IBM Smart Card Security Kit

OPTIONS
by IBM

User Reference Manual

Software for Windows NT 4.0
Version 2.0

Copyright

Patents

The public key technology referred to in this guide (RSA), is licensed exclusively by RSA Data Security, Inc., a Security Dynamics Company, US Patent No 4,405,829.

Smart Cards and Smart Card Readers are patent protected by INNOVATRON and produced by GEMPLUS under license.

Patented by Bull CP8 - Patented by Innovatron.

Other patents are held by Gemplus.

Trademarks

Security Dynamics, the Security Dynamics logo, ACE, ACE/Server, SecurID, SoftID, and WebID are registered trademarks, and ACE/Agent, ACE/Sentry, Comcryption, Concryption, PASSCODE, PINPAD, SecurID Protected, SecurID Ready, SecurESS, SecurPC, SecurSight, SecurSSO, and SecurVPN are trademarks, of Security Dynamics Technologies, Inc.

RC4 is a registered trademark; and, RSA SecurPC, RSA Emergency Access, and AutoCrypt are trademarks of RSA Data Security, Inc., a Security Dynamics Company.

Microsoft, MS, and MS-DOS are registered trademarks; and, Internet Explorer, Windows, Windows NT, Windows for Workgroups, and Windows 95 are trademarks of Microsoft Corporation.

Adobe and Adobe Acrobat Reader are registered trademarks of Adobe Systems Incorporated.

Netscape Navigator is a trademark of Netscape Communications.

All other products or services mentioned in this document are covered by the trademarks, service marks, or product names as designated by the companies who own or market them.

Software Version 2.0 for Windows NT 4.0.
Document Version: DAURM20P

other countries, and the information is subject to change without notice. Consult your local IBM representative for information on the products, services, and features available in your area.

It is possible that this publication may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM products, programming, or services in your country.

Requests for copies of this publication and for technical information about IBM Personal Computer products should be made to your IBM authorized reseller or IBM marketing representative

Product Warranty and Notices

The following warranty information applies to products purchased in the United States, Canada, and Puerto Rico. For warranty terms and conditions for products purchased in other countries, see the enclosed Warranty insert, or contact your IBM reseller or IBM marketing representative.

International Business Machines Corporation   Armonk, New York, 10504

Statement of Limited Warranty

The warranties provided by IBM in this Statement of Limited Warranty apply only to Machines you originally purchase for your use, and not for resale, from IBM or your reseller. The term "Machine" means an IBM machine, its features, conversions, upgrades, elements, or accessories, or any combination of them. Unless IBM specifies otherwise, the following warranties apply only in the country where you acquire the Machine. If you have any questions, contact IBM or your reseller.

      Machine: Smart Card Security Kit
      Warranty Period * : 1 Year

      * Contact your place of purchase for warranty service information.

Production Status

Each Machine is manufactured from new parts, or new and used parts. In some cases, the Machine may not be new and may have been previously installed. Regardless of the Machine's production status, IBM's warranty terms apply.

The IBM Warranty for Machines

IBM warrants that each Machine 1) is free from defects in materials and workmanship and 2) conforms to IBM's Official Published Specifications. The warranty period for a Machine is a specified, fixed period commencing on its Date of Installation. The date on your receipt is the Date of Installation, unless IBM or your reseller informs you otherwise.

During the warranty period IBM or your reseller, if authorized by IBM, will provide warranty service under the type of service designated for the Machine and will manage and install engineering changes that apply to the Machine.

For IBM or your reseller to provide warranty service for a feature, conversion, or upgrade, IBM or your reseller may require that the Machine on which it is installed be 1) for certain Machines, the designated, serial-numbered Machine and 2) at an engineering-change level compatible with the feature, conversion, or upgrade. Many of these transactions involve the removal of parts and their return to IBM. You represent that all removed parts are genuine and unaltered. A part that replaces a removed part will assume the warranty service status of the replaced part.

If a Machine does not function as warranted during the warranty period, IBM or your reseller will repair it or replace it with one that is at least functionally equivalent, without charge. The replacement may not be new, but will be in good working order. If IBM or your reseller is unable to repair or replace the Machine, you may return it to your place of purchase and your money will be refunded.

If you transfer a Machine to another user, warranty service is available to that user for the remainder of the warranty period. You should give your proof of purchase and this Statement to that user. However, for Machines which have a life-time warranty, this warranty is not transferable.

Warranty Service

To obtain warranty service for the Machine, you should contact your reseller or call IBM. In the United States, call IBM at **1-800-772-2227**. In Canada, call IBM at **1-800-565-3344**. You may be required to present proof of purchase.

IBM or your reseller will provide certain types of repair and exchange service, either at your location or at IBM's or your reseller's service center, to restore a Machine to good working order.   Types of service may vary from country to country. IBM or your reseller will inform you of the available types of service for a Machine based on its country of installation.

When a type of service involves the exchange of a Machine or part, the item IBM or your reseller replaces becomes its property and the replacement becomes yours. You represent that all removed items are genuine and unaltered. The replacement may not be new, but will be in good working order and at least functionally equivalent to the item replaced. The replacement assumes the warranty service status of the replaced item. Before IBM or your reseller exchanges a Machine or part, you agree to remove all features, parts, options, alterations, and attachments not under warranty service. You also agree to ensure that the Machine is free of any legal obligations or restrictions that prevent its exchange.

You agree to:

1.   obtain authorization from the owner to have IBM or your reseller service a Machine that you do not own; and

2.   where applicable, before service is provided -

      a.   follow the problem determination, problem analysis, and service request procedures that IBM or your reseller provide,
      b.   secure all programs, data, and funds contained in a Machine, and
      c.   inform IBM or your reseller of changes in a Machine's location.

IBM is responsible for loss of, or damage to, your Machine while it is 1) in IBM's possession or 2) in transit in those cases where IBM is responsible for the transportation charges.

Extent of Warranty

IBM does not warrant uninterrupted or error-free operation of a Machine.

The warranties may be voided by misuse, accident, modification, unsuitable physical or operating environment, improper maintenance by you, removal or alteration of Machine or parts identification labels, or failure caused by a product for which IBM is not responsible.

THESE WARRANTIES REPLACE ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.   THESE WARRANTIES GIVE YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF EXPRESS OR IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU. IN THAT EVENT SUCH WARRANTIES ARE LIMITED IN DURATION TO THE WARRANTY PERIOD. NO WARRANTIES APPLY AFTER THAT PERIOD.

Limitation of Liability

Circumstances may arise where, because of a default on IBM's part or other liability you are entitled to recover damages from IBM. In each such instance, regardless of the basis on which you are entitled to claim damages from IBM (including fundamental breach, negligence, misrepresentation, or other contract or tort claim), IBM is liable only for:

1. damages for bodily injury (including death) and damage to real property and tangible personal property; and
2. the amount of any other actual direct damages or loss, up to the greater of U.S. $100,000 or the charges (if recurring, 12 months' charges apply) for the Machine that is the subject of the claim.

UNDER NO CIRCUMSTANCES IS IBM LIABLE FOR ANY OF THE FOLLOWING:
1) THIRD-PARTY CLAIMS AGAINST YOU FOR LOSSES OR DAMAGES (OTHER THAN THOSE UNDER THE FIRST ITEM LISTED ABOVE);
2) LOSS OF, OR DAMAGE TO, YOUR RECORDS OR DATA; OR
3) SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), EVEN IF IBM OR YOUR RESELLER IS INFORMED OF THEIR POSSIBILITY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU.

Trademarks

IBM is a registered trademark of International Business Machines Corporation.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

Contents

Preface

This User Reference Manual contains instructions for installation, setup, use and de-installation of the IBM® Smart Card Security Kit hardware and software for Microsoft® Windows® NT 4.0. The CD-ROM disk contains an Administrator Reference Manual and a User Reference Manual in a format that can be viewed on-line or printed for off-line reading. Before installing your Smart Card Security Kit, please read this User Reference Manual and become familiar with its contents. Refer to the README.TXT file on the software CD for last-minute information not appearing in the manuals.

The Smart Card Security software (SCsecurity) is structured to allow diskettes to be made from the software CD for those who do not have a CD-ROM drive in their system. Diskettes can be generated from within the Install utility by clicking on the **Make Diskettes** button.

The IBM Smart Card Security Kit's setup is a two-step process. First, the administrator customizes the IBM Smart Card Security Kit software for implementation. The administrator should review the Administrator Reference Manual for a complete understanding of the options available to the administrator.

The user then sets up the individual aspects of the software, such as the encryption options.

NOTE: You will be prompted to enter a Personal Identification Number during the installation of the Smart Card Security Kit. The preset or default User Personal Identification Number (PIN) and Administrator PIN for all smart cards is 1234. However, you must replace the user PIN with another PIN of your choice during the installation.

Introduction

The IBM Smart Card Security Kit provides fast and easy security for your computer. It provides single user authorization by requiring that the smart card be inserted into the smart card reader and that your Personal Identification Number (PIN) be authenticated by the smart card.

It also ensures the privacy of files stored on the computer's hard drive. The IBM Smart Card Security Kit enables the user to encrypt one file, a group of files, or all the files in a folder, with the user's smart card. Even when a file is encrypted, the user can follow familiar Windows NT 4.0 procedures. For example, double-clicking on a file launches any associated application and opens the file, as usual. The file automatically decrypts while opening, and re-encrypts upon closing. In addition, all encrypted files are available from the File | Open menu option of Windows NT 4.0 applications. Files on hard drives, mapped network folders, and removable disks can be encrypted.

The IBM Smart Card Security Kit's AutoCrypt feature works behind the scenes. When the user adds a folder to the AutoCrypt List, the folder's contents are automatically encrypted. The IBM Smart Card Security Kit automatically decrypts and re-encrypts files as the user opens and closes them. AutoCrypt folders are distinguished with a locked folder icon.

An emergency access key unlocks encrypted files when the user's smart card is inaccessible. For additional security and to protect the user's privacy, an organization can choose to split the Emergency Access key into parts. Different people (referred to as "trustees") hold a part of the key file. While each trustee holds a key file, only a specified portion of the total number of trustee key files are required to decrypt user files.

The IBM Smart Card Security Kit enables secure file sharing by encrypting files with sharable passphrases. These encrypted files can be shared with any Windows 95/98, Windows 3.1, or Windows NT user, with or without the IBM Smart Card Security Kit installed.

The setup of the IBM Smart Card Security Kit is a two-step process. The administrator customizes the Smart Card Security Kit for implementation. Then, the user sets up the encryption software. This User Reference Manual takes you through the process, step-by-step.

IBM Smart Card Security Kit complies with the following applicable industry standards:

ISO 7816-1, -2, -3, 4 (Smart Card), ISO 7811-1 (Embossed Card)

T=0 and T=1 Smart Card Protocol

Type II PC Card (PC Card Standard, dated 3/97)

Version 2.1 PCMCIA Interface Software (Card & Services)

Microsoft PC/SC 1.0

Open Card Framework

PCCS #11 and CAPI

X.509 Digital Certificates

EIA/TIA-232 Serial Port

PS/2 Compatible Keyboard Port

Document Conventions

As you begin using this documentation, note the following typographical conventions.

- Key names are in small capital letters. For example:

    Type the user's name and press ENTER.

    When you are instructed to press ENTER, pressing RETURN will have the same effect.

- Information an administrator enters is shown in a monospace, boldfaced type. Information an administrator enters that varies is shown in italic boldfaced type. When typing a command, enter the information the italicized words represent, not the words themselves. For example:

    ***drive letter*:\setup** (enter **d:\setup**, if the drive letter is d:)

- References in the text to the Smart Card Security Kit file names are shown in bold type. For example:

    Select the **setup.exe** file from the IBM Smart Card Security Kit folder.

- Options in dialog boxes are shown in bold type. For example:

    Select the **Encrypt as <u>self-extracting Windows file (.exe)</u>** check box.

- Menu options in the application are shown in bold type. For example:

    Select **Use <u>S</u>mart Card Key** from the **<u>E</u>ncrypt** contextual menu.

