IBM Smart Card Security Kit

OPTIONS
by IBM

Administrator 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, Windows 95 and Windows 98 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: DAARM20P

IBM and GEMPLUS reserve the right to change the functions and specifications of its products at any time without prior notice.

This document was prepared by GEMPLUS and IBM for both its clients and for its own internal use. The information contained herein is the property of GEMPLUS and IBM. This information shall not under any circumstances be reproduced without prior consent of both companies.

The following paragraph does not apply to the United Kingdom or any country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time.

This publication was produced in the United States of America. This publication was developed for products and services offered in the United States of America. IBM may not offer the products, services, or features discussed in this document in 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 Administrator Reference Manual contains instructions for installation and setup of the IBM® Smart Card Security Kit hardware and software for Microsoft® Windows® NT 4.0. The complete User and Administrator Reference Manuals are contained on the Smart Card Security Kit CD 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 Administrator Reference Manual and become very familiar with its contents.

The IBM Smart Card Security software (SCsecurity) allows diskettes to be made from the software CD for users without a CD-ROM drive. Diskettes can be generated from within the Installation utility by clicking on the appropriate button.

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

The user then sets up the user software, using parameters generated during the administrator software installation. Refer to the User Reference Manual on the CD-ROM for a complete description of the options available.

NOTE: An IBM Smart Card Order Form is available at the end of this Administrator Reference Manual. Use it to order additional smart cards.

NOTE: You will be prompted to enter a Personal Identification Number during the installation of the Smart Card Security Kit. The preset or default Administrator Personal Identification Number (PIN) and User PIN for all smart cards is 1234. However, you must replace the Administrator 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 individual 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 contents of the folder 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 will unlock 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 (referred to as "trustees") hold different parts of the key file. While each trustee holds a key file, only a specified proportion 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 using 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.

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 Keyboard Port

Document Conventions

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

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

  Enter 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 **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 self-extracting Windows file (.exe)** check box.

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

  Select **Use Smart Card key** from the **Encrypt** menu.

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

  Enter the user name in the **Name** field and click **OK**.

The terminology used in this Administrator Reference Manual appears in the Glossary starting on page 63.

IMPORTANT: Notes, cautions and other important information are enclosed between two lines before and after the text that you must read and act upon to prevent potential problems.

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 Administrator 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 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

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 section of the this Administrator Reference Manual describes the features of the IBM Smart Card Security Kit, the organization of a security system, and it explains the installation and setup of the Administrator 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 Administrator 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.
- **Administrator Overview** – How to plan for and implement the IBM Smart Card Security Kit.
- **Security Plans** – How the IBM Smart Card Security Kit adapts to organizations of different sizes.
- **How Emergency Access Works** – How to recover data in an emergency.
- **Emergency Passphrase Suggestions** – How to compose robust passphrases.

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. 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 Administration Module

Powerful Encryption Technology

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 into 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 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:

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

A secure screen saver blocks access to your system if the smart card is removed from the reader. Access is available after entering the proper PIN when the smart card is reinserted into the reader.

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 number of trustee key files are required to decrypt user files.

Backup Restore Utility

The Backup Restore Utility allows the backup of card information. The contents of a backup, such as user information, can be restored to a card by an administrator. The Backup Restore Utility can only be accessed during a user session.

Remote Administration

Emergency file recovery can take place at the administrator's computer. The Smart Card Security Kit safeguards privacy with a method of distributing authority over file recovery. The Smart Card Security Kit's security log file provides a record of all emergency file recovery activity.

Multicard Support

Multicard support allows the use of applications for other smart cards. When security is suspended, other smart cards can be inserted into the reader and used with their associated application software.

Administrator Overview

This section provides an overview of how to strengthen your file security plan with your IBM Smart Card Security Kit.

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 and Setup 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, using a diskette or a network folder.

Some Considerations

To customize the setup for your users, you must make the following decisions:

- **On what computer do you want to keep the administrator software?**

If possible, the administrator software should be kept on an administrative computer. It should be accessible to the administrator and trustees only.

- **How do you want to distribute the Emergency Access key?**

You can split up the Emergency Access key among responsible members (trustees) of your organization. Gaining access to data then requires a minimum number of the trustees to agree to unlock a user's encrypted file. "How Emergency Access Works" on page 23 will help you make an informed decision.

