www.gemalto.com

gemalto
security to be free

Classic Client 6.0

User Guide

gemalto
security to be free

GEMALTO, B.P. 100, 13881 GEMENOS CEDEX, FRANCE.

Tel: +33 (0)4.42.36.50.00 Fax: +33 (0)4.42.36.50.90

Printed in France.

Document Reference: DOC118688B

December 18, 2009

Contents

List of Figures

List of Tables

Welcome to Gemalto Classic Client.

You have made a wise investment by purchasing Classic Client as a safeguard for secure network services.

This chapter presents an overview of Classic Client, the documentation provided with it, and additional resources available for working with Classic Client.

Classic Client

Classic Client is for individual users, who want to use a smart card/token to protect information and transactions made via computers, including stand-alone workstations and Citrix client-server environments.

Note: A token is in fact a smart card embedded in a device that can be plugged into the USB port of a PC. In this document, “connecting a device” can mean inserting a card in a reader or plugging a token in the USB port of a PC.

With Classic Client you can use a digital certificate stored on a smart card/token to:

- Securely log on and off a Windows 2000, XP, Vista or 7 workstation; or Windows Server 2003/2008/2008 R2.
- Lock and unlock a Windows 2000, XP, Vista or 7 workstation; or Windows Server 2003/2008/2008 R2.
- Sign Microsoft Office, or XP macros and Adobe Acrobat documents.
- Open and verify signed documents.
- Send and receive secure e-mail using Microsoft or Mozilla e-mail software.
- Connect securely with a Web server.

Classic Client also includes features for managing certificates and smart card/token security.

This guide introduces you to Classic Client and provides easy-to-follow instructions. Read the entire guide for assistance in the installation, configuration, and use of Classic Client.

Classic Client includes two user profiles, the administrator and the user.

Who Should Read This Book

This guide is intended for Classic Client users who are familiar with smart cards/tokens and smart card reader technology, as well as PC hardware and software, the Internet and the World Wide Web.

It is assumed that the user of Classic Client has:

- an understanding of the basic operations in Windows.
- administrative privileges for the computer on which Classic Client will be installed.
- an understanding that the procedures in this manual refer to the **Administrator** and **User** as two separate people, but they may be the same person using a stand-alone workstation.

This guide gives the user simple easy-to-follow instructions for installing, configuring, and using Classic Client.

Documentation

Classic Client documentation includes:

- *Classic Client User Guide*
- *Classic Client Administration Guide*
- *Release Notes.pdf.* A separate file is included with each Classic Client software release version and contains the complete version history.
- *End User License Agreement* (EULA)

Classic Client 6.0 documentation is available as .pdf document files. The *Classic_Client_Administration_Guide.pdf* is located on the Classic Client 6.0 CD and in the Classic Client installation folder or through the Documentation plug in the Classic Client Toolbox GUI.

The *Classic_Client_User_Guide.pdf* is selected by the administrator to be included in each particular user setup.

The EULA is displayed during installation. It can be found after installation in the *install dir*\Documentation and depending on the User Setup may also be access through the Documentation Plug-in the toolbox.

These files can be printed out or read on screen using the Adobe Acrobat Reader.

To obtain the Adobe Acrobat Reader, you can download it from Adobe's Web site at: www.adobe.com.

These files are best viewed with the Acrobat Reader, version 9.0 or later.

Conventions

The following conventions are used in this document:

Typographical Conventions

Classic Client documentation uses the following typographical conventions to assist the reader of this document.

Convention	Example	Description
`Courier`	transaction	Code examples.
Bold	Enter **myscript.dll**	Actual user input or screen output.
>	Select File > Open	Indicates a menu selection. In this example you are instructed to select the **"Open**" option from the "**File"** menu.

Note: Example screen shots of the Classic Client software are provided throughout this document to illustrate the various procedures and descriptions. These screen shots were produced with Classic Client running on Windows 2000, XP or Vista.

Additional Resources

For further information or more detailed use of Classic Client, additional resources and documentation are available by contacting Gemalto technical support.

Contact Our Hotline

If you do not find the information you need in this manual, or if you find errors, contact the Gemalto hotline at http://support.gemalto.com/.

Please note the document reference number, your job function, and the name of your company. (You will find the document reference number at the bottom of the legal notice on the inside front cover.)

1

Installation

This chapter discusses information related to the installation of Classic Client 6.0 The installation requirements are outlined below.

This chapter describes:

- The hardware and software you need to use Classic Client 6.0.
- How to install Classic Client 6.0 on your computer.
- How to check that the necessary Windows Services are running, and how to install them if they are not.

System Requirements

The following sections describe the hardware, operating systems, peripherals and software you need to use Classic Client 6.0.

For any computer on which Classic Client 6.0 will be installed, the user installing the software must have administrator rights to that computer.

Note: For information about the operating systems, applications, smart card devices and smart card readers that are supported by Classic Client, please refer to the *Release Notes*.

Computer

The workstation must meet the normal system requirements to run its version of Windows.

The Classic Client Toolbox is best viewed with a screen resolution of 90 dpi. If your computer uses a different resolution, this does not affect performance, but the appearance of the toolbox may not be perfect.

Operating Systems

Classic Client 6.0 comes in two versions, one for 64–bit operating systems and one for 32–bit operating systems (OS). Install the version according to your OS. The “What’s In?” section of the *Release Notes* summarizes the OS that Classic Client supports for the two versions.

Gemalto recommends that your machine has a RAM at least equal to that normally recommended for the OS. If this RAM requirement is met, Classic Client should run normally.

Applications

For a detailed list of applications supported by Classic Client 6.0, please refer to the *Release Notes*. Here are some useful links where you can download the latest versions of some software applications free of charge:

Microsoft Internet Explorer from Microsoft Internet Explore Download

Mozilla Firefox and Thunderbird from www.mozilla.org

Adobe Acrobat and Adobe Acrobat Reader from http://www.adobe.com/

Peripherals

Classic Client requires an available USB or PCMCIA port (not needed if your PC has a reader embedded).

For a detailed list of the smart cards and smart card readers supported by Classic Client 6.0, please refer to the *Release Notes*.

Installing Classic Client 6.0

Removing Previous Versions of Classic Client

Installing Classic Client 6.0 automatically removes versions 5.2, 5.1 and 5.0. – then known as GemSafe Standard Edition. However it does not automatically uninstall previous versions older than 5.0. These must be removed manually. Remember that versions older than 5.0. are called “GemSafe Libraries”.

Note: For versions of GemSafe Libraries previous to 4.0, a special Uninstall Tool has been developed and is available from Gemalto Support Services. If you have problems uninstalling previous versions, contact Gemalto Technical Support (refer to “Contact Our Hotline” on page ix).

For every workstation on which a new version of Classic Client is to be installed, the administrator must check that all older versions are removed successfully.

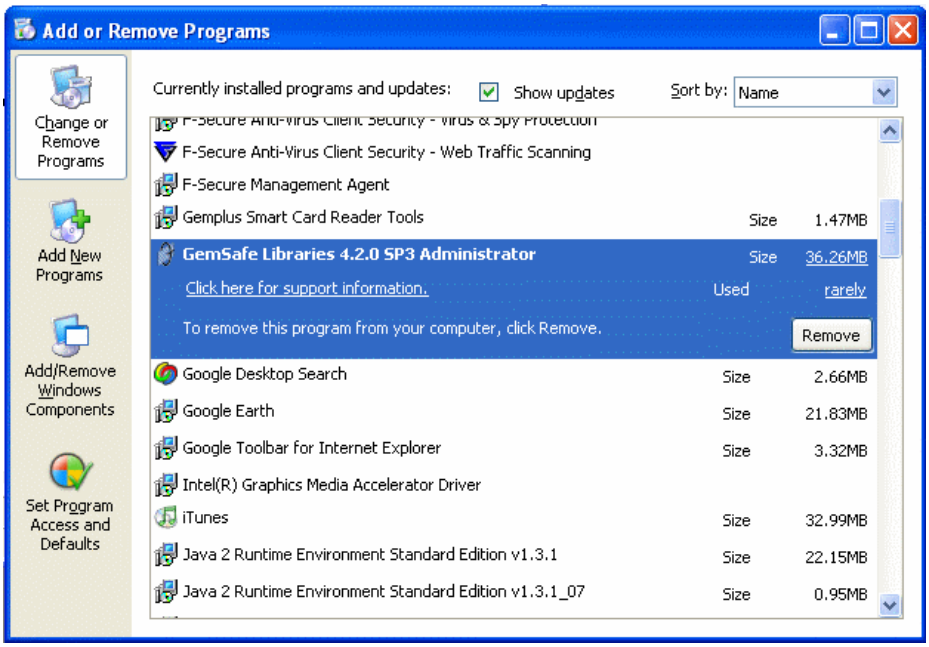
If you have other middleware installed on your PC, you may also need to uninstall this, depending on how it works. For further information consult your Gemalto technical consultant.

Caution: Before removing the software, make sure you disconnect all devices (smart cards/tokens).

To remove a previous version of GemSafe Libraries:

1. Open the **Control Panel** (**Start > Settings > Control Panel**).
2. Click **Add or Remove Programs**.
3. Locate **GemSafe Libraries** as shown in “Figure 1”.

Figure 1 - Add/Remove Programs Window



Note: The text in your installation will say “GemSafe Libraries” instead of “GemSafe Libraries Administrator”. Otherwise the windows are as shown in this chapter.

4 Click **Remove**. A window appears asking if you are sure that you want to remove GemSafe Libraries.

5 Click **Yes**. A progress bar displays while GemSafe Libraries is removed.

6 At the end of the removal, the progress bar closes, removal is complete and GemSafe Libraries is removed from your computer.

7 If prompted, restart your computer.

Note: The Smart Card reader installations are not removed.

Installing the Classic Client Software

This section describes how to install Classic Client.

Caution: Before installing the software, make sure you disconnect all devices (smart cards/tokens).

Note: Remember that the installation of Classic Client does not automatically remove versions of Classic Client older than 5.0.i. These must be manually removed as described in “Removing Previous Versions of Classic Client” on page 2.

To install Classic Client 6.0:

1 Do one of the following:

a) If your administrator has provided an installation CD-ROM, insert the CD-ROM into the CD-ROM reader of your computer.

If your computer is configured to autorun a CD, the installation wizard starts automatically.

If the installation wizard does not start automatically, do the following:

1. In Windows, navigate to **Start > Run** to open the **Run** dialog box.

2. Enter ***d:*\Classic_Client_32_User_setup.msi** in the **Run** dialog box, where *d:* is your CD-ROM drive.

Note: If you are installing the 64–bit version of Classic Client, enter ***d:*\ Classic_Client_64_User_setup.msi** instead.

3. Click **OK** to start installing the software.

Alternatively, navigate to the location of the installation file on the CD and double click on the Classic_Client_32_User_setup.msi file.

b) If your administrator has made the installation program available from a network device, navigate to the network location.

When you have located the Classic_Client_32_User_setup.msi file in either of these locations, double-click on the file to start installing the Classic Client software.

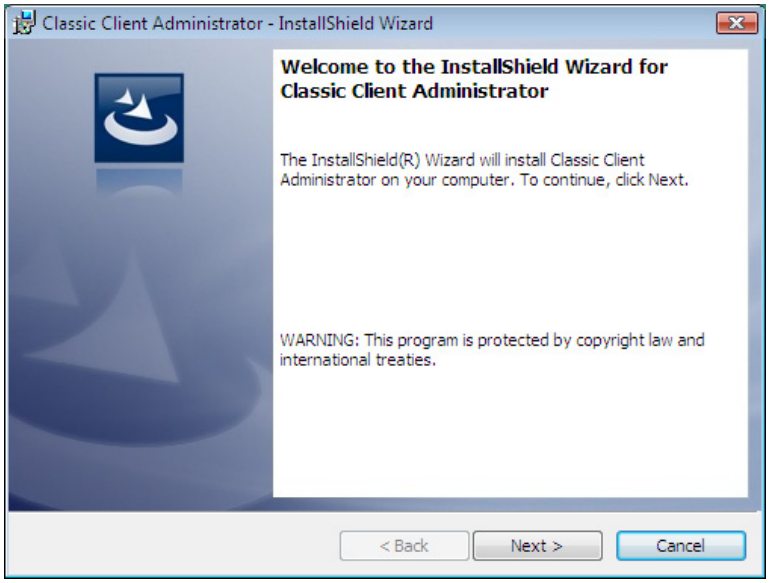
2 Microsoft Vista/7/Server 2008 and Server 2008 R2 only: If User Access Control is activated, the warning “An unidentified program wants access to your computer” appears. Choose **Allow**.

The **Classic Client InstallShield Wizard** displays the window indicating that it is preparing to install.

Allow the installation to continue until the **Welcome** window appears.

Note: The text in your installation will say “Classic Client” instead of “Classic Client Administrator”. Otherwise the wizard is as shown in this chapter.

Figure 2 - InstallShield Wizard Welcome Dialog Box

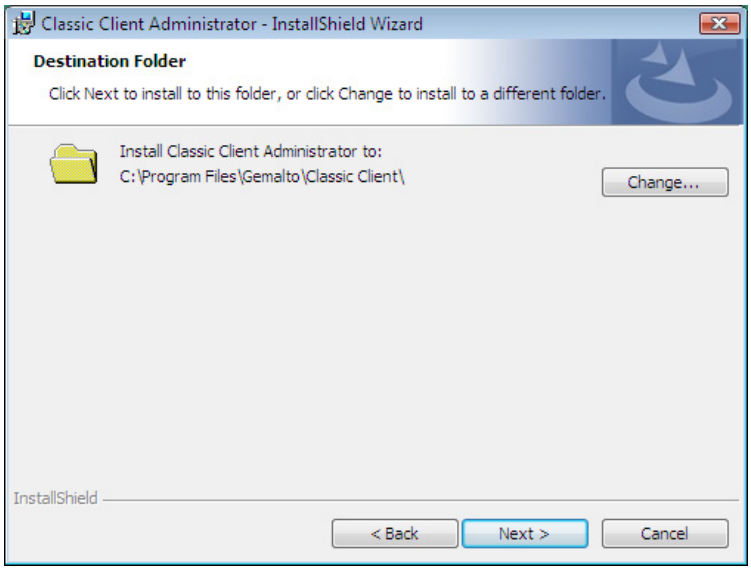


3 When the **Welcome** dialog box appears, click **Next** to continue; the **Classic Client InstallShield Wizard** displays the **License Agreement** window.

4 Read the **Gemalto License Agreement.** Accept the terms if you wish to continue by choosing “**I accept the terms in the license agreement...**” button and then click on **Next.**

The **Classic Client InstallShield Wizard** displays the **Destination Folder** window.

Figure 3 - InstallShield Wizard Destination Folder Window



5 The destination folder is the location where the plug–ins and other files are installed. Either click **Next** to accept the proposed default (recommended) or use the **Change** function to choose another location and click **Next**.

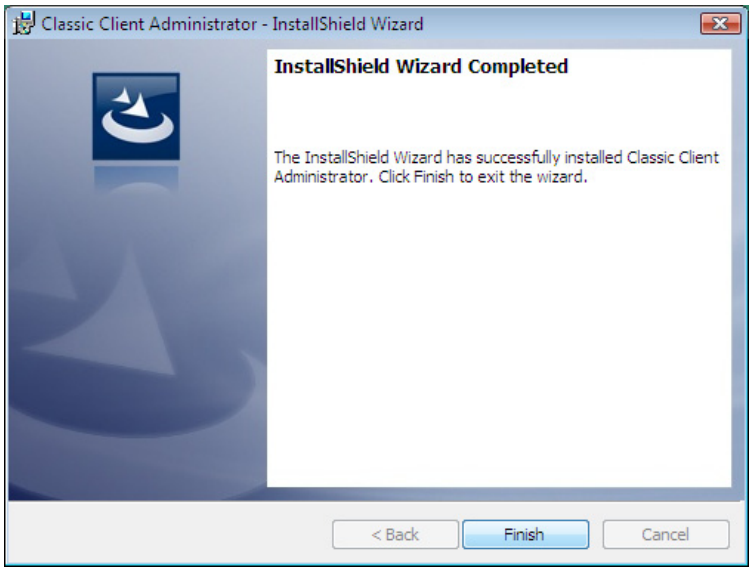
Caution: For 64–bit operating systems; if you choose a different location, the location must not be under c:\Program Files\... You can choose c:\Program Files (x86)\...or another location.

The **Ready to Install the Program** dialog appears.

6 Click **Install** to start the installation. An “Installing” window displays showing a progress bar during the installation.

When the **Classic Client InstallShield Wizard** has completed the installation, the “Completed” dialog appears as shown in the following figure:

Figure 4 - InstallShield Wizard Completed



7 Click **Finish** to complete the installation. The **Classic Client InstallShield Wizard** displays the **Reboot Dialog**.

8 Click **Yes** to restart the system immediately or **No** if you want to restart your computer later.

Classic Client is now installed on the computer.

Note: You will not be able to use the Classic Client software until you have restarted your computer.

Connecting the Smart Card Reader

To use Classic Client 6.0 on your workstation, you must connect a smart card reader to your computer.

If the card reader is not recognized on your workstation, you may need to install the latest card reader drivers. You can download these from http://support.gemalto.com.

Installing Gemalto Cryptographic Security Modules

Security Modules are software add-ons that provide a variety of cryptographic services, such as secure browsing, and support the use of smart cards/tokens.

In Classic Client 6.0, the installation of Security Modules can be done either automatically or manually, depending on the application with which Classic Client is being used.

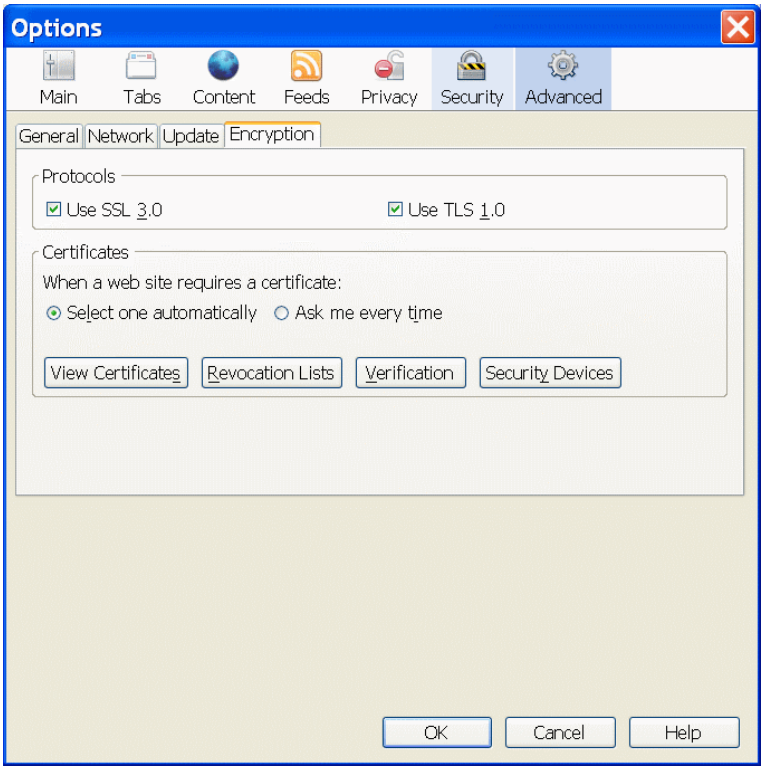
Classic Client must be declared as a security module, so that applications can communicate with it. For some applications, such as Firefox for example, the security module cannot be installed automatically and must be done manually.

To manually install a security module for Firefox:

1 Open **Firefox** and from the **Tools** menu choose **Options**. The **Options** dialog opens.

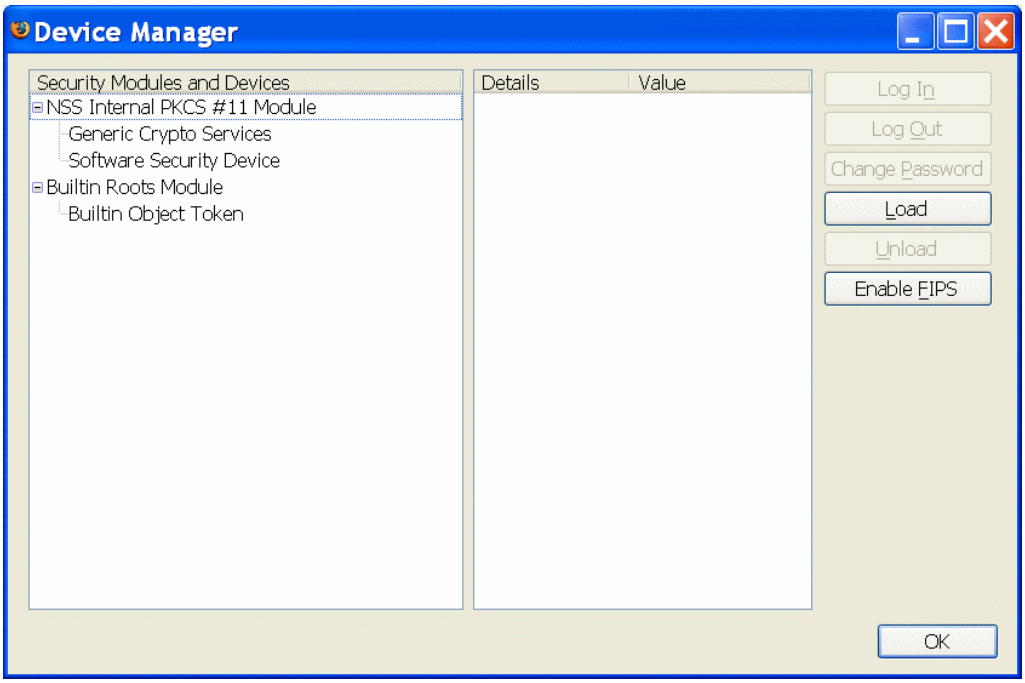
2 Click the **Advanced** icon, then the **Encryption** tab to display the settings as shown in “Figure 5”.

Figure 5 - The Options Dialog



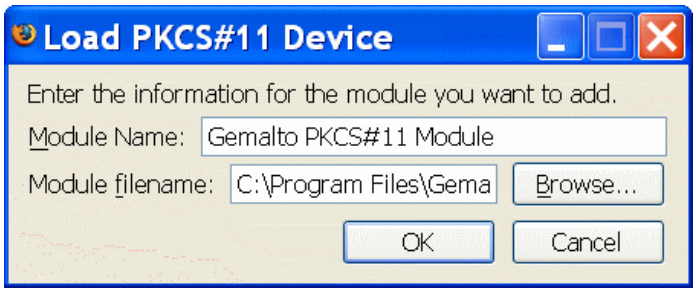
3 Click **Security Devices** to display the **Device Manager** window. This displays the modules currently available as shown in “Figure 6”.

Figure 6 - Device Manager



4 Click the **Load** button to the right in the dialog. This displays the **Load PKCS#11 Device** window, as shown in “Figure 7”.

Figure 7 - The Device Manager Dialog and the Load PKCS#11 Device



5 Enter a **Module Name.**

6 In **Module filename**, use the **Browse** button to select the gclib.dll file as follows:

- For 32-bit versions of Windows, this is in *install dir*\BIN\, where *install dir* is the directory where you installed Classic Client. By default, *install dir* is c:\Program Files\Gemalto\Classic Client\
- For 64-bit versions of Windows, the location of the gclib.dll depends on whether you are using the 32-bit version of Firefox or the 64-bit version.
  - For a 32-bit version of Firefox, the gclib.dll is in *install dir*\BIN\. By default, *install dir* is c:\Program Files (X86)\Gemalto\Classic Client\
  - For a 64-bit version of Firefox, the gclib.dll is in c:\Program Files\Gemalto\Classic Client\BIN\

Caution: Not all tokens are supported for the 64-bit version of Windows. Please refer to the Release Notes to know which these tokens are.

---

7 Click **OK**. The “Confirm” dialog appears asking if you are sure that you want to install the security module.

8 Click **OK**.

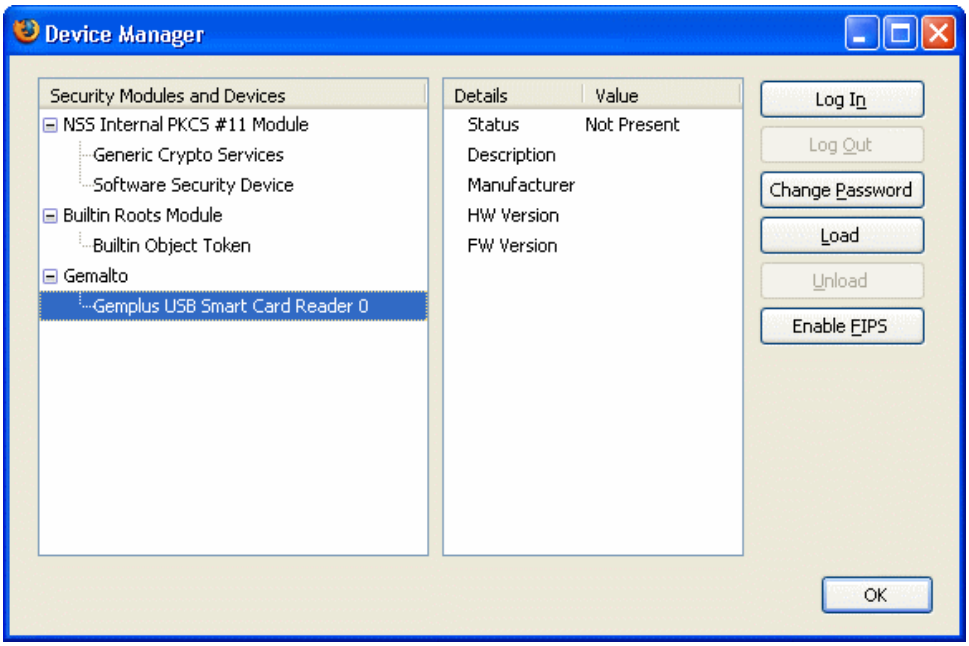
A brief progress dialog appears indicating that the module is being loaded.

When this is completed an “**Alert**” indicates that the module has been installed.

9 Click **OK** to close this **Alert**.

The **Device Manager** indicates the presence of the new module as shown in “Figure 8”:

Figure 8 - Cryptographic Modules Available



Note: The example shown in “Figure 8” shows the name of the reader (Gemplus USB Smart Card Reader 0) because no card is inserted in the reader. If a card is inserted at the time you are loading the module, then the name of the card appears instead of the reader.

Uninstalling Classic Client 6.0

This example shows the Administrator version. The procedure to remove the User version is the same except that the program appears as “Classic Client” instead of “Classic Client Administrator”.