- Field, button, and checkbox labels are shown in bold type. For example:

    Enter the user name in the **<u>N</u>ame** field and click **OK**.

The terminology used in this User Reference Manual appears in the Glossary starting on page 58.

IMPORTANT: Notes, cautions and other important information are enclosed by a line before and after the text that you must read and act upon to prevent potential problems, such as data loss.

Getting Support and Service

If you have questions about your new Options By IBM (OBI) product, or require technical assistance, visit the IBM Personal Computing Support web site at

http://www.pc.ibm.com/support

Additional Technical Support Resources

On-line technical support is available throughout the life of your product. On-line assistance can be obtained through the Personal Computing Support web site, the PSG Electronic Bulletin Board System, and the IBM Automated Fax System.

On-line Technical Support	
IBM Personal Computing Web Page	www.pc.ibm.com
IBM PSG BBS	1-919-517-0001
IBM Automated Fax System	1-800-426-3395 1-800-465-3299 (in Canada)

You can also get help and information through the IBM PC Help Center, 24 hours a day, seven days a week. Response time may vary depending on the number and nature of the calls received. For the support telephone number and support hours by country, refer to the following table.

Support 24 hours a day, 7 days a week	
Canada	1-800-565-3344
U.S.A. / Puerto Rico	1-800-772-2227

If you call 90 days or more after the date of withdrawal of this product or after your warranty has expired, you might be charged a fee.

Step 1. Problem Solving

You may be able to solve the problem yourself. Before calling the Help Center, please prepare for the call by following these steps:

1. If you are having installation or configuration problems, refer to the detailed sections on installation found in this User Reference Manual, and review any README.TXT files found on the installation CD.

2. Visit the Personal Computing Support web site specific to the model of the option you have purchased. Updated installation instructions, hints and tips, or updated system-specific notes are often published in this section. You might find that later device drivers are available that will improve the performance and compatibility for your new option.

3. If you are installing this option in an IBM computer, also visit the applicable support web page for that computer model. These pages might also contain useful hints and tips related to installation of this option and might refer to BIOS or device-driver updates required for your computer model. If you are installing the option in a non-IBM computer, refer to the manufacturer's web site.

4. Uninstall and then reinstall the option. Be sure to decrypt all files before uninstalling SCsecurity software. During the uninstall process, be sure to remove any files that were installed during the previous installation.

CAUTION: If you re-install the SCsecurity software, you will be unable to decrypt files that were encrypted with user diskettes customized by any previous installation. **Each installation is protected by a different key.**

Step 2: Preparing for the Call

To assist the technical support representative, have available as much of the following information as possible:

1. Option name: IBM Smart Card Security Kit

2. Option number: The information you recorded in the front of the Quick Reference Manual.

3. Proof of purchase

4. Computer manufacturer, model, serial number (if IBM), and manual

5. Exact wording of the error message (if any)

6. Description of the problem.

7. Hardware and software configuration information for your system.

    1) Right click My Computer

    2) Select Properties to display the **System Properties** dialog box

    3) If it is not in front, select the **General** tab
       The information appears under the header System

If possible, be at your computer. Your technical support representative might want to walk you through the problem during the call.

Part I

The first part of this User Reference Manual explains what the IBM Smart Card Security Kit is and addresses the installation and setup of the IBM Smart Card Security Kit software.

1

Welcome to the IBM Smart Card Security Kit

This chapter introduces the basics of the IBM Smart Card Security Kit's encryption method. It also provides an overview of User Setup. Topics include:

- **What is the IBM Smart Card Security Kit?** – How the IBM Smart Card Security Kit fits into the Windows NT 4.0 environment and protects your data.

- **Features of the IBM Smart Card Security Kit** – Describes the main features of this security kit.

What is the IBM Smart Card Security Kit?

The IBM Smart Card Security Kit provides fast and easy file security. It ensures the privacy of files stored on local and mapped network folders. Individual files are encrypted at the source where they are created, copied, e-mailed, etc. The Smart Card Security Kit is a utility program that appears as **File** menu options in Microsoft's Windows NT 4.0 environment.

In addition, the Smart Card Security Kit provides a smart card that is used to limit access to a machine where the SCsecurity software is installed. The user must enter his valid Personal Identification Number (PIN) to access the desktop before the Smart Card Security Kit file encryption or decryption can occur. The same smart card is also used to safely store the Smart Card Security Kit encryption key and the Private/Public key pair used for digital signatures.

Features of the IBM Smart Card Security Kit

The Smart Card Security Kit uses the RC4 symmetric cipher, a method of file encryption and decryption that is secure and fast. Analysis shows that RC4 runs very quickly in software, which provides the security of a smart card without a performance penalty.

Integration with Windows NT 4.0

The IBM Smart Card Security Kit integrates with Windows NT 4.0 through the user's desktop, the Start menu, and the File menu in My Computer, Windows Explorer, and Find File. Special Smart Card Security Kit move and copy menu options are available, when a file or folder is transferred, using the right mouse button.

Protection Against Unauthorized Access

The Smart Card Security Kit uses a smart card containing a Personal Identification Number (PIN), and an encryption key.

When the computer is running, a secure screen saver blocks system access if the smart card is removed. Access is gained by entering the correct Personal Identification Number (PIN) when the smart card is reinserted in the reader.

File Security

The IBM Smart Card Security Kit enables the user to encrypt one file, a group of files, or all the files in a folder, either with the user's "smart card key" or a shared passphrase. When the user changes his smart card PIN, any file encrypted with that user's "smart card encryption key" can still be decrypted. This is because the user's "smart card key" does not change, only the PIN changes.

AutoCrypt

The AutoCrypt feature works behind the scenes. When the user adds a folder to the AutoCrypt List, the folder's contents are automatically encrypted. The IBM Smart Card Security Kit automatically decrypts and re-encrypts files as the user opens and closes them. AutoCrypt folders are distinguished with a special icon.

Folders and the files contained in them can be added to the AutoCrypt list via a contextual menu.

Individual File Encryption

Encrypting a single file with a "smart card key" protects files one-by-one. Even when a file is encrypted, the user can follow familiar Windows NT 4.0 procedures. For example, double-clicking on a file launches any associated application and opens the file, as usual. The file automatically decrypts when opening, and re-encrypts upon closing. In addition, all encrypted

files are available from the File | Open menu option of Windows NT 4.0 applications. Files on hard drives, mapped network folders, and removable disks can be encrypted.

Sharing Encrypted Files

The IBM Smart Card Security Kit enables secure file sharing by encrypting files with sharable passphrases. These encrypted files can be shared with any Windows 95, Windows 98, Windows 3.1, or Windows NT user, with or without a Smart Card Security Kit installed.

Secure File Transfer

The IBM Smart Card Security Kit can create a self-extracting encrypted file that can be read on an unprotected system.

Secure Screen Saver

The IBM Smart Card Security Kit will automatically lock the workstation whenever a secure screen saver activates.

Any screen saver that is password protected will be considered secure. Alternately, administrators can configure all screen savers to be secure, regardless of whether they are password protected or not.

Emergency Access Key Decryption of Files

An Emergency Access Key unlocks encrypted files when the user's smart card is inaccessible. For additional security and to protect user privacy, an organization can choose to split the emergency access key into parts. Different people (referenced as "trustees") hold a part of the key file. While each trustee holds a key file, only a specified proportion of the total number of trustee key files is required to decrypt user files.

Backup Restore Utility

The Backup Restore Utility allows the backup of card information. The administrator can restore backup information to the user's card.

Multicard Support

Multicard support allows for the use of other smart card applications. If security has been suspended, smart cards other than the one supplied with the IBM Smart Card Security Kit can be inserted into the reader. Application software to support that smart card must be installed on the system for it to be used. The smart card vendor can supply the required software.

Administration Module Overview

This section provides an overview of how to strengthen your file security plan with your IBM Smart Card Security Kit. The Kit provides features such as multiple key protection and emergency access of data. See the IBM Smart Card Security Kit Administration Reference Manual for more detailed information.

IBM Smart Card Security Kit's Security Components

- **Administrator preferences** determine how the Smart Card Security Kit will be configured for your organization's users.
- **Trustee key parts** enable emergency access to files.
- **User smart card** is the key to file encryption and decryption.

Administrator Setup Overview

- Select trustees.
- Install administrator software.
- Set up emergency access.
    - Set Emergency Access for a Single User.

    OR

    - Split Emergency Access among trustees.
    - Assist in Trustee Key Diskette creation.
- Generate Administrator Preferences.
- Back up special administrator files.

Distribute the administrator preference file to users, through diskettes or a network folder.

Security Plans — Three Examples

The IBM Smart Card Security Kit software consists of administrative and user features. Dividing tasks in this way enables several desirable effects. The administrative features can meet an organization's security requirements and enable the administrator to access needed data. The user features give the user security control as files are created.

A Smart Card Security Kit setup consists of two parts:

- **Administrator Setup** – for enforcing organizational security policy, by designing your users' file security plan

- **User Setup** – for installing encryption and decryption software

As you go through the administrator setup, you decide what settings best fit your organization. Base your choices on the type of organization you are administering and your file security plan. The following examples illustrate three typical ways to set up the software:

- for a single user

- for an organization

- for an organization with distinct internal groups

Detailed information and step-by-step instructions for Administrator Setup are provided in the Administrator Reference Manual.

Implementing the Smart Card Security Kit for a Single User

An individual user of the Smart Card Security Kit can set up the administrator software and the user software on one computer or separate computers. The user can act also as the administrator of Emergency Access.

A single user must perform the following steps on a desktop or laptop computer:

1. Set up the administrator software on the designated administrator system.

2. Set up the user software on the user's system.

Implementing the Smart Card Security Kit for an Organization

A security administrator can tailor the software to a particular organization's needs.

To implement smart card security for an organization with more than one user, an administrator must perform the following steps:

1. Set up the administrator software on the administrator's station.

2. Distribute the customized administrator files (also called User Preference Files) to users, using a diskette or a network folder.

Implementing the Smart Card Security Kit for a Large Organization

A large organization with multiple groups can designate an administrator for each group. Each administrator can then separately install the administrator software and tailor the SCsecurity software to that particular group's needs. Each group will have its own Emergency Access key and trustees.

To implement Smart Card Security for multiple groups, the organization's security administrator distributes to each group's administrator copies of the organization's security requirements. Each administrator then implements Smart Card Security according to the procedures in "Implementing the Smart Card Security Kit for an Organization" on page 6. Each group's name must be unique. Each group's administrator then distributes the administrator files using a diskette or network folders accessible only to that group. Only members of a particular group should have access to the administrator files that were customized for that group.

Your organization may choose to implement more complex plans than those described in this section. For example, you may have an umbrella group that needs emergency file access for several subgroups. The umbrella group can secure the subgroups' trustee key parts. Needed data can then be accessible vertically, to the umbrella group, but remain inaccessible to all unrelated subgroups. For more information on this and other advanced file security solutions, contact your local IBM SCsecurity representative.

How Emergency Access Works

The emergency access feature provides the ability to recover the encrypted files of any user in an organization when the user's smart card is not available.

During administrator setup, the administrator creates a Smart Card Security public/private key pair for access to encrypted files. The administrator places the public key portion on the Customized Administrator Diskette, copies the diskettes, and distributes them to users. The *Emergency Access Key* is the private key portion and is protected by either a single passphrase or multiple trustee passphrases. For our purposes, the Smart Card Security Kit distinguishes these two options as choosing either to keep the Emergency Access Key whole or to split it into parts.

The Emergency Access Key is placed in the trust of member(s) of the organization. This distribution can occur in one of two ways:

- The Emergency Access Key is kept whole. It is protected by a single passphrase on the machine where the administrator software is installed.

 OR

- The Emergency Access Key is split up and placed on multiple diskettes (Trustee Key Diskettes), each held by a different person (a trustee) and each protected by its own passphrase.