- **How may trustees participate in the IBM Smart Card Security Kit's Emergency Access procedures?**

During Emergency Access setup, if you do choose to split the Emergency Access key, you designate the number of trustees and the threshold number (for example, 4 out of 7) required to access encrypted data. All trustees must participate in Emergency Access setup.

Emergency file access requires that trustees be present as well, but only the minimum required number of trustees designated as necessary for recovering data. "How Emergency Access Works" on page 23 will help you make an informed decision.

Security Suggestion

Allow only the Emergency Access trustees and administrator to observe the emergency decryption process. Such a restriction avoids the possibility of others seeing the entry of the Emergency Access key passphrases, knowing the required number of trustees, or even knowing what the Emergency Access key diskettes look like.

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.

The Smart Card Security Kit setup consists of two parts:

- **Administrator Setup –** for installation of applications that allow the emergency recovery of files, creation of the passphrases, and enforcement of organizational security policy. In essence, it designs your users’ file security plan.
- **User Setup –** for the installation of encryption and decryption software and the implementation of the file security plan defined by the administrator.

As you step 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 defined 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 several distinct internal groups

Implementing the IBM 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 on separate computers. The user can act also as the administrator for 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.

These two steps are executed sequentially if the Stand-Alone option is chosen during installation.

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 system.
2. Distribute the user setup diskettes to users or store equivalent files in a network folder.

Implementing IBM 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 22. Each group's name must be unique. Each group's administrator then distributes the customized user setup files through diskettes 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 representative.

How Emergency Access Works

The Emergency Access feature allows recovery of the encrypted files for 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 accessing encrypted files. The administrator places the public key portion on the User Setup Diskette, copies the diskette, and distributes the copies 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 entrusted to 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 or the user can copy the user's encrypted files into a directory or removable media 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.

The administrator can verify that a user who requests emergency decryption is the same user who encrypted the file during the file recovery process. Additional Emergency Access information can be found in the security log file. For more information, see "Security Log File" on page 60.

Emergency Access Passphrase Suggestions

Creating a strong passphrase is vital for ensuring the security of data. To create strong passphrases:

- Use at least 10 characters: the IBM Smart Card Security Kit requires a minimum of 8 characters.
- Use various uppercase and lowercase letters, spaces, numbers, punctuation, and symbols.
- Avoid using any character more than twice.
- To prevent a potential intruder from discovering the passphrase through a dictionary search, avoid words listed in the dictionary.
- Avoid using personal information that a potential intruder could guess or find: the name of your spouse, child, or parent; your home or work street name, number, or city; your birthday, telephone number, or social security number.
- Create a passphrase you can commit to memory. Do not reveal it to anyone. If you write it down, store the paper in a secure, locked place.

Weak Passphrases	Strong Passphrases
Abcdefghi	*4 score & 7 years ago*
Qwerty	>>I R8 her Hily!<<
Junior Johnson	Jr. wakes up like this (:-o)

2

Installation

The IBM Smart Card Security Kit protects your computer from intrusion and keeps your data private. 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 computer.

The IBM Smart Card Security Kit provides an Emergency Access capability. If necessary, user files can be decrypted with the cooperation of individuals within the organization. These individuals are chosen by the administrator; each holds a part of the organization's Emergency Access key (referenced as "trustees.") If the user forgets his smart card or forgets to decrypt files before an absence, the trustees can work together to recover vital data.

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

- **Compatibility with Windows 3.1 and Windows 95/98** – Explains the compatibility level with the other Microsoft operating system.
- **Migrating to the IBM Smart Card Security Kit** – Instructions for users of other encryption software.
- **Minimum Hardware and Software Requirements** – List the minimum hardware and software requirement for using the IBM Smart Card Security Kit.
- **Before Installing the Software** – Explains what has to be done before installing the software.
- **Installing the Administrator SCsecurity Software** – How to install 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 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 disk space, a VGA 640x480 screen 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 1.44MB 3.5-inch floppy drive;
- Access to a CD-ROM drive;
- Microsoft Windows NT 4.0 with Service Pack 4.

File System

- Install the IBM Security Kit on a NTFS system volume for increased security, rather than a FAT volume. *NT supports NTFS which is native to NT and the old DOS/Win9x FAT system.*

[1] From this point on, we refer to Windows NT 4.0 simply as Windows, 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 support for devices like smart cards was available. 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 the Software

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

Before performing the installation, save all documents, backup important files and close **ALL** running applications including anti-virus programs. You should only leave Explorer and other necessary Windows utilities operational.

