



GE Interlogix
CASI

***Contact Smart Card
Applications
Programmer
Operator's Guide
Version 2.0***

***GE Interlogix, CASI Division
791 Park of Commerce Boulevard
Suite 100
Boca Raton, Florida 33487
(561) 998-6100***

Part Number 460356001B
September 2002

The information in this manual is revised periodically. Revisions will be provided to the user in the form of addenda.

This publication may contain examples of data reports used in daily business operations. Examples include fictitious names of individuals and companies for illustration only; any similarity to names and addresses of actual business enterprises and persons is entirely coincidental.

This document is distributed on an *as is* basis, without warranty either expressed or implied. Successful implementation depends solely upon the customer's ability to integrate each program into the total inventory of "in-house" programs. While each offering has been reviewed for its transferability and maintainability, no assurance of successful installation can be given.

The customer accepts full maintenance responsibility. (A full scope of software and hardware maintenance contracts are available to the customer.)

Copyright 1998 - 2002 GE Interlogix
All Rights Reserved
Printed in the USA

GCR400, GCR410, and GEMPC410 are registered trademarks of Gemplus

Contents

Chapter 1: Using This Manual	1.1
Purpose.....	1.1
Who Should Read this Manual	1.1
Related Documentation.....	1.1
Notational Standards.....	1.2
Special Keys	1.2
Commands	1.2
Typeface Standards.....	1.2
Menu Titles.....	1.2
Push Buttons	1.2
Terminology.....	1.3
Click.....	1.3
Select.....	1.3
Press	1.3
Command.....	1.4
Chapter 2: System Overview	2.1
Introduction	2.1
Hardware Requirements.....	2.2
Software Requirements	2.3
Disabling the Hardware Device.....	2.3
Windows 2000.....	2.3
Windows 98.....	2.7
Chapter 3: Installation and Removal.....	3.1
Software Installation.....	3.1
Removal.....	3.2

Chapter 4: System Administrator4.1

Configuration and Setup.....	4.1
Getting Started.....	4.2
Passwords.....	4.3
Console Password	4.3
System Administrator Password ...	4.5
Change the Encrypted Console Password	4.6
Create a Setup Card	4.8
Change the Issuer Key.....	4.9
Update the Master P.I.N.....	4.10
Change the Starting Badge Number.	4.11

Chapter 5: Security Personnel5.1

Using the Contact Smart Card Programmer	5.1
Getting Started.....	5.1
Logging On	5.3
Programming a New Badge	5.5
Resetting/Changing a P.I.N.	5.6
Exiting the Program.....	5.8

Purpose

This manual provides instructions for installation of the **Contact Smart Card Applications Programmer (SAP)**, initial setup and configuration. Information for operating the system once it is installed is also included.

Who Should Read this Manual

This manual is intended for system administrators who are responsible for the planning and implementation of the system design, and who perform system configuration and setup.

Operators using the system should read the chapters which relate to their duties.




The material in this manual has been prepared for persons responsible for, and familiar with the security needs of the customer facility.

Related Documentation

- *Models 820/825 Contact Smart Card Reader Installation Guide*
This manual provides information for the system administrator to set up, configure, and manage the CASI Models 820 and 825 Contact Smart Card Readers.

Notational Standards

Special Keys



Keyboard keys appear as graphics. For example,  denotes the key labeled “Enter” or “Return”. , , etc., indicate the function keys across the top of the keyboard.


Keys that display on the screen as push buttons appear in bold. For example, **Quit**, **Save**, **View**, **New**, **Find**, **Ok**, **Close**.

Commands

Examples of commands show the exact spacing and upper- or lower-case letter for you to type. For example:

`rc.pperf -K`

If an example ends with , type the command then press . For example:

`rc.pperf -K `

Typeface Standards

Menu Titles

The titles of menus, submenus, forms, form boxes, picklists, and pop-ups appear in bold. For example, the **Site Config** form, the **Communications Options** picklist.

Push Buttons

The names of push-buttons on forms and picklists appear in bold. For example, **Quit**, **Save**, **View**, **New**, **Find**, **Ok**, **Close**.

Terminology

Click

To “click” means to press and release a mouse button while the pointer is on a designated area of the screen in order to display a window or select an option. The press-and-release makes a clicking sound.


The term “double-click” means to press and release a mouse button twice in rapid succession. “Left-click” and “right-click” mean to click the button on the left or right side of the mouse.

Select




The word “select” indicates that you choose an item from the current menu, submenu, form, or picklist displayed on the screen. Use the mouse or the cursor keys to select the item. For example:

Select **Next 11 Digit Badge Number**, then select a P.I.N.

The statement above tells you to select a certain submenu and then to select a certain item from that submenu. If you make the selections with a mouse, you will point to the main menu and click the left mouse button. When the submenu appears, you will point and click the desired item to select it.