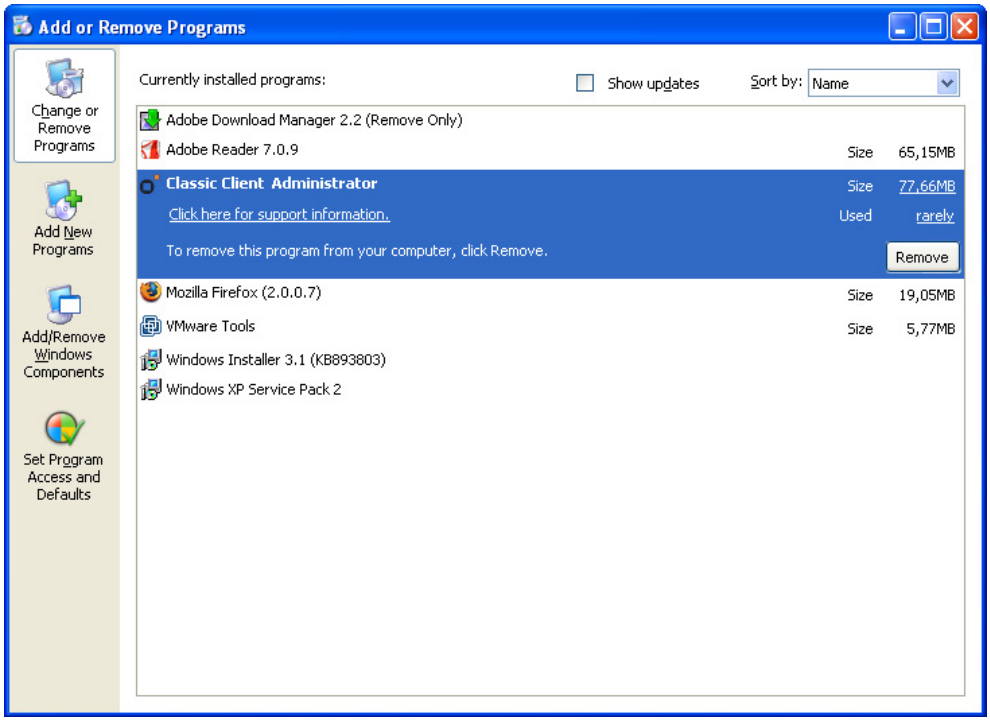
To remove Classic Client 6.0 in Windows 2000, XP and Server 2003:

1 Open the **Control Panel** (**Start > Settings > Control Panel**).

2 Click **Add or Remove Programs**.

3 Locate **Classic Client** as shown in “Figure 9”.

Figure 9 - Add/Remove Programs Window (Classic Client 6.0)



4 Click **Remove**. A message box displays asking “Are you sure you want to remove Classic Client 6.0 from your computer.

5 Click **Yes** to confirm the removal of Classic Client 6.0. A progress bar appears during the removal.

At the end of the removal, the progress bar closes, removal is complete and Classic Client is removed from your computer.

6 If prompted, restart your computer.

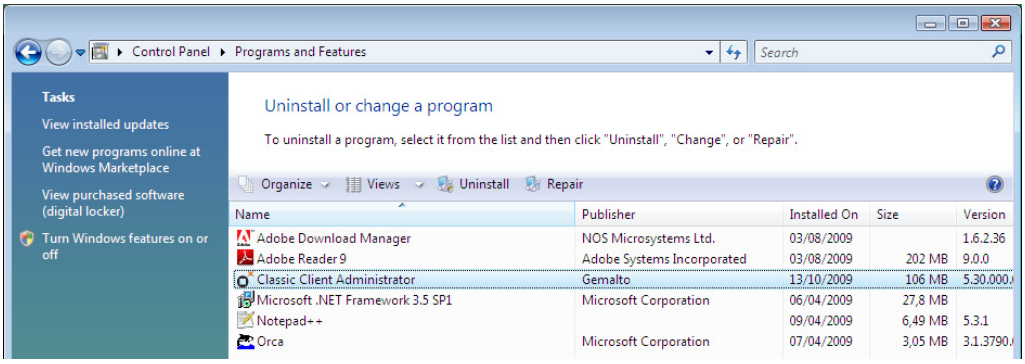
To remove Classic Client 6.0 in Windows Vista, 7, Server 2008 & Server 2008 R2:

1 Open the **Control Panel** (**Start > Control Panel**).

2 Double-click **Programs and Features** (if you are using the Control Panel view under Vista/Server 2008 or the Category view under 7/Server 2008 R2, then under **Programs**, click **Uninstall a program** instead).

3 Select **Classic Client 6.0** as shown in “Figure 10” and click **Uninstall** (the **Uninstall** button appears when you select Classic Client 6.0).

Figure 10 - Programs and Features Window



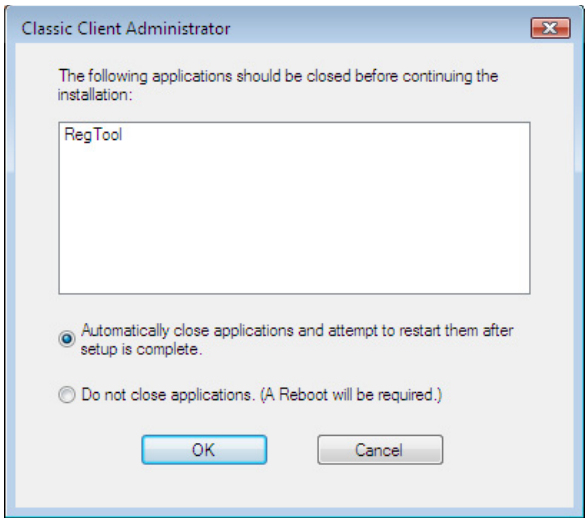
4 A message box displays asking “Are you sure you want to uninstall Classic Client 6.0.

5 Click **Yes** to confirm the removal of Classic Client 6.0.

6 If User Account Control is activated, the warning “An unidentified program wants access to your computer” appears. Choose **Allow**.

7 Again, if User Account Control is activated, a message like the one shown in “Figure 11” may appear to tell you to close certain applications, in particular the Registration Tool.

Figure 11 - Close Applications Message



Choose the **Automatically close applications** option and click **OK**.

8 A progress bar appears during the removal.

At the end of the removal, the progress bar closes, removal is complete and Classic Client is removed from your computer.

9 If prompted, restart your computer.

Checking the Windows Services

To run Classic Client correctly, the following Windows Services must be running on the computer where Classic Client is installed:

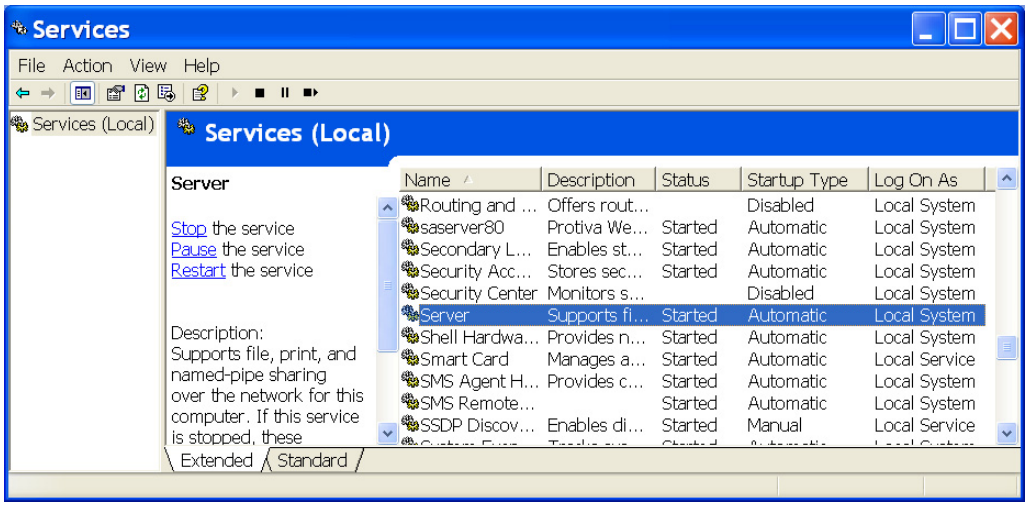
- Server
- Smart Card

To check if these services are running:

1 Open the **Services** window (**Settings** > **Control Panel** > **Administrative Tools**).

2 If the services are running, they appear as shown in “Figure 12”, with a **Status** of “Started” and **Startup Type** of “Automatic”.

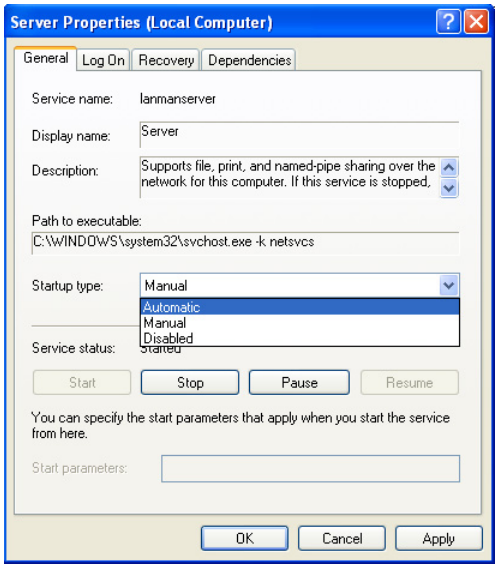
Figure 12 - The Services Window



3 If the status is not “Automatic”, set it to “Automatic” as follows:

a) Right-click the service and choose **Properties**.

Figure 13 - Properties Window for a Service



b) In the **Properties** window, select **Automatic** as the **Startup Type** as shown in “Figure 13”.

c) Click **OK**.

4 If the service does not appear in the Services window (“Figure 12” on page 12), it needs to be installed — in which case contact your system administrator.

2

The Classic Client Toolbox

This chapter discusses the Classic Client Toolbox, the dedicated tool for working with Classic Client.

The Classic Client Toolbox is made up of a number of tools that enable the user to perform tasks associated with the use of Classic Client products. Some of the tools are product specific and will include the product name in the title.

About PINs

The User PIN

A PIN (*Personal Identification Number*) is a private code. It can be a sequence of numeric or alphanumeric characters or a mix of the two and is used as a type of password. As a user, your User PIN must be verified before you can perform security tasks with the card/token, such as logging on to a workstation, or creating a digital signature.

The user PIN of a smart card/token may be the original PIN value set at the time of manufacture *or* it may be a PIN value assigned by the administrator.

The user PIN should be unique to the user's card/token and known only to the user. If the administrator gives the user the rights, it is standard practice, upon reception of a smart card/token, to change the user PIN value so that only the user knows it. The administrator can even force the user to change the PIN value upon first use in the software.

To perform a security operation, the card/token user must demonstrate knowledge of the PIN. Software that performs a security operation usually displays a window requesting the user enter the PIN before performing the security operation or there is a field where the user can enter the PIN, as is shown in the Classic Client Toolbox.

- When creating a digital signature, successful PIN validation proves that the user is the correct card/token holder and permits the user to sign with the selected key.
- By using the PIN to log on a network, the user proves both that the user card/token is valid in the system and that the card/token holder, is physically there. If the PIN is truly secret, the person entering the PIN must also be the card/token holder.

Caution: Do not allow the User PIN for your card/token to be blocked. If, for example, you forget the user PIN and enter a predetermined number of failed validation attempts (the PIN is entered incorrectly), the card/token becomes blocked and you cannot perform any further security operations with it. If you know the Admin PIN you can unblock your card/token as described in "How to Unblock a User PIN" on page 35. However most companies' security policy does not allow this, in which case you must ask the Classic Client system administrator to unblock the card/token using the Admin PIN. If your user setup allows it, you may be able to unblock your card/token remotely. This operation is described in "How to Remotely Unblock a Connected Smart Card/ Token" on page 36. Sometimes card/token technology or software on-board the card/ token limits the absolute number of these unblocking operations. For more information, see your card/token technology documentation.

The Administrator PIN

This is the PIN used to unblock a User PIN. As a user you will not know the value of this PIN unless allowed by your company's security policy.

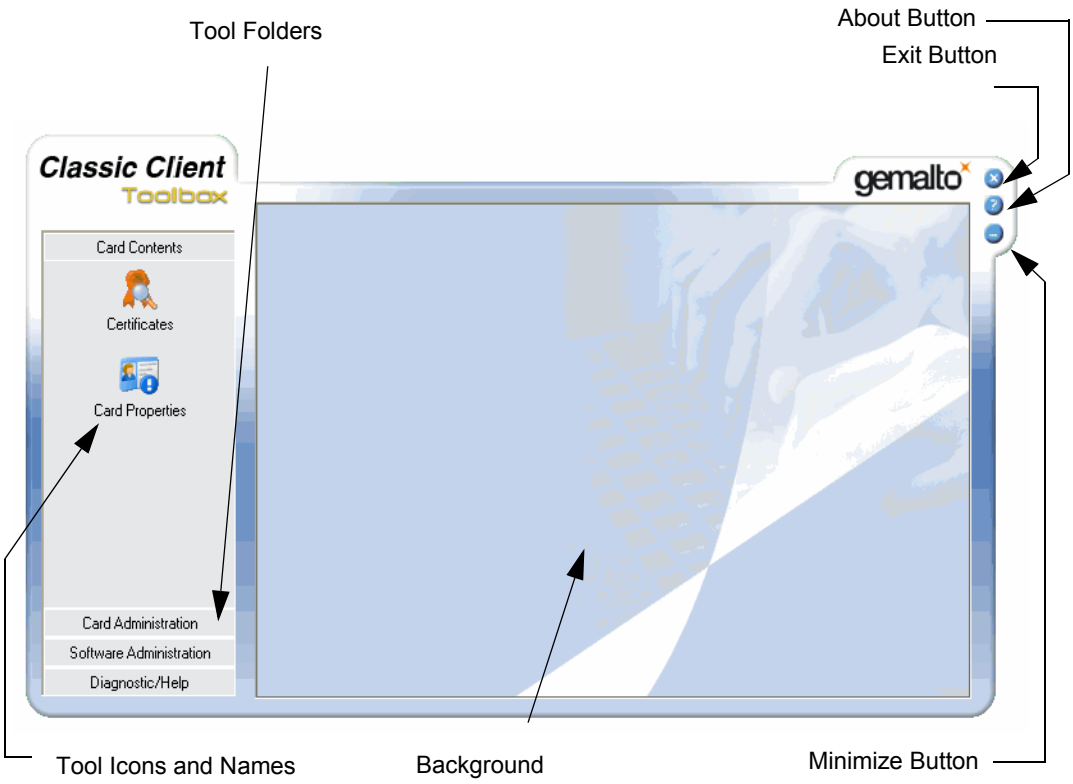
The Classic Client Toolbox Graphical User Interface

Note: Since Classic Client is distributed to you by your administrator, you may not receive all of the tools mentioned below. The actual tools you receive is determined by your company's security policy and how it is applied by the Classic Client administrator in creating your user setup.

To access the tools in the Classic Client Toolbox:

Navigate through **Start > All Programs > Gemalto > Classic Client > Classic Client Toolbox** to open the Toolbox.

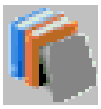
Figure 14 - Classic Client Toolbox Graphical User Interface



In the left panel of the GUI, the tools are located in folders with labelled tabs. The various tools are located within each folder, grouped according to tool use.

Note: The Software Administration folder appears only in the Administrator setup and not the usual User setup.

Card Contents folder	
	**Certificates**: The Certificates tool allows you to view information on the objects on your card/token. According to PKCS#11, these objects can be certificates, keys and data objects.
	**Card Properties**: The Card Properties tool allows you to view information associated with a particular smart card/token.
Card Administration folder	
	**PIN Management**: The PIN Management tool allows you to make changes to the PIN associated with a particular smart card/token.
ECC Management folder (useful for IAS ECC cards only)	
	**PKCS#15**: The PKCS#15 tool allows you to browse the PKCS#15 file structure and save it as an XML file.

	**Personal Data**: The **Personal Data** tool allows you to read and update personal data in IAS ECC cards.
Diagnostic/Help folder	
	**Diagnostic Tool**: The Diagnostic Tool is used to examine all components of the Classic Client installation to determine if there are problems using Classic Client.
	**Documentation**: The Documentation folder displays all the documentation available to you, and will vary according to your user setup. It includes the Release Notes, the EULA and may include the *Classic Client User Guide* if your administrator specified this in your user setup.

Click the folder tab and view the tools within. Click the tool icon to display tool parameters in the right panel. Some information is available for viewing without logging in using the PIN.

Most options are self explanatory in the graphical user interface. Further explanations follow.

Logging in with a PIN

Note: Certain tasks in the toolbox require you to log in to the card by entering the User PIN. You only need to do this once in the session to access all the tools in the toolbox. If the User PIN entry is correct, the padlock icon changes from closed to open to indicate a successful login.

Note: If the use of a tool is not possible even after logging in, this tool is not available to you.

Card Contents Folder

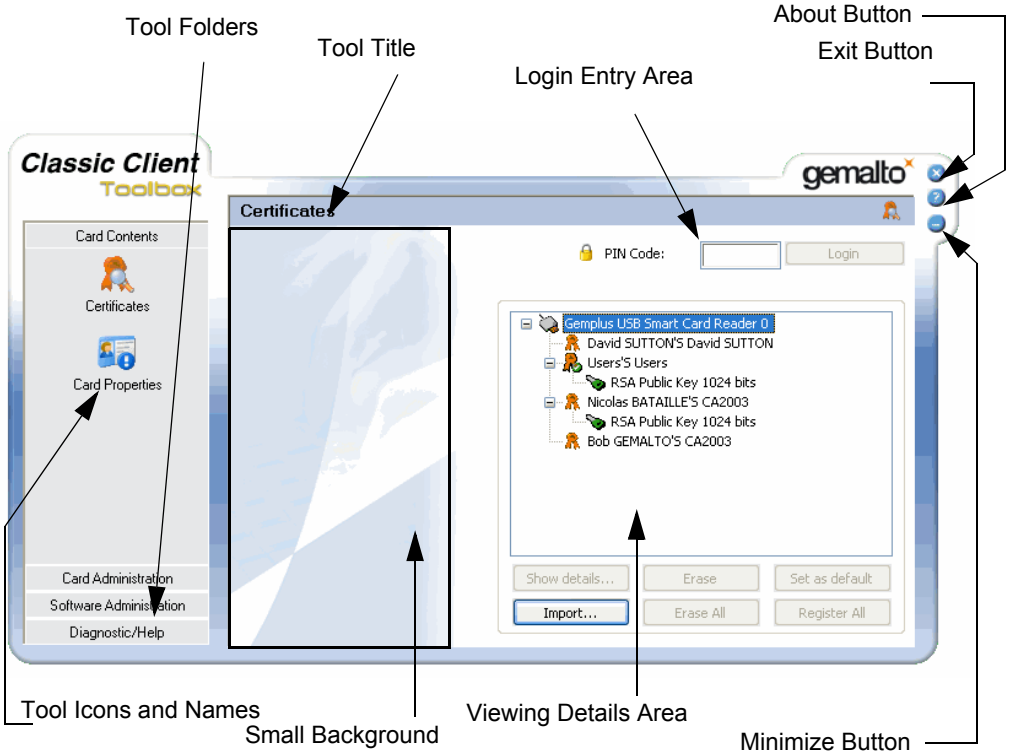
The **Card Contents** folder contains all the tools associated with viewing and interacting with the contents of a particular smart card/token. These tools are the **Certificates** tool and the **Card Properties** tool.

Certificates Tool

The Certificates Tool allows you to view information on certificates and key pairs in the smart card/token.

Note: The Certificates Tool is only available if the Administrator has included it in the user setup.

Figure 15 - Certificates Tool Window (Not logged in)



The Certificate Tool displays information about the following certificates and key pairs:

- Certificate Authority (CA) and User Certificates:
  - Serial number
  - Expiration date
  - Owner
  - Issuing Certificate Authority (if applicable)
  - The keys associated with each certificate
- Keys:
  - Public keys
  - Private keys (some cards/tokens require that you log in first)

The **Certificates Tool** allows you to:

- Manually register all certificates
- Set a default certificate

- Erase one or more certificates or key pairs in the smart card/token (if this feature is enabled by the administrator)

Note: The option to **Erase** or **Erase All** using the Certificates Tool does not determine the capability of other applications that can also perform these functions.

- Show details about a certificate or a key
- Import and export a certificate.

  There are some important points to note:

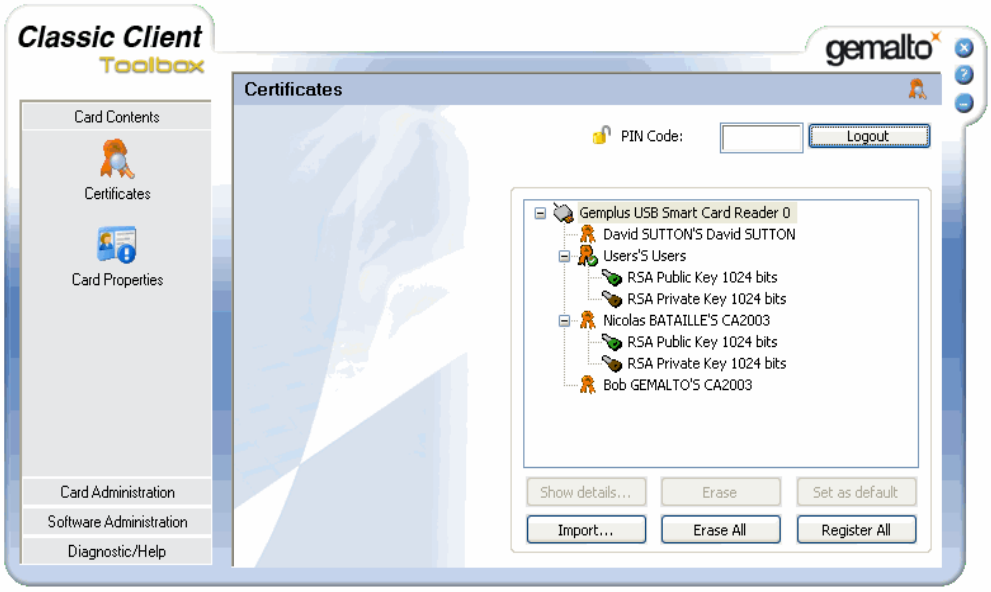
  – You can import a certificate without logging in, because certificates are always imported to the card's/token's public area. But if you do not log in, and the certificate has a key pair associated with it, the key pair is not imported.

  – You must login before you can perform any export operations with the Certificates Tool.

  – You can never export a certificate's associated key pair.

  – If you are not logged in, you may not be able to view private objects on the card/token. This depends on the card/token technology and the on-board software. If you cannot view a private key that you are sure you imported in a previous session, make sure that you are logged in before you conclude that the import process did not work.

Figure 16 - Certificates Tool Window (Logged in)



For the procedures to follow to perform tasks with the Certificates Tool, refer to "Managing Certificates" on page 64.

Certificate and Key Icons

The Certificate Tool can display the following icons, each representing a PKCS#11 object.

Certificate

Default Certificate

Imported Public Key

On-board Public Key

Imported Private Key

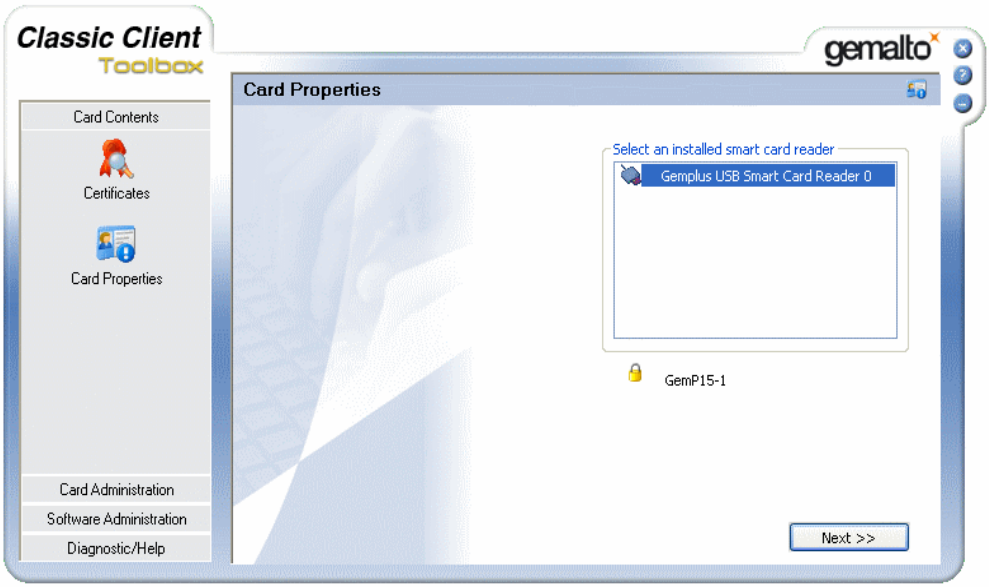
On-board Private Key

Card Properties Tool

The **Card Properties** tool allows you to view information associated with a particular smart card/token.

The **Card Properties** window displays all available card readers or PKCS#11 slots.

Figure 17 - Card Properties Window

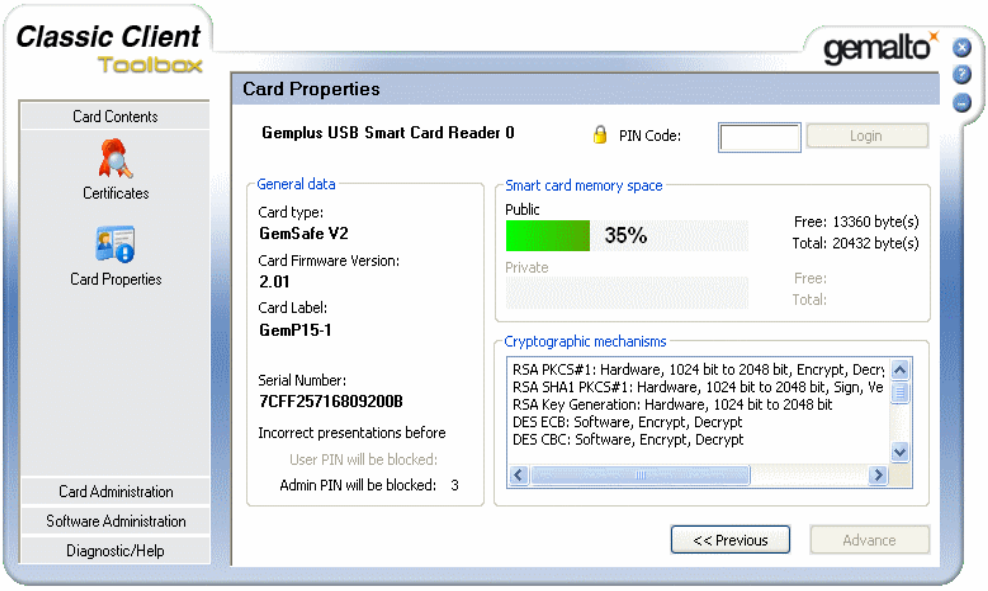


To view information on a smart card/token.

1 Choose the smart card reader from the list that holds the card/token you are interested in and then click on **Next** to continue.

Information on the card/token is displayed:

Figure 18 - Card Properties Window (Not logged in)



Classic Client may not be able to display all information on the smart card/token because not all smart cards/tokens have the same technology and the same on board software.

In general, you can see information about:

- Card/Token Type and Firmware
- Card/Token Label and Card/Token Serial Number
- Maximum number of incorrect PIN entry attempts (when supported) before blocking occurs
- Smart Card/Token Memory Space

Some smart cards/tokens do not allow Classic Client to view the number of PIN attempts remaining before the card/token becomes blocked. See “How to Check The PIN Ratification Counter” on page 34 for information on how to work around this.

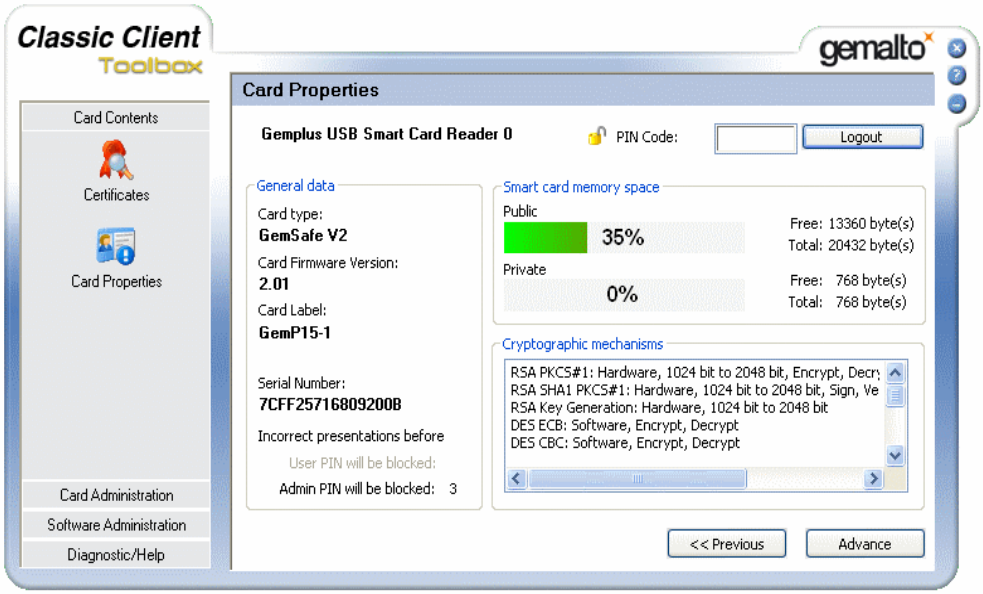
2 Enter the PIN associated with the smart card/token in the **PIN Code** area and click on **Login**.