If the Emergency Access Key is split among multiple trustees, a minimum ("threshold") number of trustees must be present to activate it. For example, an organization might have seven trustees and a threshold of four. The presence of any four of the seven trustees is required to decrypt a

user's files. The number of trustees can be as large as 255. The threshold number can be the total number, although most security plans call for a smaller threshold number.

If a user's smart card is lost, the administrator can copy the user's encrypted files into a directory accessible to the administrator. Emergency decryption requires passphrases to activate the Emergency Access key. Either the administrator enters the single Emergency Access passphrase or the threshold number of trustees insert their Trustee Key Diskettes and enter their emergency access passphrases.

During the recovery process, the administrator can verify that a user who requests emergency decryption is the same user who encrypted the file. Additional emergency access information can be found in the security log file. For more information, see "Security Log File" in the IBM Smart Card Security Kit Administration Reference Manual.

2

Operational Overview of the IBM Smart Card Security Kit

The use of the IBM Smart Card Security Kit smart card is similar to the use of a car key. Without it the user cannot have access to the computer. Before starting the computer, the user inserts the card into the reader and powers up the computer.

Unlocking the keyboard of the computer requires a Personal Identification Number (PIN) which is coded into the card for verification. Moving the mouse or pressing a key displays the dialog box used to get access to the computer. When the user enters the correct PIN, the computer provides access to the computer.

NOTE: Even though the card can remain in the reader, it is strongly suggested to remove it and avoid unauthorized used of the computer.

This section discusses the following subjects:

- **Attaching the smart card reader** – How to install the smart card reader.
- **Inserting a card into the reader** – How to insert the smart card properly.
- **If the computer is already running** – How to logon to your computer.
- **Doing your work** – How does SCsecurity affect your work?
- **Removing the smart card** – What happens when the smart card is removed?
- **Identifying Encrypted Files** – How to easily identify an encrypted file.

Attaching the Smart Card Reader

PCMCIA Reader

To install the PCMCIA reader, hold the smart card reader by the edges with the IBM logo on top and the 68-pin PC Card connector next to the PCMCIA slot. Insert the PC Card into the PCMCIA slot and push it until it is firmly seated. The IBM smart card reader must be inserted into the PCMCIA slot **before** powering ON or re-booting your system. Avoid inserting or removing the smart card reader during a system power ON/OFF sequence. You can plug your smart card reader into any PCMCIA slot.

Tip: It is preferable to insert the PCMCIA smart card reader into the bottom PC card slot. This makes insertion of the smart card into the reader easier.

Serial Port Reader

To install the serial port reader, connect the reader to your PC's serial port. If your system unit will not accept a 9 pin "D" shell serial connector, you will need to purchase an adapter to convert the reader 9 pin connector to the connector on your system. Disconnect the keyboard from the system keyboard port. Attach the reader keyboard plug to the system's keyboard port. Connect your keyboard to the reader's keyboard connector. If your system will not accept a PS/2 keyboard mini connector, you will need to purchase an adapter to convert the reader's mini connector to the connector on your system.

Inserting a Smart Card into the Reader

CAUTION: Avoid inserting or removing the smart card reader during a system power ON/OFF sequence.

Using a PCMCIA reader

Before inserting your smart card into your smart card reader, make sure that the gold contacts are facing up and inserted into the reader first. Insert the smart card between the bottom of the reader and the reader flap.

1. Hold the card so that the gold contacts face up when it is inserted in the reader.

Tip: It is preferable to insert the PCMCIA smart card reader into the bottom PC Card slot. This makes insertion of the smart card into the reader easier.

2. Insert the card straight into the reader until you feel some resistance.

CAUTION: Do not push the card further in the reader, otherwise damage could occur.

Using a Serial Port Reader

Before inserting your smart card into your smart card reader slot, make sure that the arrow on the smart card and the arrow on the reader are aligned and the gold contacts are facing up towards the top of the reader. Avoid inserting or removing the smart card during a system power ON/OFF sequence.

1. Make sure the arrow of the smart card and the arrow on the reader are aligned.

2. Insert the card straight into the reader until you feel some resistance.

If The Computer Is Already Running

1. Insert the smart card into the reader.

   If the computer is running already, the **Secure Logon** dialog box will ask for a PIN.

2. Enter the PIN and click **Logon** or press the ENTER key.

   The PIN must be 4 to 8 digits in length. It may include any digits from 0 through 9 inclusive.

   The secure screen saver will unlock, providing full access to the computer.

Working After Access Has Been Gained

Once the card is inserted, the IBM Smart Card Security Kit software allows transparent access to all the encrypted files—as if the software and the card reader were not installed on the computer. You can do everything you need to do with the assurance that with the increased protection provided by the IBM Smart Card Security Kit your information is safe.

The use of an encrypted document is simple: do what you normally do. Open a document from within an application or double-click on the icon of a document to launch the appropriate application and open the file. The IBM Smart Card Security Kit software decrypts the document as it is opening, and automatically encrypts the document once it is closed.

Removing the Smart Card

Removing the smart card from the reader when the computer is running activates the secure screen saver automatically.

Always remove the smart card when the computer is not being used and place it in a safe location.

CAUTION: Do not leave your computer unattended without first closing files and applications. Other users could access your data by inserting their smart card in the reader and entering their PIN.

Identifying Encrypted Files

You can look at a file's property sheet to determine whether or not that file is protected by the Smart Card Security Kit. The property sheet for an encrypted file or AutoCrypt folder will have an Encryption tab. The individual files in an AutoCrypt folder do not have an Encryption tab on their property sheet.

Property Sheets

To view a file's File Property sheet:

1. Select a file by right clicking its name in Windows Explorer.

2. In the **File** menu, choose **Properties** (usually, the bottom menu option).

   The file's Properties sheet opens.

3. If there is an **Encryption** tab, select it.

   You know the file is not encrypted if there is no **Encryption** tab. If the file is encrypted, it will have an **Encryption** tab. Of course, self-extracting encrypted files (those having an .exe file type) do not have an **Encryption** tab.

   The **Encryption** tab bears the following information:

   - The organization where the file is encrypted;
   - The group to which the encrypted file belongs;
   - The original file size; and
   - The encryption type: smart card key or shared passphrase

Encrypted File Icons

File encrypted with the smart card

The icon of a file encrypted using the smart card remains unchanged, however, the filename is changed by adding an exclamation mark set between parenthesis: **Text(!).txt**.

Encrypted files in an AutoCrypt folder retain their original name.

File encrypted with a shared passphrase

A file encrypted with a passphrase is distinguished by a locked folder icon:

The icon of the self-extracting file encrypted with a passphrase is distinguished by a locked computer icon:

AutoCrypt Folder Icon

On your computer, you have two types of folders, AutoCrypt folders and non-AutoCrypt folders. A folder with the padlock icon: is an AutoCrypt folder. A folder not protected by Smart Card Security Kit has a default folder icon. As with files, folders have Encryption property sheet tabs.

See page 44 to learn more about the AutoCrypt feature.

Files Encrypted with Another User's Smart Card

When you cannot open, copy, move, or rename a file, that file has probably been encrypted with another person's smart card. To move or copy these files, select them with the right mouse button and use the Smart Card Security Kit menu options. For more information on how to use these special Smart Card Security Kit menu options, see the section, "Moving and Copying Encrypted Files without Decrypting."

If another user wants to share an encrypted file with you and the file was encrypted using the **Use Smart Card Key** menu option, ask the user to decrypt the file, and then re-encrypt the file using the **Use Shared Passphrase** menu option.

NOTE: When viewing the property sheet of a file encrypted with another user's smart card, you may get an error message. You are still able to read the property sheet.

3

Installation

The IBM Smart Card Security Kit keeps your data private and provides a measure of protection against intrusion for your computer. The IBM Smart Card Security Kit's encryption disguises a file by making the readable data inside unreadable. Decryption returns a file to its original state, making it readable again. The Smart Card Security Kit also enables you to share encrypted files with others—even if they do not have the IBM Smart Card Security Kit installed on their computers.

The IBM Smart Card Security Kit provides an Emergency Access capability. If necessary, your files can be decrypted with the cooperation of individuals within your organization. These individuals have been chosen by your administrator; each holds a part of your organization's emergency access key. (We refer to these people as "trustees.") If you forget your smart card or forget to decrypt files before an absence, your trustees can work together to recover vital data.

This chapter explains how to set up the IBM Smart Card Security Kit user software. Topics include:

- **Compatibility with Windows 3.1 and Windows 95/98** – Explains the compatibility level with the other Microsoft operating system.

- **Migrating to IBM Smart Card Security Kit** – Provides instructions for users of other encryption software.

- **Before Installing the Software** – Explains what has to be done before the installation of the software.

- **Minimum Hardware and Software Requirements** – Lists the minimum hardware and software requirements for the IBM Smart Card Security Kit.

- **Installing the Security Software** – Shows the installation procedure for the IBM Smart Card Security Kit, step-by-step.

Compatibility with Windows 3.1 and Windows 95/98

This version of the product is intended for Windows NT 4.0 **only**. It is not intended for Windows 3.1, Windows 95/98, or other Windows NT operating systems.

To share files with Windows 3.1 or Windows 95/98 users, the files should be encrypted with a shared passphrase or the file encryption should be removed before copying the files to an appropriate media.

NOTE: To maintain filename compatibility with Windows 3.1, the IBM Smart Card Security Kit creates an encrypted a file with an eight-character name. The encrypted files can then be shared with any Windows 95, Windows 98, Windows 3.1 or Windows NT user, with or without the IBM Smart Card Security Kit installed.

Migrating to the IBM Smart Card Security Kit

IMPORTANT: If you have any other smart card access or data encryption software installed, you must first **decrypt all encrypted files** and uninstall that program before installing the IBM Smart Card Security Kit. . Files encrypted with other security programs **cannot** be decrypted by the IBM Smart Card Security Kit.

Minimum Hardware and Software Requirements

Before installing the IBM Smart Card Security Kit, you must have the following computer and software:[1]

- An IBM or IBM-compatible computer (486SX microprocessor, 33 MHz or faster) with 16 MB of RAM and 90 MB of free hard disk space, a VGA screen with a resolution of 640x480 pixels capable of displaying 256 colors;
- One available Type II PCMCIA Interface Slot with PCMCIA Interface Software (Card and Socket Services) version 2.1 (notebook kit only);
- One standard serial port and a standard PS/2 keyboard port (desktop kit only);
- A 1.44 MB 3.5-inch floppy drive;
- Access to a CD-ROM drive;
- Microsoft Windows NT 4.0 with Service Pack 4..

File System

- An NTFS system volume for increased security is required, rather than a FAT volume. *NT supports both NTFS which is native to NT and the DOS/WIN 9x FAT system.*

---

[1] From this point on, we refer to Windows NT 4.0 as Windows NT unless necessary.

CAUTION: It is imperative that you update your system with the latest BIOS and device drivers BEFORE attempting to install any of the Smart Card software contained on the CD. In most cases, your system was manufactured before there was support for devices like Smart Cards. Refer to your systems support organization to obtain the latest updates for your system.

To obtain updates, IBM PC customers can logon to: http://www.pc.ibm.com/us/support

Before Installing

NOTE: The IBM Smart Card Security Kit should not be installed on a file server.

Before doing the installation, save all documents, backup important files and quit **ALL** running applications including anti-virus programs. Anti-virus software should be deactivated because it may interfere with the installation process.

Before closing your anti-virus protection program, scan your system and any diskettes which will be used for installation.

Making diskettes from the CD-ROM

If your system does not support using both the diskette drive and CD drive at the same time, you should install from diskettes. During the Administrator installation, a diskette is generated and used during the User installation to modify the users security files

IMPORTANT: If you need to create diskettes from the CD-ROM, follow these steps:

To create 1.44MB floppy disk images from the CD-ROM:

1. Have a box of blank formatted 1.44 MB diskettes at hand. The number of diskettes needed will depend on the type of installation you choose.

2. Start Windows NT 4.0 and insert the CD into the CD-ROM drive. If AutoRun is enabled, the installation utility will automatically load after you insert the CD into the CD-ROM drive.