If you make the selections with a keyboard, you will use the cursor keys instead of a mouse pointer, and the  key instead of the left mouse button.

Press

The phrase “press the ____ button” means to use the mouse (or the keyboard) to “press” a designated button on the screen. To press a button with the mouse, point then click the left button. To press a button with the keyboard, use the  key and press  or .

Command

The word “command” indicates a command which would be typed as specified.

Introduction

The Contact Smart Card Applications Programmer is designed to program badges used with the CASI Model 820/825 Contact Smart Card Readers. This program allows the system administrator to easily control badge security by means of passwords, an Issuer Key and a Setup Card.

Your Contact Smart Card Applications Programmer package includes:

- a GCR400, GCR410 or GEMPC410 Reader and related hardware
- two diskettes to install the software on your PC
- Contact Smart Card Applications Programmer Operator's Guide

The Contact Smart Card Applications Programmer supports operations in a Windows 95, 98, 2000, or NT environment where the PC is connected to a GCR400, GCR410, or GEMPC410 programmer by means of an RS-232 cable. This allows the physical connection of the reader to the host PC.

NOTE

Diskettes should be kept in a secure location before and after installation.



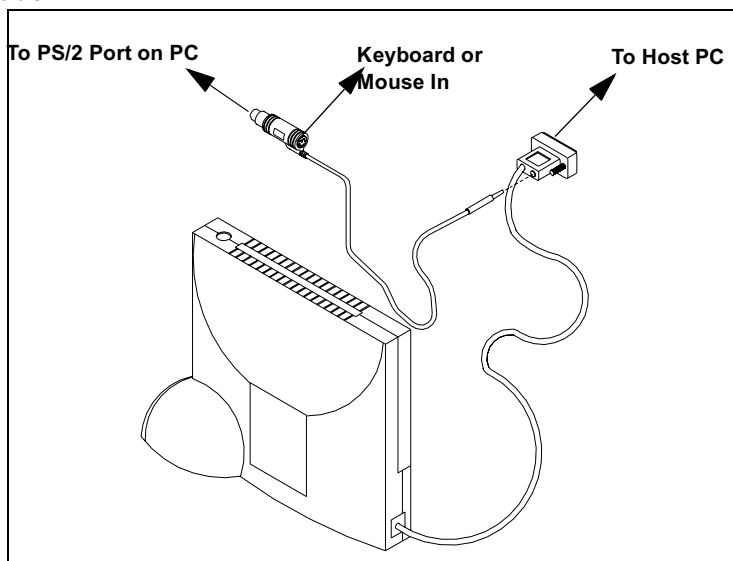
Hardware Requirements

For the Contact Smart Card Programmer System:

- a Windows compatible PC
- a GCR400, GCR410, or GEMPC410 Reader

Refer to Figure 1, below, for an overview of the hardware connections between the Contact Smart Card Applications Programmer host PC and the GCR400, GCR410, or GEMPC410 Reader.

FIGURE 1: Overview of the Host PC and the GCR or GEMPC Reader



1. Connect the reader to the serial port of your PC by means of the DB9 serial connector as shown.
2. Connect the PS/2 connector to the PS/2 port on your PC and then connect your mouse or keyboard into the PS/2 connector, as shown.
3. Reboot your PC.

2.2 Contact Smart Card Applications Programmer

Software Requirements

- Contact Smart Card Applications Programmer Model 82P Version 2.0
- Windows 95, 98, 2000, or NT operating system

NOTE

If using the Gemplus GEMPC410 Contact Smart Card Programmer with Windows 98, 98SE, or Windows 2000, you will need to disable the hardware device.

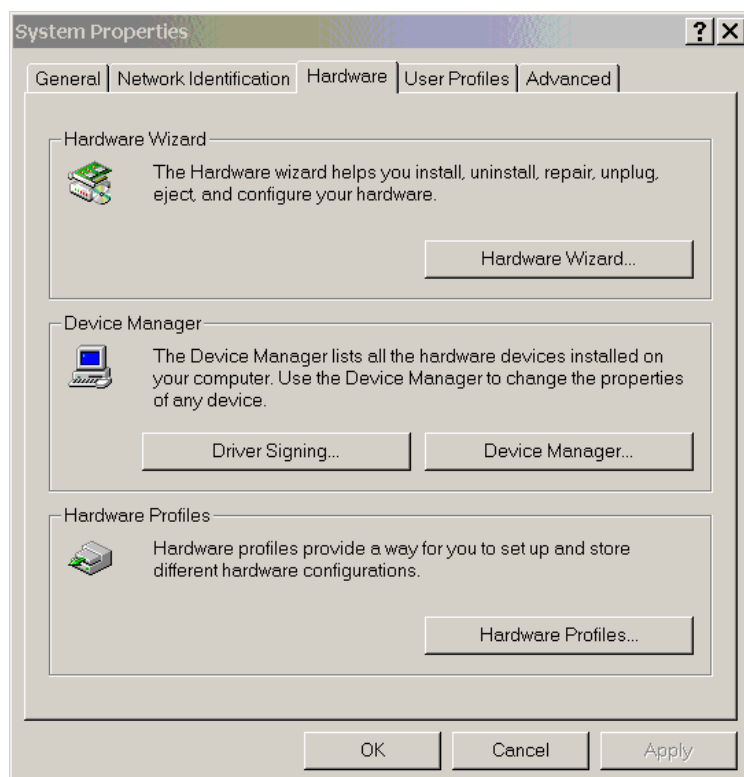
See “Windows 2000” on page 2.3.