  – The padlock symbol in the GUI unlocks to indicate that the user is successfully logged in with that smart card/token and PIN, as shown in “Figure 19” on page 21.

  – With cards/tokens where private information on the card/token is PIN protected, logging in enables this information to become visible, for example, Cryptographic Mechanisms and Key lengths.

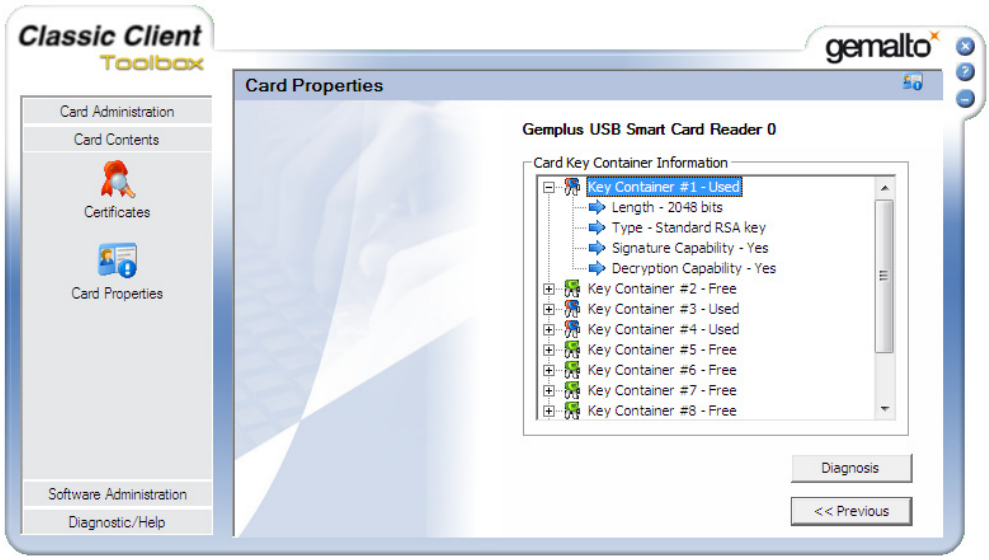
  – The **Advance** button becomes available.

Figure 19 - Card Properties Window (Logged in)



3 By clicking on the **Advance** button, all key containers associated with the card/ token are displayed and additional information can be viewed by clicking on the plus symbol to expand the key container. This information includes how many keys are available in the container or if it is free.

Figure 20 - Card Properties Window (Showing Key Containers and Attributes)



The **Diagnosis** button provides an extra tool you can use if you have a problem with your card that you think may be linked to key sets and/or certificates. For more information about this took please refer to “I think there may be a problem with the key sets and/or certificates in my card - How can I check?” on page 87.

Card Administration Folder

The **Card Administration** folder contains the **PIN Management** tool.

PIN Management Tool

The **PIN Management** tool allows you to make changes to the PIN associated with a particular smart card/token. It also allows you to view the PIN policy that has already been defined by the administrator for this particular installation.

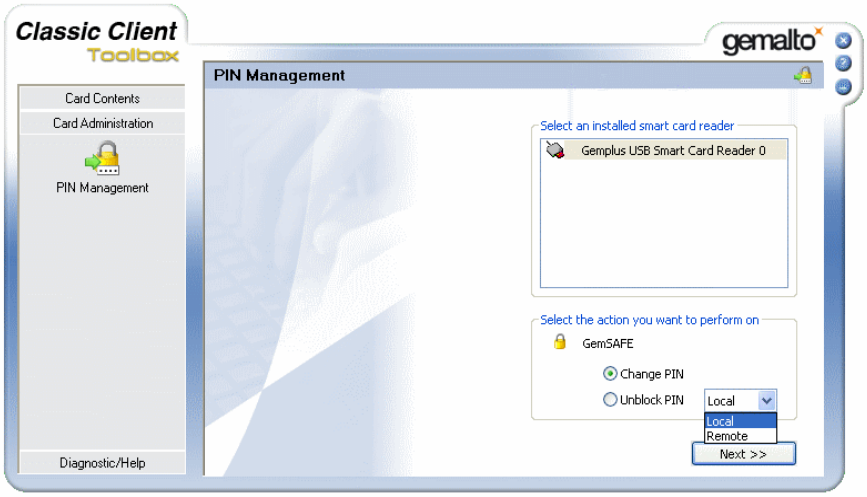
Caution: PIN policies are established according to a company's security policy, but they are also established in relation to the particular type of smart card/token you use and the on-board software the card/token features. Please refer to your card/token documentation to make sure that your PIN policy is consistent with any limitations imposed by the card/token/applet. In particular, please note the following:

- Some cards/tokens allow a user PIN to be a minimum of 4 characters, while others insist on it being a minimum of 6 characters.
- For the Classic Applets V2 and V3 (and IAS Classic Applets V2 and V3), the maximum PIN length is 16 ASCII bytes. The maximum PIN length for global PINs in Classic Applet V3 (and IAS Classic Applet V3) is 12 bytes.
- For Classic Applet V1, only numeric values are allowed for PINs.

To access the PIN Management Tool:

Click the **PIN Management** icon in the **Card Administration** folder. This displays the tool as shown in "Figure 21" on page 22.

Figure 21 - PIN Management Tool Window



From this window, choose the function you want to perform, **Change PIN** or **Unblock PIN** and click **Next**.

Note: The list next to the **Unblock PIN** option appears only if you have been granted both "unblock" and "remote unblock" rights in your user setup.

For the procedures of how to perform these functions, refer to "PIN Management" on page 33.

PIN Types

Classic Client recognizes three types of PIN that may be in a smart card/token:

- User PIN – the standard PIN used by a user to access the card/token
- Admin PIN – the PIN that is necessary to unblock the card/token (for example after too many consecutive incorrect presentations of the User PIN)
- IdenTrust PIN – a PIN similar to the User PIN with some particular rules (minimum length of 6 characters). This PIN appears only on certain types of smart card/token.

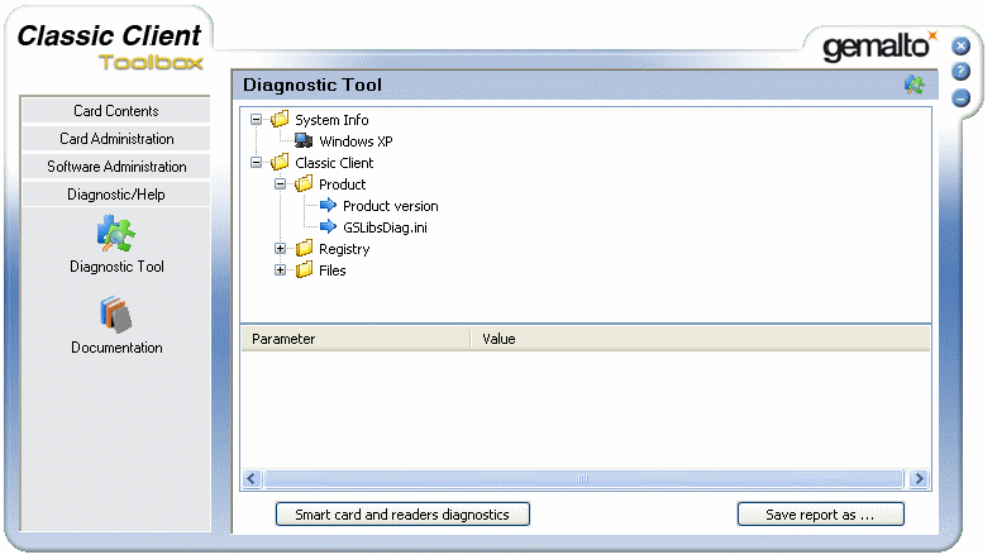
Diagnostic/Help Folder

The **Diagnostic/Help** folder contains the **Diagnostic** Tool which is used to troubleshoot any problems you may encounter when using Classic Client and the **Documentation** plug-in which contains all the relevant documentation.

Diagnostic Tool

The Diagnostic Tool is used to examine all components of the Classic Client installation to determine if there are problems using Classic Client. The Diagnostic Tool is then able to diagnose where potential problems may be.

Figure 22 - Diagnostic Tool Window



Expand the folders to reveal further items. Click an item in the top pane to display information about that component in the lower pane.

From the **Diagnostic Tool** window you can view the status of the program. The Diagnostic Tool provides the following:

- System Information
- PKCS#11 registry values and files
- Classic Client product information
- Classic Client registry values

- Status of the Classic Client installation files (executables, dynamic link libraries)

Note: For 64-bit OS, there are two registry folders “Registry” (for the 32-bit values) and “Registry 64” (for the 64-bit values).

The following table provides a key to the symbols found in the Diagnostic Tool.

Table 1 - Diagnostic Tool Icons

Icon	Description
	The PC icon shows details about operating system of the Classic Client installation.
	A green magnifying glass icon shows that the registry item is stored and functioning correctly.
	A red magnifying glass icon indicates that the registry item is absent. In this case, you should remove the current installation of Classic Client and re-install it.
	A blue magnifying glass icon shows that the registry item is optional.
	A file icon with a green tick shows that the file or dll is installed and functioning correctly.
	A white cross on a red background indicates that the file does not correspond to a known version. In this case, you should reinstall Classic Client.
	A file icon with a question mark tick indicates that the file could not be read or is an unexpected version.
	A blue arrow indicates that more information is available.

To generate a status report of the application click **Save report as**. From the **Save as** window save the .txt file to a suitable location.

Smart Card/Token and Reader Diagnostics

You can also view the smart card/token and smart card reader properties using the SmartDiag Tool.

The SmartDiag Tool verifies the availability of the following:

- Operating system services that allow smart card/token support
- Smart card readers
- Smart cards/tokens

The tool also reports any software or hardware problems and gives troubleshooting information. If the displayed information still does not solve the problem, you can

generate a diagnostic report. This report will be required if you ask Technical Support for help.

Note: SmartDiag tests only the smart card's/token's basic functionality. It does not test the suitability of your smart card/token for use with a specific application.

To use the Gemalto SmartDiag Tool

1 Open the SmartDiag Tool using one of the following ways:

- In the **Diagnostic Tool** window (see "Figure 22" on page 23) click **Smart card and readers diagnostics**.
- Navigate through **Start > Programs > Gemalto > SmartDiag > SmartDiag.exe**.

This opens the **Welcome** window as shown in "Figure 23".

Figure 23 - SmartDiag Welcome Window

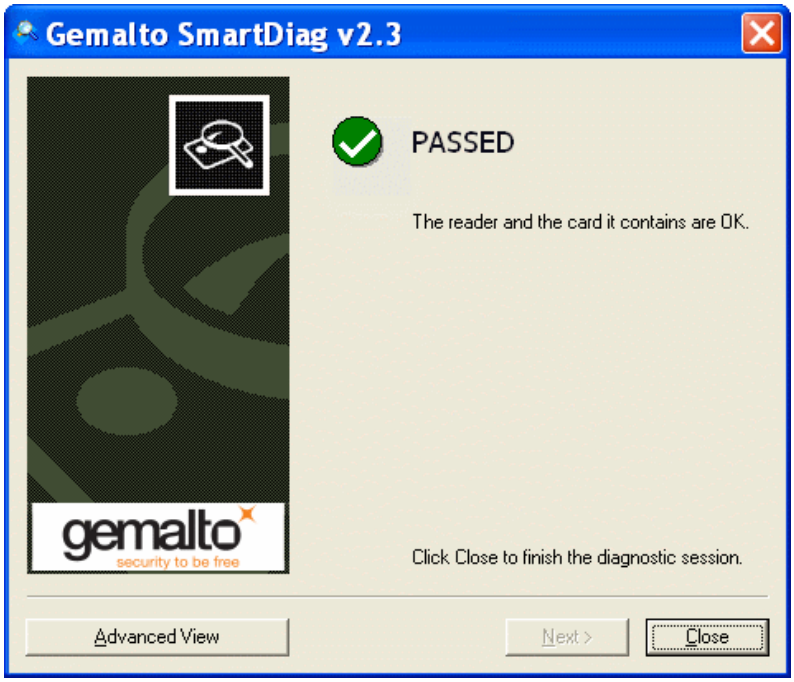
2 Click **Start** to begin a diagnostic session. The SmartDiag Tool begins a diagnostic session to examine possible problems with the installation of the smart card reader or the smart card/token used.

There are three possible outcomes:

- Passed
- Failed
- Warning

3 If all components are as they should be, the following dialog appears.

Figure 24 - SmartDiag Passed Window



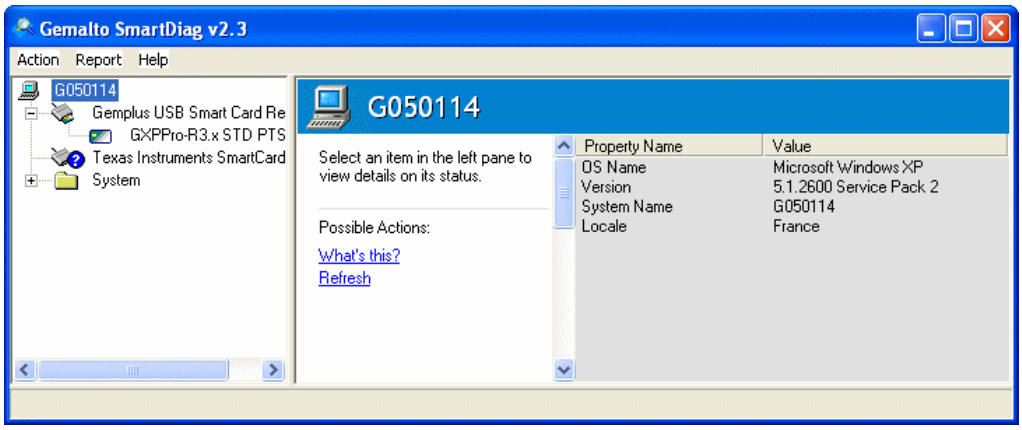
a) If the result is **Warning**, it is recommended that you click **Advanced View** to obtain all the details.

The **Advanced View** provides information on the smart card/token sub-system and the program's management facility.

The Advanced View's purpose is to give a real-time status and description of smart card/token related resources. This can be particularly useful to reveal obscure and low-level problems, or to identify the version of various software and hardware smart card/token components.

The window shown in "Figure 25" screen is displayed.

Figure 25 - SmartDiag Advanced Window



From the **Gemalto SmartDiag** window you can view the status and other information about:

- Smart card readers and smart cards/tokens
- Services (application compatibility, reader identification)

– System (Resource Manager, driver library, Smart Cards Database).

By expanding the folders and selecting the required node, the information for each is displayed in the right frame.

A blue question icon indicates that there is no smart card/token inserted in the smart card reader or there is an error reading the smart card/token.

To generate a status report of the information, from the **Report** menu choose **Generate**. From the **Save as** window save the .txt file to a chosen location.

Reports containing this information can be generated and saved as text files and may be valuable should you need to communicate with your Technical Support department. They can be saved as a **Report** in a text (.txt) file format.

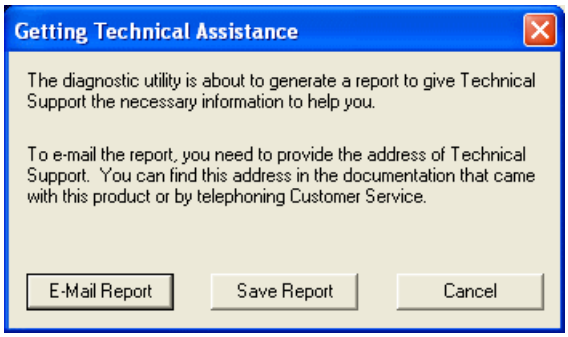
Note: For more information about using the SmartDiag Tool, navigate to the **Help** drop-down list to access the SmartDiag online help.

Click **Close** to quit the tool.

b) If the outcome of the diagnostic session is **Failed**, read the accompanying message carefully. It explains the most probable source of the problem and how to get your smart card and reader working. In addition, you can generate a diagnostic report by clicking on **Get Assistance**. This displays the window shown in “Figure 27”.

Figure 26 - SmartDiag Failed Window

Figure 27 - SmartDiag Getting Technical Assistance Window



Product Support

If you experience problems getting your smart card/token or reader to work, and the advice given by SmartDiag does not solve the problem, contact Gemalto Technical Support, using the information given in this document (refer to “Contact Our Hotline” on page ix). You may want to generate and send a diagnostic report that your Technical Support representative will need in order to help you.

Documentation

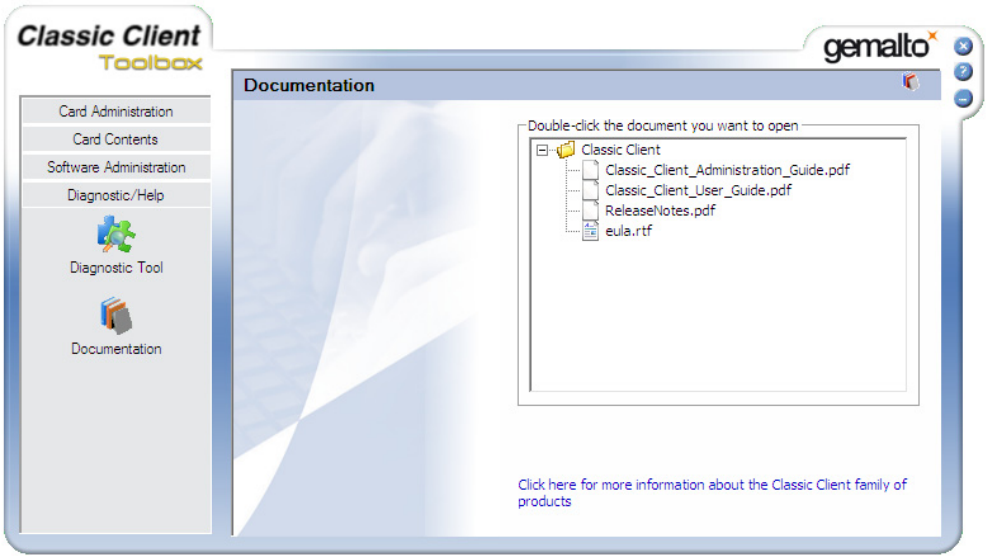
The **Documentation** plug-in contains all the documentation associated with the product. This is available only if the administrator chose to include it when creating the user setup.

To open the documentation:

1 Click **Documentation** to open the **Documentation** window.

2 Expand the **Classic Client** folder to display the available documents, as shown in the following figure.

Figure 28 - Documentation Window



3 Double–click the document that you want to open.

3

The Registration Tool

If the **Registration Tool** is installed, it automatically starts when you start Windows.

Note: When the Registration Tool is installed, each smart card reader connected to the computer is represented by a card reader icon in the system tray.

When a smart card/token is connected, the **Registration Tool** automatically reads the data on the card/token and attempts to register any certificates for CAPI applications that it finds on the card/token.

When you remove a card/token, the Registration Tool removes the certificates from the IE store.

Under Windows 2000, XP and Server 2003, there is an equivalent Microsoft application, that registers certificates. However, unlike the Registration Tool, it does not remove the certificates from the IE store, when you remove your card/token.

Under Windows Vista, 7, Server 2008 and Server 2008 R2, if the Registration Tool is present, Classic Client deactivates the equivalent Microsoft tool.

The tool's status is reflected by changes that appear in the system tray icon:

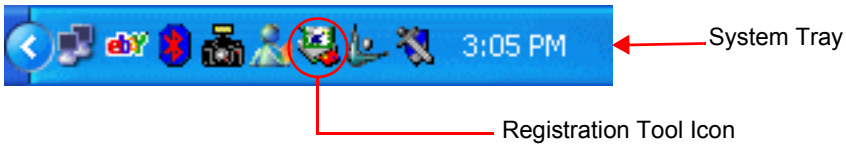


Table 2 - Registration Tool Status Icons

Icon	Definition
	Registration Tool icon indicating that no card/token is connected.
	Registration Tool icon with card inserted in the reader but indicating that no certificates are on the card/token.
	Registration Tool icon with card inserted and indicating that there are registered certificate(s).
	Registration Tool icon with green box over the card end indicates that the Tool is in the Pause mode.
	Registration Tool icon with a red X over the reader indicates that no card reader is detected.

You can display information about the reader and the card/token in it by hovering the mouse over the icon in the system tray as shown in “Figure 29”.

Figure 29 - Registration Tool Icon in the System Tray

Contextual Menu

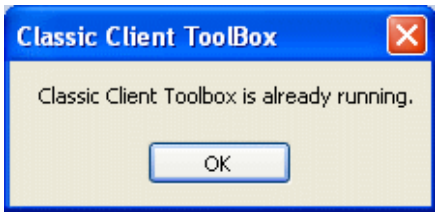
The tool has no interface, as it functions automatically. However, the user can interact with the tool by right clicking on the icon so that the tool displays a contextual menu from which to choose actions to take with the tool, as shown in “Figure 30”, and explained below.

Figure 30 - Registration Tool Right-Click Action Options

Launch Toolbox

Selecting Launch Toolbox will open the Classic Client Toolbox if this has been included in the user setup and is available. If it is already open, a dialog appears.

Figure 31 - Classic Client Toolbox Active



Start/Pause

Selecting **Start/Pause** allows the user to manually start and pause the Registration Tool without having to remove the card/token, which may be useful if other applications need exclusive access to the card/token. The Tool can be simply restarted by selecting this option again to restart it.

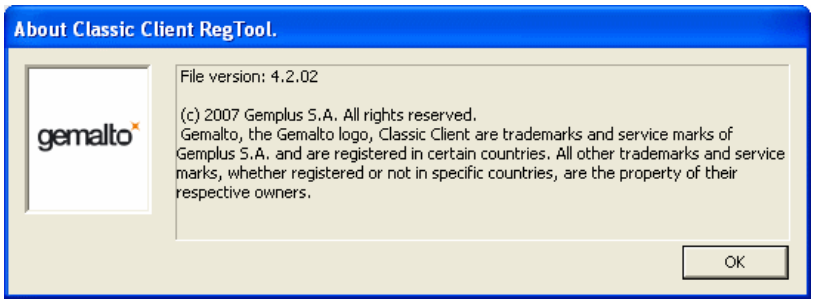
Stop

Selecting **Stop** allows the user to manually stop the Registration Tool without having to remove the card/token. Navigate through the **Start/Programs...** to restart the Registration Tool, see.“Restarting the Registration Tool” on page 31.

About

Selecting **About** displays information about the Registration Tool, as shown in “Figure 32”.

Figure 32 - “About” the Reg Tool



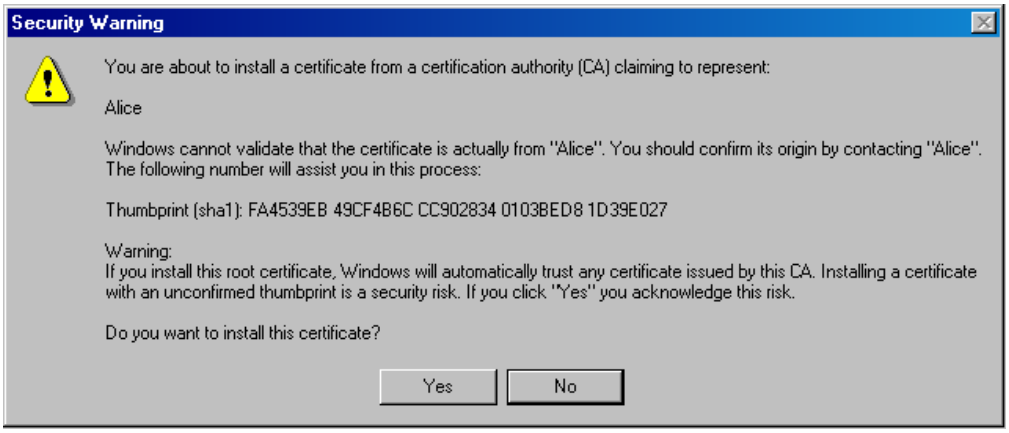
Restarting the Registration Tool

If you stopped the Registration Tool and want to restart it, you need to do this from the Start Menu, by choosing **Start > Programs (or All Programs) > Gemalto > Classic Client > Reg Tool**.

Registration Tool Management of Certificates

If the Registration Tool finds any CA certificates in the card/token, it will ask your for confirmation that you want to install (or register) them. This is a precaution because by installing a CA certificate, Windows will automatically trust any certificate issued by that CA. This confirmation appears as a security warning, as shown in “Figure 33” on page 31.

Figure 33 - Registration Tool: Install Certificate



Note: The above screen only appears for CA certificates

Click **Yes** to install the certificate to the IE Certificate store, or **No** to not install the certificate at this time.

If you close the card/token session (remove the card/token), and then reinsert the card/token, the tool again offers you the choice to install any unregistered certificates it finds.

Note: If you are working on a Citrix workstation, the Registration Tool is not installed on your workstation. You can register or install certificates without the Registration Tool by using the Certificates Tool (if your Citrix administrator has included the tool in the distributed end user setup).

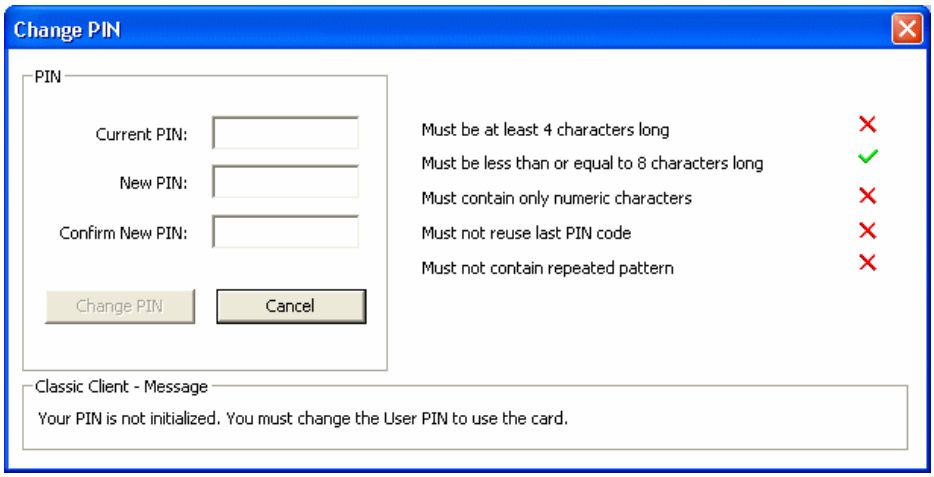
Forced Change PIN

The Registration Tool may detect that the User PIN in the card/token must be changed. There are two main reasons for this:

- The card/token is a brand new card/token whose PIN has not yet been initialized.
- The card/token has had its User PIN reset by the administrator, for example because it was blocked, and the administrator has set **Force User to Change PIN**.

In either case, when you connect the card/token a **Change PIN** dialog appears as shown in “Figure 34”.

Figure 34 - The Reg Tool Change PIN Screen



Enter the values, and when all the rules on the right show green ticks, click **Change PIN**.

For details about forced PIN changes when using a PIN Pad reader, see “Forced PIN Change with the PIN Pad Reader” on page 43.