Making diskettes from the CD-ROM

IMPORTANT: If you need to create diskettes from the CD-ROM, follow the following 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. Locate a computer that has both a CD-ROM drive and a floppy drive.
3. 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.
4. If AutoRun is not active, select **Start**, and then select **Run**. 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.
5. Select the **Install** button under SCsecurity software.
6. Choose **Make Diskettes** from the Installation Configuration screen.
   a. Select a drive.
   b. Insert a diskette into the diskette drive and click **Generate** in the Make Diskette Install Utility dialog box.
   c. Label each diskette appropriately for proper installation.

7. When the last diskette has been prepared, a message confirming that SCsecurity installation was successfully copied to the diskettes will appear. Select **OK**.
8. In the **Make Diskette Install Utility**, select **Close** to return to the Installation Configuration screen.
9. Use these diskettes to install SCsecurity. For more information, refer to the section “Step 1 b: Installing the Administrator Software From Diskette” on page 29.

Installing the Administrator SCsecurity Software

IMPORTANT: Read all instructions to ensure proper installation.

The following installation scenarios are possible:

1. One person acting as administrator AND user. This type of installation is called “Stand-Alone Security”.

   In the Installation Configuration dialog box, select **Stand-Alone Security**.

   For the Administrator software, see the section on installing the Administrator software on page 29 of this Administrator Reference Manual.

2. One person acting as administrator for several users.

   Install the Administration software **only** on the administrator’s computer. In the Installation Configuration dialog box, select **Administrator**.

   Install the User software on each user system. In the Installation Configuration dialog box, select **User**. Detailed instructions for installing the User software are available in the User Reference Manual.

NOTE: To customize the installation, select **Custom** in the Installation Configuration dialog box. This option allows for a full selection of the security components to be installed. Custom installation should only be used by persons with intimate knowledge of the SCsecurity software and the hardware that it is being installed on.

Using the Installer

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

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.

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

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

Read the International License Agreement. Accept the Agreement to continue with the Installation. Otherwise, the installation will abort.

In the Installation Configuration dialog box, select the type of configuration you wish to install. Select **Help** for information about each installation type.

Step 1a: Installing the Administrator Software From the CD-ROM

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

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**. 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.
3. Select **Install** under SCsecurity Software. The **Welcome** screen will appear.
4. Click **Next** to continue with the installation.
5. 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.
6. In the **Installation Configuration** screen, select the type of configuration you wish to install. Select **Help** for information about each type of installation. To install the administrator software, select **Administrator**.
7. The **Choose Destination Location** window opens. Select a location (directory) where the files will be installed.
8. Click **Next** to begin the installation.
9. Follow the installation steps displayed on your screen.
10. For more information, refer to Chapter 3, IBM Smart Card Security Kit Administrator Setup, on page 31 of this Administrator Reference Manual.

Step 1b: Installing the Administrator Software From Diskette

1. Start Windows NT 4.0, and insert the first 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 software. The Installation welcome screen will appear and explain how to install the application software. Choose **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. On the Installation Configuration screen, select the type of configuration you wish to install. To install the Administrator Security Kit, select **Administrator**.
7. The Choose Destination Location dialog box opens. Select a location (directory) where the files will be installed using **Browse** or accept the default.

8. Click **Next** to begin the installation.
9. Follow the installation steps displayed on your screen.

   For more information, refer to Chapter 3, IBM Smart Card Security Kit Administration Setup on page 31.

Part II

This section addresses the setup of the IBM Smart Card Security Kit Administration Software.

3

IBM Smart Card Security Kit Administrator Setup

This chapter describes how to set up the IBM Smart Card Security Kit administrator's software and preferences. Your trustees must be present to set up the IBM Smart Card Security Kit's Emergency Access if you are splitting the Emergency Access key. Topics include:

- **Before You Begin** – The resources needed for Administrator Setup.
- **Setting Up Emergency Access** – How to create and split up the Emergency Access key.
- **Testing Emergency Access** – How to confirm Administrator Setup.
- **Distributing the User Setup Diskette** – How to make sure the users have the data they need.

Before You Begin

This section lists the resources you need at hand during Administrator Setup.

People who hold emergency key files are called "trustees". Choose trustees with two criteria in mind:

(1) they should be reliable, trusted individuals

(2) they should not all be traveling frequently.