See “Windows 98” on page 2.7.

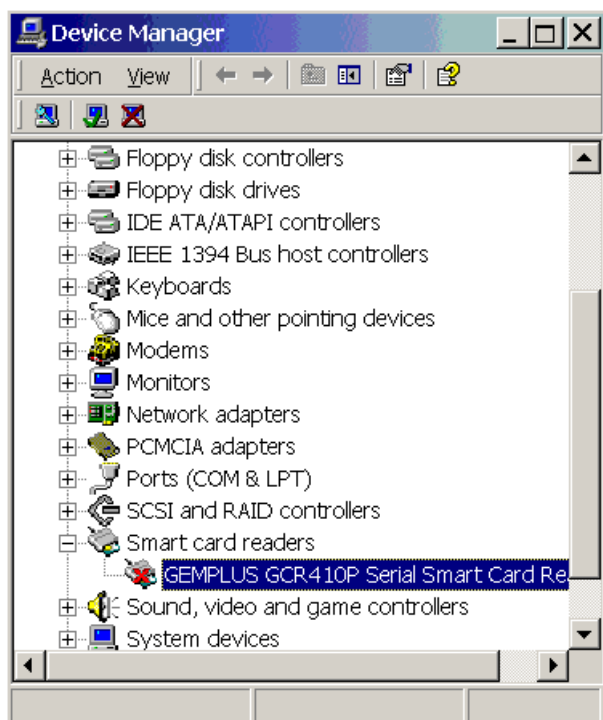
Disabling the Hardware Device

Windows 2000

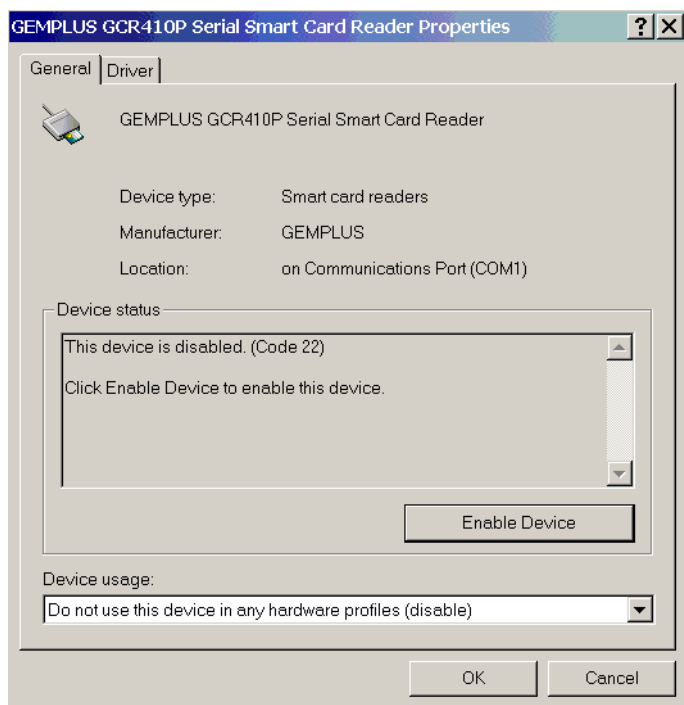
1. From the **Control Panel**, select **System**, then the **Hardware Tab**.
2. Press the button labeled **Device Manager**.