3. If AutoRun is not active, select **Start**, and then select **Run**.

4. Type *d:\setup*, where *d:* is the letter designating the CD-ROM drive. A letter other than d: may be used on your system. Press ENTER and an introduction screen will be displayed. Select **Help** for information about each type of installation.

5. Locate a computer that has both a CD-ROM drive and a floppy drive.

6. Select the **Install** button under SCsecurity software.

7. Click **Make Diskettes** on the Installation Configuration screen.

    a. Select a drive.
    b. Insert a diskette into the diskette drive and select **Generate** in the **Make Diskette Install Utility** dialog box.
    c. Label each diskette appropriately for proper installation.

8. When the last diskette has been prepared, a message confirming that SCsecurity installation was successfully copied to the diskettes will appear. Select **OK**.

9. In the Make **Diskette Install Utility**, select **Close** to return to the Installation Configuration screen.

10. Use these diskettes to install SCsecurity. For more information, refer to the section "Step 1 b: Installing the Administrator Software from Diskette".

Using the Installer

An install utility makes it easier to install the various components of your Smart Card Security Kit. If AutoRun is enabled on your system, the install utility will automatically be loaded when the installation CD is inserted into the computer.

The IBM SCsecurity screen will appear. Click **Install** under SCsecurity Software to install the software. The Welcome screen will appear. Click **Next** to go to continue the installation.

Read the International License Agreement. Accept the Agreement to continue with the Installation.

In the Installation Configuration dialog box, select the type of configuration you wish to install.

Select **Help** for information about the installation type.

The Administration software should be installed by the Security Administrator, usually only on the administrator's system.

NOTE: Some software will require a system restart after installation. If so, go back to the Install utility to continue the installation.

Step 1a: Installing the User Software from the CD

(If you are installing from diskette, see Step 1b.)

Installing the User Software without the Installer

1. Start Windows NT 4.0 and insert the CD into the CD-ROM drive. If AutoRun is enabled, the installation utility will automatically load after you insert the CD into the CD-ROM drive.

2. If AutoRun is not active, select **Start**, and then select **Run**.

3. Type *d:\setup*, where *d:* is the letter designating the CD-ROM drive. A letter other than d: may be used on your system. Press **Enter** and an introduction screen will be displayed. Select **Help** for information about each type of installation.

4. Select **Install** under SCsecurity Software.

5. The **Welcome** screen will appear.

6. Click **Next** to continue with the installation.

7. Read the Software License Agreement. Do not continue **if you do not agree with the terms of the license**. If you answer **Yes** the installation will proceed.

8. In the Installation Configuration screen, select the type of configuration you wish to install. To install the user software, select **User**.

9. The Card Reader Selection window will open.

10. Select the type of card reader.

    ▪ Select **PCMCIA** if you have a PCMCIA smart card reader.
    ▪ Select **Serial Port Attached** if you have a serial reader.

11. Attach the reader if it is not already attached. You may be asked to choose the COM port. Refer to the Installation Help for more information.

12. After the driver installs, select **Next**.

13. You will be asked to select the administrator public key file (**pkfile**) that was created during the administrator setup. After browsing to find the file (usually located on the User Setup diskette supplied by the administrator), select **Open**.

14. You will be asked if you want to install the secure screen saver as the default Windows screen saver. We recommend that you select **Yes**.

15. Setup has finished. Select **Restart**. The system will restart.

16. When the installation continues, the **SCsecurity** logon screen appears. Insert the smart card or press **Ctrl**+**Alt**+**Del** to log on.

17. The **Smart Card Security** Login screen appears. Enter your **User Name** and **Password** and select **OK**.

18. Select **Smart Card**. In the **Smart Card Options**, select **Change PIN**. The **Smart Card Options (PIN Maintenance)** windows appears.

19. Enter the PIN for the card and select **Administrator** or **User**.

20. Enter the new PIN in the **New PIN** field and confirm it in the **Confirm PIN** field. Select OK to validate the changes.

21. In the **Smart Card Options** window, select **Cancel** to return to the **SCsecurity Login** window.

Step 1b: Installing the User Software from Diskette

Installing the User Software

1. Start Windows NT 4.0 and insert the first installation diskette in the drive.

2. Open Windows Explorer and select the diskette.

3. Double click on the installation file (**setup.exe**).

4. An installation program will be loaded to make it easier to install the various components of your Smart Card Security Kit and associated software. The Installation welcome screen will appear and explain how to install the application software. Click **Next** to proceed with the installation.

5. Read the License Agreement. Do not continue **if you do not agree with the terms of the license**. If you answer **Yes** the installation will proceed.

6. In the Installation Configuration screen, select the type of configuration you wish to install. To install the user Security Kit, select **User**.

7. The Choose Destination Location dialog box opens. Select a location (directory) where the files will be installed using the **Browse** button.

8. Click **Next** to begin the installation.

9. Follow the installation steps displayed on your screen.

NOTE: Once the Smart Card Security Kit has been installed, you will be prompted to reboot your computer. YOU MUST REBOOT YOUR COMPUTER SO THAT WINDOWS WILL RECOGNIZE THE NEWLY INSTALLED SOFTWARE. This software must be active for the following steps. Since you are installing the user software from diskettes, remove the diskette from the drive before re-booting.

Step 2a: Installation of the IBM PCMCIA Smart Card Reader Driver

IMPORTANT: If a previous version of a Gemplus GPR400 driver is already installed on your machine, you must uninstall it.

1. The Card Reader Selection dialog box will open. Select PCMCIA as the type of card reader.

2. The Installation Help will guide you through the installation process.

3. Click **Next**.

4.   Restart the computer.

NOTE: After returning from a SUSPEND operation, a message box may tell you that your smart card reader was removed and then reinserted. If this occurs, click **OK** and continue with what you were doing.

Step 2 b: Installation of the IBM-410p Smart Card Reader Driver

1. The Card Reader Selection dialog box will open. Select Serial Port Attached reader.

2. The Installation Help will guide you through the installation process.

3. Click **Next**.

4.   Restart the computer.

NOTE: After returning from a SUSPEND operation, a message box may tell you that your smart card reader was removed and then reinserted. If this is the case, simply click on the message box **OK** and continue on with what ever you were doing.

Part II

The chapters in this section aid the user after the IBM Smart Card Security Kit User Software has already been installed.

4

User Setup

The IBM Smart Card Security Kit keeps your data private and provides a measure of protection against intrusion for your computer.

The Smart Card Security Kit's encryption disguises a file by making the readable data inside unreadable. Decryption returns a file to its original state, making it readable again. The Smart Card Security Kit also enables you to share encrypted files with others – even if they don't have the IBM Smart Card Security Kit.

Your administrator has set up emergency access. If necessary, your files can be decrypted with the cooperation of individuals within your organization. These individuals have been chosen by your administrator; each holds a part of your organization's Emergency Access Key. (We refer to these people as "trustees.") If you lose your smart card or forget to decrypt files before an absence, your trustees can work together to recover vital data.

This chapter explains how to set up the Smart Card Security Kit user software after logging in. As well, all aspects of the IBM Smart Card Security Kit that deal with securing computer access are described. These include:

- Login and logoff.
- Locking and unlocking the computer.
- Secure screen savers.
- Changing the PIN.
- Changing the password.

Setting Up the User Software

To set up the IBM Smart Card Security Kit user software:

1. You will be asked to select the administrator public key file (**pkfile**) that was created during the administrator setup. After browsing to find the file (usually located on the User Setup diskette supplied by the administrator), select **Open**.

2. You will be asked if you want to install the IBM Smart Card Security Kit screen saver as the default Windows screen saver.

3. Setup has finished. Select **Restart**. The system will restart.

4. When prompted, insert the smart card into the reader or press **Ctrl**+**Alt**+**Del** to log in. If you want to log in with smart card support, wait for the smart card icon to appear on the initial **SCsecurity** screen.

5. The **SCsecurity** Login screen appears. Enter your **User Name** and **Password** and select **OK**.

6. Select **Smart Card**. In the **Smart Card Options**, select **Change PIN**. The **Smart Card Options (PIN Maintenance)** dialog box appears.

7. Enter the PIN for the card and select **Administrator** or **User**.

8. Enter the new PIN in the **New PIN** field and confirm it in the **Confirm PIN** field. Select **OK** to validate the changes.

9. In the **Smart Card Options** dialog box, select **Cancel** to return to the **SCsecurity Login** window.

NOTE: Before inserting your smart card into the PCMCIA smart card reader, make sure that the gold contacts are facing up. Insert the smart card, gold contacts first, between the bottom of the reader and the reader flap. If you are using a serial port reader, make sure that the arrow on the smart card and the arrow on the reader are aligned and the gold contacts are facing up towards the top of the reader. Avoid inserting or removing the smart card during a system power ON/OFF sequence.

IMPORTANT: Access to the system will be denied until a valid PIN has been entered. Keep in mind that the smart card will be blocked, if you enter your PIN incorrectly three (3) consecutive times. If this happens, the card can only be unblocked by the administrator.

Logging In

Both automatic and manual logins are supported:

Logging in *automatically* accesses the account stored on the smart card.

A *manual* login provides access to all other accounts available on the computer.

Note: If you are powering on or re-starting the computer and want to log in with smart card support, you must wait for the smart card icon to appear on the initial **SCsecurity** screen.

If you log in manually before the smart card icon appears, smart card services will be disabled. To enable smart card services, you will have to log off and log in again after the smart card icon appears. See "Logging Off a Computer or Domain" on page 28 and "Automatic Login", below.

Regardless of whether you log in automatically or manually, you will always be authenticated with the credentials stored on the smart card (if smart card services are active).

Automatic Login

To log in automatically:

1. Insert the smart card into the smart card reader. The **SCsecurity Login** dialog box will appear.

2. Enter the smart card user PIN, in the **User PIN** textbox.

3. Select **OK**.

Note: You are not considered logged in until the PIN is entered and the account authenticated.

If you insert the smart card into the smart card reader, but cancel before entering the PIN, the card will have to be removed and re-inserted.

Unauthenticated shutdown, if it has been set up in Windows NT System Policies, will be available at the login stage. This allows you to restart or shut down the computer, without entering account credentials.

Various SCsecurity and smart card options are also available at this stage. See "SCsecurity Options" on page 27 and "Smart Card Options" on page 29.

Manual Login

You may want to log in manually for the following reasons:

▪   To access an account other than the home domain account on a local computer.

- To access a multiple trust account. Multiple trust accounts may exist between various domains that may or may not be cardholder accounts.

For both types of manual login, you need to provide complete account credentials.

To log in manually:

1. Press Ctrl+Alt+Del. The **SCsecurity Login** dialog box will appear.

2. Enter the user name, password and domain in the appropriate text boxes. The domain can be selected from a drop-down list that includes the local computer, the home domain account and all trusted domains.

3. Select **OK**.

4. Enter the smart card PIN. You will be logged in with the manually entered credentials, but authenticated using smart card credentials.

Depending on Windows System Policies, the following features could be included at the login stage:

- Unauthenticated shutdown.

- Dial-up networking.

Note: NT System and User Policies will be observed and enforced during the login process.

Smart Card or Smart Card Reader Removal

Smart Card Removal

If the smart card is removed from the reader while you are logged in, the computer will lock automatically. You will have to re-insert the card and enter your PIN to unlock the computer. See "Locked Workstations" and "Unlocking a Locked Workstation" on page 27.

Smart Card Reader Failure or Removal

If the smart card reader is removed or fails, you will not be able to access your computer. However, administrators, with accounts registered on the local computer, will be able to disable security and allow general access to all users.

NOTE: *Disabling security* is not the same as *suspending security*.

Suspending security temporarily disables smart card services. This is useful if you need to insert a different smart card into the reader. See "Suspending Security" on page 30.

Disabling security removes the administrator requirement from the Emergency Unlock feature. Both administrators and users will be able to log in. All SCsecurity and Smart Card Options will be disabled, including file encryption and decryption.

SCsecurity Options

The following options can be accessed, at any time during a user session, by pressing Ctrl+Alt+Del.