All trustees must be present during setup. Each trustee must have a formatted diskette to store a part of the Emergency Access key.

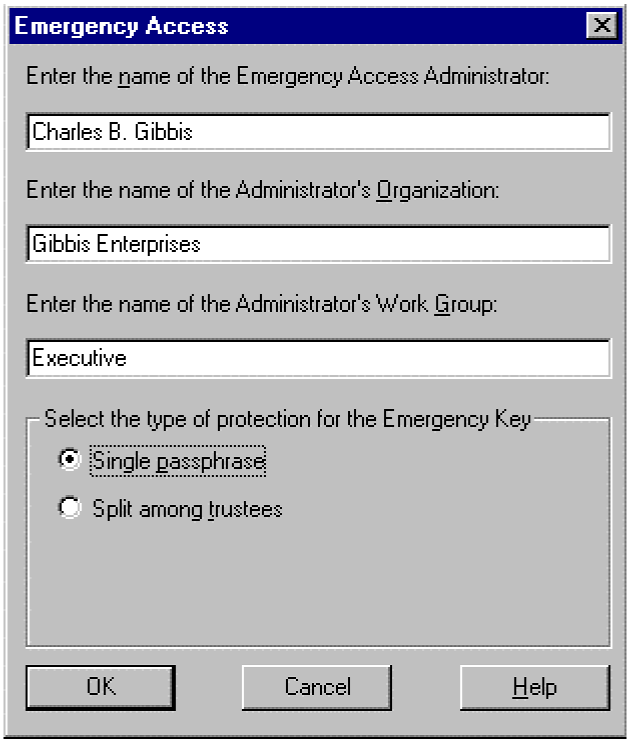
During administrator software setup, you create Administrator files which are copied to a location of your choice. These files will be used during user setup.

After you have set up the administrator software, have a diskette available for backing up the administrator preference files. This backup diskette must be created and strictly guarded.

At this point, the administrator needs to set up the Emergency Access procedure.

Setting Up Emergency Access

The Emergency Access dialog box appears:



Emergency Access

Enter the name of the Emergency Access Administrator: Charles B. Gibbis

Enter the name of the Administrator's Organization: Gibbis Enterprises

Enter the name of the Administrator's Work Group: Executive

Select the type of protection for the Emergency Key

● Single passphrase

○ Split among trustees

Fill in the Emergency Access dialog box as follows:

1. Type the name of the Emergency Access Administrator in the top text box, and press TAB.
2. Type the name of the Organization in the middle text box, and press TAB. The organization refers to the administrator’s organization (this information will be used to locate the administrator when emergency access is needed).
3. Type the name of the Work Group in the bottom text box, and press OK. The Work Group refers to the administrator’s work group (this information will be used to locate the administrator when emergency access is needed).
4. Select the type of protection for the Emergency Key. Refer to the section on **Emergency Key Protection** on page 33.

IMPORTANT: The organization text box and the work group text box can be used for different purposes. They can be used to provide information on the administrator and how to locate him in case of emergency. If the administrator is controlling several groups, the text boxes can also be used to identify a specific security group and subgroup.

The emergency access information should not be left empty. Remember that users will access this information in emergency situations. For more information, refer to the section on Viewing Emergency Access Information on page 37.

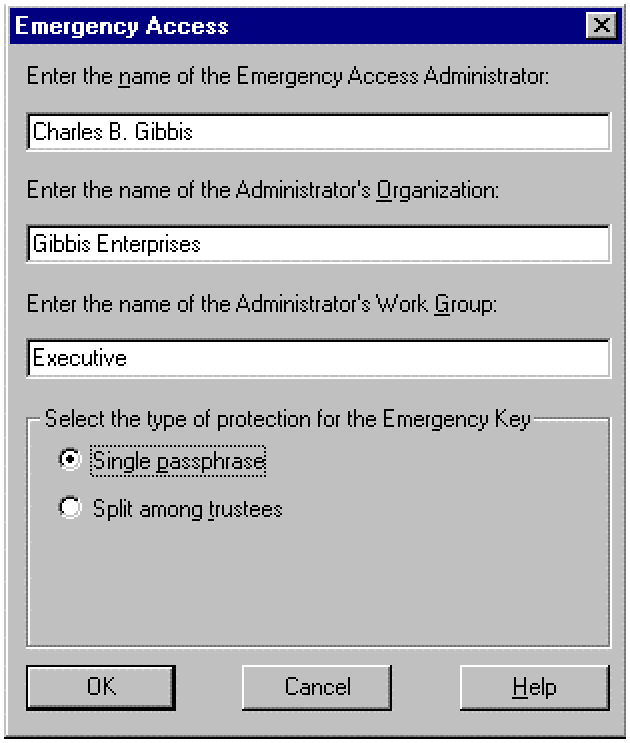
Emergency Key Protection

Choose one of the following options:

- If you chose **single passphrase** to protect the Emergency Access key, go to **Option 1**, below.