3. From the resulting list, double click on the **Gemplus Contact Smart Card Programmer**.



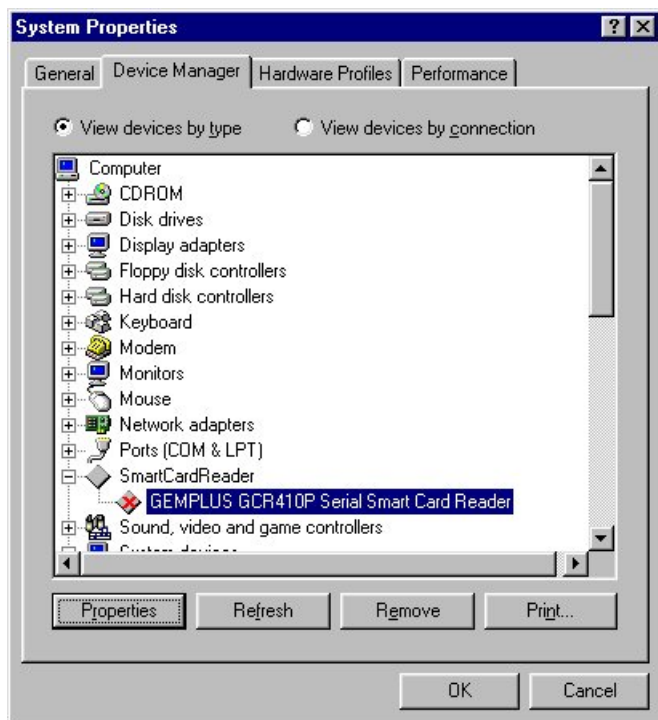
4. From the **General Tab**, click on the down arrow labeled **Device usage**.



5. Select the option **Do not use this device in the current hardware profile (disable)**
6. Click on **OK**.
7. Reboot the PC.

Windows 98

1. From the **Control Panel**, select **System Properties**, then the **Device Manager Tab**.



2. Highlight the **Gemplus Contact Smart Card Programmer** and press the button labeled **Properties**.

3. From the resulting **General Tab**, under **Device usage**, check the option: **Disable in this hardware profile**



4. Click on **OK**.
5. Reboot the PC.

Installation and Removal

Software Installation

The Contact Smart Card Applications Programmer is supplied on diskettes. These diskettes should be kept in a secure location before and after installation.

► **To install the Contact Smart Card Applications Programmer Software on a Windows 95, 98, 2000, or NT operating system:**

1. Retrieve the Contact Smart Card Applications Programmer Model 82P diskettes from their secure location.

2. Insert Disk 1 of 2 into drive A:

3. Click on **Start**, then **Run**.

Result: The **Run** window appears.

4. In the **Open** box, type **a:\setup** and press **OK**.

Result: The **Installation** window appears.

5. Return the Contact Smart Card Applications Programmer Model 82P diskettes to their secure location.

6. Follow the installation prompts. Accept the defaults or customize as desired.

Result: Files are copied from the diskettes to your hard drive and the program is installed. A program group named **CASI-RUSCO Model 82P** will appear under **Start/Programs**.

Removal

► **To Remove the Contact Smart Card Applications Programmer Software:**

1. From the **CASI-RUSCO Model 82P** Program group, select the **Uninstall** option.

Result: An **Open** window appears.

2. Verify that the `install.log` file is highlighted in this window. Click on **OK**.

Result: The **Select Uninstall Method** window appears.

3. Select **Automatic** for the default uninstall options and click **Next** to continue.

Result: The **Perform Uninstall** window appears.

4. Click **Finish** to remove the program.

System Administrator

Configuration and Setup

The Contact Smart Card Applications Programmer system allows the System Administrator to manage and control the security of Contact Smart Card badges. Prior to using the system, the following setup and configuration is required:

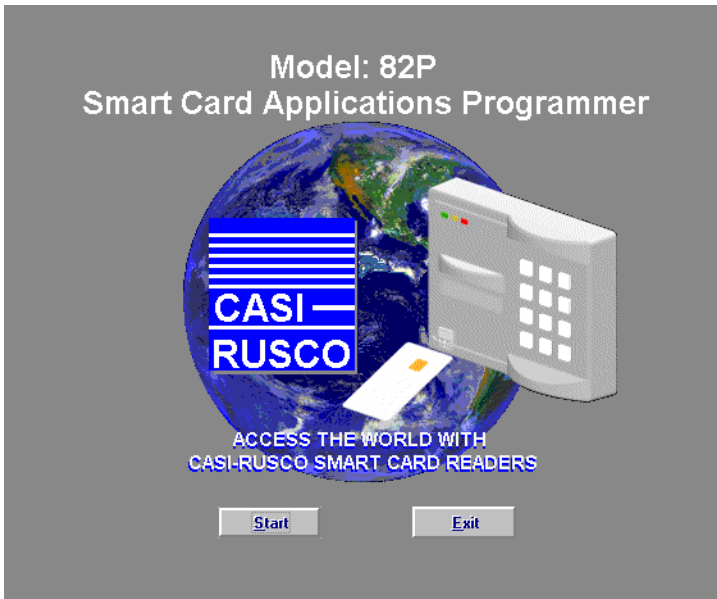
- Change the encrypted Console Password
- Set up the System Administrator's Password
- Create a Setup Card
- Change the Issuer Key
- Update the Master P.I.N.
- Change the Starting Badge Number

These items are detailed in the following sections.