- Lock Workstation.

- Logoff.

- Shut Down.

- Change Password.

- Task Manager.

- Smart Card.

These options are defined below.

Locked Workstations

The IBM Smart Card Security Kit has the functionality to lock the computer or workstation both automatically and manually.

Automatic Lock

While a user is logged in, the computer will lock in the following situations:

- A smart card is removed from the smart card reader.

- A smart card reader fails.

- A smart card reader is removed from the computer.

- A secure screen saver is activated.

The **Workstation Locked** message box will appear on the screen.

Manual Lock

At any time during a user session, the user can choose to lock the computer. When the computer is locked, applications and documents remain open, but are inaccessible without the user's smart card PIN.

To lock the computer:

1. Press Ctrl+Alt+Del. The **SCsecurity Options** dialog box will appear.

2. Select **Lock** <u>W</u>**orkstation**. The Locked Workstation message box will appear on the screen.

Unlocking a Locked Workstation

A locked computer (workstation) can be unlocked in two ways:

- Automatically by the user.

▪ Manually by administrators.

The procedure for unlocking the computer manually is detailed in the *Administrator Reference Manual.* See "Unlocking a Locked Workstation" in "Part III, Administrator's Tasks".

Unlocking the Computer Automatically by the User

As long as smart card readers are functioning properly, users will be able to unlock their computers by following the procedure below:

1. Re-insert the smart card into the smart card reader. The **Unlock Workstation** dialog box will appear.

2. Enter the User PIN and select **OK**.

If the credentials on the inserted smart card match the credentials of the currently logged user, this will unlock the computer.

Secure Screen Savers

The IBM Security Kit will lock the computer when a secure screen saver activates.

To configure a secure screen saver:

1. In Windows **Control Panel**, double-click **Display**.

2. Select the **Screen Saver** tab.

3. Select Password protected.

Alternately, an administrator can force all screen savers to be secure no matter how they are configured. This procedure is detailed in the Administrator Reference Manual. See "Secure Screen Savers".

Logging off a Computer or Domain

1. Close all applications.

2. Press Ctrl+Alt+Del. The **SCsecurity Options** dialog box will appear.

3. Select **Logoff**.

4. A verification message will appear.

5. Select **OK**.

IMPORTANT: Do not leave your smart card in the reader or with your computer when your are not using it.

Shut Down

Users and administrators can shut down or restart the computer at any time during a user session.

To shut down or restart the computer.

1.   Close all documents and applications.

2.   Press Ctrl+Alt+Del. The **SCsecurity** dialog box will appear.

3.   Select <u>**Shut Down**</u>. The **Shutdown Options** dialog box will appear.

Three options are available on the **Shutdown Options** dialog box:

▪   Restart: *This allows the user to restart the computer.*

▪   Shut Down: *This shuts down the computer and provides the user a safe power off.*

▪   Shut Down and Power Off: *If this feature has been set up by the administrator, this shuts down the computer and turns off the power.*

Changing a Password

To change the password on the account stored on the smart card:

1.   Log in to the account.

2.   Press Ctrl+Alt+Del. The **SCsecurity** dialog box will appear.

3.   Select <u>**Change Password**</u>.

4.   Enter the existing password.

5.   Enter and confirm the new password in the appropriate text boxes.

6.   Select **OK**.

Note: If security has been suspended, the change Password function will be disabled.

See "Suspending Smart Card Security" on page 30.

Task Manager

Selecting <u>**Task Manager**</u> on the **SCsecurity Options** dialog box invokes the Windows NT Task Manager.

Smart Card Options

Smart card options include the following list. Not all options are enabled at all times. Some are available only to administrators, as explained below.

▪   **Change PIN** displays the options for changing or unblocking a PIN. See Changing a PIN.

▪   **Change Profile** allows the administrator to change user's account credentials, stored on the smart card. This option is not available to users.

▪   **Card Backup** displays the Backup Restore Utility. This allows the administrator to backup the contents of a user's card. The Backup Restore Utility is not accessible to the user.

- **Suspend Security** is available to users, if the option has been enabled by the administrator. Suspending smart card security temporarily disables smart card options, allowing the user to remove the smart card without having the computer lock automatically. See "Suspending Security" on page 30 and "Unlocking a Workstation" on page 27.
- **Disable Security** is available only to administrators who have logged in without smart card support. This allows users and administrators to log in, when the smart card reader fails or is removed. All smart card options and file encrypting/decrypting functions will be disabled.
- **Card Diagnostics** is available during a user session. This displays details on the inserted smart card and the smart card reader. See Card Diagnostics.

Changing a PIN

The default User PIN is 1234. The user should change this at the first opportunity.

To change a PIN:

1. Press Ctrl+Alt+Del. The **SCsecurity Options** dialog box will appear.
2. Select **Smart Card**. The **Smart Card Options** dialog box will appear.
3. Select **Change PIN**. The **Smart Card Options (PIN Maintenance)** dialog box will appear.
4. Enter the PIN in the PIN field and select **User**. This is the default.
5. Select **Change**.
6. Enter and confirm the new PIN in the appropriate fields and select **OK**.

Alternately, you can select **Smart Card** on the **SCsecurity Login** screen, then follow steps 2-7.

The above procedure explains how to change a user's PIN. The administrator's PIN is changed in the same way, except that **Admin** is selected in Step 3. To change the administrator's PIN, the user has to be logged in as an administrator. Refer to the Administrator Reference Manual for details. See "Changing PINs" in "Part III, Administrator's Tasks".

Unblocking a PIN

A user's PIN will be blocked after three failed verification attempts, an administrator's after seven.

Only administrators can unblock the users' PINs. Refer to the Administrator Reference Manual for details. See "Unblocking a PIN" in "Part III, Administrator's Tasks".

Suspending Security

If the computer is in *Secure* mode, the IBM Security Kit will automatically lock the computer whenever the smart card is removed from the smart card reader.

Provided the administrator has granted the right, you can suspend security and temporarily disable this feature. Suspending Security makes it possible to insert a different smart card into the smart card reader.

To suspend security:

1. Press Ctrl+Alt+Del.

2. Select **S̲mart Card** on the **SCsecurity** dialog box.

3. Select **S̲uspend Security**.

The following points on *Secure* mode should be noted:

▪ The suspension of Secure mode is only maintained for the current active session.

▪ Secure mode will automatically be reinstated when the user logs off, locks or reboots the computer.

▪ Secure mode will automatically be reinstated when a secure screen saver is activated.

▪ To reactivate Secure mode without logging off, a user must first lock the computer.
  ➢ The user can unlock as described above. See "Unlocking a locked workstation" on page 27.

Card Diagnostics

The **Card Diagnostics** window is available during the user session. This displays details on the installed smart card and smart card reader.

To view Card Diagnostics:

1. Press Ctrl+Alt+Del.

2. Select **S̲mart Card** on the **SCsecurity** dialog box.

3. Select **Card D̲iagnostics**.

5

Important Information You Must Know

This chapter describes how to set up the IBM Smart Card Security Kit step-by-step. Topics include:

- **Files that cannot be encrypted** – Lists the file types that cannot be encrypted so that Microsoft Windows and IBM Smart Card Security Kit work correctly.

- **Files that can be encrypted** – Explains what types of files should be encrypted.

- **File naming conventions** – Explains how the IBM Smart Card Security Kit names the encrypted files in a consistent, uniform manner.

Files That Cannot Be Encrypted

Some files cannot be encrypted. Doing so could disable DOS, Windows, application programs, or the Smart Card Security Kit software itself.

The Smart Card Security Kit will not encrypt these files:

- Files that are already encrypted with other applications.

- Smart Card Security Kit program files.

- System files.

- Files with any of the following extensions: **.386**, **.bat**, **.bin**, **.cfg**, **.com**, **.dll**, **.drv**, **.exe**, **.fon**, **.fot**, **.grp**, **.ico**, **.ini**, **.lnk, .ovl**, **.pif**, **.sys**, **.ttf**, **.vbx**, **.e!!**, **.u!!**, **.mpd**, **. ocx**, and **.vxd.**

The Smart Card Security Kit will encrypt these files:

- Files in the folders **\Windows\Temp**, **\Windows\Desktop**, and each user's **\Desktop** subfolder (**\Windows\Profiles\User name\Desktop**), as long as the files do not contain the reserved extensions listed above.

IMPORTANT: It is impossible to add Windows directories to the AutoCrypt list, except for the **\Windows\Temp** and **\Windows\Desktop** directories and each user's **\Desktop** subfolder (**\Windows\Profiles\User name\Desktop**).

NOTE: On a dual boot system, only the system files from the active operating system are protected from encryption. System files for the non-active operating system are treated like any other files and therefore can be encrypted. If these files are encrypted, the operating system will not function properly.

Files That Can Be Encrypted

All documents and files generated by a word processor, spreadsheet, contact organizer, email, etc. can be encrypted. Files with built-in compression like in the Video for Windows (.avi) or the QuickTime format (.mov) can also be encrypted safely. If in doubt, contact the program's publisher to establish if the data file of a specific program may be encrypted safely.

File Naming Conventions in the Smart Card Security Kit

When you use your Smart Card Key, names of encrypted files follow a uniform naming convention governed by two rules:

1. All encrypted files in AutoCrypt folders and subfolders retain their original names. Moving or copying files into or out of AutoCrypt folders (without using the Smart Card Security Kit's special menu items) does not change their names, regardless of whether or not they are encrypted.

2. All files encrypted outside of AutoCrypt folders have an exclamation mark character between parenthesis characters "**(!)**", just before the dot that separates the filename from the file type; for example, **plan.doc** becomes **plan(!).doc** when encrypted outside of an AutoCrypt folder.

3. All files encrypted by changing their filenames [e.g., by adding "(!)"] will have their filenames changed to uppercase.

In short, a file is encrypted with the smart card key if, and only if, the file is in an AutoCrypt folder or has "**(!)**" before the period that separates the file name from the file type.

NOTE: A file that does not have "**(!)**" before the period that separates the file name from the file type and that is moved out of or copied from an AutoCrypt folder is not encrypted. For instance, when moving or copying files or folders from an AutoCrypt folder to a backup system, the IBM Smart Card Security Kit decrypts files without the "**(!)**" naming convention.

These file-naming conventions allow you to encrypt files easily by renaming them. To encrypt a file outside of an AutoCrypt folder, append the "**(!)**" sequence to the file name, just before the extension. If you rename **plan.doc** to **plan(!).doc,** for example, you automatically encrypt the file. Similarly, if you rename **plan(!).doc** to **plan.doc** (and it is not in an AutoCrypt folder), the file becomes decrypted. If you execute **Save** or **Save As** on a file from an application and name the file with the "**(!)**" convention, the file is automatically encrypted.

See page 44 to learn more about the AutoCrypt feature and AutoCrypt folders.

The icon of the file does not change when the smart card key is used to encrypt the file.

When the Shared Passphrase is used, a separate file is created and the file extension changes to a lowercase character "s" followed by two exclamation marks (**.s!!**). The icon of the file changes to a rolled-up document inserted into the hasp of a padlock:

If the self-extracting file checkbox of the shared passphrase was checked, the new file will have (**.exe**) as the file extension.

6

Using the Smart Card Security Kit

With the Smart Card Security Kit installed on your computer, encrypting and decrypting files is simple. You can manually encrypt files on your hard disks, diskettes, networks and removable drives. Also, the AutoCrypt function automatically encrypts files in folders on your hard drive or in mapped folders, including any files you add to the AutoCrypt folder at a later time.

This chapter explains how to encrypt and decrypt files with the Smart Card Security Kit. Topics include:

- **Activating the Smart Card Security Kit** – How to log on and use the Smart Card Security Kit.

- **Smart Card Security Kit Menu Options Overview** – How to use each menu option.

- **Emergency Access of the data** – how to access the data in an emergency.

- **Encrypting Files with your Smart Card** – How to encrypt files with your "secret key".

- **Encrypting Files with a Shared Passphrase** – How to encrypt files for sharing with others.

- **Decrypting Files with your Smart Card** – How to decrypt files with your "secret key".