OR

- If you chose **split among trustees** to split the protection among several trustees, go to **Option 2** on page 36.



Emergency Access

Enter the name of the Emergency Access Administrator: Charles B. Gibbis

Enter the name of the Administrator's Organization: Gibbis Enterprises

Enter the name of the Administrator's Work Group: Executive

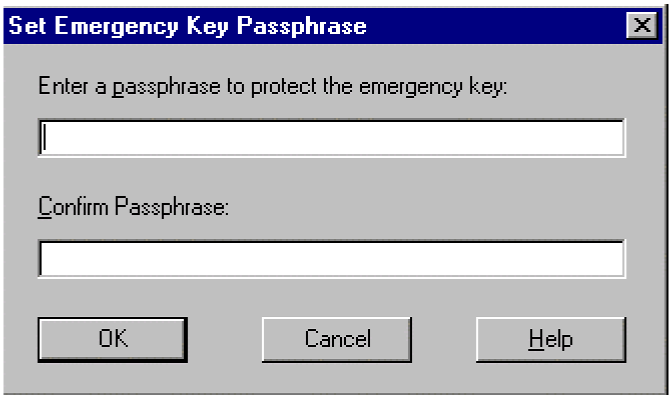
Select the type of protection for the Emergency Key

● Single passphrase

○ Split among trustees

Option 1: Protecting the Emergency Access Key with a Single Passphrase

If you chose **Single passphrase**, the Set Emergency Key Passphrase dialog box opens.


Set Emergency Key Passphrase
Enter a passphrase to protect the emergency key:
Confirm Passphrase:
OK
Cancel
Help

The Emergency Access key passphrase you enter will decrypt any IBM Smart Card Security Kit-encrypted file in your organization, so craft the passphrase carefully.

To protect the Emergency Access key with a single passphrase:

1. Type the passphrase in the top text box, and press TAB.

   The passphrase must have a minimum of eight (8) characters.

2. Type the passphrase again in the lower text box, and choose **OK** or press ENTER.
3. At this point, you are prompted to back up the Administrator preference file (pkfile).
4. Go to the section "**Backing Up the Administrator Preference File**".

Option 2: Splitting the Emergency Access Key Among Trustees

You will be reminded to assemble diskettes to hold the number of Emergency Access key parts you specified.

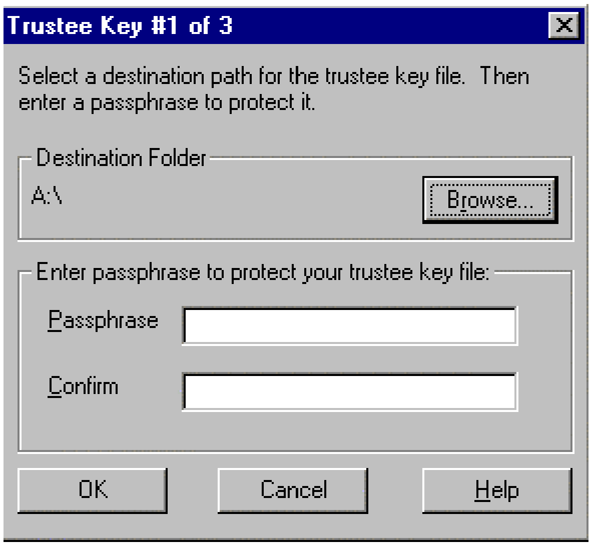
To protect the Emergency Access key with multiple passphrases:

1. If you select Split among trustees, you will have to fill out information about the number of trustees. Enter the number of trustees in the Split among Trustees section. After you have gathered formatted diskettes (one for each trustee) and all trustees are present, choose **OK** or press ENTER to create a Trustee Key Diskette for each trustee.

   Each of the next dialog boxes prompts each trustee to place a trustee key file on a Trustee Key Diskette.