Getting Started

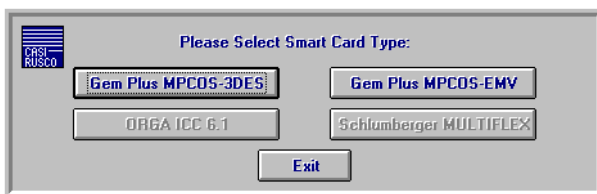
► To launch the Contact Smart Card Application Programmer on a Windows 95, 98, 2000, or NT operating system:

1. Click on **Start, Programs, Casi-Rusco Model 82P, then Sap.**



2. Press **Start**.

Result: The selection window below appears.



3. Press **Gem Plus MPCOS-3DES**, or **Gem Plus MPCOS-EMV** to continue or **Exit** to exit the program.

4.2 Contact Smart Card Applications Programmer

Passwords

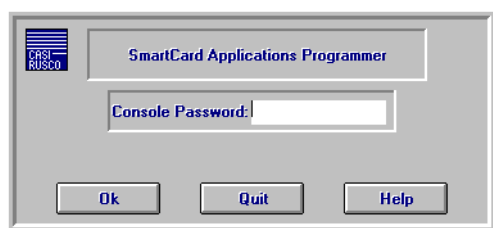
CASI-RUSCO designed the Contact Smart Card Applications Programmer software to be as secure as the Models 820/825 Contact Smart Card Readers. Security starts at the console; therefore, all passwords are stored on your hard drive as encrypted files using the United States Government Standards for Encryption DES or Triple DES, along with the ABA's Standard for encryption MAC. The System Administrator has the ability to change the console passwords.

NOTE



For the Gemplus MPCOS-3DES card, DES or 16 bit encryption is used. For the Gemplus MPCOS-EMV card, triple DES or 128 bit encryption is used.

Console Password



► To enter the Console Password:

1. Enter the **Console Password** provided with your system. **CASI-SAP** is the default. All characters entered are echoed back in the form of an * character to prevent anyone from seeing what you are typing.

NOTE

All passwords are 1 - 8 characters. They are not case sensitive.



If your are using a laptop, make sure that **NUMLOCK** is turned off.

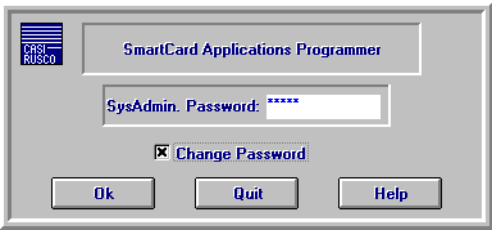
2. Click **OK** or press the  key.

Result: If the password was incorrect, you will be prompted to enter a password again. All attempts (correct or incorrect) are recorded in a log file. If the password was correct, the following window will appear.



3. Press **SysAdmin** to continue or **Exit** to exit the program.

Result: If you elected to continue, the following screen will appear.



System Administrator Password


➤ To enter the System Administrator password:

1. Enter the **SysAdmin** password provided with your system (**sapit** is the default). All characters entered are echoed back in the form of an * character to prevent anyone from seeing what you are typing.

NOTE


All passwords are 1 - 8 characters. They are not case sensitive.

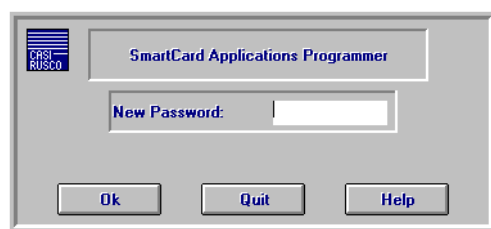


2. Click **OK** or press the  key.

Result: If the password was incorrect, you will be prompted to enter a password again. All attempts (correct or incorrect) are recorded in a log file. If the password was correct, the **System Administrator** window will appear.

➤ To change the System Administrator Password:


1. Type the default or current password.
2. Click **Change Password**, then press  or click **OK**. You will be prompted for a new password.