4

User Tasks

This chapter discusses information related to specific tasks that you will most often be required to carry out when using the Classic Client software and where to find the information about them. These tasks are:

PIN Management

How to Change a User PIN or IdenTrust PIN

Use the PIN Management tool to change the user PIN.

To perform this operation, your Classic Client setup must have been granted the “Change User PIN allowed” access rights by your administrator.

To change a User PIN or IdenTrust PIN

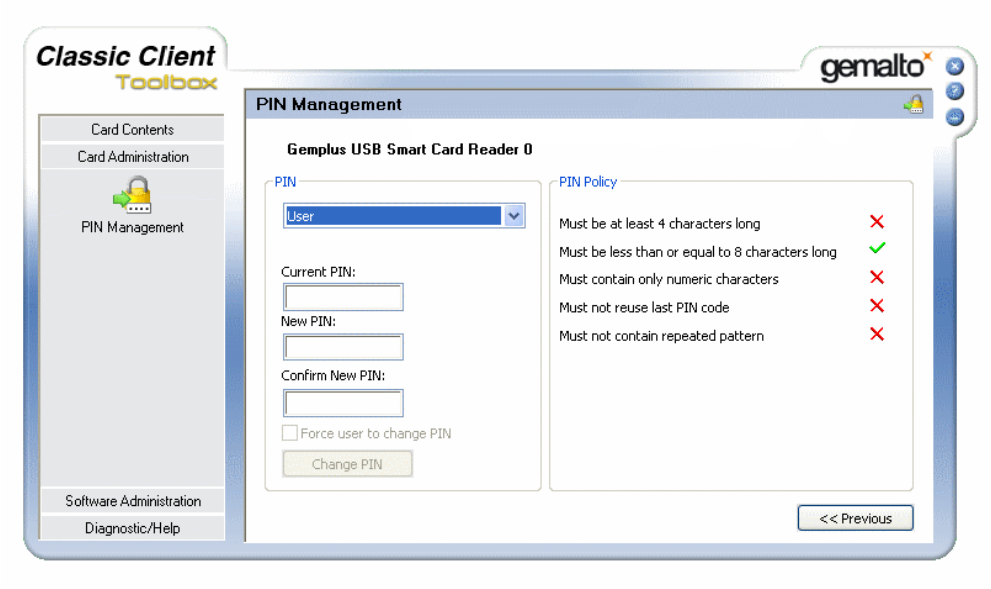
1 Connect the smart card/token whose User PIN you want to change.

2 Click on the **PIN Management** tool icon in the **Card Administration** folder; the **PIN Management** tool interface is displayed in the right hand area of the GUI. If you don't see the tool, you don't have the rights to change the PIN.

Note: The Classic Client padlock icon is either open or locked to indicate if you are logged in or not logged in. You do not have to log in, in order to change a PIN.

3 From the PIN Management Tool, choose the **Change PIN** option (see "Figure 21 - PIN Management Tool Window" on page 22) and click **Next**. The window shown in "Figure 35" appears:

Figure 35 - Change PIN Window



4 In the **PIN** section, select the type **User** or **IdenTrust**. The options available depend on the PINs that exist in the card/token and the rights given to by the Administrator in your User Setup.

PIN Policy in the right pane displays your company's policy for the type of PIN chosen. Ticks or crosses next each rule to tell you if your **New PIN** value respects the policy rules.

5 Enter the current PIN value in **Current PIN**, and the new value in **New PIN**.

6 If all the rules in **PIN Policy** display green ticks, reenter the new value in **Confirm New PIN**, otherwise choose a different value for **New PIN** until **PIN Policy** displays only green ticks.

7 Click **Change PIN**. A pop-up window confirms a successful PIN change.

If the PIN change is unsuccessful an error message is displayed with details of why the operation was unsuccessful.

How to Check The PIN Ratification Counter

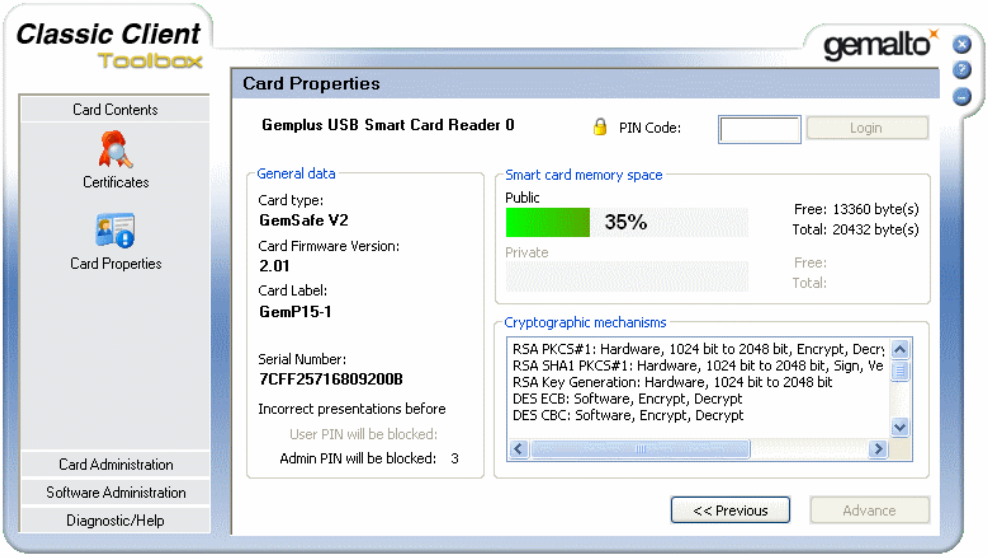
Smart cards/tokens are security protected against brute force PIN attacks by the ratification counter. The counter decreases by one each time you enter the wrong PIN code. When you enter the correct PIN, the ratification counter resets to its initial (highest) value. However, if the ratification counter reaches zero, it becomes blocked.

Depending on the technology of the card/token and its on-board software features, it may be possible to display the value of the PIN ratification counter value.

To check the PIN ratification counter (for cards/tokens that allow this feature)

1 In the **Card Contents** folder, click **Card Properties**, select the reader and click **Next**.

Figure 36 - Card Properties



2 The detail of the PIN ratification counter is in the lower left of the right pane. If you do not see any numerical values for the counter, then the card/token does not support this feature.

How to Unblock a User PIN

If you know the Admin PIN for your card/token, and your User Setup has been granted the necessary access rights by your administrator, you can unblock your User PIN by following the procedure “To unblock a PIN”. In most cases, you will not know the Admin PIN – it depends on your company’s security policy.

If you do not know the Admin PIN, you may be able to unblock the User PIN remotely. This depends on the rights granted to you in your User Setup by your Administrator. For details on how to unblock your card/token remotely, see “How to Remotely Unblock a Connected Smart Card/Token” on page 36.

To unblock a PIN

1 Connect the blocked smart card/token to the PC.

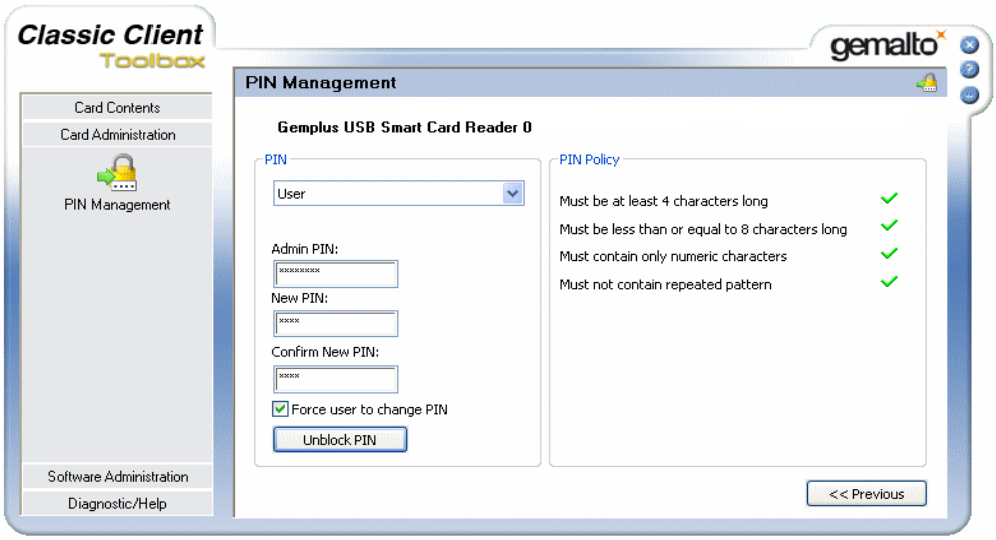
2 Click on the **PIN Management** tool icon in the **Card Administration** folder; the **PIN Management** tool interface is displayed in the right hand area of the GUI as shown in “Figure 21 - PIN Management Tool Window” on page 22.

3 Check **Unblock PIN** and if the list next to it is visible, choose **Local**.

4 Click **Next**; The window shown in “Figure 37” appears:

Note: The **Unblock PIN** option is available even if the card/token is not blocked. However, it is only available if you were given the right to use it in the user setup.

Figure 37 - PIN Management Tool: Unblock PIN



5 In the **PIN** section, select the PIN you need to unblock. Depending on your rights and the connected smart card/token, you can choose from User, Admin and IdenTrust.

6 Enter the **Admin PIN**, the **New PIN**, and the **Confirm New PIN** in the areas provided. Modify the **New PIN** value if the rules in **PIN Policy** display any red crosses.

7 If required check **Force user to change PIN**. This means that the user must change his or her PIN the first time he or she tries to access his smart card/token.

Note: Do not use the **Force user to change PIN** option if your security policy does not grant the user the right to change his or her PIN.

8 Click **Unblock PIN**.

A pop up dialog will inform you if the PIN has been successfully unblocked.

How to Remotely Unblock a Connected Smart Card/Token

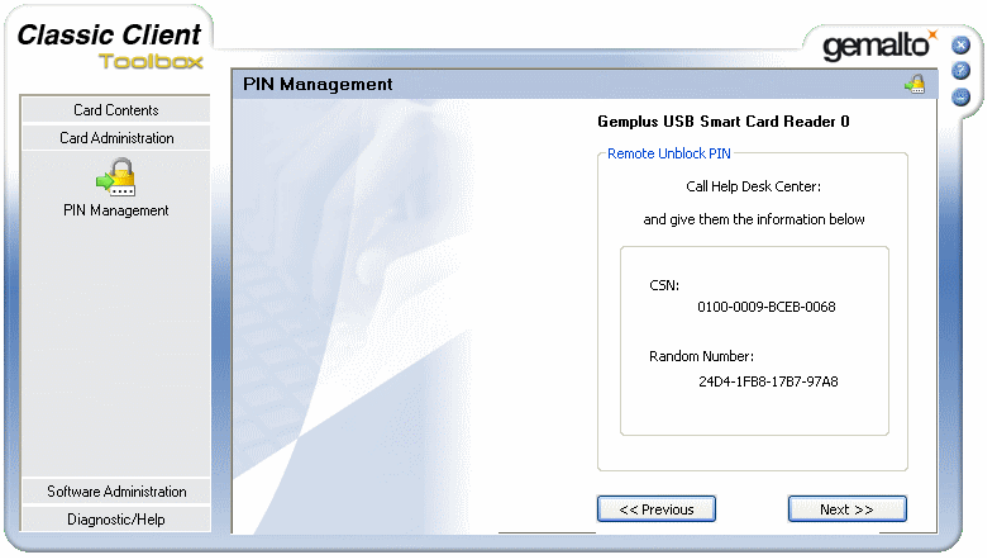
To unblock a smart card/token remotely

Note: You can do this only if the administrator has set “User can remotely unblock connected card” in your user setup.

1 Connect the blocked smart card/token, click on the **PIN Management** tool icon in the **Card Administration** folder,

2 Select **Unblock PIN** and if the list next to it is visible, choose **Remote**. This displays the window shown in “Figure 38”.

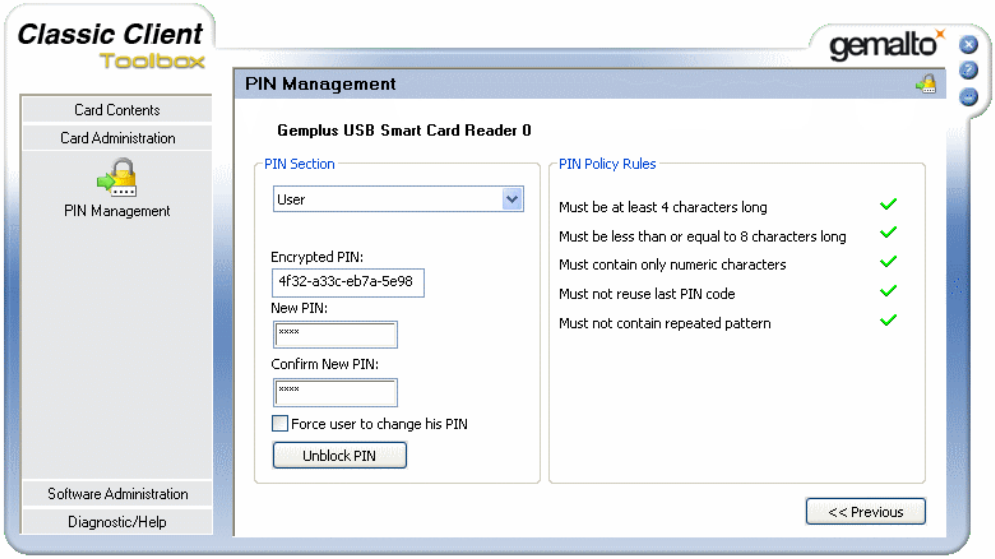
Figure 38 - PIN Management-Remote Unblock PIN



3 Telephone the help desk and tell them the card serial number (CSN) and the random number. With this information, the help desk will generate an encrypted unblock PIN and tell you its value.

4 Click **Next** to display the window shown in “Figure 39”.

Figure 39 - PIN Management-Remote Unblock PIN (2)



5 In **Encrypted PIN**, enter the value given to you by the help desk. Enter your new PIN value in **New PIN** and again in **Confirm New PIN**.

6 Leave **Force user to change PIN** unchecked.

7 Make sure that all the rules in PIN Policy show green ticks. If they do not, re–enter the values until they do.

8 Click **Unblock PIN**. A pop up dialog confirms if the card/token has been successfully unblocked.

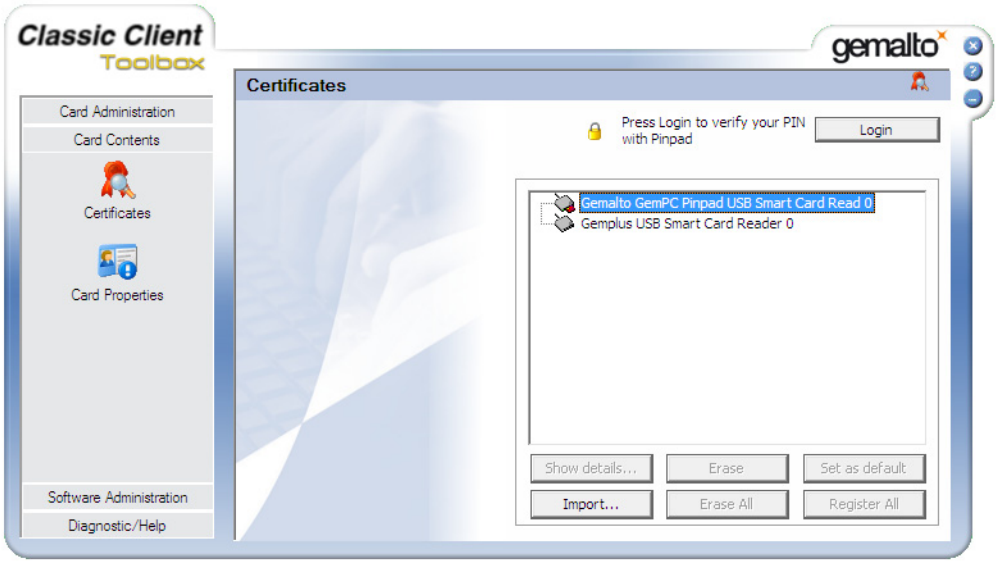
How to Use a PIN Pad Reader with Classic Client

How to Log in with a PIN Using a PIN Pad and the Toolbox

1 Insert the smart card in the PIN Pad reader.

2 Open the **Classic Client Toolbox** and in **Card Contents**, click **Certificates** to open the **Certificates Tool** as shown in “Figure 40”.

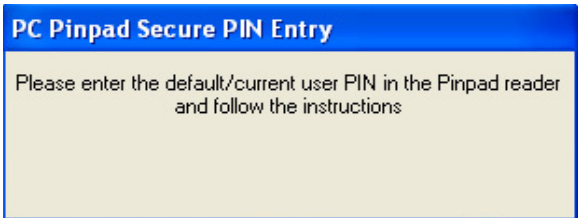
Figure 40 - Logging in Using a PIN Pad



3 Click the **Login** button.

The following dialog box is displayed:

Figure 41 - Secure PIN Entry Dialog Box

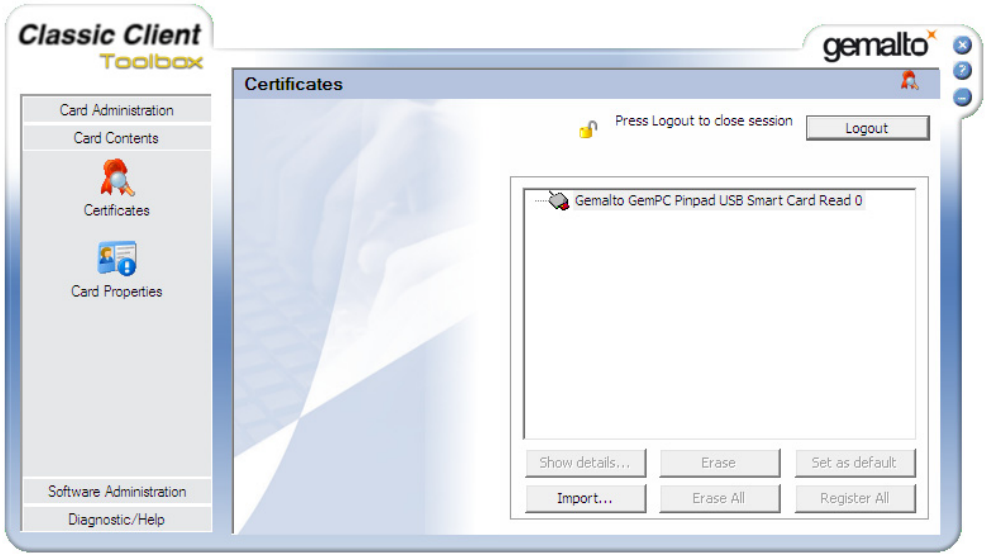


The PIN Pad prompts you to enter the User PIN.

4 Enter the PIN in the PIN Pad (remember to press the confirmation button on the pad, for example, **Enter**, **Valid**, **OK**).

5 The PIN Pad displays an OK message and the Certificate Tool changes to show that you are logged in:

Figure 42 - Logged in Using a PIN Pad



How to Change a User PIN or IdenTrust PIN with a PIN Pad and the Toolbox

To perform this operation, your Classic Client setup must have been granted the "Change User PIN allowed" access rights by your administrator.

To change a User PIN or IdenTrust PIN

1 Insert the smart card/token whose User PIN you want to change into the PIN Pad reader.

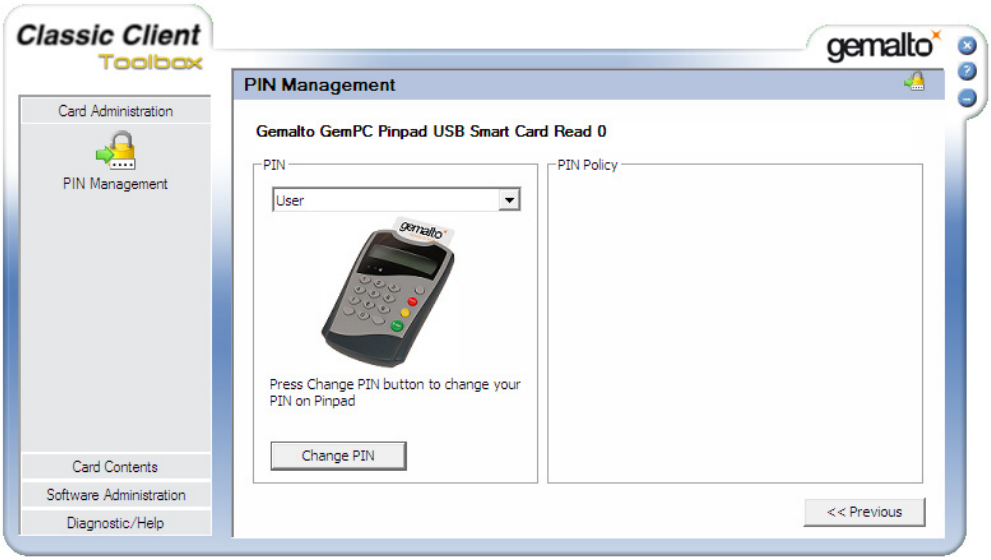
2 Click on the **PIN Management** tool icon in the **Card Administration** folder; the **PIN Management** tool interface is displayed in the right hand area of the GUI. If you don't see the tool, you don't have the rights to change the PIN.

Note: The Classic Client padlock icon is either open or locked to indicate if you are logged in or not logged in. . You do not have to be logged in at this point, in order to change a PIN.

---

3 From the PIN Management Tool, choose the **Change PIN** option (see "Figure 21 - PIN Management Tool Window" on page 22) and click **Next**. The window shown in "Figure 43" appears:

Figure 43 - PIN Management with PIN Pad Reader Window



4 In the **PIN** section, select the type **User** or **IdenTrust**. The options available depend on the PINs that exist in the card/token and the rights given to by the Administrator in your User Setup.

PIN Policy in the right pane provides a reminder of your company's policy for the type of PIN chosen.

5 Click **Change PIN**.

Note: If you have already logged in with the PIN that you want to change, the next step (6) is missed out.

---

6 The window in "Figure 44" appears and the PIN Pad display asks you to enter the user PIN.

Figure 44 - PC Pinpad Secure PIN Entry Window

Enter the current User PIN in the PIN Pad, then press the confirmation button.

7 When the window shown in "Figure 45" appears, follow the instructions displayed on the PIN Pad as follows:

Figure 45 - PC Pinpad Secure PIN Change Window

8 When prompted by the PIN Pad, enter the current User PIN.

9 Enter the new User PIN value.

10 Enter the new User PIN value again. If successful, the window in “Figure 44” on page 40 reappears to prompt you to relog in to the toolbox.

11 Enter the new current User PIN.

12 When the “PIN changed” message appears, click **OK**.

How to Unblock a User PIN or IdenTrust PIN with a PIN Pad and the Toolbox

To perform this operation, your Classic Client setup must have been granted the “User can unblock card” access rights by your administrator.

To unblock a User PIN or IdenTrust PIN

1 Insert the smart card/token whose User or IdenTrust PIN you want to unblock into the PIN Pad reader.

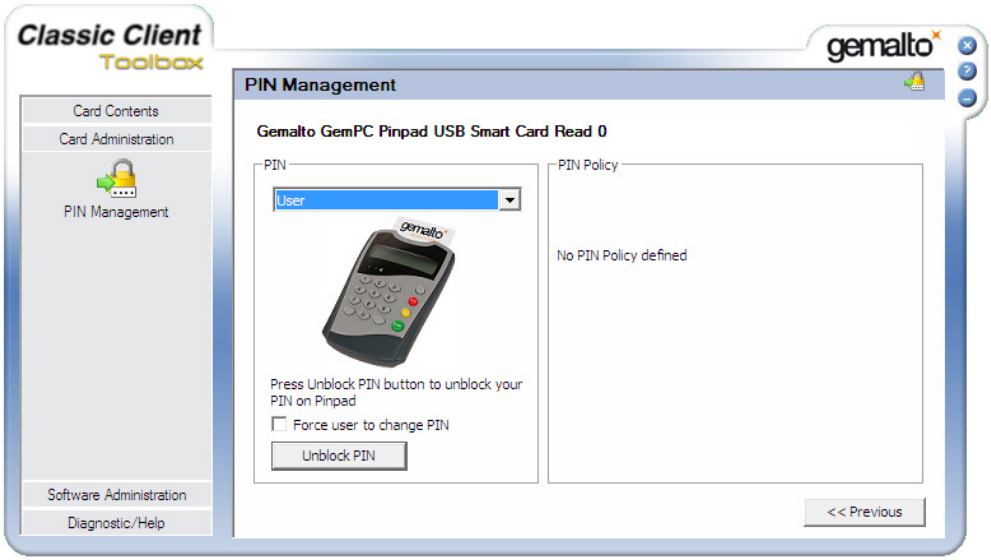
2 Click on the **PIN Management** tool icon in the **Card Administration** folder; the **PIN Management** tool interface is displayed in the right hand area of the GUI. If you don’t see the tool, you don’t have the rights to update the PIN.

Note: The Classic Client padlock icon is either open or locked to indicate if you are logged in or not logged in. . You do not have to log in, in order to unblock a PIN.

---

3 From the PIN Management Tool, choose the **Unblock PIN** option (see “Figure 21 - PIN Management Tool Window” on page 22) and click **Next**. The window shown in “Figure 43” appears:

Figure 46 - PIN Management with PIN Pad Reader Window

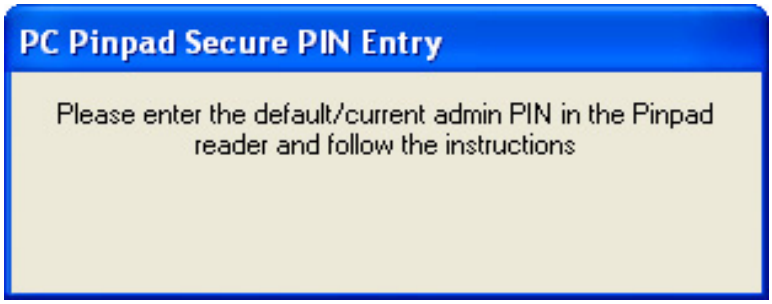


4 In the **PIN** section, select the type **User** or **IdenTrust**.

PIN Policy in the right pane provides a reminder of your company's policy for the type of PIN chosen.

5 Click **Unblock PIN**. The window in "Figure 47" appears and the PIN Pad display asks you to enter the Admin PIN (sometimes known as the SO PIN).

Figure 47 - PC Pinpad Secure PIN Entry Window



6 Enter the Admin PIN in the PIN Pad, then press the confirmation button.

When the window shown in "Figure 48" appears, follow the instructions displayed on the PIN Pad as follows:

Figure 48 - PC Pinpad Secure PIN Unblock Window

7 When the PIN Pad prompts you, enter the Admin PIN.

8 Enter the new User PIN value.

9 Enter the new User PIN value again as confirmation. If successful, the window in "Figure 47" on page 42 reappears to prompt you to relog in to the toolbox.

