDA is effective until terminated. Upon any violation of any of the provisions of this SDA, rights to

use the Software shall automatically terminate and the Software must be returned to EnterSafe or all copies of the Software destroyed. You may also terminate this SDA at any time by destroying all copies of the Software in your possession or control. If EnterSafe makes a request via public announcement or press release to stop using the copies of the Software, you will comply immediately with this request. The provisions of paragraphs 2, 3, 4, 5 and 6 will survive any termination of this SDA.

CE Attestation of Conformity

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

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

Test report No. 70407310011
Test standards: EN 55022/1998 EN 55024/1998

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

FCC certificate of approval

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

USB

This equipment is USB based.

WEEE

Dispose in separate collection.

Contents

1 Overview 1

2 EnterSafe Minidriver PIN Management for Windows 1

2.1 Changing a User PIN 1

2.1.1 Changing a User PIN with Windows 2000, XP or Server 2003 1

2.1.2 Changing a User PIN with Windows Vista, 2008 2

2.2 Unblocking EnterSafe Minidriver 3

2.2.1 Example Unblock Procedure 3

2.2.2 Unblocking a Smart Card with Windows 2000, XP or Server 2003 4

2.2.3 Unblocking a Smart Card with Windows Vista, 2008 5

2.2.4 Administrator Tools for Card Unblock 10

1 Overview

EnterSafe Minidriver is a new smart card minidriver developed by EnterSafe for Microsoft Windows Smart Card Framework.

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

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

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

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

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

2 EnterSafe Minidriver PIN Management for Windows

2.1 Changing a User PIN

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

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

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

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

User PIN as follows:

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

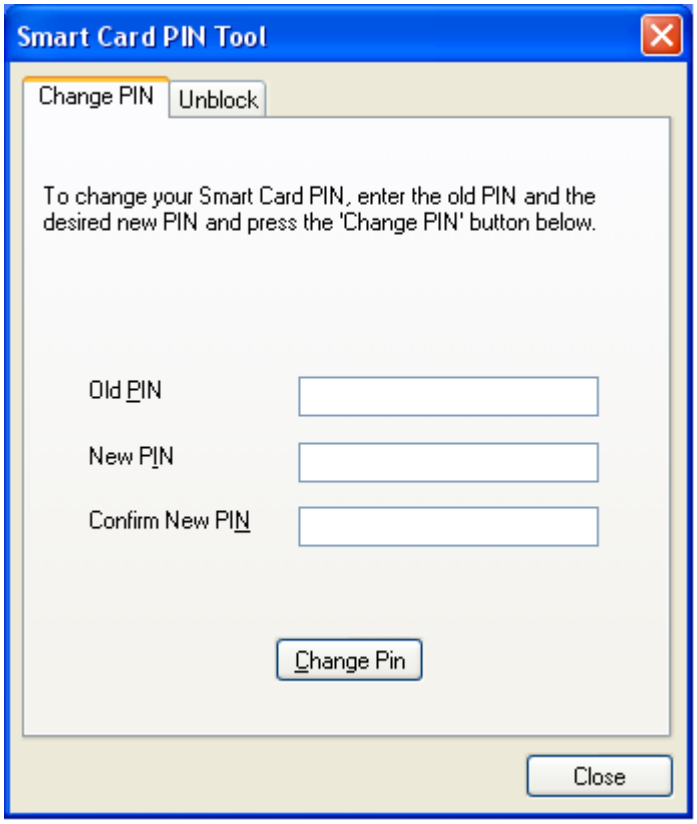


Figure 1 Smart Card PIN Tool – Change a User PIN

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

Note: The EnterSafe_Minidriver default PIN is **12345678**.

2.1.2 Changing a User PIN with Windows Vista, 2008

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

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

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

1. Press **Ctrl+Alt+Delete** to access the Secure Desktop screen.
2. Select the **Change a Password** option.
3. Attach EnterSafe Minidriver to a USB Port of the computer.
4. Select the smart card user tile.
5. Enter the old PIN, the new PIN and confirm the new PIN in the appropriate fields. As shown in Figure 2:

Figure 2 Secure Desktop - Change a User PIN

2.2 Unblocking EnterSafe Minidriver

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

Note: The EnterSafe Minidriver default maximum number of wrong PIN attempts is 10.

2.2.1 Example Unblock Procedure

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

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

1. The user retrieves a **Challenge** from the card.
2. The user communicates the **Challenge** to the IT Admin/Helpdesk.
3. IT Admin/Helpdesk combine the **Challenge** (8 bytes) and the user's **Admin Key** (24 bytes) using the Triple DES algorithm to calculate the unique **Response** (8 bytes) to the challenge.