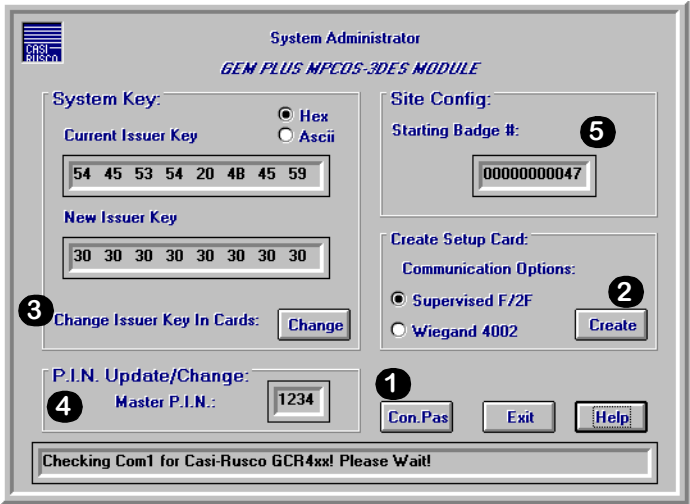
3. Enter your new password and press **Enter** or click **OK**.

NOTE

All passwords are 1 - 8 characters. They are not case sensitive.



Result: A screen, similar to the following, will appear:



❶ Change the Encrypted Console Password

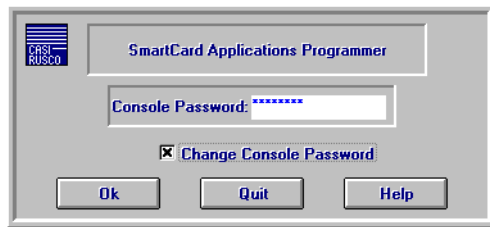
The System Administrator has the capability of changing the encrypted Console Password from the **System Administrator** screen shown on page 4.6

1. Access the **System Administrator** screen.

NOTE

If this is the initial setup of the system, you will need to complete the section, “System Administrator Password” on page 4.5 prior to continuing.

2. Click the **Con.Pas** button and the following window will display.



3. Type the default or current **Console Password**.
4. Click **Change Password**, then press **Enter** or click **OK**. You will be prompted for a **New Password**.
5. Type in your new password and press **Enter** or click **OK**.

NOTE

If you forget the Console Password once you change it, you must reinstall the program in order to restore the default password. Any existing data files will not be affected.

② Create a Setup Card

The Model 820 and 825 Contact Smart Card Readers require a single Setup Card to be inserted at the time of installation. The Setup Card transports an encrypted key to the internal processor located inside the Reader(s). Once the encrypted key is installed, the processor will decrypt the encrypted key and check the validity of the Setup Card being used to update the Reader(s). If found to be an invalid Setup Card (the key does not match that of the reader), the transported key will be destroyed and the reader will go into an error mode. If the Setup Card validates, the now decrypted key is stored in a protected bank of EEPROM internal to the processor.

CAUTION

If the reader is ever tampered with, the key will be destroyed, taking that reader out of service.



➤ To create a Setup Card:

1. Depending on your initial choice of Smart Card type, insert a blank Gemplus MPCOS-3DES or Gemplus MPCOS-EMV Contact Smart Card into the GCR400, GCR410 or GEMPC410 Reader.
2. Click the **Change** button. The Issuer key has now been changed on this Setup Card and is reflected in the **Current Issuer Key** box.
3. Select your **Communication** options and then click the **Create** button.
4. Remove the now programmed Setup Card from the reader and store in a secure location.

NOTE



All badges created after this session should be created using the same Issuer Key that was just installed into the Setup Card. See “Change the Issuer Key” on page 4.9

③ Change the Issuer Key

When Gemplus MPCOS-3DES or MPCOS-EMV Contact Smart Cards are shipped, they carry a pre-installed Issuer Key. This must be changed to match the Issuer Key in the Reader. The **Contact Smart Card Applications Programmer** provides methods to change the Issuer Key or update the badges to match your existing Issuer Key.



NOTE

For the Gemplus MPCOS-3DES card, the Issuer Key consists of 8 ASCII characters. For the Gemplus MPCOS-EMV card, the Issuer Key consists of 16 ASCII characters.

The process described below must be performed for all badges when they are received from Gemplus. If you attempt to program a badge whose issuer key does not match that of the reader, you will receive an error message similar to the following:

Warning! Key does not match issuer key.

➤ **To change the Issuer Key in Hex format:**

1. Click **Hex** to display Hex format.
2. Position your mouse to the far left of the **New Issuer Key** display box and click.
3. Using the  key, delete the first two digits.
4. Enter two new digits.
5. Use the  key to move right to the next two digits and repeat steps 2 through 4 until finished.

➤ **To change the Issuer Key in ASCII format:**

1. Click **ASCII** to display in normal characters.
2. Position your mouse in the **New Issuer Key** display box and


highlight the character(s) to be changed. Type the new information. This field is restricted to:

- 8 characters, in the case of a Gemplus MPCOS-3DES
 - 16 characters, in the case of a Gemplus MPCOS-EMV
- and cannot end with a space.

④ Update the Master P.I.N.