2. Each new trustee will be prompted to enter emergency information.

   - Insert a blank diskette to create a Trustee Key Diskette.



Select a destination path for the trustee key file. Then enter a passphrase to protect it.

Destination Folder: A:\

Enter passphrase to protect your trustee key file:

- Type a passphrase, and press TAB. The passphrase must have a minimum of eight characters.
- Type the passphrase again.
- Choose **OK**.

3. Choose **OK**, and repeat step **2** with each of the remaining trustees.

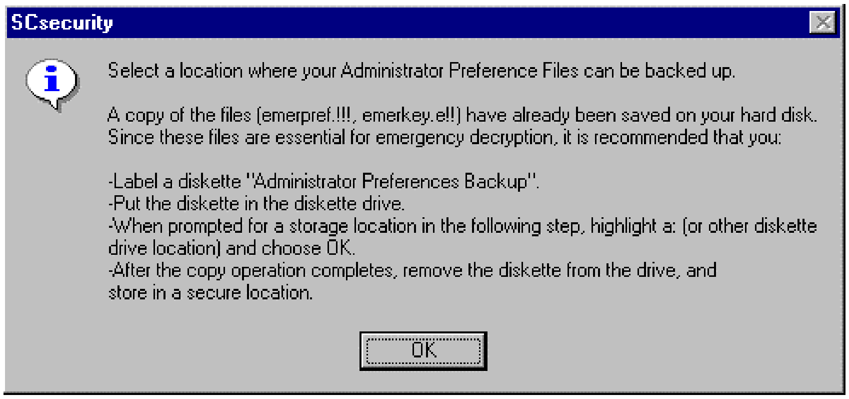
   The Emergency Access Key Generation dialog box opens.

4. Choose OK or press ENTER.

Backing Up the Administrator Preference File

The next step in the setup is to back up the administrator preference file that will be used for Emergency Access.

1. Select the location to save the backup copy of the preference file.
2. If you are backing up to a diskette, insert a blank diskette labeled “Administrator Preferences Backup”.



Select a location where your Administrator Preference Files can be backed up.

A copy of the files (emerpref.!!!, emerkey.e!!) have already been saved on your hard disk.
Since these files are essential for emergency decryption, it is recommended that you:

-Label a diskette "Administrator Preferences Backup".
-Put the diskette in the diskette drive.
-When prompted for a storage location in the following step, highlight a: (or other diskette drive location) and choose OK.
-After the copy operation completes, remove the diskette from the drive, and store in a secure location.

IMPORTANT: The file is copied to the administrator's hard drive automatically. The administrator preference files should also be copied to a diskette as a backup. This backup diskette should be kept in a secure location at the Administrator's office.

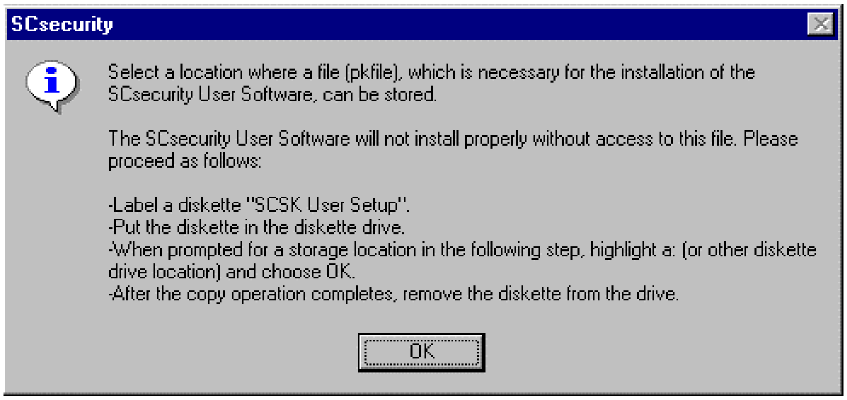
Creating the User Setup Diskette

The next step in the setup is to create the user setup diskette.

3. Select the location where you want to store the user setup file (pkfile) that contains the administrator public key.
4. Insert a blank diskette labeled "User Setup".

IMPORTANT: The administrator public key will be required by the SCsecurity user software installation.

Each user must now install the Smart Card Security Kit user software from the CD-ROM or from diskettes if diskettes were created beforehand. A copy of the user setup file will be required for each user installation. For more information, refer to the User Reference Manual.