4. IT Admin/Helpdesk communicates the **Response** to the end user.

5. The end user enters the **Response** value and defines a new value for the **User PIN**, which will be established once the Card Unblock has completed.

6. The smart card confirms that the **Response** provided is correct, by comparing the value entered by the user with one generated within the card using the **Challenge** generated by the card and the Admin Key stored in the card. If both values match, the card unblock is successful, the new user PIN is established and the PIN attempt counter is reset.

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

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

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

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

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

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

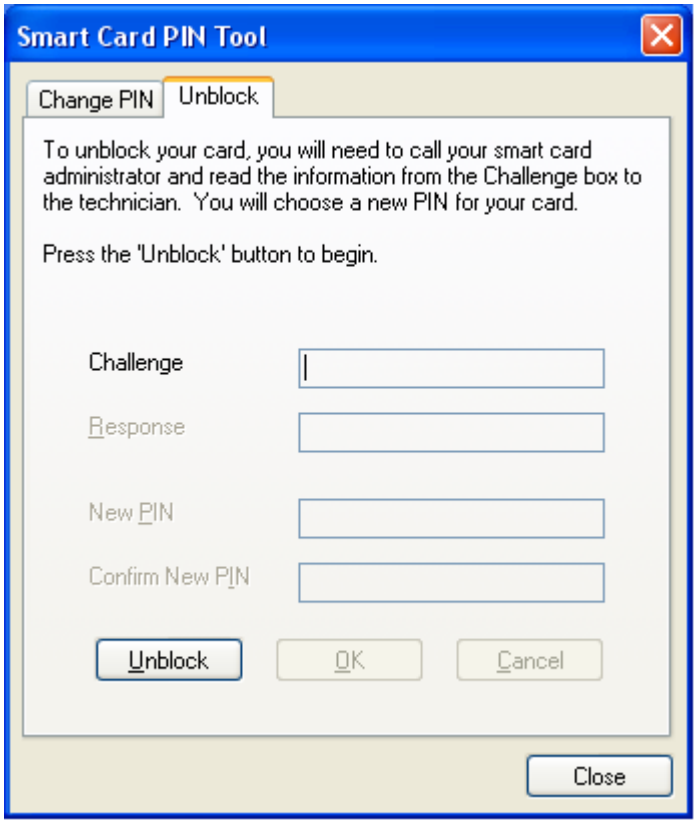


Figure 3 Smart Card PIN Tool – Unblock

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

2.2.3 Unblocking a Smart Card with Windows Vista, 2008

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

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

2.2.3.1 Enabling Unblock Card with Windows Vista, 2008

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

1. Click **Start** button, type **MMC** in the Start Search field and then press **Enter**.

2. When prompted to run Command Prompt as an administrator, click **Allow**. This will open the **Microsoft Management Console** dialog.

3. In the **Console 1** dialog, click on the **File** menu and select **Add/Remove Snap-in**.

4. In the **Add or Remove Snap-ins** dialog box, select **Group Policy Object Editor** in the **Available Snap-ins** pane on the left side, and then click **Add**, as shown in Figure 4:

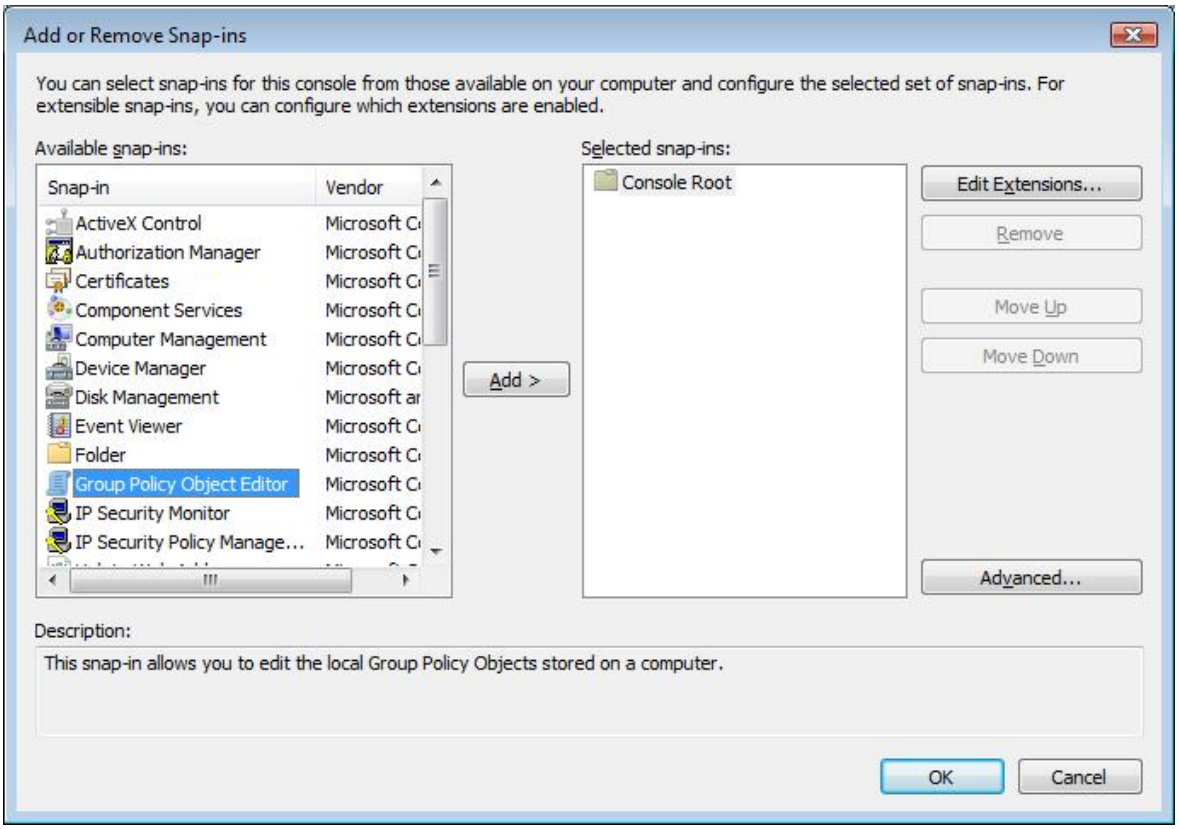


Figure 4 Add Group Policy Object Editor

5. You can either enable unblock for the local computer only, or for all computers in the domain.

1) To enable unblock on the local machine (only), you must be an administrator on the local computer. Select **Local Computer** in the **Group Policy Object** control. Click **Finish** to close the **Select Group Policy** dialog.
2) To enable unblock on all machines in the domain, you must be a Domain Administrator logged on to a Domain Controller and select **Default Domain Policy** in the **Group Policy Object** control. In the **Select Group Policy Object** dialog box, click **Finish**.

6. Click **OK** in the **Add or Remove Snap-ins** dialog box to close it.

7. Click on the **Local Computer Policy** node in the left side pane, then click on **Computer configuration**—>**Administrative Templates**—>**Windows Components**—> **Smart Card**. And then double-Click **Allow Integrated Unblock screen to be displayed at time of logon** in the **Setting** list, as shown in Figure 5:

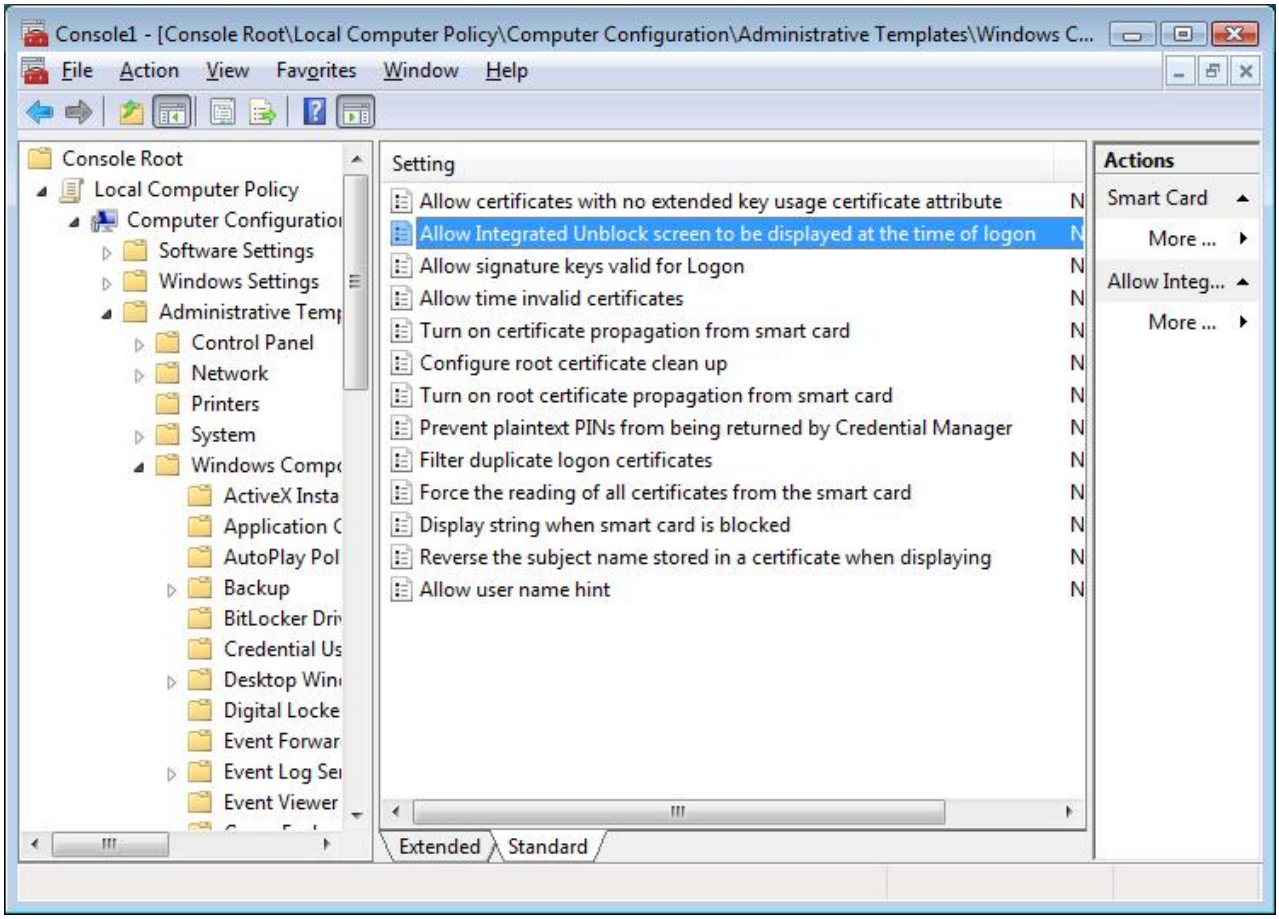


Figure 5 Unblock Smart Card setting

8. Select the **Enabled** option button, and then click **OK**, as shown in Figure 6:

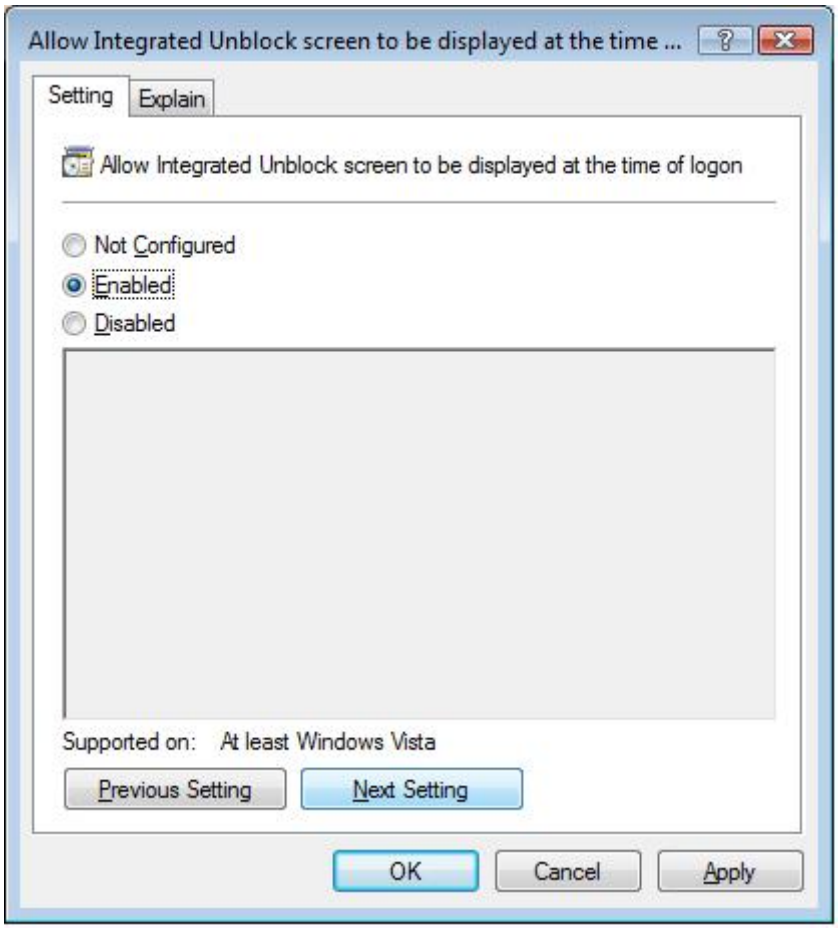


Figure 6 Enabled Unblock Smart Card

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

9. Back in the **Console 1** dialog, select the **Local Computer Policy** —> **Computer Configuration** —> **Administrative Templates** —> **Windows Components** —> **Smart Card**, and double-click on **Display string when smart card is blocked** on the right side pane.

10. Select the **Enabled** option button and type the string to display on the Unblock screen in the **Display sting when smart card is blocked** text box, and then press **OK**, as shown in Figure 7:

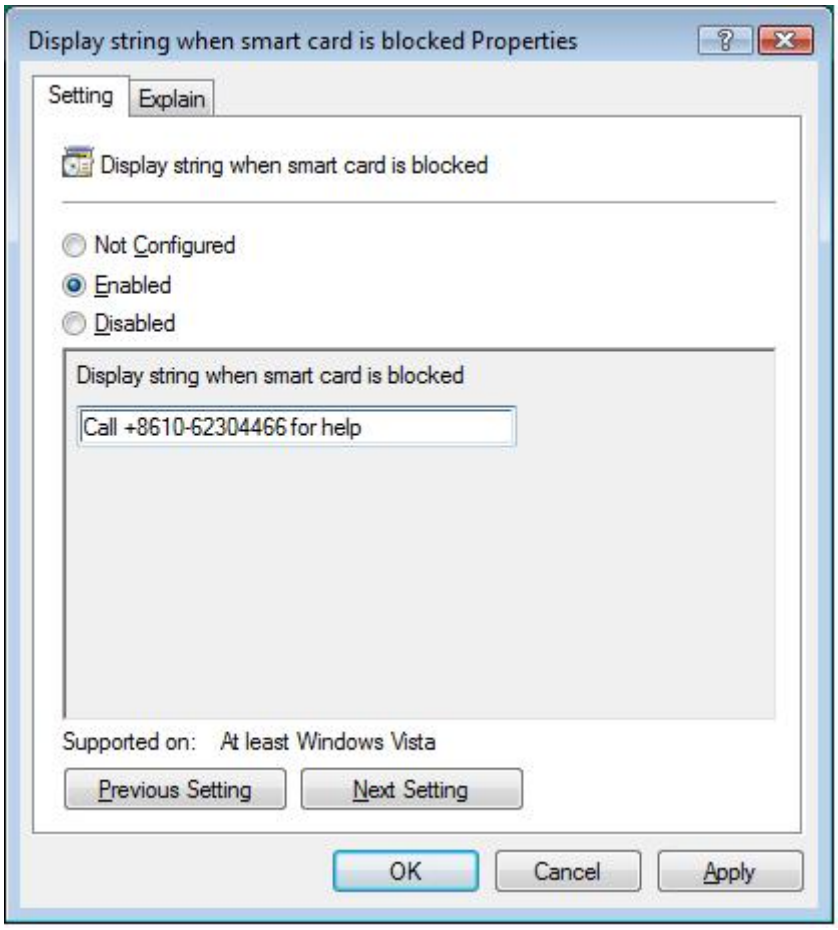


Figure 7 Display string when smart card is blocked Properties

2.2.3.2 Unblocking a Smart Card with Windows Vista, 2008

Same as for the Change PIN function, the Smart Card Unblock is integrated into the Windows Vista and 2008 **Secure Desktop**. However, it is not configured by default and must be explicitly enabled via Group Policy as 2.2.3.1 described. When this feature is enabled, the user is presented with the Smart Card Unblock screen when logon is attempted using a blocked smart card,, as shown in Figure 8:

Figure 8 Secure Desktop – Smart Card Unblock

2.2.4 Administrator Tools for Card Unblock

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

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

None of the Windows operating systems provide any means for administrators to handle the secure back-end storage of the user's smart cards Administrative keys, nor do they provide a back-end tool to calculate the response to a challenge. These features will be commonly provided by any commercial Base CSP compliant Card Management System (CMS), including Microsoft's Identity Lifecycle Manager (ILM).