The master Personal Identification Number (P.I.N.) should only be changed one time. This P.I.N. will be used by the Contact Smart Card Applications Programmer to allow Security Officers to perform normal P.I.N. changes as well as to change the P.I.N. codes in badges that have been blocked.

► To change the P.I.N.:

1. Point your mouse to the far left of the **Master P.I.N.** display box and click.
2. Using the  key, delete all four numbers.
3. Enter your new **Master P.I.N.** consisting of four new numbers.

NOTE The above field requires all four digits.




4. Click on the **Exit** button to save your change.

NOTE All changes will be saved by clicking on the Exit button.



⑤ Change the Starting Badge Number

► To change the Starting Badge Number:

1. Click in the **Starting Badge #**: display box.
2. Using the  key, delete all eleven digits.
3. Enter your new **Starting Badge #** consisting of eleven new numbers.

NOTE

The above field requires all eleven digits.



4. Press the **Exit** button.

NOTE

All changes will be saved by clicking on the Exit button.



NOTES

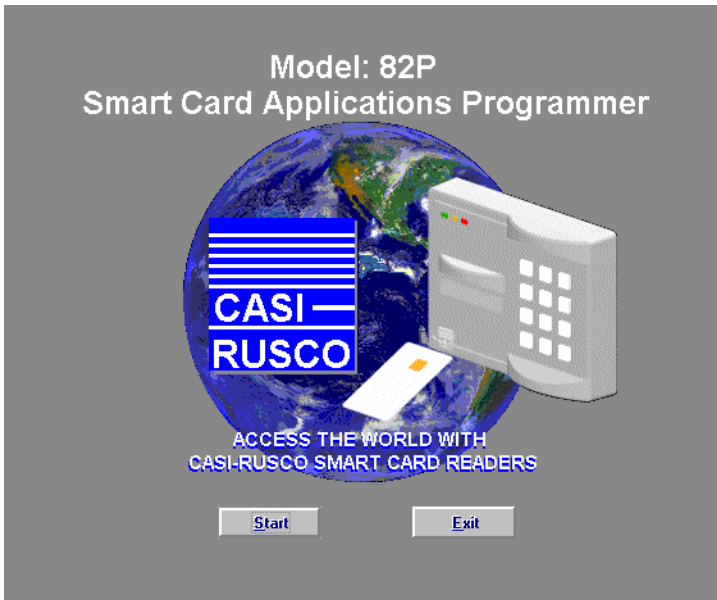
Using the Contact Smart Card Programmer

The Contact Smart Card Applications Programmer system allows Security Personnel to program badges and Personal Identification Numbers (P.I.N.).

Getting Started

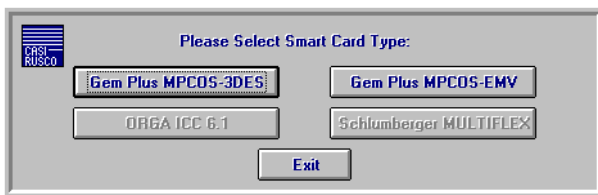
To launch the Contact Smart Card Applications Programmer on a Windows 95, 98, 2000, or NT operating system:

1. Click on **Start, Programs, Casi-Rusco Model 82P**, then **Sap**.



2. Press **Start**.

Result: The selection window below appears.

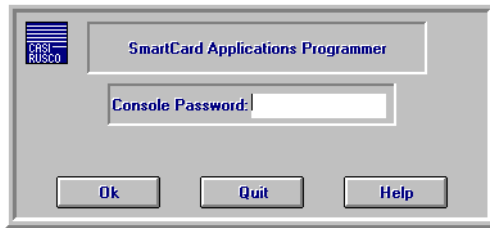


3. Press **Gem Plus MPCOS-3DES** or **Gem Plus MPCOS-EMV** to continue or **Exit** to exit the program.

5.2 Contact Smart Card Applications Programmer

Logging On

To enter the Console Password:



1. Enter the **Console Password** provided by your System Administrator. All characters entered are echoed back in the form of an * character to prevent anyone from seeing what you are typing.

NOTE

All passwords are 1 - 8 digits. They are not case-sensitive.




2. Click **OK** or press the **Enter** key.

Result: If the password was wrong, you will be prompted to enter it again. All attempts (correct or incorrect) are recorded in a log file. If the password was correct, the following window will appear.



3. Press **SecPersonnel** to continue or **Exit** to exit the program.

Result: If you elected to continue, the following screen will appear.



Security Personnel Menu
GEN PLUS MPC05-3DES MODULE

5

PIN

Reset/Change P.I.N.

4

Prog.

Create Badge(s).

6

Exit

Help

☒ Use Next 11 Digit Badge Number: 1

☐ Custom 11 Digit Badge Number:

☒ Custom 4 Digit P.I.N. Code: 2

☐ Random 4 Digit P.I.N. Code:

3

Badge Holder's Name:

Menu/Results

Please insert Badge and update all fields!