10 Enter the Admin PIN. This last time is to relog in to the toolbox.

11 When the "PIN unblocked" message appears, click **OK**.

PIN Presentation

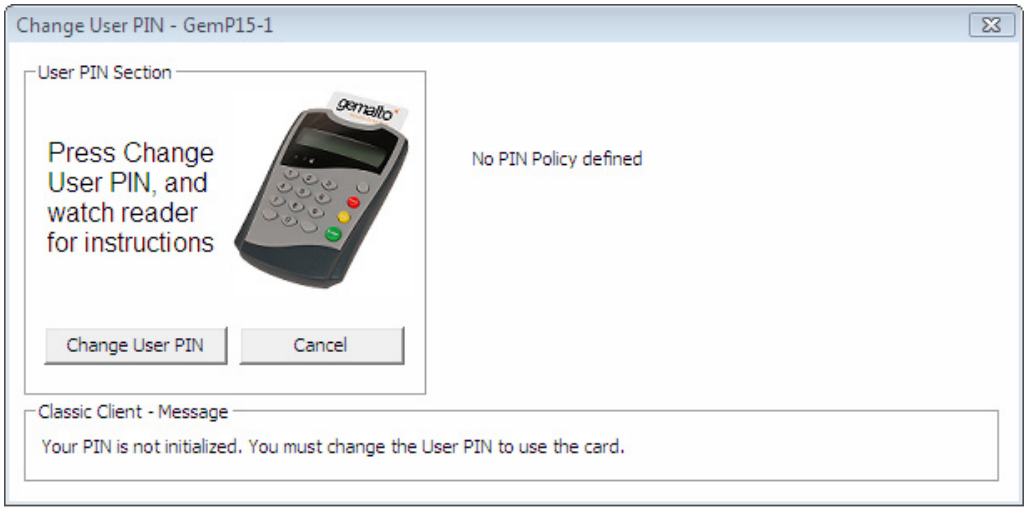
Caution: The PIN Pad reader is managed by the application that calls Classic Client. Consequently the PIN Pad's behavior when interacting with Classic Client will vary according to the application.

Under some circumstances, the PIN Pad Reader requires several presentations of the PIN by the User to gain access to certain tasks. When enrolling a user on the smart card, for example, 3 presentations of the PIN is required.

Forced PIN Change with the PIN Pad Reader

If the administrator set the option "**Force user to change PIN**", or if the User PIN is not initialized, the Registration Tool displays the following message when you insert the smart card in a PIN Pad reader.

Figure 49 - Forced PIN Change with PIN Pad Reader Window



Click **Change User PIN** and follow the instructions in "How to Change a User PIN or IdenTrust PIN with a PIN Pad and the Toolbox" on page 39. When the final message displays to tell you the change is successful, click **OK**.

How to Use Windows Secure Logon

Classic Client makes it easy and convenient to use the support for smart card/token security that is built into the following operating systems and applications:

- Windows 2000
- Windows XP and Windows Server 2003
- Windows Vista and Windows Server 2008.
- Windows 7 and Windows Server 2008 R2

All you need is a smart card reader and a card/token containing the appropriate certificate.

This section describes how to do the following with Classic Client for these OS and applications:

- Log on and off your workstation.
- Lock your workstation.

You must have a certificate on your smart card/token to use the features described in this chapter as well as be a member of the network domain and have a certificate registered for you in this domain.

For information on getting certificates, refer to "Managing Certificates" on page 64

Note: The following procedures and associated screen shots may vary according to the version of Windows being used.

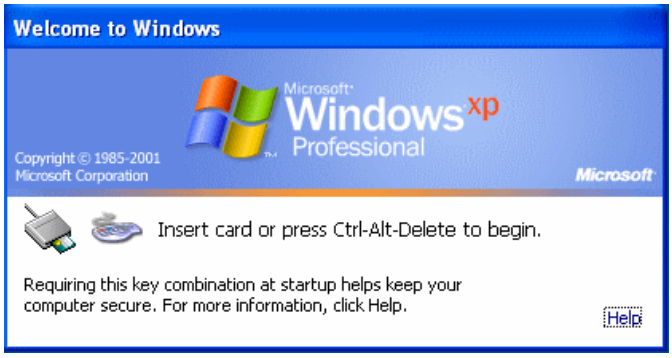
How to Log on with a Smart Card/Token

Logging on to Windows with a smart card/token is fast and easy.

To log on to Windows 2000, Windows XP and Windows Server 2003 with a smart card/token

1 Start Windows. A **Welcome to Windows** message box similar to the one in "Figure 50" opens.

Figure 50 - Welcome to Windows Screen



2 Connect your smart card/token to open a **Log On to Windows** dialog box like the one shown in "Figure 51".

Figure 51 - Windows Log On Dialog Box

3 Enter your **PIN** then click **OK.**

To log on to Windows Vista, 7, Server 2008 or Server 2008 R2 with a smart card/ token

Note: This function is not supported for GPK 16000 cards.

1 Start Windows. The window shown in “Figure 52” opens.

Figure 52 - First Windows Vista Screen

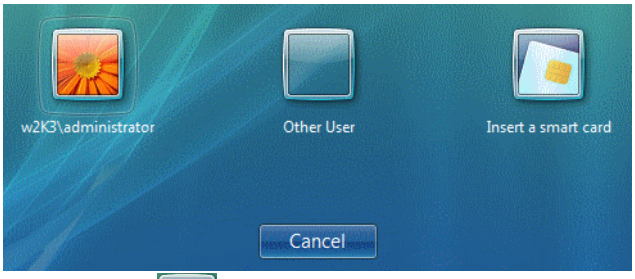
2 Press <CTRL> <ALT> <DEL>. The window that displays next can be one of the following different cases:

- If an administrator or user icon displays, as shown in “Figure 53”, follow the steps that follow “Figure 53”.
- If all the user icons and smart card icon  display, as shown in “Figure 54”, follow the steps that follow “Figure 54”.
- If the smart card icon displays on its own with the text “Insert a smart card” as shown in “Figure 55”, follow the steps that follow “Figure 55”.
- If the smart card icon displays on its own with the name of the card/token user underneath as shown in “Figure 56”, follow the steps that follow “Figure 56”.

Figure 53 - Vista Logon Window 2

3 Click **Switch User** to display the window shown in “Figure 54”.

Figure 54 - Window Vista – Select User

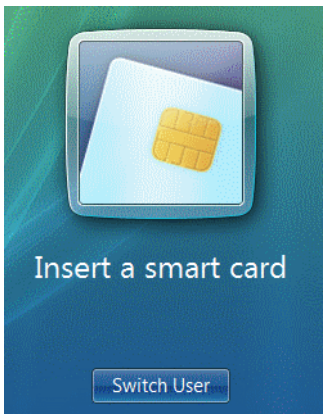


4 Click the smart card icon  .

If the text underneath the smart card icon says **Insert a smart card**, the window in “Figure 55” appears. Follow the steps that follow “Figure 55”.

If the text underneath the smart card icon has the name of the card/token user, the window in “Figure 56” appears. Follow the steps that follow “Figure 56”.

Figure 55 - Windows Vista – Insert a Smart Card Window



5 Connect your smart card/token. If the card/token is valid, the window changes to display the name of the card/token user as shown in “Figure 56”.

Figure 56 - Windows Vista – Smart Card User Displayed

6 Enter the PIN and click  . If your PIN is correct, the Welcome message appears during logon and disappears when the logon is successful.

How to Lock and Unlock your Computer Using a Smart Card/Token

Windows 2000, Windows XP and Windows Server 2003

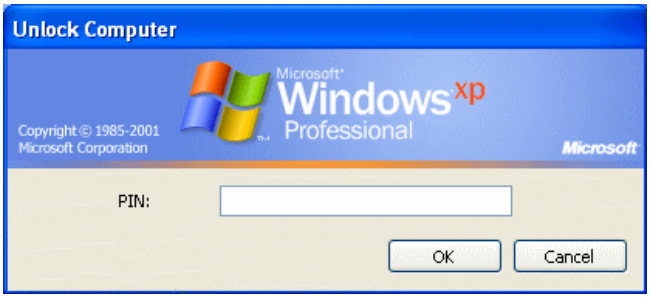
If your smart card removal policy is set to lock your PC when you remove your card/ token, then removing the card/token locks your PC and displays an information box similar to the one shown in “Figure 57”.

Figure 57 - Windows Computer Locked Screen

To unlock a computer in one of the above versions of Windows:

1 Re-insert your smart card/token. The **Unlock Computer** dialog box opens.

Figure 58 - Windows Unlock Computer Dialog Box



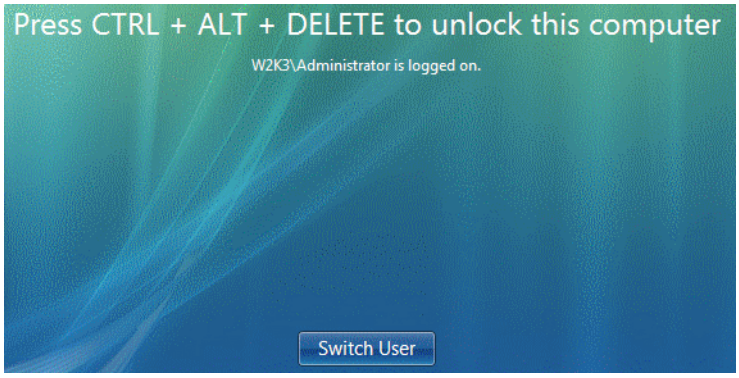
2 Enter your User **PIN** and click **OK** to log back on.

Windows Vista, 7, Server 2008 and Server 2008 R2

If your smart card removal policy is set to lock your PC when you remove your card/ token, then removing the card/token locks your PC and displays an information box similar to the one shown in “Figure 59”.

Note: This function is not supported for GPK 16000 cards.

Figure 59 - Windows Computer Locked Screen



To unlock a computer in Windows Vista, 7, Server 2008 or Server 2008 R2:

1. Press <CTRL> <ALT> <DEL>.
2. Re–insert the smart card/token. In Windows Vista, if the card/token is already connected, it is read automatically and does not need to be re–inserted.
3. Enter your User PIN and click 

How to Use E-mail Securely

The following sections explain how to send secure e-mail using Classic Client.

About Secure E-mail

With Classic Client, you can improve e-mail security by using the digital certificate on your smart card/token to:

- Sign your e-mail so that the recipient can verify that the message is really from you and has not been altered.
- Encrypt, or “scramble” a message so that only the intended recipient can read it. This eliminates concerns about intercepted messages and e-mail monitoring.
- Sign or encrypt your message using one e-mail program, while your intended recipient can read it with any other S/MIME-enabled e-mail program.
- Receive signed and encrypted e-mail messages.

Setting up Secure E-mail

You must do the following before you can send secure e-mail:

- **Choose a certificate**

  Choose the digital certificate you will use with your e-mail account.
- **Configure security settings**

  Set the security settings for digitally signing and/or encrypting the contents and attachments of outgoing messages.

The following sections describe how to configure these settings and send secure e-mail using several common e-mail programs. The dialog boxes shown may differ slightly from your own software, depending on what version you are using.

For more information on managing certificates, refer to “Managing Certificates” on page 55.

General Guidelines for Sending Secure E-mail

You can use your Classic Client smart card/token to send and receive secure e-mail.

To use e-mail with your Classic Client smart card/token:

1. Connect your smart card/token.
2. Start your e-mail application (**Outlook 2003, Mozilla Thunderbird** etc.).
3. Send a signed e-mail to yourself.
4. When you receive the signed e-mail, add the user (yourself) to your **Contacts** folder (**Outlook 2003**).

Note: You can skip this step if you are using Mozilla Thunderbird.

5. Reply to yourself with an encrypted e-mail.

Once you have completed these steps to test that signing and encryption are working correctly you can send signed and/or encrypted e-mails to other people.

The complex cryptographic calculations used to encrypt the message are conveniently transparent to both sender and receiver.

Working with Outlook 2003

The following sections explain how to set up and exchange secure e-mail with Microsoft Outlook 2003.

Setting up Secure E-mail

Note: In Outlook 2003, choosing the certificate is part of the security settings.

*To set up secure e-mail with **Outlook 2003***

1 Make sure your smart card/token is connected and the certificate is registered using the Card Details Tool.

In **Outlook 2003**, from the **Tools** menu choose **Options** to open the **Options** dialog box.

2 In the **Options** dialog box, click the **Security** tab.

Figure 60 - Outlook Options Dialog Box

3 Click **Settings** to display the **Change Security Settings** dialog box.

Figure 61 - Change Security Settings Dialog Box

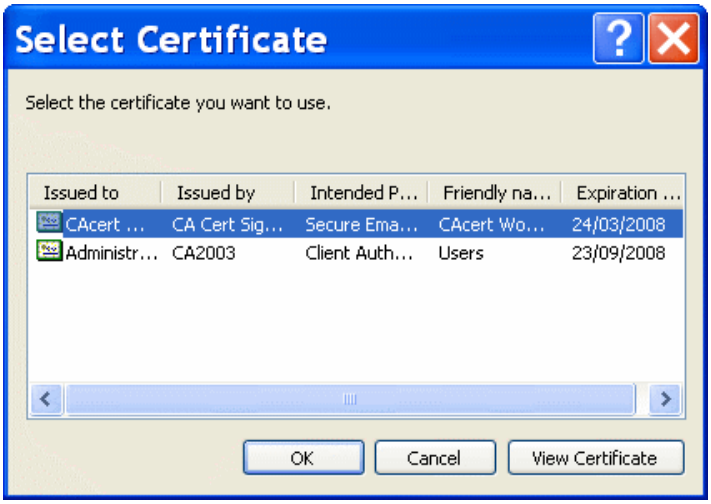
4 Enter or choose the appropriate information in the entry fields.

In **Security Settings Name**, enter a name for your settings

Make sure that **S/MIME** is selected in the **Cryptography Format** box.

5 Click **Choose** beside the **Signing Certificate** box to open the **Select Certificate** dialog box. This displays the certificates that are on your card/token.

Figure 62 - Select Certificate Dialog Box



6 Select a certificate for signing e-mail messages.

Make sure that the address on the certificate matches your e-mail address. You can see this information by clicking **View Certificate**.

7 Click **OK** to return to the **Change Security Settings** dialog box.

The certificate name is displayed next to **Signing Certificate** and **Encryption Certificate**. The **Hash Algorithm** and **Encryption Algorithm** options become active as shown in “Figure 63”.

Figure 63 - Change Security Settings with Signing Certificate

8 In the **Hash Algorithm** option list, choose **SHA** for signing data.

9 Click **Choose** beside the **Encryption Certificate** box to open the **Select Certificate** dialog box again.

10 In **Encryption Certificate**, either leave the certificate as it is (if you want to use the same certificate for encryption and signatures) or click **Choose** and select a different certificate for encrypting data. Make sure the address on the certificate matches your e-mail address.

11 In the **Encryption Algorithm** option list, choose **3DES** for encrypting data.

12 Make sure that **Send these certificates with signed messages** is selected.

Click **OK** to close **Change Security Settings** and return to the **Options** dialog box.

13 In the **Options** dialog box, shown in “Figure 60” on page 50, select the secure e-mail options you want:

- Encrypt contents and attachments for outgoing messages

  Select this to encrypt the contents and attachments of all outgoing messages.

- Add digital signature to outgoing messages

  Select this to add your digital signature to all outgoing messages.

- Send clear text signed messages

  Select this so that users whose e-mail applications do not support S/MIME signatures can read your signed messages without verifying the digital signature.

14 Click **OK** to close the **Options** dialog box.

The settings you have made will be used with all e-mail you send, by default.

Sending Secure E-mail

To test secure e-mail, you must send a signed message to yourself so that Outlook can store your public key. You then use this public key to encrypt another message, which you also send to yourself. You will be able to decrypt this message with the private key stored on your smart card/token.

To send secure e-mail with Outlook 2003:

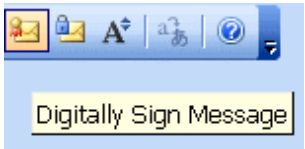
1 Make sure your smart card/token is connected.

2 Click **New** in **Outlook 2003** to open the message editor.

3 Write a short message ***addressed to yourself***.

4 Click the signature icon in the toolbar to sign the message as shown in **"Figure 64"**.

Figure 64 - Outlook 2003 – Signature Icon



5 In the message editor, click **Send**.

6 Enter your PIN when prompted. The message is placed in your **Outbox** or "**Sent**" folder.

Note: You only need to enter your PIN once during an Outlook session.

7 Press **F5** to check for new mail.

8 You should receive a message telling you that you have received signed e-mail.

9 Scroll through the message to find a button allowing you to read the e-mail.

10 You'll notice that the sender is added to your contact list. This means that you have the sender's public key and that you now can send encrypted e-mail to that person. Keep in mind that in this case the sender is you.

11 In the contact list, double–click your user name to create a new message addressed back to you.

12 This time click the **Encryption** icon, to encrypt your message. as shown in "Figure 65".

Figure 65 - Outlook 2003 – Encryption Icon

13 Type something in the subject line as well as in the body of the message.

14 Click **Send**.

15 In Outlook 2003, select the encrypted e-mail in your **Outbox**.

16 To read the message, scroll down and click **Continue**.

You are now able to read your encrypted e-mail.

That's it! You are ready to start using secure e-mail with **Outlook 2003**.

Working with Mozilla Thunderbird.

The following sections explain how to set up and send secure e-mail with Mozilla's Thunderbird e-mail program and e-mail client. There are three stages:

1 Load the Security Module, described on page 54.

2 Select the certificates that will be used to sign and encrypt e-mails, described on page 54

3 Send an e-mail, described on page 57.

Loading the Security Module in Mozilla Thunderbird

You only need to load the module once and the method to do this is almost identical to Firefox.

To load the security module with Mozilla Thunderbird

1 Make sure your smart card/token is connected.

2 Start **Mozilla Thunderbird**.

3 Enter your password if you are prompted for it and click on **OK**.

4 For the rest of the procedure, follow the instructions in "To manually install a security module for Firefox:" on page 6, except that in step 2 of those instructions, choose the **Certificates** tab instead of the **Encryption** tab.

This new module will be used with all e-mail you send with Thunderbird.

Setting up Secure E-mail

You only need to do this the first time you use your card/token to sign or encrypt an e-mail.

Note: Although selecting the certificates is mandatory, this does not mean that you must sign and encrypt e-mails.

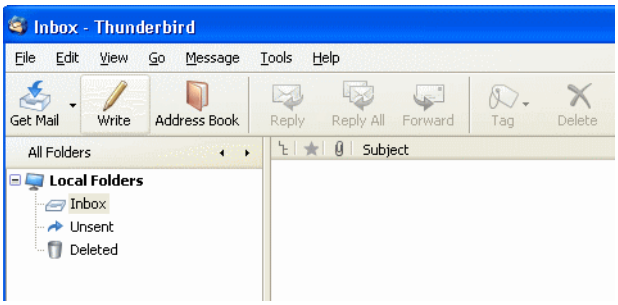
1 Make sure your smart card/token is connected.

2 Start **Mozilla Thunderbird**.

3 Enter your password if you are prompted for it.

4 In **Thunderbird**, click the **Write** icon as shown in "Figure 66".

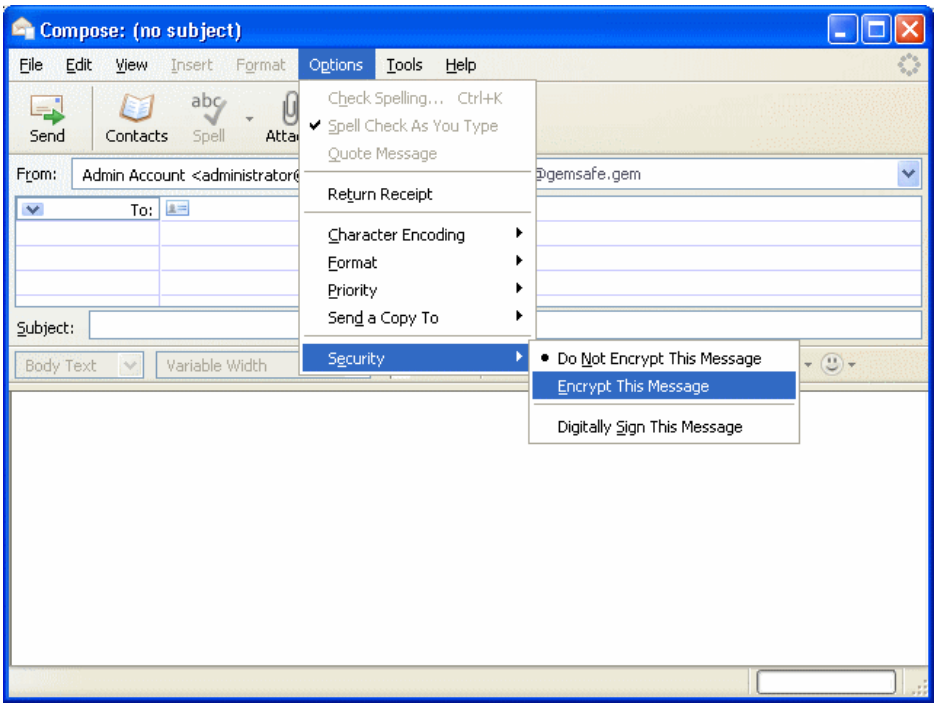
Figure 66 - Thunderbird Write Icon



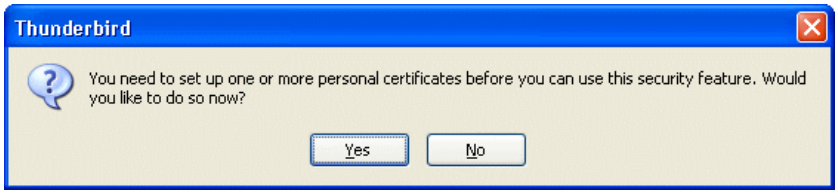
This opens the **Compose** window.

5 In the **Compose** window's **Options** menu, choose **Security** > **Encrypt this Message** as shown in "Figure 67".

Figure 67 - Thunderbird – Encrypt This Message

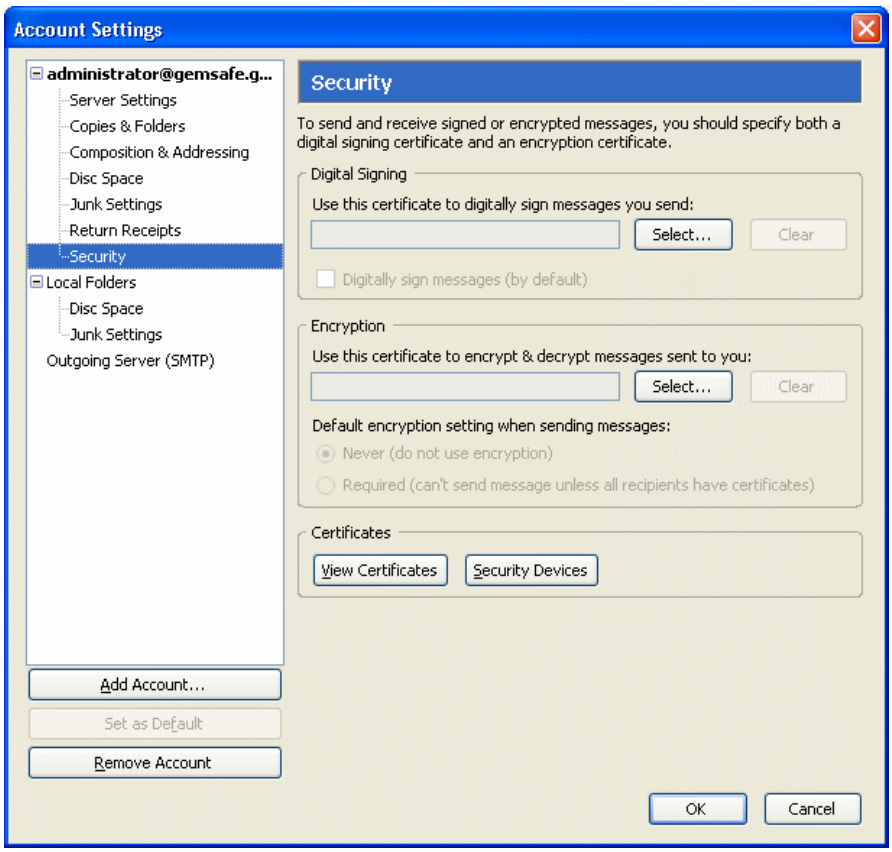


As the certificates in the card/token are not yet set up, the following message appears:



6 Click **Yes**. This opens the Account Settings window for your e-mail account as shown in "Figure 68".

Figure 68 - Thunderbird – Account Settings

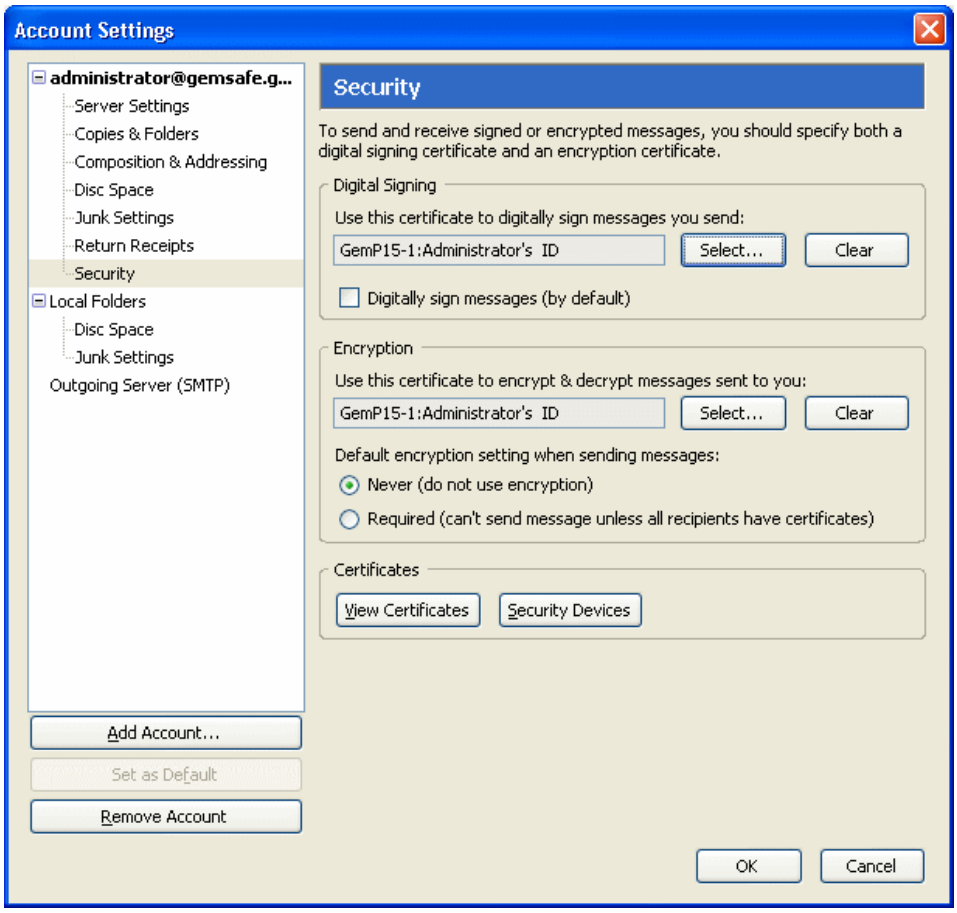


7 In **Digital Signing**, click **Select** and choose the certificate you want to use from the list that appears. The following message appears:

Figure 69 - Thunderbird – "Use Same Certificate" Message

8 If you want to use the same certificate to encrypt and decrypt messages, click **OK**. This selects the certificate for you in the Encryption panel as shown in "Figure 70" on page 57. Otherwise click **Cancel**.

Figure 70 - Thunderbird – Account Settings (2)



9 If you want all of your e-mails to be digitally signed by default, check the box **Digitally sign messages (by default)**.

10 In **Encryption**, if you chose not to use the same certificate as the one used for digital signing, click **Select** and choose the certificate from the list that appears. A message similar to the one in “Figure 69” on page 56 appears, but this time asking if you want to use the Encryption certificate for digital signing. This is just in case you select your encryption certificate before you select your digital signature certificate.

11 In **Default encryption setting when sending messages**, choose one of the option buttons **Never** or **Required**.

12 Click **OK** to close the **Account Settings** window.

Note: If you want to modify the account settings at any point, open the **Account Settings** window from the **Tools** menu by choosing **Account Settings**. This can be done either from the **Compose** window or directly in Thunderbird.