- **Decrypting Files with a Shared Passphrase** – How to decrypt files with a shared passphrase.

- **AutoCrypt Folders** – How to encrypt files in a folder automatically.

- **Disabling/Enabling Automatic Decryption** – How to disable and enable automatic decryption of files.

Activating the IBM Smart Card Security Kit

To use your IBM Smart Card Security Kit, you must first log on to your computer by inserting your smart card and entering your PIN. This provides the IBM Smart Card Security Kit with your "smart card key", which it needs to encrypt and decrypt files.

Smart Card Security Kit Menu Options

After you have set up the user software and logged on to the desktop, you can view the Smart Card Security Kit menu options using Windows Explorer, My Computer, or with the Windows **Start** button on your desktop.

Accessing Smart Card Security Kit Menu Options

You can access your Smart Card Security Kit's menu options in the following ways:

- In Windows Explorer, select a file or folder in the Contents window on the right, choose **File** from the menu bar. Select a command from the menu.

- In Windows Explorer, select a file or folder in the right pane of Windows Explorer, and click the right mouse button to display the contextual menu. Select the appropriate command from the menu.

- Select a file in My Computer, and choose **File** from the menu bar or click the right mouse button to display the contextual menu. Select the appropriate command from the menu.

- Select a file on your desktop, and right-click on the file to display the contextual menu. Select the appropriate command from the menu.

Overview of IBM Smart Card Security Kit Menu Options

Encrypt

- **Use <u>S</u>mart Card Key...** encrypts one or more selected files or folders with your smart card key.

- **Use S<u>h</u>ared Passphrase...** encrypts one or more selected files with a passphrase that you can share with others for secure file exchange.

Dec<u>r</u>ypt

- **Use <u>S</u>mart Card Key...** decrypts one or more selected files or folders with your "Smart Card key."

- **Use S<u>h</u>ared Passphrase...** decrypts one or more selected files with a shared passphrase.

<u>A</u>utoCrypt

- **<u>A</u>dd folder to AutoCrypt list** adds the selected folder and all its subfolders to the AutoCrypt List. Your Smart Card Security Kit software then automatically encrypts all files in the selected folder and its subfolders. IBM Smart Card Security Kit also automatically encrypts new files and the contents of new subfolders as they are added to the AutoCrypt folder. AutoCrypt folders show a file stuffed through the hasp of a lock:
.

- **<u>R</u>emove folder from AutoCrypt list** removes the selected folder and all its subfolders from the AutoCrypt List. Your Smart Card Security Kit software then automatically decrypts all files in the selected folder and its subfolders. The padlock disappears from the folder icon.

- **<u>E</u>dit AutoCrypt List…** displays the AutoCrypt List dialog box and enables you to add and remove folders from the AutoCrypt List.

<u>S</u>Csecurity Features

- **Disable/Enable Automatic Decryption**

  This feature lets you decide when files should be encrypted or decrypted automatically.

  - **Disable Automatic <u>D</u>ecryption:** disables automatic file decryption when the file is accessed by an application.

  - **Enable Automatic Decryption:** enables automatic file decryption when the file is accessed by an application.

- **<u>A</u>bout...** displays copyright information, software version, etc.

<u>S</u>Csecurity <u>U</u>ser Help...

provides information on the IBM Smart Card Security Kit User features, procedures, menu options, dialog boxes, etc.

Encrypting Files with Your Smart Card Key

You encrypt files with the "secret key" on your smart card by selecting them, and then choosing the **Use <u>S</u>mart Card Key** menu option. You can encrypt files from several places in Windows.

Important: You cannot encrypt files from Network Neighborhood. Network Neighborhood drives are unmapped. Your computer has no permanent connection to these drives or their folders. To encrypt files or folders on the network, open My Computer, and use mapped drives.

🔲 **To view the Smart Card Security Kit's menu options:**

1. In Windows Explorer, select a file or folder in the right pane (Contents) window.

2. Right-click on the file or folder.

Encrypting One File

🔲 **To encrypt a file manually:**

1. From Windows Explorer, select the file you want to encrypt.

2. Right-click on the file name, select **Encrypt**, and choose **Use <u>S</u>mart Card Key**.

OR

On the **<u>F</u>ile** menu, select **Encrypt**, and choose **Use <u>S</u>mart Card Key**.

The Encrypt – Smart Card Key dialog box opens.

3. Choose **OK**.

The file name has changed to reflect its encrypted state. For example, the file **myfile.doc** becomes **myfile(!).doc**.

NOTE: The addition of "(**!**)" to the file name occurs only for files that you manually encrypt and keep outside of AutoCrypt folders. Files inside AutoCrypt folders are also encrypted, but their names do not reflect their encrypted state.

If an encrypted file is moved or copied to an AutoCrypt folder, the name will not change, it will keep the "(**!**)" even when in the AutoCrypt folder.

The Encrypt Dialog Box

When you choose **Encrypt** and then **Use <u>S</u>mart Card Key**, the Encrypt – Smart Card Key dialog box opens. This dialog box contains the name of the current directory, the file about to be encrypted, the user name, and the Emergency Access information.

The sub-section Emergency Access lets the user see the following information by clicking on the **More** button:

- The name of the Emergency Access Administrator, Organization, and Group.

- Emergency Access Authentication number, which is a unique number created when Emergency Access was installed.

- Emergency Access Key Protection type.

The user's name appears in each user's Encrypt dialog box so that the Emergency Access key can be verified. The organization should publicize the authentication number to its users. Users can compare this number with the one displayed in their Encrypt dialog box. If the two numbers are the same, the user is assured that the Emergency Access key has not been altered or replaced.

Encrypting Multiple Files

To encrypt multiple files:

1. In Windows Explorer, to select a series of adjacent files for encryption, left-click the first file name, hold the SHIFT key, and left-click the last file name in the series.

OR

In Windows Explorer, to select a number of nonadjacent files for encryption, hold the CTRL key as you left-click each file name.

2. Right-click on one of the selected files, and choose **Encrypt**, **Use Smart Card Key**.

The Encrypt – Smart Card Key dialog box opens.

3. Choose **OK**.

The file names have changed to reflect their encrypted state.

Encrypting All Files in a Folder

To encrypt all files in a folder on your computer or in a mapped network folder:

1. Select the folder in Windows Explorer or My Computer.

2. Right-click on the folder, and choose **Encrypt**, **Use Smart Card Key**.

All files in that folder and all of its subfolders will be encrypted.

IMPORTANT: Encrypting files manually is not the same as adding a folder to the AutoCrypt List. When you manually encrypt all files in a folder, any new files you add to this folder will not be encrypted automatically. Instead of manually encrypting all files in a folder, you may want to add that folder to the AutoCrypt List. Any new file added to an AutoCrypt folder will be encrypted automatically.

CAUTION: Never share a folder or hard disk that contains files that are encrypted with the **Use Smart Card key** menu option. If you do and the shared users access an encrypted file, the transparent decryption feature will automatically decrypt your files for the shared users if you have your smart card inserted in the reader and are logged on.

Never send anyone files that are encrypted with your smart card key. If you do, the recipient will not be able to decrypt the file.

To send a file that is currently encrypted with the **Use Smart Card Key option**, you must first decrypt it, then encrypt the file using the **Encrypt, Use Shared Passphrase** menu option (see "Encrypting Files with a Shared Passphrase" below. A file encrypted with a shared passphrase is safe to send through e-mail.

If a file is located in the AutoCrypt folder, you can choose not to decrypt the file automatically, using **Scsecurity Features, Disable Automatic Decryption** contextual menu option. There may be times when you do not want a file to decrypt automatically, for example, when you perform a back up (see "Disabling and Enabling Automatic Decryption" on page 46).

Encrypting Files with a Shared Passphrase

With the Smart Card Security Kit, you can share encrypted files with others. File encryption for the purpose of sharing the file is similar to file encryption methods described earlier in this chapter. The Smart Card Security Kit enables you to use a shared passphrase when sharing files with others. Any Windows 3.1, Windows 95, Windows 98, Windows NT or Smart Card Security Kit user who knows the shared passphrase can decrypt the files. Files encrypted with your smart card can only be decrypted using your smart card. Thus, a recipient of such encrypted files would be unable to decrypt them.

You can use the Smart Card Security Kit's file sharing features by:

- Selecting **Encrypt**, then choosing **Use Shared Passphrase** to encrypt one or more selected files or folders with a passphrase you can share with another person

- Selecting **Decrypt**, then choosing **Use Shared Passphrase** to decrypt one or more selected files or folders using a passphrase that has been shared with you by another person

Shared Passphrase Encryption

To send an encrypted file to a user who has a Smart Card Security Kit installed, use the following procedure.

To encrypt a file with a shared passphrase:

1. In Windows Explorer, select the file you want to encrypt for sharing.

2. From the **File** menu, select **Encrypt**, and choose **Use Shared Passphrase**.

   The Encrypt - Shared Passphrase dialog box opens. This dialog box displays the name of the current directory, the file about to be encrypted, and two text boxes where you enter and verify a shared passphrase.

3. Type a shared passphrase in the **Passphrase** text box, and press TAB.

   CAUTION: Because this passphrase will be shared with others, it should be different from any other passphrases or passwords you may use.

4. Type the passphrase again in the **Verify** text box.

5. Select the appropriate options to encrypt the file as a self-extracting one, to delete the original file or both. See "Creating a Self-Extracting, Encrypted File to Share" below.

6. Choose **OK**.

   During encryption, a separate file is created to store the encrypted data for each file. The original files will not be erased unless you checked the **Delete original file(s)** option. If the **Encrypt as <u>self</u> -extracting Windows file (.exe)** checkbox was **not** checked, the Smart Card Security Kit changes the file name and icon, and adds the extension of **.s!!** to indicate that the file has been encrypted with a shared passphrase.

7. Tell the person receiving your file the shared passphrase.

   > **Important**:   Communicate the passphrase in a secure manner: in person, by phone, or by fax. Do not include the passphrase in e-mail.

Creating a Self-Extracting, Encrypted File to Share

You may want to share a file with a Windows user who does not have the Smart Card Security Kit. You can encrypt the file and provide a way for a Windows user to decrypt it. When the Windows user double-clicks on the file and enters the shared passphrase, the file decrypts itself. It is a self-extracting file.

> **NOTE:** To maintain compatibility with Windows 3.1 users, the Smart Card Security Kit software creates a file with an eight-character name. You may want to rename the file in advance with this in mind.

To create a self-extracting, encrypted file:

1. Select the file to be encrypted.

2. From the **<u>F</u>ile** menu, select **<u>E</u>ncrypt**, and choose **Use <u>S</u>hared Passphrase**.

   You can encrypt only one file at a time when creating a self-extracting file.

   The Encrypt - Shared Passphrase dialog box opens. This dialog box displays the name of the current directory, the file about to be encrypted, and two text boxes where you enter and verify a shared passphrase.

3. Type a shared passphrase in the **<u>P</u>assphrase** text box, and press TAB.

   > **CAUTION:** Because this passphrase will be shared with others, it should be different from any other passphrases or passwords you may use.

4. Type the passphrase again in the **<u>V</u>erify** text box.

5. Select the **Encrypt as <u>self</u>-extracting Windows file (.exe)** checkbox.

6. Choose **OK**.

7. Tell the person receiving your file the shared passphrase.

   > **Important**: Communicate the passphrase in a secure manner: in person, by phone, or by fax. Do not include the passphrase in e-mail.

During encryption, a separate file is created to store the encrypted data for the original file. The original file will not be deleted unless you checked the **Delete original file(s)** option in the Encrypt - Shared Passphrase dialog box.

The Smart Card Security Kit changes the file extension to **.exe** to show that it has been encrypted as an executable file. To enhance confidentiality, you can rename the encrypted executable file. When the file is decrypted, the Smart Card Security Kit restores the original name of the file.

Decrypting Files with Your Smart Card

Decrypting files is as straightforward as encrypting them.