Programming a New Badge

Programming a new badge requires a badge that has an Issuer Key chosen by your System Administrator already programmed into it.

To create a new badge:

1. Insert a badge into a GCR400, GCR410 or GEMPC410 Reader.
- ❶ 2. Select either **Next 11 Digit Badge Number** or **Custom 11 Digit Badge Number**.
 - If you selected **Next 11 Digit Badge Number**, proceed with the next step.
 - If you selected **Custom 11 Digit Badge Number**, click in the box on the right. Enter an 11 digit number for the new badge number.

NOTE

The Custom 11 digit Badge Number field requires exactly 11 digits in the range of (0-9).



- ❷ 3. Select either **Custom 4 Digit P.I.N.** or **Random 4 Digit P.I.N.**.
 - If you selected **Custom 4 Digit P.I.N.**, click in the box on the right. Enter a 4 digit number for the new P.I.N.

NOTE

The custom P.I.N. field requires exactly 4 digits in the range of (0-9).



- If you selected **Random 4 Digit P.I.N.**, a 4 digit P.I.N. will appear in the display box.
- ❸ 4. Type the badge holder's name in the **Badge Holder's Name** display box.
 - ❹ 5. Click the **Prog** button. The results will be displayed in the **Menu/Results** display box in the lower section of your window.

NOTE Badges can only be programmed once.



Resetting/Changing a P.I.N.

This feature is used by Security Personnel to change the P.I.N. or un-block a badge that has been blocked by the Model 825 Reader. A new P.I.N. number may be required when an unauthorized person has gained access to the number. A badge can be blocked when multiple access attempts have been made using an incorrect P.I.N.. After verifying the badgeholder's access rights, to unblock the badge you may either reset the old P.I.N. number or change it to a new number.

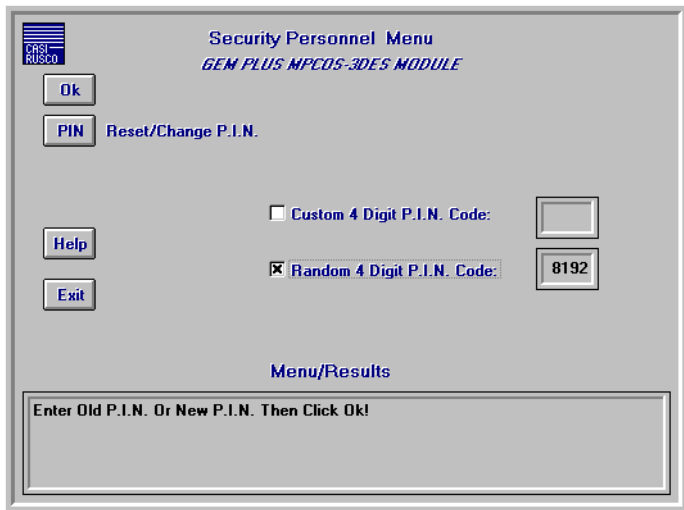
► **To reset or change a P.I.N.:**

- 5 1. Insert the badge into a GCR400, GCR410, or GEMPC410 Reader and click the **PIN** button.

Result: The following screen appears:

The screenshot shows a dialog box titled "Security Personnel Menu" with the subtitle "GEM PLUS MPCOS-3DES MODULE". On the left side, there are four buttons: "Ok", "PIN", "Help", and "Exit". The "PIN" button is highlighted, and next to it is the text "Reset/Change P.I.N.". In the center, there are two options: "Custom 4 Digit P.I.N. Code:" with a checked checkbox and an empty text box, and "Random 4 Digit P.I.N. Code:" with an unchecked checkbox and an empty text box. At the bottom, there is a section titled "Menu/Results" containing a text box with the instruction "Enter Old P.I.N. Or New P.I.N. Then Click Ok!".

2. To reset the original P.I.N. number, select **Custom 4 Digit P.I.N.**, click in the box on the right and enter the original 4 digit P.I.N. number.
3. To change the P.I.N. to a new number, choose one of the following methods:
 - If you select **Custom 4 digit P.I.N. Code**, click in the box on the right. Enter a 4 digit number for the new P.I.N.
 - If you select **Random 4 Digit P.I.N. Code**, a 4 digit P.I.N. will appear in the **Random 4 Digit** display box.



4. Click the **OK** button located in the upper left of your window. You will see the results in the **Menu/Results** display box located at the bottom of the window.
5. Once the P.I.N. has been changed, remove the badge from the GCR400, GCR410, or GEMPC410 Reader.

Exiting the Program

- 6 Click on **Exit** to exit the program.