Sending Digitally Signed E-mail with Mozilla Thunderbird

When you send a signed e-mail, you sign it with the private key. The recipient receives the corresponding public key with the mail which he or she uses to decipher your mail.

Before you can send e-mails to anybody else, you need to send a signed message to yourself in order for Thunderbird to store your public key.

Then you can send your public key to other people, for example by sending them a signed message. Once they have your public key, they can use it to encrypt mails they send to you (which you decipher using your private key).

To send a signed e-mail to yourself with Mozilla Thunderbird

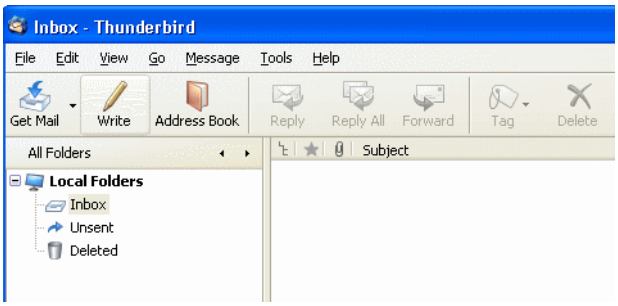
1 Make sure your smart card/token is connected.

2 Start **Mozilla Thunderbird**.

3 Enter your password if you are prompted for it.

4 In **Thunderbird**, click the **Write** icon as shown in “Figure 71”.

Figure 71 - Thunderbird Write Icon

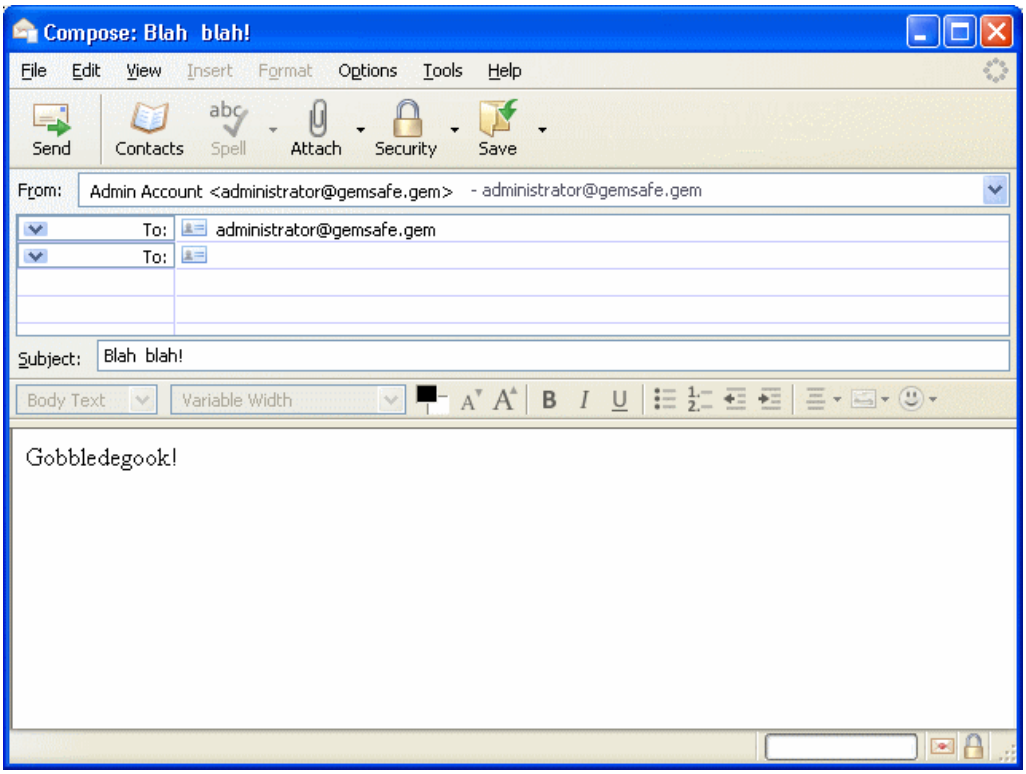


This opens the **Compose** window.

5 In the **Compose** window, write a short message ***addressed to yourself***.

Be sure to include a subject heading.

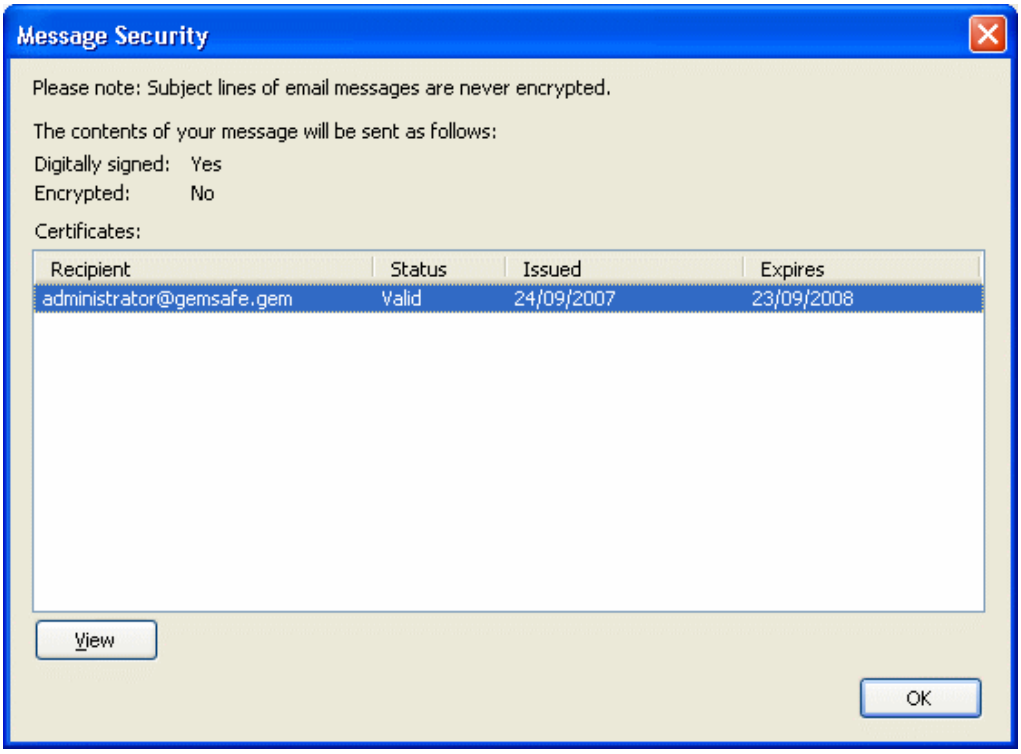
Figure 72 - Thunderbird New Msg Composition Window



6 From the **Options** menu in the **Compose** window choose **Security > Digitally Sign this Message** in order to sign the message.

Note: You can check the security settings for your message in the **Compose** window by choosing **View** > **Message Security Info**. This displays the Message Security window as shown in “Thunderbird Message Security Window”.

Figure 73 - Thunderbird Message Security Window



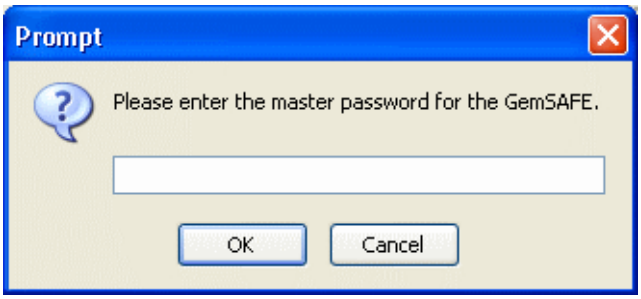
You can display details about the certificate by clicking **View**.

7 Click **OK** to close the **Message Security** window.

8 Back in the **Compose** window, click **Send**.

If you are prompted for a master password for your security module, as shown in “Figure 74”, then enter the User PIN for your smart card/token.

Figure 74 - Module Password Protection



9 Open the message you sent yourself from in your inbox.

Notice the icon  in the upper right corner of the message window showing you that the message has been signed.

You have successfully sent yourself a digitally signed e-mail.

Now that Thunderbird recognizes your public key, you can send signed messages to other people, thus sending them your public key.

Sending Encrypted E-mail with Mozilla Thunderbird

Once you have configured your e-mail account in **Mozilla Thunderbird**, you can retrieve a person's public key when he or she sends a signed message to you. When you send e-mail to that person, you use his or her public key to encrypt the e-mail. This is done automatically by Thunderbird; you just need to specify the recipient(s) of the mail. Since no one except the person who has the private key can decrypt it, the e-mail is secure.

To send an encrypted e-mail:

Follow the same steps as "To send a signed e-mail to yourself with Mozilla Thunderbird" on page 58, except in the **Compose** window, choose **Encrypt this message** from the **Options** menu.

Viewing Secure Web Sites

Communicating and conducting business on the Web is quickly becoming the most convenient, effective means of transaction. Therefore, Web sites must be secure to protect the corporation, the individual and the information exchanged.

With your Classic Client smart card/token, you can browse secure Web sites knowing that your private key and digital certificate are safely stored on your smart card/token instead of your hard drive, where they might be susceptible to unauthorized access.

Note: All secure Web site addresses must begin with https://. Browsers display a lock icon at the bottom of the browser window indicating that the site is secure. A closed lock indicates that you are operating in secure mode. You may need to configure your organization's network to allow secure browsing.

When you connect to a secure Web site, your certificate must be specified in your browser so that you can authenticate yourself to the Web server. For example, when you bank online, your bank must be sure that you are the correct person to get account information. Your certificate confirms your identity to the online bank.

The following sections explain how to check that your certificates are correctly registered in your browsers when authenticating with secure web sites using Internet Explorer and Mozilla Firefox.

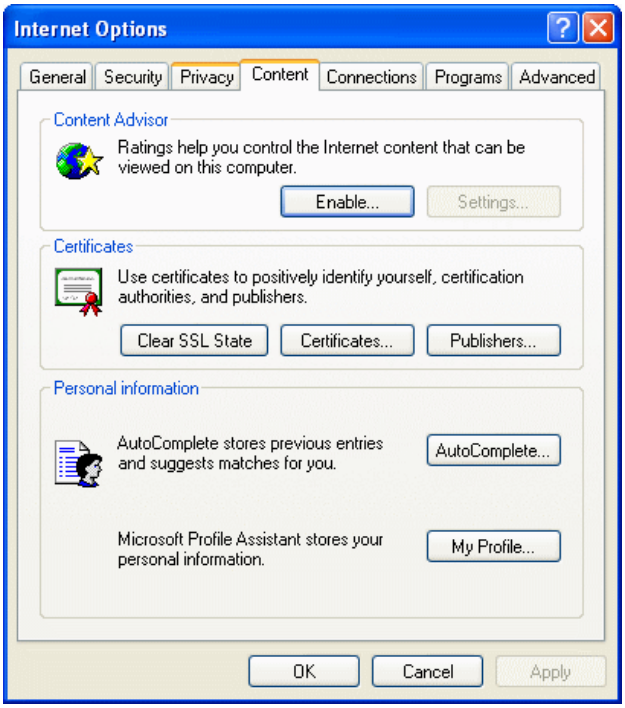
Displaying a Certificate Used to View Web Sites Using IE

For your certificates to work with Internet Explorer, they must be registered in the IE store.

To check that an authentication certificate is in the IE store and view its properties:

1. Make sure your card/token is connected.
2. In Internet Explorer, click **Tools > Internet Options** to open the **Internet Options** dialog box.
3. Click the **Content** tab.

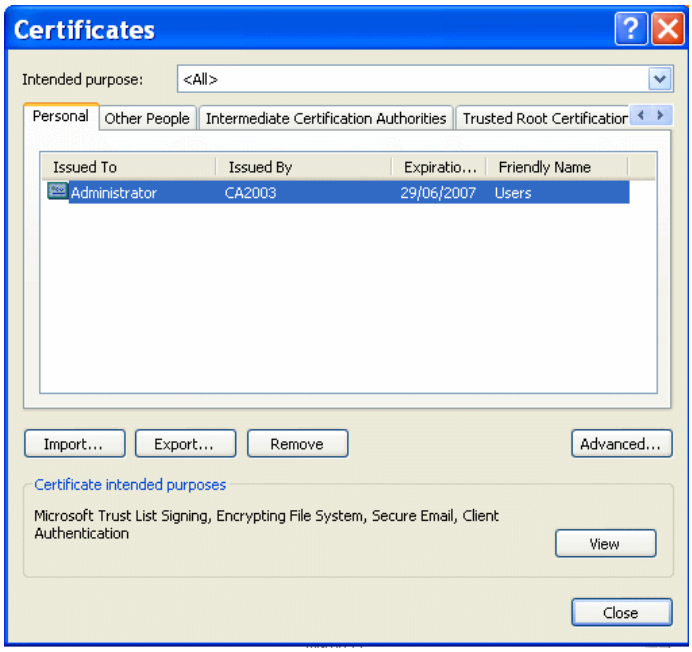
Figure 75 - Internet Explorer Internet Options Dialog Box



Note: The controls described here and the corresponding screen shots may differ depending on your version of Internet Explorer and/or the certificate available.

4 Click **Certificates** to open the **Certificates** dialog box.

Figure 76 - Internet Explorer Certificate Manager Dialog Box

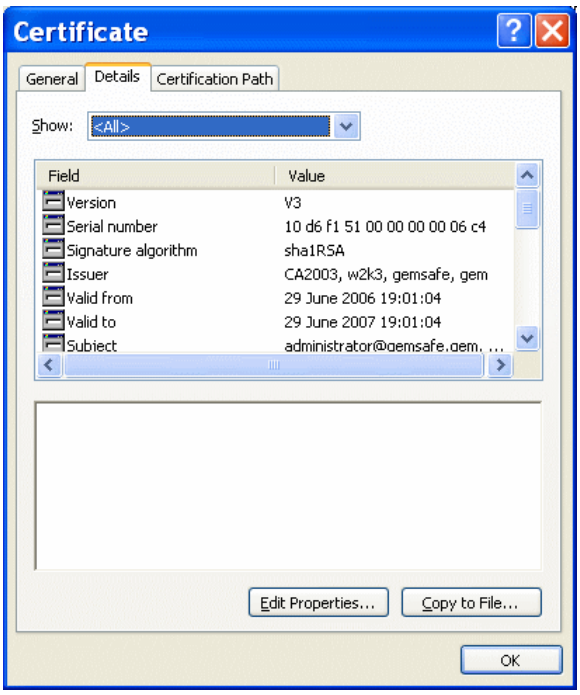


5 Click the certificate you want to use for authentication. Make sure the certificate you select is on your smart card/token.

6 Click **View** to open the **Certificate** dialog box.

7 Click the **Details** tab of the **Certificate** dialog box.

Figure 77 - Internet Explorer Certificate Details



Displaying a Certificate Used to View Web Sites Using Mozilla Firefox

To authenticate using Mozilla Firefox, your certificate must be registered in the Firefox browser. This section describes how to check that a certificate is registered and also how to tell Firefox whether it should select the certificate itself, or ask you.

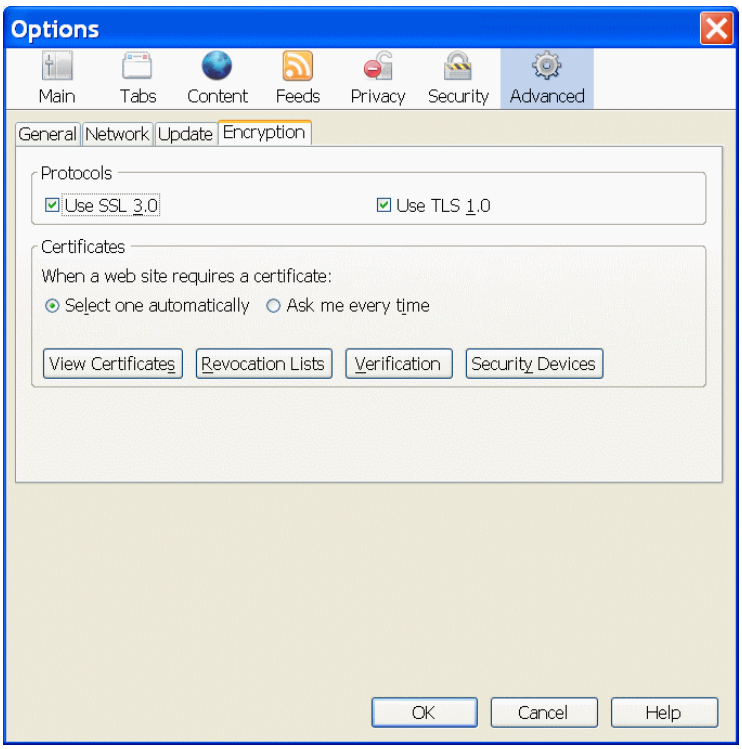
To check certificates registered in Mozilla Firefox:

1 Make sure your card/token is connected.

2 Open the **Mozilla Firefox** browser and from the **Tools** menu choose **Options**. The **Options** dialog opens.

3 Click the **Advanced** icon, then the **Encryption** tab as shown in “Figure 78”.

Figure 78 - Mozilla Firefox Options Dialog

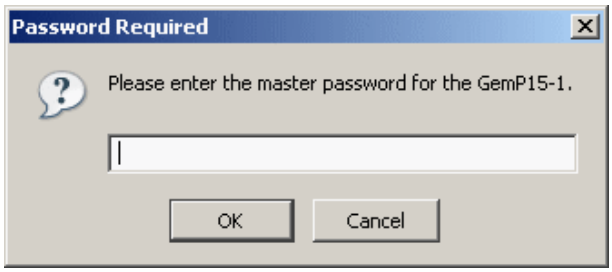


4 In **Certificates**, choose one of the options for the action to take when a web site requires a certificate:

- Select one automatically
- Ask me every time

5 To display the certificates that are on your card/token, click **View Certificates**. You will be prompted for a password as shown in “Figure 79”.

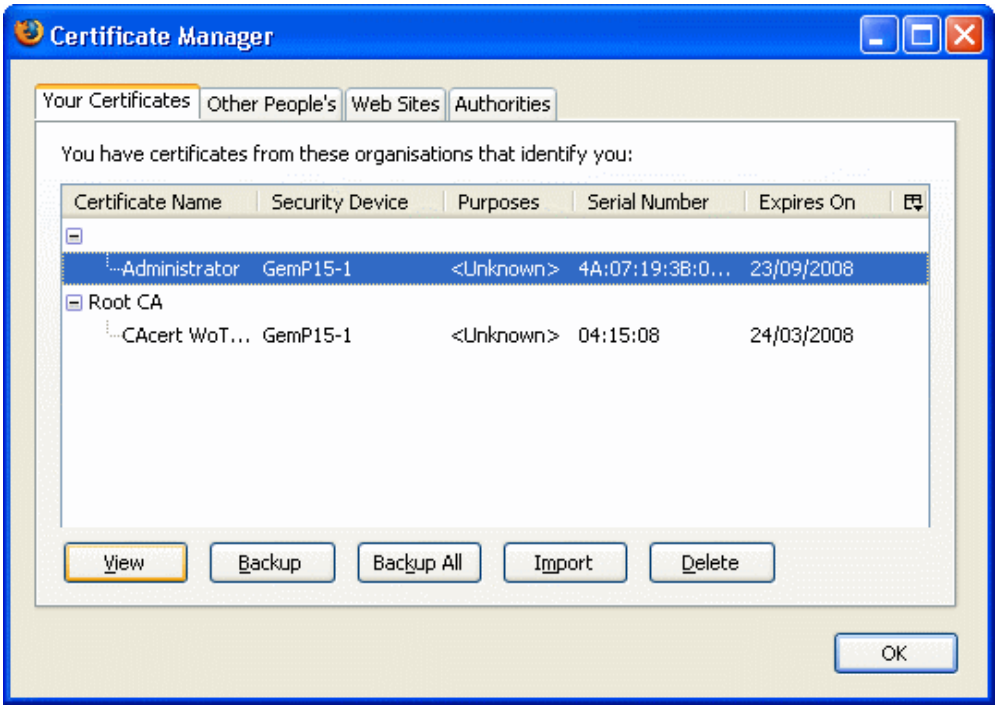
Figure 79 - Password Required



6 Enter the User PIN for your card/token

The **Certificate Manager** window appears.

Figure 80 - Certificate Manager Window



7 Under **Your Certificates** appears the certificates that are stored on the card/token. To display the properties of a particular certificate, select it and click **View**.

Managing Certificates

Introduction

This section talks about using smart cards/tokens with certificates.

Cards/Tokens and Certificates

A digital certificate contains information about the user and the user's public key, and is used to authenticate the user's identity during secure transactions. The certificate identifying the user must be registered with a certificate authority and this information must be available to both parties. To use smart cards/tokens and certificates together, the user must generate a key pair on his card/token and then get a digital certificate corresponding to the public key and store it on the card/token.

Working with Different Cards/Tokens

Many types of cards/tokens are supported by Classic Client. You can check if a card/token is supported simply by connecting it. For unsupported cards/tokens, the reader icon displays a warning sign like this: 

Note: 1) You cannot change anything on read-only cards/tokens.

Note: 2) Some cards/tokens, such as IdenTrust cards/tokens may have two user keys, intended for two different purposes.

How to Import a Certificate

You can import certificates to a card/token if the administrator gave you the rights to do so in your user setup. You can import certificates from the IE certificate store or from a certificate file.

When importing certificates, note the following important points:

- You cannot import certificates to a read-only card/token.
- You can import a certificate without verifying your user PIN (logging in), but if the certificate has an associated key pair, the key pair is not imported: you must be logged in to import an associated key pair.
- Your PIN must be initialized, that is, it's value must have been changed from the original value set when the PIN was issued (or set by the administrator if it has been unblocked).

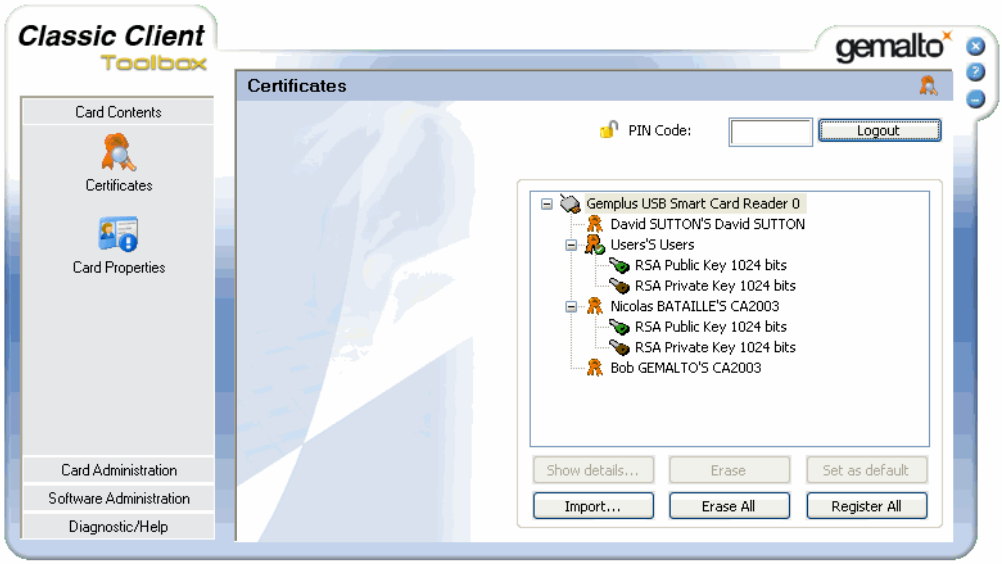
It is recommended that you read the section "Introduction" on page 64 before performing these tasks.

To import a certificate to a smart card/token:

1 In the **Classic Client Toolbox**, click **Certificates** in the **Card Contents** folder.

Make sure that the smart card/token for which you want to import a certificate is connected.

Figure 81 - Certificates Tool Window



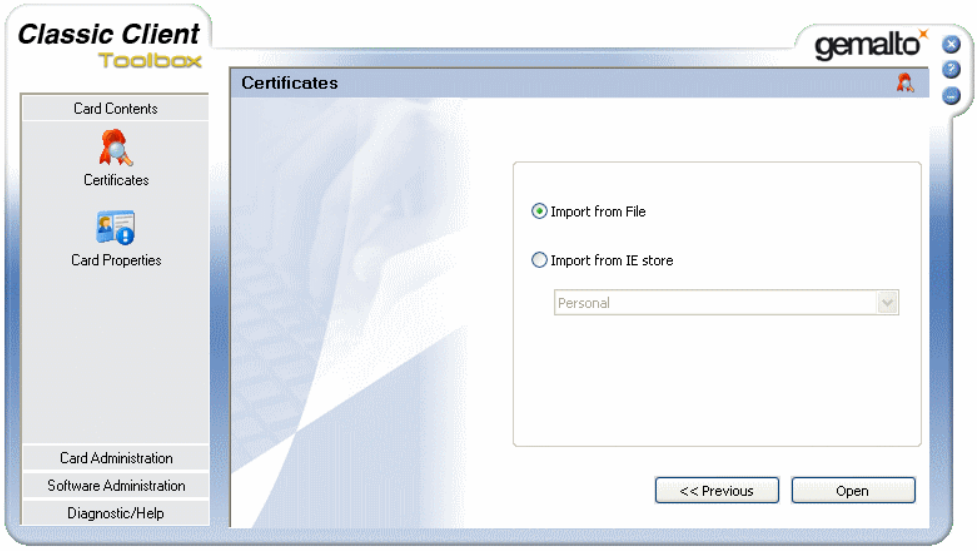
Note: This example treats the case of a smart card/token featuring two operational modes: the *Standard* mode, and the *IdenTrust* mode.

You can import a certificate without verifying your user PIN, but if the certificate has an associated key pair, the key pair is not imported unless you can verify your user PIN when requested.

2 Select the smart card reader. This activates the **Import** button.

3 Click **Import** (you can also do a right–click on the reader and select **Import** from the contextual menu). You are offered a choice of two ways to import the certificate as shown in the following figure:

Figure 82 - Choice of Methods to Import a Certificate



4 Choose the option and follow the instructions for your choice:

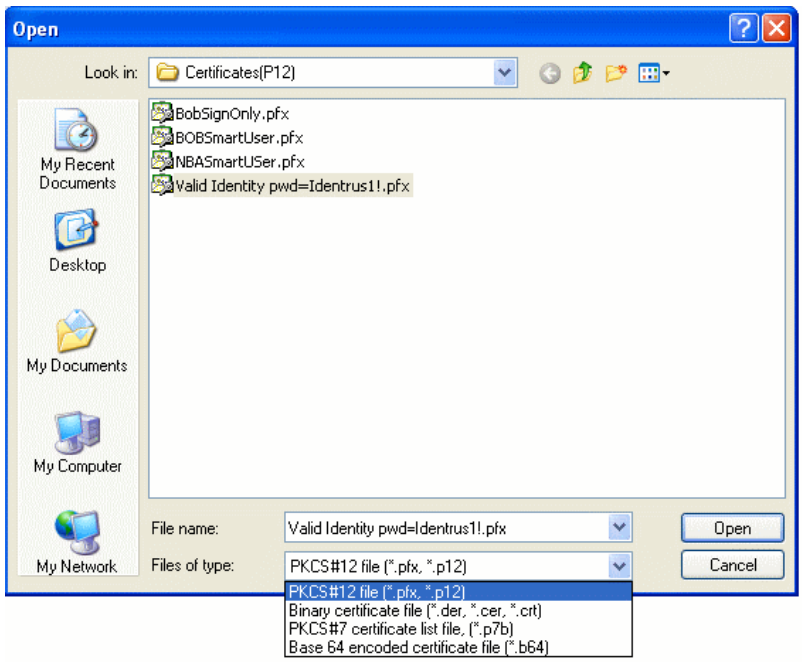
- If importing from a file, see page 66.
- If importing from the IE certificate store, see page 68.