Select a location where a file (pkfile), which is necessary for the installation of the SCsecurity User Software, can be stored.

The SCsecurity User Software will not install properly without access to this file. Please proceed as follows:

-Label a diskette "SCSK User Setup".
-Put the diskette in the diskette drive.
-When prompted for a storage location in the following step, highlight a: (or other diskette drive location) and choose OK.
-After the copy operation completes, remove the diskette from the drive.

Testing Emergency Access

Before making multiple copies of your organization’s master User Setup Diskette or placing the files in a network folder, confirm that Emergency Access works.

To test Emergency Access:

1. Install the user software on one computer (for the test, it can be the same machine that holds the administrator software).
2. Place the smart card in the reader and enter a PIN. See the “User Setup” in the User Reference Manual for instructions.
2. Have the user encrypt a file.

   See “Encrypting Files with a Smart Card” in the User Reference Manual for instructions.
3. Decrypt the test file.

   Use the Emergency Access procedure. Refer to “To decrypt a user’s files with the Emergency Access Key” on page 56.

Viewing Emergency Access Information

To display the Emergency Access Information dialog box:

Choose **Emergency Access Info** from the **SCsecurity Emergency** menu.

The Emergency Access Information dialog box opens.

The dialog box shows the following information:

- 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 (and the number of diskettes (trustees) required to decrypt the file).

The organization'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.

Distributing the User Setup Diskette

If the test was successful, make the appropriate number of copies from the master IBM Smart Card Security Kit User Setup Diskette and distribute them to users for installation. Alternatively, you can copy the diskette contents to a directory on your network and instruct users as to where they can find the files for use during user installation.

The SCsecurity CD-ROM contains an Administrator Reference Manual (**admin.pdf**) and a User Reference Manual (**user.pdf**) in portable document format. You can place the IBM Smart Card Security Kit User Reference Manual (**user.pdf**) and the Adobe Acrobat Reader setup program (**ar40eng.exe**) on a network drive for the users' reference during user installation.

Part III

This section addresses the features of the IBM Smart Card Security Kit Administration Software.

4

Administrator’s Tasks

This chapter explains how to use SCsecurity and Smart Card Options to secure your computer, how to recover files, how to access the security log, and how to regain complete security after file recovery. Topics include:

- **Using SCsecurity and Smart Card Options –** Login and logoff, how to initialize smart cards, locking and unlocking the workstation, creating user profiles, and changing PINs and passwords.
- **Overview of the IBM Smart Card Security Kit Administrator Contextual Menu** – Gives a brief overview of the Administrator options available when the contextual menu appears.
- **Using Emergency Access** – How to recover files.
- **Changing Emergency Access Key Protection** – How to update Emergency Access.
- **Security Administrator Help** – How to access on-line help.
- **Security Log File** – Information that is stored concerning emergency recovery attempts.

SCsecurity and Smart Card Options

This next section of the Administrator Reference Manual defines all aspects of the IBM Smart Card Security Kit that deal with securing computer access, including:

- Login and logoff
- Initializing smart cards
- Locking and unlocking the workstation
- Secure screen savers
- Changing PINs and passwords
- Creating user profiles
- Suspending and disabling security

Smart Card User's Home Domain Account

The smart card holds a single user account. This account includes user name, password and domain and is considered the *home domain account.* It is created and modified by the administrator with the exception of the password, which can also be changed by the user.

Logging In

Both *automatic* and *manual* logins are supported:

- In an *automatic* login, the user enters the smart card into the reader and enters the user PIN. Account credentials are read from the smart card. Logging in *automatically* accesses the account stored on the smart card (the home domain account).
- In a *manual* login, the user manually enters account credentials. A manual login provides access to all other accounts available on the computer and on trust domains.

Regardless of whether an automatic or a manual login is performed, users will always be authenticated with the credentials stored on the smart card (if smart card services are active).

NOTE: When you power on the computer, it will always start up with manual keyboard support only. Smart card services will be added when the smart card service loads.

Visually, the initial SCsecurity screen will have the keyboard icon and text only. The smart card icon and text will be added when the smart card service loads. Functionally, if the user logs in manually before the smart card service loads, smart card services will be disabled. To enable smart card services, the user needs to log off, then log in, once smart card service has loaded.

Automatic Login

To log in automatically:

1. Insert the smart card into the smart card reader.
2. Enter the smart card user PIN, in the **User PIN** textbox of the **SCsecurity Login** dialog box and select **OK**.