To decrypt files:

1. From Windows Explorer, select the encrypted files.

   Remember, file names for manually encrypted file names include the characters: **(!)**. You cannot decrypt files in an AutoCrypt folder. You must remove files from the AutoCrypt folder to decrypt them.

2. Right-click on the file names, select **Decrypt**, and choose **Use Smart Card Key**.

   The Decrypt – Smart Card key dialog box opens.

3. Choose **OK** or press ENTER to decrypt the files.

   The files are renamed to their original names. (For example, the file **myfile(!).doc** becomes **myfile.doc**.) This name change reflects the decrypted state of the files.

Decrypting and Opening a File

With the Smart Card Security Kit, you can decrypt a file automatically when opening it from any Windows application.

To open a file:

1. Open the application as you would normally.

2. Select **File** from the menu bar, and choose **Open**.

   The File Open dialog box opens.

3. Select the file you want to open, and choose **OK**.

   The file is decrypted automatically when it opens using the application that created it. When you close the file, it returns to an encrypted state.

Windows lets you open a data file using its associated application by double-clicking on the file in Windows Explorer or My Computer application. The Smart Card Security Kit extends this capability to encrypted files.

Decrypting Files with a Shared Passphrase

Shared Passphrase Decryption

When someone sends you a file with the **.s!!** extension, you can decrypt the file if you know the shared passphrase used to encrypt it.

To decrypt one or more files that have been encrypted with the same shared passphrase:

1. Double-click on the file or files.

OR

Select the encrypted files in Windows Explorer, choose **Decrypt** from the **File** menu; then choose **Use Shared Passphrase**.

The Decrypt - Shared Passphrase dialog box opens with the name(s) of the file(s) to be decrypted.

2. Type the passphrase in the edit box. If you enter the wrong passphrase you will not be asked to enter it a second time. Double-click on the file or files again to re-enter your passphrase in the edit box.

3. If you want to erase the encrypted file, click the **Delete encrypted file(s)** check box.

4. Choose OK or press ENTER to decrypt the files.

The original encrypted files will not be erased unless you checked the **Delete encrypted file(s)** option on the Decrypt - Shared Passphrase dialog box. The decryption process restores each file to its original file name.

Decrypting a Self-Extracting, Encrypted File

To decrypt a file that has been encrypted as a self-extracting file:

1. Double-click on the file.

The following dialog box opens.

2. Enter the shared passphrase used for encryption.

3. If you want to place the decrypted file in a different folder, do the following steps:

- Select the **Decrypt into a different location** checkbox.

- Select the folder and change the network drive. (You can change the file name if you want.) Choose **OK**.

This may be useful, for example, if you do not have write access to the folder that contains the self-extracting file (such as a CD-ROM or network without write access).

If you entered the correct passphrase, the encrypted information is decrypted and placed in the folder you specified. The self-extracting encrypted file remains in its original folder.

Launching and Decrypting a Self-extracting File

To decrypt a file and open it within its associated application:

In Windows Explorer this is done in two operations:

1. Double-click the encrypted file to decrypt it;

2. Double-click the decrypted file to launch the application that is associated with it.

AutoCrypt Folders

When you select a hard drive or mapped folder and activate the AutoCrypt feature, that folder becomes an AutoCrypt folder. All the files in an AutoCrypt folder are automatically encrypted (except for special files, as noted in "Files That Cannot Be Encrypted" on page 33). Also, any new files created in or moved to an AutoCrypt folder or any of its subfolders are encrypted.

You can create AutoCrypt folders from folders on the hard drive and the network folders that appear in My Computer. You cannot create AutoCrypt folders from folders on unmapped drives or on removable media (such as diskette, Zip, and CD-ROM disks). Therefore, do not use the Smart Card Security Kit through Network Neighborhood.

CAUTION: Never share files that are encrypted with your smart card key. If you do, recipient will not be able to decrypt the file.

To share a file that is encrypted with the **Use Smart Card Key** option, you must first decrypt it, then encrypt the file using the **Encrypt, Use Shared Passphrase** contextual menu option (see "Encrypting Files with a Shared Passphrase" on page 40). A file encrypted with a shared passphrase is safe to share through e-mail.

If a file is located in the AutoCrypt folder, you can choose not to automatically decrypt the file, using the **SCsecurity Features**, **Disable Automatic Decryption** contextual menu option. There may be times when you do not want a file to decrypt automatically, for example, when you perform a back up (see "Disabling and Enabling Automatic Decryption" on page 46.)

Activating AutoCrypt

⊟ To automatically encrypt all files in a folder on a hard drive or mapped network drive:

1. In Windows Explorer, select one or more folders to place on the AutoCrypt List.

    IMPORTANT: Folders in Network Neighborhood cannot be added to the AutoCrypt List.

2. In the **File** menu, select **AutoCrypt**, and choose **Add Folder to AutoCrypt List**.

3. Choose **OK** or press ENTER.

    The files within the selected folders are now encrypted. The folders and all subfolders are now AutoCrypt folders and are part of the AutoCrypt List. Individual file names within the folder do not change when a folder becomes an AutoCrypt folder. The folder's icon changes to display a lock; any file placed inside becomes encrypted (except for special files, as noted in "Files That Cannot be Encrypted" on page 33), but the filename does not change.

Removing AutoCrypt

The **Remove folder from AutoCrypt list** feature removes a folder and its subfolders from the AutoCrypt List, and decrypts all files inside. All encrypted files will be decrypted, and any files added at a later time will not be encrypted automatically.

⊟ To remove a folder and its subfolders from the AutoCrypt List:

1. Close any files that reside in the AutoCrypt folder you want to remove from the AutoCrypt List.

2. In Windows Explorer, select one or more folders to remove from the AutoCrypt List.

3. In the **File** menu, select **AutoCrypt**, and choose **Remove folder from AutoCrypt list**.

4. Choose **OK** or press ENTER.

The folders are no longer AutoCrypt folders and are no longer in the AutoCrypt List. Individual files within the folders are decrypted and the folder's icon returns to the normal Windows folder icon. Files placed inside this folder will no longer be encrypted automatically.

Editing the AutoCrypt List

The AutoCrypt icon indicates that the folder is on the AutoCrypt List. You can display the AutoCrypt List to see all AutoCrypt folders. From the Edit AutoCrypt List dialog box, you can add folders to the list, which is the same as activating them.

⊟ To display the AutoCrypt List:

Right-click on the Windows **Start** button, select **AutoCrypt**, and choose **Edit AutoCrypt List**.

The Edit AutoCrypt List dialog box opens.

Adding a Folder to the AutoCrypt List

🔲 **To add a folder to the AutoCrypt List:**

1. In the Edit AutoCrypt dialog box, browse to a folder you want to add to the list, and select that folder.

2. Choose the **Add** button.

   The selected folder appears under the **Optional AutoCrypt Folders:** list box.

   You can add folders from any location, except from unmapped network drives and removable disks.

3. To save the AutoCrypt List, choose **OK**.

   The folder icon changes to an AutoCrypt folder icon. The files in this AutoCrypt folder are automatically encrypted. The files decrypt when you open them, and re-encrypt when you close them assuming that the Auto Decryption feature is enabled.

Removing Folders from the AutoCrypt List:

Besides using the **Remove Folder From AutoCrypt List** feature as shown in "Removing AutoCrypt" on page 45, you can deactivate AutoCrypt folders by removing them from the AutoCrypt List. Removing a folder from the AutoCrypt List removes its subfolders and decrypts any files in those folders. Any new files added will not be encrypted automatically.

🔲 **To remove a folder from the AutoCrypt List:**

1. Close any files that reside in the AutoCrypt folder that you are removing.

2. In the Edit AutoCrypt dialog box, in the **Optional AutoCrypt Folders** list box, select the folder you want to remove from the AutoCrypt List, and click the **Remove** button.

3. Choose **OK**.

   The folder is no longer an AutoCrypt folder. Any new files you place in the folder must be manually encrypted.

SCsecurity Features

Disabling and Enabling Automatic Decryption

With the **Disable Automatic Decryption** and **Enable Automatic Decryption** features, you can choose whether or not your files automatically decrypt. There may be times when you do not want a file to decrypt automatically, for example, when you perform a backup. By default, the Smart Card Security Kit installation sets the default setting of the decryption to automatic decryption after installation.

▣ **To disable or enable automatic decryption:**

1. Right-click the Windows **Start** button.

2. Select **SCsecurity Features**, and choose **Disable Automatic Decryption** or **Enable Automatic Decryption**.

NOTE: The **Disable Automatic Decryption** and **Enable Automatic Decryption** features affect all your files, not just the files on which you are currently working. This is a toggle function and remains in the state in which it was last placed. So, if you choose Disable Automatic Decryption, the choice on the menu will change to "Enable Automatic Decryption", and it will remain in that state until next chosen.

About... displays copyright information, software version, etc.

Getting Help

SCsecurity User Help... provides information on the IBM Smart Card Security Kit User features, procedures, menu options, and dialog boxes.

Part III

The remaining chapters address other miscellaneous features of the Smart Card Security Kit user software.

7

Special IBM Smart Card Security Kit Features

Previous chapters presented the basics of your Smart Card Security Kit. This chapter adds further details about how to enhance your security with the IBM Smart Card Security Kit features.

Topics include:

- **Emergency Access** – How to decrypt a file if the smart card is not available.

- **Associating a File with an Application** – How to link a file to an application so that double-clicking a document launches the proper application.

- **Moving or Copying a File without Decrypting it** – How to move or copy a file without decrypting it.

- **Using Digital Certificates and Signatures with Netscape Navigator, Netscape Communicator or Microsoft Internet Explorer** – How to use digital certificates and digital signatures using these web browsers.

Emergency Access

To decrypt a user's files with the Emergency Access key:

Files can be decrypted on any computer where the administrator has access. To decrypt the files on a different computer:

1. Copy the encrypted files to a diskette using the **Copy Here Without Decrypt** or the **Move Here Without Decrypt** menu option.

   - Select the encrypted files.

   - Click the right mouse button and drag the files to the floppy drive.

   - Release the right mouse button and choose **Copy Here Without Decrypt** or **Move Here Without Decrypt**.

2. On the computer where the Emergency Access software resides, select the files to be decrypted from Windows Explorer or My Computer window.

3. Right-click the mouse button, select **SCsecurity Emergency**, and choose **Emergency Decrypt**.

What happens next depends on how your organization has set up the Emergency Access key, see the Administrator Reference Manual.

Associating a File with an Application

Windows uses the last three characters following the period in the file name to determine the application in which to open the file. For example, double-clicking a file with the extension **.doc** opens the file in Microsoft Word or Microsoft WordPad.

If Windows does not recognize the file's extension, you can associate a file extension with an application. In Windows Explorer, select the file, and choose **Options** from the **View** menu. Then, click the **File Types** tab to display options for associating that extension with the appropriate application.

Moving and Copying Encrypted Files without Decrypting

To view the Smart Card Security Kit move and copy menu options:

1. Select an encrypted file or AutoCrypt folder from the Contents window on the right-hand side of Windows Explorer.

2. Hold down the right mouse button, and drag the file or folder to a new location.

3. Release the right mouse button and view the menu options:

- **Mo<u>v</u>e Here Without Decrypt** moves an encrypted file to a new location without decrypting it.

- **Co<u>p</u>y Here Without Decrypt** copies an encrypted file to a new location without decrypting it.

Files Encrypted with a Different Smart Card

If you cannot open, copy, move, or rename a file, that file has probably been encrypted with someone else's smart card. To move or copy these files, select them with the right mouse button and use the Smart Card Security Kit menu options. For more information on how to use these special Smart Card Security Kit menu options, see the section, "Moving and Copying Encrypted Files without Decrypting."

If another user wants to share an encrypted file with you and the file was encrypted using the **Use Smart Card Key** menu option, ask the user to decrypt the file, and then re-encrypt the file using the **Use S<u>h</u>ared Passphrase** menu option.

NOTE: When viewing the property sheet of a file encrypted with another user's smart card, you may get an error message. You are still able to read the property sheet.

Using Windows Explorer with the Smart Card Security Kit.