To Import from a Certificate File

1 Follow the instructions in “To import a certificate to a smart card/token:” on page 65.

2 When you reach the window shown in “Figure 82”, choose **Import from File** and click **Open**. This opens the standard windows **Open** window as shown in “Figure 83”.

Figure 83 - Certificates Tool Window: Open Window



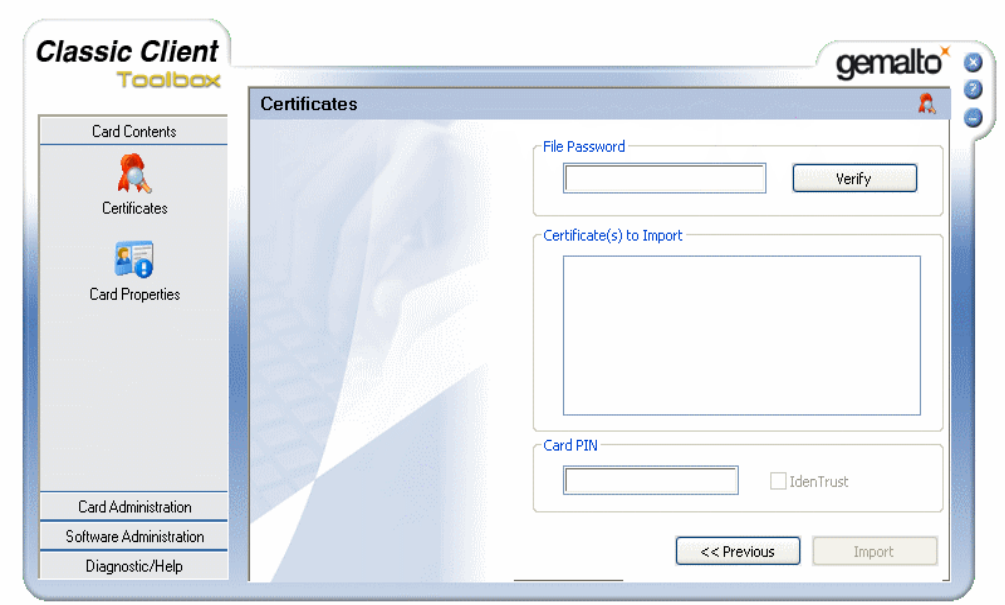
3 Navigate to the certificate file you want.

Compatible Files:

- PKCS#12 file: (*.pfx), (*.p12). These types of files can have one or more certificates and may contain the certificate's key pair value. These types of files are usually protected with a password.
- Binary certificate file: (*.der), (*.cer), (*.crt). These types of files have only one certificate and have no keys.
- PKCS#7 certificate list file: (*.p7b). These types of files can have one or more certificates and have no keys.
- Base 64 encoded certificate file: (*.b64). These types of files have only one certificate and have no keys.

4 In the example in "Figure 83", the choice is among four PKCS#12 objects. These objects can require that you prove knowledge of a password before you can work with their certificates, keys or data objects. Select a file and click **Open**. The window changes as shown in "Figure 84".

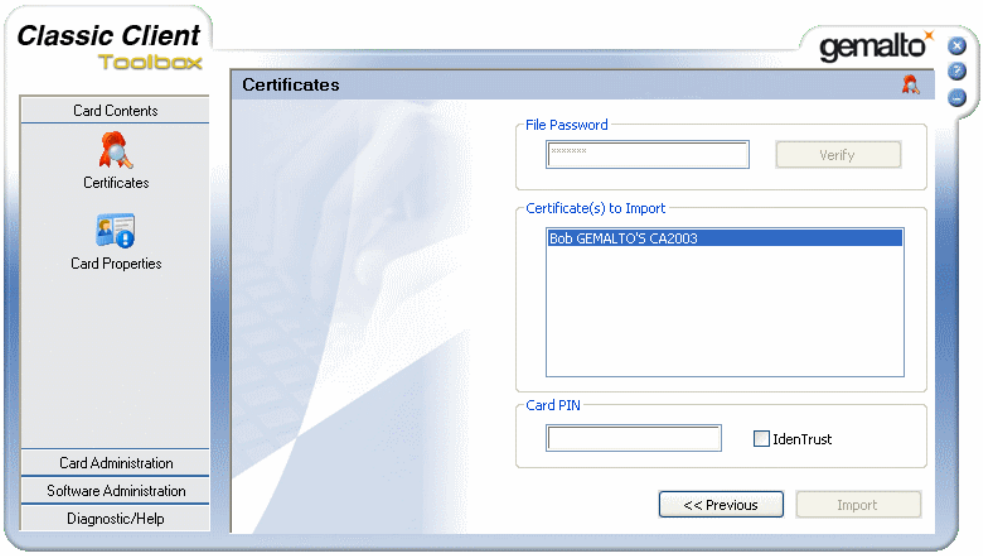
Figure 84 - Certificates Tool Window: Import Certificate File (1)



5 Enter the **File Password** and click **Verify**.

If the password is correct, in the case of a PKCS#12 object, all the certificates in the file are displayed in the **Certificate(s) to import** field as shown in "Figure 85".

Figure 85 - Certificates Tool Window: Import Certificate File (2)



All the other certificate file types don't require password verification, so you immediately see the certificate(s) without the **File password** field.

Note: 1) A P12 certificate is often associated with public and private keys. If you import the certificate, Classic Client automatically attempts to import its associated key pair, and succeeds if you can prove knowledge of the card/token PIN.

Note: 2) The Figure above displays an example of a smart card/token with two operational modes: the Standard mode, and the *IdenTrust* mode. Cards/tokens with only one mode do not display the option IdenTrust for the Card PIN field, as cards/tokens with one mode only require one user PIN.

---

6 In **Certificate(s) to import**, select the certificate you want to import.

7 Do one of the following:

- If the PKCS#11 object(s) (certificates and keys) are to be used for IdenTrust security operations, check the **IdenTrust** option and enter your IdenTrust user PIN in the Card PIN field to permit Classic Client to copy the certificate and, if present, the key pair to the card's/token's public data area.
- If the PKCS#11 object(s) (certificates and keys) are to be used for non-IdenTrust security operations, do not select **IdenTrust** and instead simply enter your user PIN to permit Classic Client to copy the certificate and if present the key pair, with the private key copied to the card's/token's private data area and the public key copied to the card's/token's public area.

8 Once you have entered a valid PIN, click **Import**. A window confirms that the selected certificate is imported.

To Import from the IE Certificate Store

1 Follow the instructions in "To import a certificate to a smart card/token:" on page 65.

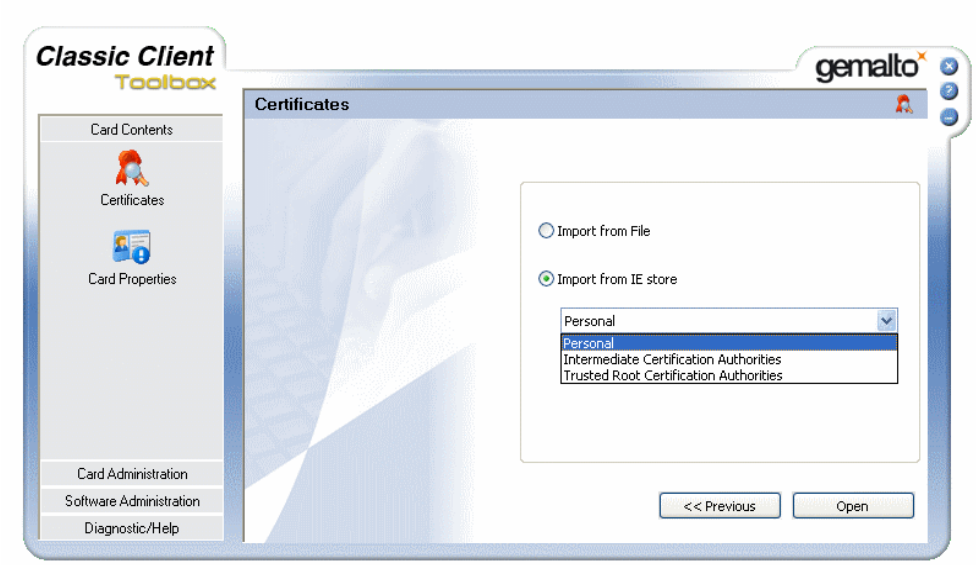
2 When you reach the window shown in "Figure 82", choose **Import from IE store** and select a store from the list:

- **Personal**: Selects a certificate from the IE Store called Personal.
- **Intermediate Certification Authorities**: Selects a certificate from the IE Store called Intermediate Certification Authorities.

– **Trusted Root Certification Authorities**: Selects a certificate from the IE Store called Trusted Root Certificates.

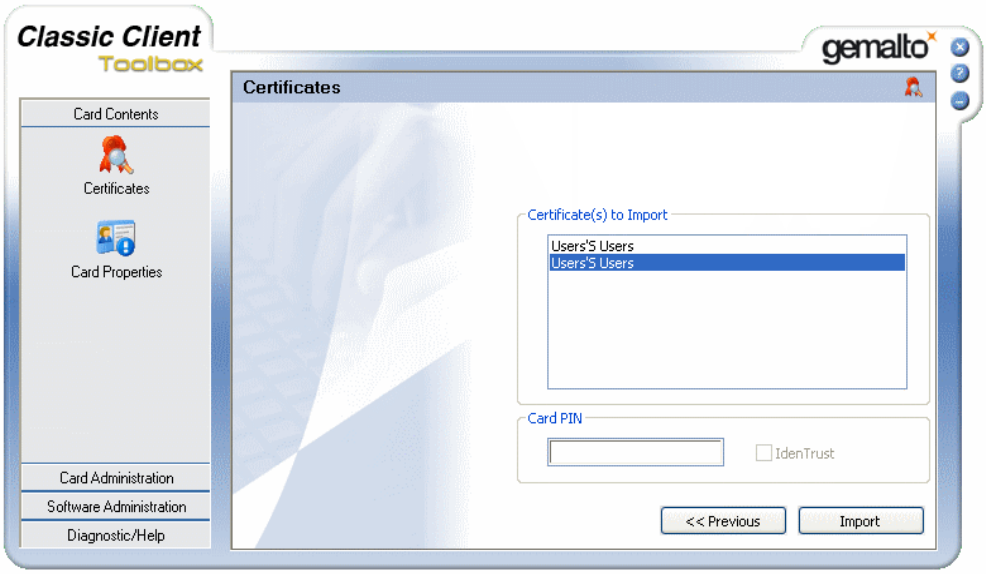
For this example, the choice is from the **Personal** store:

Figure 86 - Certificates Tool Window: Import Certificate - Selecting the store



3 Click **Open**. Classic Client displays the certificates you have in this IE store as shown in “Figure 87”.

Figure 87 - Certificates Tool Window: Import Certificate List



4 Click on the certificate you want to import. You can select more than one certificate by holding down the shift key to select a group, or the control key to add certificates to the selection one by one.

Note: 1) A P12 certificate is often associated with a public and private key pair. If you import a P12 certificate, Classic Client automatically attempts to import its associated key pair, and succeeds if you can prove knowledge of the card/token PIN.

Note: 2) P12 objects may require that you prove knowledge of a password before you can work with their certificates, keys or data objects. If you click on an item, you may be prompted to enter a password. If this occurs, enter the password and click **OK**.

The example in "Figure 87" on page 69 shows an example of a smart card/token with two operational modes: the *Standard* mode, and the *IdenTrust* mode. Cards/tokens with only one mode do not display the option **IdenTrust** for the **Card PIN** field, as cards/tokens with one mode only require one user PIN.

5 Do one of the following:

- If the PKCS#11 object(s) (certificates and keys) are to be used for IdenTrust security operations, select **IdenTrust** and enter your IdenTrust user PIN in the **Card PIN** field to allow Classic Client to copy the certificate and if present, the keys, to the card's/token's public data area.
- If the PKCS#11 object(s) (certificates and keys) are to be used for non-IdenTrust security operations, do not select **IdenTrust** and instead simply enter your user PIN to permit Classic Client to copy the certificate and, if present, the keys, with the private key copied to the card's/token's private data area and the public key copied to the card's/token's public area.

6 Once you have entered a valid PIN in **Card PIN**, click **Import**. A window confirms that the selected certificate has been imported.

How to Export a Certificate

You can export certificates from the card/token if the administrator gave you the rights to do so in your user setup.

Note: If a certificate on the card/token is associated with a cryptographic key pair, when you export the certificate, you cannot export the key pair as well.

It is recommended that you read the introductory remarks in the section "Managing Certificates" on page 64.

Export allows you to export certificates from a smart card/token, one certificate at a time (if you have been given the right to export certificates from a smart card/token). You can export certificates from the smart card/token to the IE certificate store or to a certificate file.

Caution: You cannot export any type of cryptographic key from the card/token to a file or to the IE Certificate Store.

To export a certificate from a smart card/token:

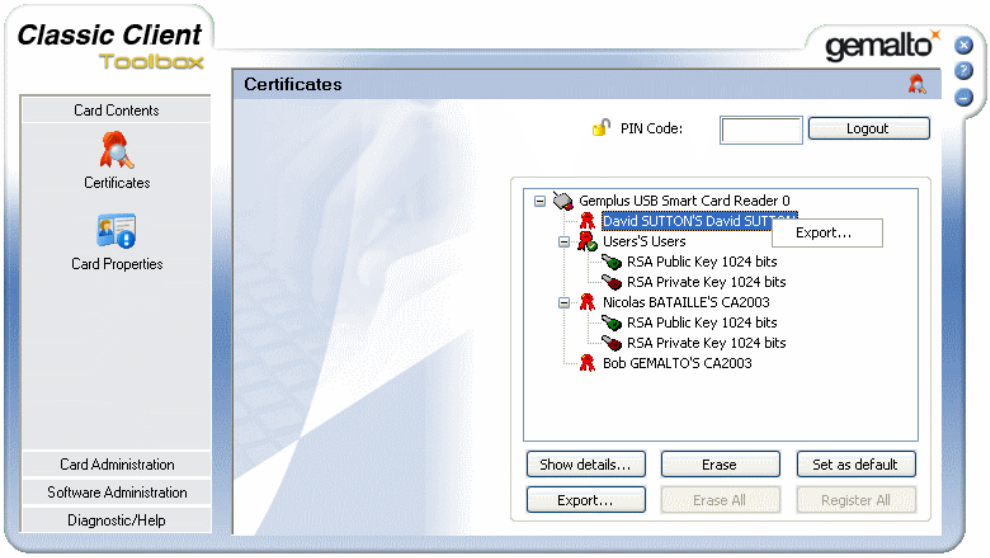
1 In the **Classic Client Toolbox**, click **Certificates** in the **Card Contents** folder.

Make sure that the smart card/token from which you want to export a certificate is connected.

2 If not already logged in, enter your PIN in **PIN Code** and click **Login**.

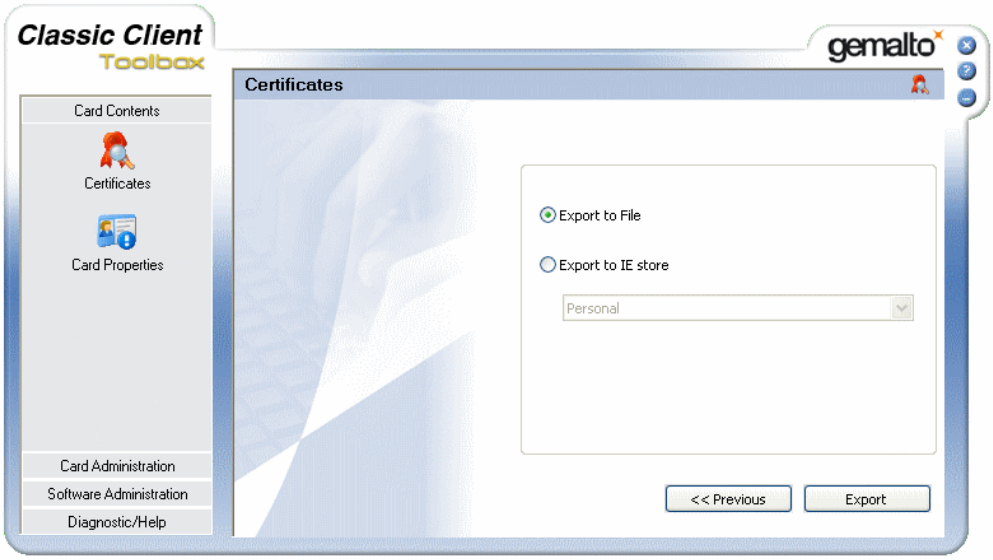
3 Select the certificate. This activates the **Export** button as shown in "Figure 88".

Figure 88 - Certificates Tool Window: Export Button Activated.



4 Click **Export** (you can also do a right–click on the reader and select **Export** from the contextual menu). You are offered a choice of two ways to export the certificate as shown in the following figure.

Figure 89 - Choice of Methods to Export a Certificate



5 Choose the option and follow the instructions for your choice:

- If exporting to a certificate file, see “To export to a certificate file” on page 71.
- If exporting to the IE certificate store, see “To export to the IE certificate store” on page 72.

To export to a certificate file

1 Select **Export to File** and click **Export**. This opens the standard Windows **Save As** window.

2 Type the file name and select among the following types of certificate files:

- Binary certificate file: (*.der), (*.cer), (*.crt). These types of files can contain only one certificate.
- PKCS#7 certificate list file: (*.p7b). These types of files can contain one or more certificates.
- Base 64 encoded certificate file: (*.b64). These types of files can contain only one certificate.

Note: You cannot export to a P12 certificate file because you cannot export any kind of cryptographic key from the card/token.

Tip: Classic Client cannot export a certificate chain to a P7 certificate file in one action. Export the root certificate to a P7 format, then export the rest of the chain into respective *.der certificate files. You can then add the *.der certificates in order to your P7 certificate file and recreate the chain.

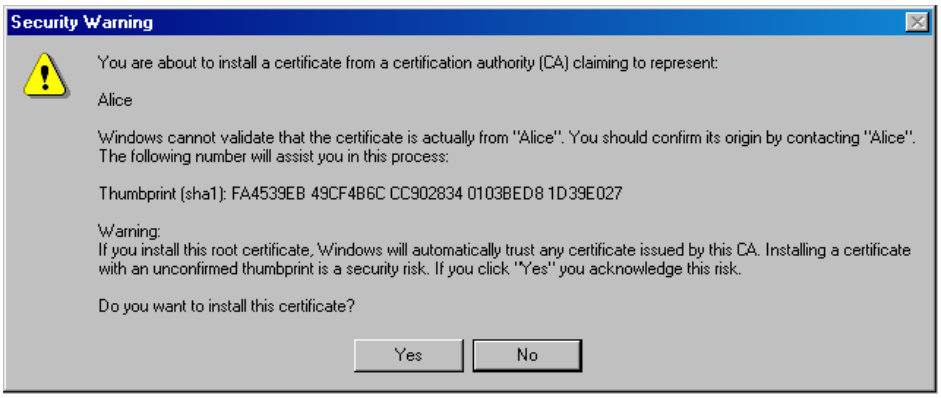
3 Click **Save as**. A window confirms that the selected certificate is exported.

To export to the IE certificate store

1 Select **Export to IE store** and select a store from the list:

- **Personal**: Exports the selected certificate to the IE Store called Personal.
- **Intermediate Certification Authorities**: Exports the selected certificate to the IE Store called Intermediate Certification Authorities.
- **Trusted Root Certification Authorities**: Exports the selected certificate to the IE Store called Trusted Root Certificates. If you export a certificate to this store, Windows prompts you to be confident as to the source of the certificate. If you are, click **Yes** to continue.

Figure 90 - Security Warning



2 Click **Export**. A window confirms that the selected certificate is exported.

How to Set Certificates as Default

You can specify which certificate on your smart card/token you want to use as the default certificate for logging on to your PC using the card/token.

Note: In versions of Windows older than Vista, the OS can use only the default certificate.

To set the default certificate:

1 Make sure that the smart card/token for which you want to set a default certificate is connected.

2 If not already logged in, enter your PIN and click **Login**.

3 Select the certificate you want to become the default certificate.

4 Click **Set as default**; the selected certificate is set as the default certificate.

How to Register Certificates to the IE Store Manually

The Registration Tool can automatically register your certificate in the IE cert store. To do this, simply start IE and connect your card/token.

Note: The Registration Tool does not copy certificate information to the IE store; it creates a link from the IE cert store to the certificate information on the card/token to ensure security.

The Registration Tool is available only if the administrator has included it in your User Setup package. You can check it is available by the presence of the icon that is displayed in the tool bar.

Note: The Registration Tool is not available in Citrix client-server environments.

For a more information about this and other registration tool features, see “Chapter 3 - The Registration Tool”.

If the Registration Tool is not available, then Windows 2000, XP and Server 2003 will perform this automatic registration in its place. However Classic Client deactivates this feature in Windows Vista, 7, Server 2008 and Server 2008 R2.

Classic Client’s Certificates Tool enables you to register all your certificates to the IE store manually. This tool is indicated by the certificate tool icon in your **Card Contents** folder. Its availability depends on whether the administrator included it in your User Setup package.

To register all certificates manually:

1 Make sure that the smart card/token for which you want to register all the certificates is connected.

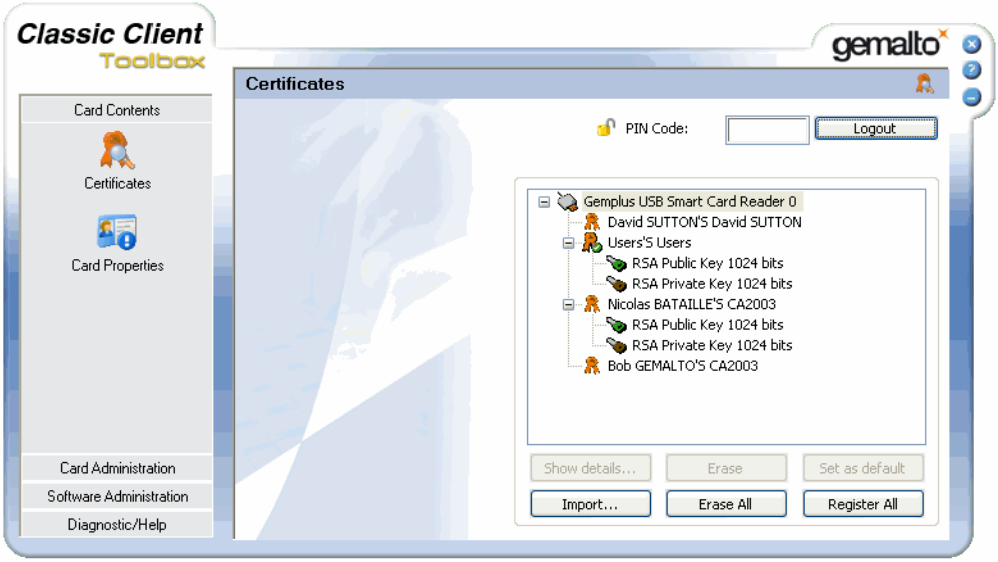
2 Open the **Certificate Tool** in the Classic Client Toolbox (**Card Contents** > **Certificates**).

3 If not already logged in, enter your PIN and click **Login**.

4 Select the smart card reader . This selects all the PKCS#11 objects stored on the smart card/token.

The register all certificates function is only available when all objects are selected.

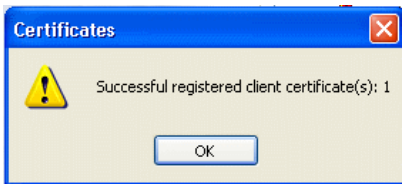
Figure 91 - Certificates Tool Window (All Objects Selected)



5 Click **Register All**.

A confirmation window summarizes how many certificates were registered.

Figure 92 - Certificate Successfully Registered



6 Click **OK** to complete the **Register All** operation.

How to Display Certificate Details

You can view details of the certificates on the card/token and see if your card/token has any data objects on it, although you cannot see details on the data itself. This is useful to ensure you have the right certificates for a particular action that you want to perform.

Note: The **Show Details** button is for certificates only.

To see the details of a certificate:

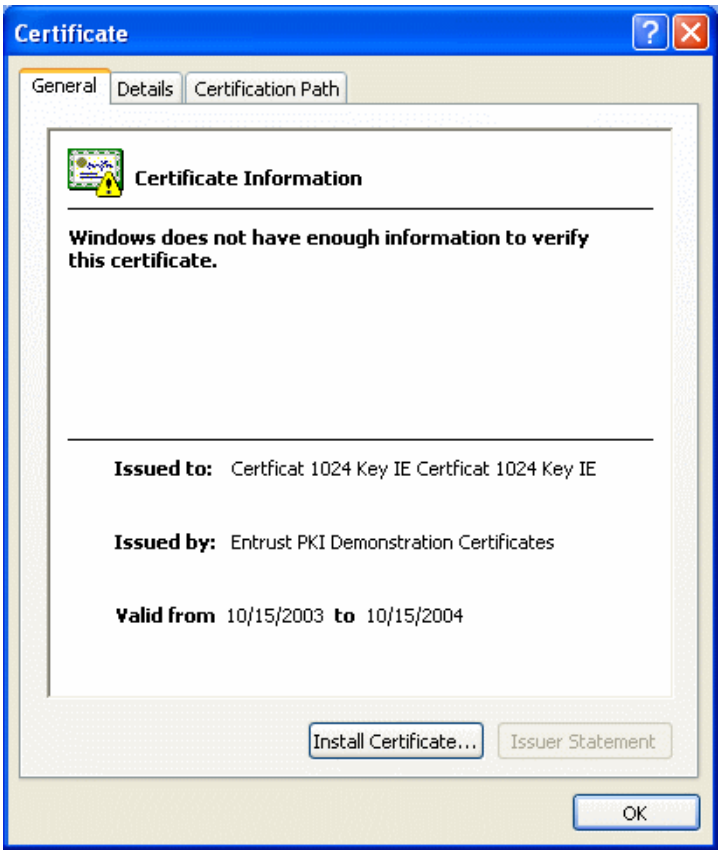
1 Make sure that the smart card/token for which you want to register certificates is connected.

2 If not already logged in, enter your PIN and click **Login**. This ensures you can see both public and private details.

3 Select the certificate you want to display information about.

4 Double click the certificate, or click **Show details**; the Microsoft Certificate viewer opens.

Figure 93 - Window Certificate Information Viewer



How to Erase Certificates (PKCS#11 Objects)

Certificates are PKCS#11 objects, as are keys and data.

You can erase all the objects on your card/token, or erase an individual object. This is useful if you have no more space on the card/token for any new objects.

Note: You cannot erase anything from a card/token that is read-only.

The introductory remarks in the section “Managing Certificates” on page 64 provide some useful background information.

Erasing All Certificates

The **Erase All** function enables you to erase ALL the PKCS#11 objects on the card/token (certificates, keys and data). The function’s availability depends on whether it was included by the Administrator in your User Setup.

Note: In some circumstances the **Erase All** option does not remove all items from the memory. The memory space may still be occupied by proprietary objects.

To erase all certificates (PKCS#11 objects):

1 Make sure that the smart card/token on which you want to **Erase All** is connected.

2 If not already logged in, enter your PIN and click **Login**.

3 Select the smart card reader. This selects all PKCS#11 objects on the smart card/token, see “Figure 91” on page 74.

The **Erase All** function is only available when the smart card reader is selected.

4 Click **Erase All**; all objects are erased from the smart card/token.

Erasing an Individual Certificate

The **Erase** function enables you to erase individual PKCS#11 objects on the card/token (certificates and keys) one at a time. The function's availability depends on whether it was included by the Administrator in your User Setup. This is useful to clear up space on the card/token and to erase old keys or certificates.

Note: The **Erase** button deletes a key pair only when the certificate it is associated with has already been deleted. The key pair associated with a certificate is displayed after the certificate with which it is associated.

To erase an individual certificate (PKCS#11 object):

1 Make sure that the smart card/token on which you want to **Erase** the certificate is connected.

2 If not already logged in, enter your PIN and click **Login**.

3 Select the object to erase and click **Erase**.

5

The Contactless Secure Data Mechanism

Contactless cards behave in the same way as contact cards. However, some contactless cards have an additional feature. This feature is available if requested from Gemalto. The contactless secure data (CSD) mechanism is designed to protect confidential data about the cardholder from being read by a third party without the cardholder's consent or knowledge.

When a reader tries to access the Classic Applet V2 or V3 (or IAS Classic Applet V2 or V3) in the smart card, the applet returns the **Classic Client CSD** dialog box as shown in "Figure 94" on page 77).

Figure 94 - The CSD Dialog Box

Enter the CSD and click **OK**. The reader can then access the Classic Applet V2 or V3 (or IAS Classic Applet V2 or V3).

The CSD is specified by the card issuer but is typically information such as the last four digits of the card serial number as printed on the card.

If you click **Cancel**, you must remove the smart card from the reader before it can be reread. Normally the **Classic Client CSD** dialog box displays once only at the beginning of each card session, that is, when the card is first read by the reader. However, under certain circumstances (such as if the card session is broken for some reason) it is possible that it may be displayed again to reprompt for the CSD.

Note: As an extra security measure against “brute force” attacks (where the reader may attempt to read the applet many times in a short time), the smart card deliberately slows down the verification of the CSD code after an incorrect CSD entry. The more incorrect CSD attempts are made, the slower the response to process the next CSD attempt.

A

Security Basics

This chapter introduces you to the IT security standards integral to Classic Client.

Cryptography

Communicating and conducting business electronically is quickly becoming the most convenient, effective means of transaction. An essential condition for the continued growth toward an electronic market is security. The identities of both corporations and individuals must be authentic. The integrity and privacy of information must be guaranteed.

Encryption/decryption enables you to send and receive secure e-mail and documents to protect confidential or private information. You can use the signature function to sign your messages. By signing messages, you can prove to the recipient that you are who you claim to be.

The IT industry uses cryptography to render information secret and known only by authorized entities.

There are two types of cryptography:

- Secret Key Cryptography.
- Public Key Cryptography

Both cryptographic systems use *keys* to digitally sign or encrypt/decrypt data. A key is a value in electronic format used to perform cryptographic functions on electronic data.

The differences between secret key and public key cryptography include:

- Key management.
- Complexity of the key structure.

Key management is central to having a successful crypto system. If keys are not managed in a secure environment, the overall security of the crypto system is at risk. Keys must also be convenient to use.

The complexity of a key length is determined by the degree of mathematical properties applied to the random numbers that comprise the key.

Secret Key Cryptography

Secret key cryptography is the traditional crypto system, which remains in widespread use even today. Secret key cryptography uses a single secret key to digitally sign or encrypt/decrypt electronic data. The most widely used secret key crypto systems are DES and RC2 (also known as symmetric key cryptography).

The sender and receiver must use the same secret key for the session in which secure information is exchanged. The sender uses the secret key to encrypt the message; the receiver uses the same secret key to decrypt the message.

The primary advantage of secret key cryptography is the speed at which data can be encrypted/decrypted.

The primary weakness of secret key cryptography regards key management. Because sender and receiver must share knowledge of the secret key, there must be a transfer of the secret key at some point. Introducing a third party (such as a telephone line or courier) to deliver the secret key to the receiver presents a security risk.

Secret keys are included in the cryptographic functionality of both Microsoft and Mozilla e-mail and browser products.

Public Key Cryptography

Public key cryptography was introduced in 1976 and is the most advanced, secure crypto system for digitally signing and encrypting/decrypting electronic data. Public key cryptography refers to a crypto system that uses key pairs. The most popular and widely-used public key crypto system uses the RSA key pair.

A key pair is a matched set of keys used to digitally sign or encrypt/decrypt electronic data. RSA key pairs, like secret keys, are strings of random numbers. However, RSA keys are not only significantly longer than secret keys, they also possess complex mathematical properties.

A single user *owns* an RSA key pair. One key is private, while the other key is public. The private key remains private and accessible only to the owner of the key pair. The public key is made available by the owner to public users. The public key is used to encrypt data. The private key is used to decrypt data.

The strengths of using an RSA key pair is that the need for sender and receiver to share knowledge of the single secret key used in secret key crypto systems is eliminated.

Classic Client takes advantage of the speed the secret key offers and the robust security and convenience of the RSA key pair. When you use Classic Client to send secure e-mail, the actual message data is encrypted using a secret key. The secret key is then encrypted using the public key of the intended recipient. Only the recipient's private key can decrypt the secret key. Only the secret key can decrypt the message data.

Classic Client offers the most advanced digital security at the greatest speed and convenience.

What is a digital certificate?

A digital certificate is an electronic document that serves as your digital passport. Your digital certificate stores your public key and other personal information about you and the certificate.

The most widely accepted standard for digital certificates is defined by *International Telecommunications Union standard ITU-T X.509*. Version three is the most current version of X.509.

The X.509v3 certificate includes the following data:

- Version.
- Serial number.
- Signature algorithm ID.
- Issuer name.
- Expiration Date.
- User name.
- User public key information.
- Issuer unique identifier.
- User unique identifier.
- Extensions.
- Signature on the above fields.

As a convenience to recipients, it is standard practice to attach your digital certificate to every secure e-mail that you send. The recipient uses your public key, included in your digital certificate, to encrypt e-mail addressed to you. If you do not attach your digital certificate to outgoing e-mails, recipients must retrieve your public key from a public directory if they want to reply to you with an encrypted e-mail.

What is a Certificate Authority?

Certificate Authorities (CAs) are trusted third parties that issue digital certificates. CAs vouch for the identity of the individual or enterprise to whom they are issuing a certificate. CAs provide a transfer of trust from CA to the individual or enterprise. When you trust the CA certificate, you can transfer that trust to all certificates published by that CA.

When you obtain your digital certificate, you provide the CA with your public key and any personal information requested by the CA. The CA verifies your personal information and the integrity of your public key. After the verification process, the CA signs your public key, stores appropriate personal information and your public key on the digital certificate, and issues your digital certificate to you.

CAs issue certificates with varying levels of identification requirements. CA policies and the level of identification of the digital certificate determine the method and requirements for proving your identity to the CA. The most simple digital certificate only requires your e-mail address and name. However, some CAs require a driver's license, notarized certificate request form, or any other personal documentation attesting to your identity. Some CAs may even go as far as requiring biometric data such as fingerprints.

The CA public key must be widely available so that users can validate the authenticity of all certificates published by this CA.

What is a digital signature?

A digital signature is a piece of information created using message data and the owner's private key. Digital signatures provide message authentication, non-repudiation of origin, and data integrity.

Digital signatures are created by mathematical, or *hash*, and private signing functions. The one-way hash function produces a message digest, a condensed version of the original message text. The message digest is encrypted using the sender's private key, turning it into a digital signature.

The digital signature can only be decrypted using the public key of the same sender. The recipient of the data decrypts the digital signature and compares the result with a message digest, recalculated from the original message text. If the two are identical, the message was not manipulated, thus is authentic.

What is S/MIME?

Secure/Multipurpose Internet Mail Extensions (S/MIME) is an open protocol standard, that provides encryption and digital signature functionality to Internet e-mail. S/MIME uses public key cryptography standards to define e-mail security services.

S/MIME enables you to encrypt and digitally sign Internet e-mail using Web messaging applications such as Microsoft Outlook, and Mozilla Thunderbird. S/MIME also enables you to authenticate incoming messages.

S/MIME provides the following security functions:

- **Sender Authentication** to verify the sender's identity. By reading the sender's digital signature, the recipient can see who signed the message and view the certificate for additional details.
- **Message Encryption** to ensure that your messages remain private. Mozilla Thunderbird and Microsoft Outlook support domestic and export-level public key and secret key encryption.
- **Data Integrity** to guard against unauthorized manipulation of messages. S/MIME uses a secure hashing function to detect message tampering.
- **Inter-operability** to work with other S/MIME-compliant software.

What is SSL?

Secure Sockets Layer (SSL), developed by Netscape Communications, is a standard security protocol that provides security and privacy on the Web. The protocol allows client/server applications to communicate securely. SSL uses both public and secret key cryptography.

The SSL protocol is application independent, which enables higher-level protocols such as Hyper Text Transfer Protocol (HTTP) to be layered on top of it transparently. Therefore, the client can negotiate encryption and authentication with the server before data is exchanged by the higher-level application.

The SSL Handshake Protocol process includes two phases:

- **Server Authentication** in which the client requests the server's certificate. In response, the server returns its digital certificate and signature to the client. The server certificate provides the server's public key. The signature proves that the server currently has the private key corresponding to the certificate.
- **Client Authentication** (optional) in which the server requests the client's certificate. In response, the client sends the digital certificate and signature to the server. If the SSL Server requests it, the client is prompted to enter a PIN to visit a secure Web site.

The SSL process is repeated for every secure session you attempt to establish unless you specify a permanent session. The SSL process will not proceed if the Web server's certificate is expired.

Note: In some instances, the SSL Handshake takes place between the Web server and the browser and does not require the client's certificate.

SSL provides the following security functions:

- **Data Encryption** to ensure data security and privacy. Both public key and secret key encryption are used to achieve maximum security. All traffic between an SSL server and SSL client is encrypted using both public key and secret key algorithms. Encryption thwarts the capture and decryption of TCP/IP sessions.
- **Mutual Authentication** to verify the identities of the server and client. Identities are digital certificates. The entity presenting the certificate must digitally sign the data to prove ownership of the certificate. The combination of the certificate and signature authenticates the entity.
- **Data Integrity** to ensure that SSL session data is not manipulated en route. SSL uses hash functions to provide the integrity service.

What is Classic Client?

Classic Client is a smart card–based solution designed to secure e–mail communications and Internet transactions. Classic Client smart cards/tokens support encryption/decryption and signature functions. Classic Client also supports Windows 2000/XP/Vista/7 secure libraries and the capability to sign Microsoft Office macros.

Classic Client and a smart card/token provide the following advantages:

- Your private key is never removed from your smart card/token.
- The smart card/token is hardware-based security.
- The PIN code protects key use.
- Classic Client is portable and convenient.

The encryption/decryption function enables you to send and receive secure e-mail to protect confidential or private information. You can use the signature function to sign your messages. By signing messages, you can prove to the recipient that you are who you claim to be.

Classic Client combines the privacy, integrity, and authentication functionality provided by cryptographic algorithms with the simplicity, portability, and convenience of smart cards/tokens. Your private key, digital certificate, and other personal information are securely stored on your Classic Client smart card/token to prevent fraudulent use of your electronic identity.

The latest industry standards such as SSL3 (for Web access) and S/MIME (for e–mail) enable inter–operability of security services between any browser interface and any Web server. However, the security hole in SSL3 and S/MIME is the management of your private key and digital certificate. Without Classic Client, your private key and digital certificate are stored on your hard drive, which makes them susceptible to unauthorized access and fraudulent use. Without Classic Client, your electronic identity is at risk.

Classic Client provides double-barreled security! Classic Client, you get the hardware-based security inherent in smart cards/tokens and software-based encryption security, as well as the added advantage of individual PIN codes. Hardware-based security is a principal security advantage. It is significantly more secure than software-only solutions. Without the possession of your smart card/token and knowledge of your PIN code, no one can use your identity.

Classic Client is your electronic passport to the digital world.

What is a Smart Card/Token?

A smart card is the size of a conventional credit card. But unlike the credit card, which has a magnetic stripe, the smart card has a silicon microprocessor chip to store and process electronic data and applications. The advantage of the smart card is **security**.

Gemalto manufactures various types of smart cards. Contact smart cards use a microprocessor chip to store and process data. They must be inserted into a smart card reader. Contactless smart cards use a microprocessor chip and antenna to store and process data.

Smart cards can also be embedded in tokens such as USB devices, that you can plug directly into a PC.

Smart cards/tokens provide the most sophisticated security available on the market.

What is the Classic Client Smart Card/Token?

Your Classic Client smart card/token stores your private key and digital certificate. In the past, your only option was to store your private key on your local hard drive, rendering it susceptible to theft and fraudulent use. With Classic Client, your electronic identity is secure. You must have both the smart card/token and PIN code to use the smart card/token.

The Classic Client smart card/token is tamper resistant. The structure and operating system of the smart card/token make it practically impossible to penetrate, probe, or pilfer smart card/token data.

Perhaps the most convenient aspect of the Classic Client smart card/token is portability. With Classic Client, you can carry your electronic passport with you at all times and use it on any Classic Client–equipped computer in the world.

The Classic Client smart card/token has a robust and flexible design. These features offer greater freedom and enhanced security.

On-board Key Generation

The Classic Client smart card/token offers on-board key generation. With this feature, every time you enroll a new certificate on your smart card/token, a new key pair is generated on your smart card/token. In other words, you are not limited to using the same key pair for every certificate that you enroll.

One significant advantage of onboard key generation is the ability to monitor and control the life span of your RSA key pairs and that the generated key pair is unique.

Increased Certificate Storage

You can store up to six key pairs and multiple digital certificates on your Classic Client smart card/token, depending upon the size of your certificates and space available on your smart card/token. This feature provides the convenience of using up to eight digital certificates for whatever purposes you want; for example, you can use certificates with varying degrees of encryption (from 1024–bit to 512–bit RSA key pairs) to communicate securely with contacts in various parts of the world.

Another reason for obtaining more than one digital certificate is the level of certification that the Certificate Authority (CA) requires. You may want to obtain and use a digital certificate from a CA that requires stringent identity certification if you are using the certificate for sensitive business communications or financial transactions. However, if you want to encrypt/sign data for personal communications, you may decide that a certificate from a CA that requires minimal identity certification meets your needs.

The costs of obtaining a digital certificate from a CA are somewhat based on the degree of identity certification the CA requires.

B

Troubleshooting

This appendix lists answers to some questions you may have about Classic Client Toolbox.

General

I lost/forgot my PIN.

If you lost or forgot your User PIN, you can try to unblock the PIN with the PIN Management Tool, only if this option has been granted to you upon installation by the Administrator. If you do not have this privilege, you must contact the Administrator to unblock your smart card.

My smart card/token appears to have stopped working

If your smart card/token stops working, consider the following reasons:

- **Your smart card's/token's PIN may be blocked** You can unblock your smart card/token as described in the section about unblocking a PIN.
- **Your smart card's/token's certificate may have expired** You need to get a new certificate. See information about getting a new certificate.
- **Your smart card's/token's certificate may not be registered** If you are using Microsoft e-mail software, you may need to register your certificate. See information about registering a certificate.
- **The problem may be hardware-related failure** Ask your Administrator for help.

Certificate Related Problems

General

I think there may be a problem with the key sets and/or certificates in my card - How can I check?

This sort of problem can arise when a card/token has been used previously with a version of Classic Client that is older than 5.0 (when it was called GemSafe Libraries).

To help you, Classic Client provides a **Diagnosis** function that checks key set and certificate data objects on the card.

To use the Diagnosis function:

1 In the **Card Contents** folder, click **Card Properties**, select the reader and click **Next**.

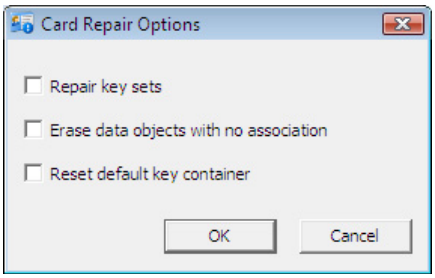
2 Enter the PIN associated with the smart card/token in the **PIN Code** area and click **Login**.

3 Click the **Advance** button, to display the window in “Figure 20” on page 21.

4 Click **Diagnosis**. Classic Client checks the integrity of the data objects that make up a key set on the card. If the structure of the data objects is correct, an “OK” message appears. Otherwise the dialog in “Figure 95” appears, to tell you that the card needs to be “repaired”.

Note: A correctly structured key set has a private key, a public key, a certificate and a descriptor object.

Figure 95 - Card Repair Options



Only the options where Classic Client has detected a problem are available.

5 Check one or more boxes according to the operations you want to perform, then click **OK**.

- **Repair key sets** – creates the descriptor object for a key set if it appears to be missing.
- **Erase data objects with no association** – erases descriptor data objects that do not appear to be linked with a key set.
- **Reset default key container** — as the first two options may affect the key set that is considered to be the default, this option enables you to reset it.

Caution: Before choosing the **Reset default key container** option, be certain that you want to do this. If after resetting the default key set the card is used once again with GemSafe Libraries, the default key set may change again. Gemalto strongly recommends that once you have used the card with Classic Client, you do nor reuse it with GemSafe Libraries.

How can I check that my certificate is stored on my Classic Client smart card/token.

Use the Certificates tool to see information about your certificate. If you cannot see information about your certificate, it might not be on your Classic Client smart card/token. Either your certificate was stored on your hard drive during download or you do not have a certificate.

If you did not select the correct CSP when you requested your certificate then your certificate is stored on your hard drive. You must obtain a new certificate and be sure to specify the correct CSP during the download process. Contact your Certificate Authority if you purchased a digital certificate. You may be able to avoid fees for obtaining a new certificate.

The correct CSPs to specify are:

- Gemalto Classic Card CSP

If your Classic Client smart card/token or browser and e-mail applications do not list your digital certificate, then there was probably an error during download or enrollment of your certificate. Contact your Certificate Authority for additional help.

Browsers

I downloaded my certificate using Mozilla and now I can't use it with Internet Explorer and Outlook.

When you download a digital certificate using Mozilla, you must register your certificate with the Certificates Tool before you can use it with Internet Explorer and Outlook. In fact, you must do this on every computer on which you want to use this certificate with Internet Explorer and Outlook.

If the Classic Client Toolbox **Registration Tool (**certificate registry) is installed, it will do this for you automatically simply by removing and reinserting your card/token.

The certificate I use with Internet Explorer doesn’t seem to work on any other computer.

If you want to use your certificate on another computer with Internet Explorer, you must register it first using the Certificates Tool.

I have an expired certificate in Internet Explorer and I can't delete it.

To delete a certificate with Internet Explorer 7.0 or later:

1. Click **Tools > Options** to open the **Internet Options** dialog box.
2. In the **Internet Options** dialog box, click the **Content** tab
3. Click **Certificates** to open the **Certificate Manager** dialog box.
4. Select the certificate you want to remove.
5. Click **Remove**.

Internet Explorer is available free for download from www.microsoft.com.

When I try to connect to a secure Web site that requests client authentication, it takes an exceptionally long time to connect if it ever connects.

If you experience an extremely slow connection when you are trying to connect to a secure server, the problem could be related to the Web server, your computer, or your digital certificate.

The best thing to do is to disconnect and try again. You may have simply had a bad connection.

You can test connections to other secure Web sites to determine if the problem is related to a specific Web server.

To rule out problems related to your computer, verify your hardware connections, communication settings, and security settings.

Finally, view your certificate to make sure it is valid and make sure your Classic Client smart card/token is properly connected.

When I try to connect to a secure Web site that requests client authentication, I am rejected.

If your certificate is rejected, try again. If your certificate is rejected again it could be for one of the following reasons:

- The certificate is not valid. Check the validity of your certificate using the **Certificates** tool.
- The Web server does not have an entry for the Certificate Authority that issued and signed the certificate.
- Your smart card reader is not properly connected or you do not have the appropriate reader driver installed.
- Your digital signature is temporarily corrupt, as in the case of an intruder trying to spy on your secure connection.

I am not warned prior to entering a secure Web site.

You can tell a Web site is secure when its address starts with the characters **https**. If you want, you can set your browser to warn you before entering a secure Web site.

In Internet Explorer 7.0 or 8.0:

1. Click **Tools > Options** to open the **Internet Options** dialog box.
2. In the **Internet Options** dialog box, click the **Security** tab
3. Select a Web content zone to specify its security settings.
4. Click **Custom Level**.
5. Select **Prompt** under the actions for which you want to be warned.

In Firefox 3.0:

1. Click **Security** to open Firefox's security window.
2. Click **Navigator** on the left side of the window.
3. Select the options you want under **Show a warning before**.

e-Mail

I tried to send a secure e-mail but received a message that something was wrong with the recipient's certificate.

Check the validity of the user certificate. You may also want to contact the user directly to inquire about the status of their certificate. The user can always send a new signed message to you so that you can refresh or add the valid certificate.

I tried to send a secure e-mail but received a message that something was wrong with my certificate.

Check the following:

- Verify that a valid certificate is linked to your e-mail account.
- Use the **Certificates** tool to make sure the certificate you are using to send secure e-mail has not expired.

If the previous conditions are met and you still get the message that something is wrong with your certificate, contact your Certificate issuer for further assistance.

When I try to send secure e-mail, I get the message that there is no certificate associated with my e-mail account.

Before you can send secure e-mail using the digital certificate stored on your Classic Client smart card/token, you must link your certificate to your e-mail account.

When I try to send secure e-mail, I get a message that says I don't have a certificate for the person I'm trying to e-mail.

You could have one of three problems:

- **You do not have a certificate for this person** If you do not have a certificate for the user, you can add the user certificate by receiving a signed e-mail from the user or by obtaining the user's certificate from a public directory.
- **You do not have a certificate linked to the user's e-mail address** If you already received a signed e-mail from the user but the certificate is not associated with the user's e-mail address, you must open the signed e-mail and add the user's certificate to your Contacts folder (Outlook 2003). If you are using Mozilla Thunderbird, you should not encounter this problem because when you receive a signed message from a user, their digital certificate is automatically linked to their e-mail address.
- **The certificate that you have for this user is not valid** You can view the user certificate to determine if it is valid using your e-mail software.

The recipients of my e-mail cannot decrypt my messages or attached files.

Your contacts may not be able to decrypt the e-mail or attachments that you send to them because of the session key length specified in your browser. A session key is the cryptographic secret key that is used to encrypt the actual message text of your e-mail and attachments. (The RSA key pair is used to decrypt/encrypt the session key).

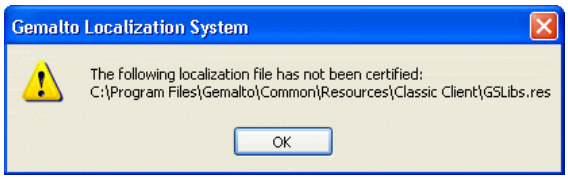
Until recently, Mozilla and Microsoft browsers and e-mail applications were subject to cryptographic export regulations. As such, if you were sending e-mail to international contacts outside of the United States and Canada, you could have been using a session key that was too long or too strong. The session key length limitation for all versions of Internet Explorer and Mozilla Firefox is 128-bits. For some countries, the limit used to be 40-bits for the international versions of both products.

In order to decrypt your e-mails, your recipients should be instructed to install Microsoft's High Encryption Package.

Localization Problems

Gemalto Localization System Warning Message

If the following warning message appears on your screen it is to inform you that the GSLibs.res file has been modified by someone else. There is no direct impact on the functionality of the software however, for details on how to remove this message from your screen you should contact Gemalto Support (see "Contact Our Hotline" on page ix).



Smart Card Reader Problems

When I start my computer, I get a message that the appropriate smart card reader driver is not installed.

Normally all the smart card reader drivers you will need are installed automatically when you install Classic Client.

If for some reason it appears you are missing a driver, then install it by running the Smart Diag Tool. Refer to “Diagnostic Tool” on page 23.

Note: If you do not have the Smart Diag Tool, download the corresponding driver from the Gemalto web site at: http://support.gemalto.com.

The LED on my smart card reader blinks while my smart card is in the reader.

Check if your Classic Client smart card is properly inserted into your reader. The smart card should be inserted such that the front of the smart card is facing the Gemalto logo on your smart card reader. You will not be able to see the microprocessor contact (the gold-plated area on the front of your Classic Client smart card) when your smart card is in the smart card reader.

Make sure that your smart card is firmly inserted. When the smart card is in the reader, the LED should remain lit.

Make sure that the smart card is supported and recognized by Classic Client Toolbox (see *Release Notes*).

The LED on my smart card reader does not blink nor does it stay on. There is no light.

If your smart card reader is properly installed and your Classic Client smart card is in the reader, the LED should show a steady green light. The LED should blink when the smart card is not in the reader.

Verify that your smart card reader is properly installed. Refer to instructions on the smart card reader box or this guide. The LED will not blink or remain on when your computer is off.

The rapid removal and re-insertion of a smart card/token causes problems.

If you quickly remove and re-insert a smart card/token the computer may “hang”. Whenever you remove or re-insert a smart card/token, be careful not to do it too quickly; wait until the computer finishes processing a task before removing the smart card/token.

Removing the smart card/token while the it is being read or written to may cause the application to interrupt the smart card/token session. During write operations, removing the smart card/token may even destroy data stored on the smart card/token.

Abbreviations

CA	Certificate Authority
CAPI	Crypto Application Program Interface
CMS	Card Management System
CSP	Cryptographic Service Provider
ECC	European Citizen Card
EEPROM	Electrically Erasable Programmable Read-only Memory
ID	Identification
IE	Internet Explorer
LED	Light Emitting Diode
PC/SC	Personal Computer/Smart Card Personal Computer to smart card. Entry point for all applications that use a smart card.
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKCS#11	Public Key Cryptography Standard **#11. For further information about this and other PKCS standards, refer to the RSA Laboratories web sit at http://www.rsa.com/rsalabs/**
PKI	Public Key Infrastructure
RSA	Rivest, Shamir, Adleman (inventors of public key cryptography standards)
S/MIME	Secure/Multipurpose Internet Mail Extensions
SO	Security Officer. The PIN Pad reader prompts for the SO PIN, which means the Admin PIN.
SSL	Secure Sockets Layer A protocol, v.3.0.v, for securing TCP/IP sessions
WinSCard	Microsoft PC/SC library which provides the smart card API (Application Programming Interface)

Glossary

Algorithm	A mathematical formula used to perform computations that can be used for security purposes.
Certificate	A certificate provides identification for secure transactions. It consists of a public key and other data, all of which have been digitally signed by a CA. It is a condition of access to secure e-mail or to secure Web sites.
Certificate Authority	An entity with the authority and methods to certify the identity of one or more parties in an exchange (an essential function in public key crypto systems).
Confirmation button	The button on a PIN pad reader that saves the data you have entered. It is often called **Enter**, or **Valid**, or **OK**. For example Gemalto's PC Pinpad readers have a green **Enter** button.
Cryptography	The science of transforming confidential information to make it unreadable to unauthorized parties.
Digital Signature	A data string produced using a Public Key Crypto system to prove the identity of the sender and the integrity of the message.
Encryption	A cryptographic procedure whereby a legible message is encrypted and made illegible to all but the holder of the appropriate cryptographic key.
Key	A value that is used with a cryptographic algorithm to encrypt, decrypt, or sign data. Secret key crypto systems use only one secret key. Public key crypto systems use a public key to encrypt data and a private key to decrypt data.
Key Length	The number of bits forming a key. The longer the key, the more secure the encryption. Government regulations limit the length of cryptographic keys.
Key Set	A key set in a smart card contains the following data objects: ■ Private key ■ Public key ■ Certificate ■ Descriptor
Public Key Crypto system	A cryptographic system that uses two different keys (public and private) for encrypting data. The most well-known public key algorithm is RSA.
S/MIME	A Standard offline message format for use in secure e-mail applications.
Splash screen	This is the picture that first appears when you start the Classic Client toolbox. This picture is currently the one with the man in the deck-chair that you will also find on the front cover of this document.
SSL	Secure Sockets Layer: A Security protocol used between servers and browsers for secure Web sessions.

SSL Handshake The SSL handshake, which takes place each time you start a secure Web session, identifies the server. This is automatically performed by your browser.

Token In a security context, a token is a hardware object like a smart card, but it could also be a pluggable software module designed to interact with a specific hardware module, such as a smart card. Token-based authentication provides enhanced security because success depends on a physical identifier (the smart card) and a personal identification number (PIN).