The procedures in this User Reference Manual use the Windows Explorer menu when giving instructions. Generally, the procedures are of the "select-and-command" style:

- Select a file or folder in the Contents window of Windows Explorer.

- Pull down the **<u>File</u>** menu.

- Select a SCsecurity Kit item for the contextual menu.

OR

- Select a file or folder in the Contents window of Windows Explorer.

- Right-click the mouse to bring up the SCsecurity Kit contextual menu.

- Select a SCsecurity Kit item for the contextual menu.

NOTE: The Smart Card Security Kit encrypts files automatically when they are closed, not when they are being saved from an active application. Any event that causes an application to terminate without closing open files will leave those files decrypted. Automatic encryption may not take place if the computer crashes or abruptly shuts down while a file is still open.

In case of a (hardware or software) crash, non-encrypted files will be in the same directory as the encrypted files.

How to install a Digital Certificate and Signature to a Web Browser

See the GemSAFE documentation located on the CD-ROM for details on how install a Digital Certificate and Signature with Netscape Navigator, Netscape Communicator or Microsoft Internet Explorer. To read the GemSAFE manual, you will need to install Adobe Acrobat Reader located on the CD-ROM.

See also the Gemplus white paper entitled "GemSAFE White Paper: Understanding the Fundamentals of Smart Card-Enabled Security for the Internet and Setting Up GemSAFE Applications."

8

Uninstalling the User software

Before Uninstalling the SCsecurity Software

Before uninstalling the software, make sure all encrypted files have been decrypted. All users must decrypt all files before uninstalling the Smart Card Security Kit.

Uninstalling SCsecurity Software

Uninstalling the user software removes the Smart Card Security Kit software from your computer. It also removes references to your Smart Card Security Kit files in the Windows registry and other locations.

IBM recommends that you use the standard Windows **Add/Remove Programs** option to uninstall the Smart Card Security Kit user software.

To uninstall the Smart Card Security Kit from your computer:

1. Log on to the Desktop.

2. Close all other programs and any Smart Card Security Kit windows.

3. From the Control Panel, choose **Add/Remove Programs**.

NOTE: You can also use the **Start** menu **Run** option to run the IBM Smart Card Security Kit Uninstall program to remove the IBM Smart Card Security Kit administrator software from the hard drive. The Add/Remove Programs Properties sheet opens.

4. Choose **SCsecurity** from the program list, then click **Remove**.

   A confirmation dialog box opens.

5. If the Remove Shared File? dialog box opens. Choose **Yes**.

   Uninstalling removes all shared programs used by the IBM Smart Card Security Kit.

5. Choose OK or press ENTER to reboot your machine and complete uninstalling. Windows will be restarted.

9

Troubleshooting

Please try the solutions provided here before calling technical support. The following table provides specific solutions for specific problems or more information about an error message you might encounter while using the Smart Card Security Kit. Problems with common solutions appear in the same box. The numbers do not represent steps, but rather multiple solutions to a single problem, as described in the "Problems" box.

Problems	Additional Information
Unknown error.	This message will appear if the program cannot find an accurate error message. If this message does appear, please contact Technical Support and provide as much detail as possible on the sequences of events that produced this message.
No card detected in the reader.	1. Remove and reinsert the smart card. 2. Remove reader from PC Card slot and re-insert it. 3. Some modem drivers may conflict with the card reader in the PC Card slot. Get an updated modem driver from the manufacturer. Discontinue use of a modem whenever possible while using the Smart Card Security Kit.
PIN is correct, but info is missing on the card.	The smart card may be blank. See your administrator or Information Technology (IT) technician.
Card blocked and unblockable., Or Card must be unblocked to continue.	The maximum number of PIN presentations has been used. See your administrator or Information Technology (IT) technician to unblock it.
You must enter the Administrator PIN for the smart card. No PIN has been presented yet., Invalid PIN has been presented., Text box "Confirm PIN" must have the same value "New PIN"., PIN is too short OR PIN is too long.	Enter a valid Personal Identification Number.
Not enough memory available on smart card.	Certificate may be too large for the card. Obtain a smaller certificate.
Wrong card or card out of order.	Obtain a replacement card from Administrator. (Keep the old card, just in case.)

Problems	Additional Information
Another program already uses the card.	Quit any program that is likely to also use a smart card.
An error has occurred during DLL loading.	Another program may be using the DLL.
An error has occurred during PKCS operation.	A generic error has occurred while communicating with the smart card.
The logon dialog box was closed because of a screen saver activation.	Move the mouse or press a key on the keyboard to display the logon dialog box.
Could not write to the disk. Disk might be write-protected.	Move write-protection tab from floppy disk or use a different floppy disk.
The user preference file may not be backed up to the user install disk.	Ask the Administrator to copy the pkfile in the user's directory.
Failed to open your preference file. The preference file is either corrupted or doesn't exist. Do you want to restore your preference from the backup disk ?	Answer "NO" to the question, then locate the file "userpref.!!!", erase it, remove the card from the reader and restart the computer. The IBM Smart Card Security Kit will create a new file.
Cannot display Administrator Options	The smart card is damaged beyond repair. Have the card replaced.
The maximum number of PIN presentations has been reached. All of the options are now unavailable. Smart Card blocked!	Contact your administrator to have the card unblocked.
The maximum number of PIN presentations has been reached. All of the administrator options are now unavailable.	The Administrator will provide a new card. The card has been permanently blocked.
If the above solutions were ineffective:	Save all open documents, close all applications and restart the computer. If the restart does not solve your problem, contact technical support.

Glossary

Account Credentials	Account credentials provide proof of the user's identity on the network. They include at least user name, password and domain.
Administrator	The person who holds supervisory rights to customize the User Setup and initiate the emergency file access procedure.
Administrator Preferences	Settings created by the administrator, which are used during a user installation. These settings are placed in files and normally written to the user setup diskette at the end of Administrator Setup.
Administrator Setup	The setting up of administrator software, including emergency file access, and user software configuration.
Administrator Software	The part of the IBM Smart Card Security Kit used to configure and maintain administrative control over the Smart Card Security Kit User Setup.
AutoCrypt	The Smart Card Security Kit feature that automatically encrypts and decrypts files in folders (and subfolders) the user or administrator has chosen to keep secure.
Card Diagnostics Window	Displays details on the installed smart card and smart card reader.
Cryptography	The practice and study of encryption and decryption. The encoding of data so that only authorized individuals have access to it.
Cryptography	The practice and study of encryption and decryption. The encoding of data so that only authorized individuals have access to it.
Decryption	The reverse of encryption. Decryption returns data to its original state, making it readable again.
Disabling Security	Removes the administrator requirement from the Emergency Unlock feature. Both administrators and users will be able to log in. All Scsecurity and smart card services will be disabled, including file encryption and decryption.

Domain	In Windows NT 4.0, a group of computers that share a directory database and security policy. A domain provides access to user accounts and group accounts and is identified by a unique name.
Emergency Access	The Smart Card Security Kit feature that enables trusted individuals to gain access to files without the password of the user who encrypted the files.
Encryption	The transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended.
Group	A collection of individuals within an organization who share the same administrator. The group can also refer to the administrator's work group. This information is used for emergency access purposes.
Home Domain	The domain that is identified on the user's smart card account.
Home Domain Account	The NT user account that is stored on the smart card. This account includes user name, password and domain. It is created and modified by an administrator with the exception of the password, which can also be changed by the user.
Key	A very large number the Smart Card Security Kit uses to encrypt and decrypt a file.
Key Generation	The creation of a key for encryption and decryption.
Locked Workstation	The IBM Smart Card Security Kit has both an automatic and a manual lock. When the workstation is locked, applications and documents remain open, but are inaccessible. A locked workstation can only be unlocked by re-inserting the smart card and entering the user PIN.
Log in	To identify oneself on a computer or network, in order to access an account that has been set up in a particular domain. The IBM Smart Card Security Kit supports an automatic login to access the smart card account, and a manual login to access all other accounts available on the computer. To be considered logged in to the smart card account, the user's PIN must be entered and the account authenticated.
Log off	To end a user session and remove the account from active use until the next login.
Organization	A collection of individuals who share the same administrator. The organization can also refer to the administrator's organization. This information is used for emergency access purposes.
Passphrase	A string of characters used to gain authorized access to a computer and its data. Passphrases are usually longer than passwords, and therefore, more secure.
Personal Identification Number (PIN)	A string of 4 to 8 characters used to gain authorized access to a computer and its data.
Personal Security Device (PSD)	A smart card or encrypted file. The PSD contains information about the user including the user's X.509 certificate and the IBM Smart Card Security Kit "smart card key."

Pkfile (User preference file)	The user preference file (**pkfile**) containing your administrator's public key and Emergency Access information. The IBM Smart Card Security Kit uses the information in this file combined with your PIN protected smart card to generate your "dynamic" user preference file, at the time you log onto the computer.
Plain Text	Readable text. Text that is not encrypted. Clear text.
Privacy	The protection of a message such that only intended recipients can read a message.
RC4® Symmetric Cipher	The technology behind file encryption. RC4 uses randomly seeded keys to encrypt files.
RSA Public Key Cryptosystem™	The technology behind Emergency Access. The IBM Smart Card Security Kit public key is the key exchanged between the administrator and the users of the IBM Smart Card Security Kit. It enables the emergency decryption of files.
Screen Saver	The Smart Card Security Kit feature that prevents access to, or use of , a computer (excluding the mouse and keyboard) until a smart card is present and a PIN is entered
Scsecurity Options	Include locking the workstation, changing a password, and performing a logoff or computer shutdown.
Smart Card Key	The key generated during User Setup. This key personalizes each user's version of the IBM Smart Card Security Kit. The "smart card key" is stored in the Smart Card and is protected by the user PIN. The user's "smart card key" is used to encrypt and decrypt a file when the **Use S̲mart Card key** menu option is selected.
Security Log File	A file found in the Smart Card Security Kit administrator's directory. It records any attempts to recover files.
Shared Passphrase	A string of characters used to gain authorized access to data. Passphrases are usually longer than passwords, and therefore, more secure. Shared passphrases are used to encrypt and decrypt files the user wishes to share with other users.
Smart Card	A personal security device that can perform its own cryptographic calculations and have an access control system.
Smart Card Options	Include changing the PIN, changing the user's profile, backing up the smart card, card diagnostics, suspending security, and disabling security.
Smart Card Services	Include Smart Card Options, SCsecurity Options, and all file encryption and decryption functions.
Suspending Security	Temporarily disables smart card checking during an active user session. This allows the user to remove the smart card from the reader and insert a different one.
Trust Accounts	In Windows NT, the user's login information can be passed to a separate *trusting* domain, where the user will be authenticated. A trusting domain is one that honours information passed from a *trusted* domain, where the user has logged in. User or group rights and resource permissions can be defined in the trusting domain, although an account has not been set up there for the user or group.

Trustee	One person out of a group of people entrusted to authorize Emergency Access to the user's encrypted files.
Trustee Key Diskette	A diskette that holds one trustee key file.
Trustee Key File	One file that enables access to the Emergency Access key. The Emergency Access key is split up and placed in multiple files (trustee key files), each held by a different person (a trustee) and each protected by its own Emergency Access passphrase.
User Name	A unique name used to log on to a computer or network service to access information.
User Preference File (pkfile)	The user preference file (**pkfile**) contains your administrator's public key and Emergency Access information. The IBM Smart Card Security Kit uses the information in this file, combined with your PIN-protected smart card, to generate your "dynamic" user preference file, at the time you log on to your system.
User Setup	Installing and setting up the Smart Card Security Kit user software on a computer.
User Setup Diskette	The diskette that holds the administrator public key file (pkfile). This diskette must be generated by the administrator before users make use of it.
Windows System Policies	Windows System Policies are created with the System Policy Editor to define and restrict the user's work environment. System Policies can be set for individual users, computers, groups or for all users. System Policies will override settings created by the user.
Windows User Policies	In Windows NT, define the rights and permissions set by the administrator for a user or group.

Index