NOTE: The user will not be considered logged in until the PIN is entered and the account authenticated.

If the user inserts the smart card into the smart card reader, but clicks **Cancel** before entering the PIN, the card will have to be removed and re-inserted.

Login Options

Unauthenticated shutdown, if it has been set up in Windows NT System Policies, will be available at the login stage. This allows the user 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 44, and "Smart Card Options" on page 47.

Manual Login

Users 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, users need to provide complete account credentials.

To login 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. Users 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. This allows the user to login to the account from a remote location.

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

Automatic Card Initialization

Administrators can initialize smart cards, or groups of smart cards, at the login stage. To initialize a smart card:

1. When the initial **SCsecurity** screen appears on the screen, insert a new smart card into the reader. *The initial SCsecurity screen prompts the user to press Ctrl+Alt+Del or insert the smart card into the reader*.
2. Enter the default PIN: 1234. A message will appear indicating that the profile has not been found and the **PIN Request** dialog box will appear.
3. Enter both the User PIN and the Admin PIN in the appropriate text boxes and select **OK**.
4. On the **Smart Card Options (Profile Maintenance)** dialog box, enter:
   - The Cardholder name as it appears on the NT account
   - User name
   - Password
   - Domain
5. Select or deselect **User can suspend smart card security**. If enabled, this allows the user to temporarily suspend smart card options. See “Suspending Security” on page 49.
6. Select or deselect **Consider all screen savers secure**. If enabled, whenever a screen saver is activated, the workstation will automatically lock.
7. Select **OK**. The cardholder account will be stored on the smart card. The specified user will be able log in using the default PIN 1234. See “Changing PINs” on page 48.

See “Changing a User’s Profile” on page 48.

Smart Card Removal

If the smart card is removed, during a user session, the workstation will automatically lock. To unlock it, the user will need to re-insert the smart card and enter the PIN. See “Locked Workstations” and “Unlocking a Locked Workstation” on page 45.

Smart Card Reader Failure or Removal

When a smart card reader is removed or fails, the workstation locks automatically, and becomes inaccessible to the user. However, administrators, with accounts registered on the local computer, are able to allow general access to all users, by disabling security.

To disable security:

1. Re-boot the computer.
2. Press Ctrl+Alt+Del, when prompted. The **Emergency Unlock Workstation** dialog box will appear.
3. Enter administrator credentials for the account and select **OK**.
4. On the next dialog box, select **Smart Card**.
5. On the **Smart Card Options** dialog box, select **Disable Security**.

The following points on *disabling security* should be noted:

- Disabling security is not the same as suspending security.
- Suspending security temporarily disables smart card checking during an active user session. See "Suspending Security" on page 49.
- 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 sevices 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

Automatic Lock

While users are logged in, their workstations will lock automatically 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 activates.

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

Manual Lock

Users are able to lock their workstations at any time during a user session, by following the procedure, below:

1. Press Ctrl+Alt+Del.
2. Select **Lock Workstation** on the **SCsecurity** dialog box.

Unlocking a Locked Workstation

A locked workstation can be unlocked in two ways:

- Automatically by users
- Manually by administrators

Unlocking the Workstation Automatically

As long as smart card readers are functioning properly, users will be able to unlock their computer 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**.

For this procedure to work, the credentials on the inserted smart card must match the credentials of the currently logged user.

Unlocking the Workstation Manually

Alternately, administrators are able to unlock the workstation through the following procedure:

1. Press Ctrl+Alt+Del. The **Emergency Unlock Workstation** dialog box will appear.
2. Enter the user name, password and domain in the appropriate text boxes and select **OK**.

The following conditions must be met:

- The credentials entered are identical to those of the logged user.
- The account has administrative privileges.

The above procedure forces the current user to log off. It does not give access *Secure* mode: All smart card functions are suspended except for the recognition of a card insertion.

If the workstation is unlocked in this manner and a smart card is inserted into the smart card reader, the workstation will re-lock automatically.

Secure Screen Savers

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

NOTE: Any screen saver that is password protected will be considered secure.

To enable password protection for a 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. To do this:

1. On the **Smart Card Options** dialog box, select **Change Profile**.
2. Select **Consider all screen saver secure** and select **OK**.

Logging off a Computer or Domain

To log off a computer or domain:

1. Select **Logoff** on the **SCsecurity** dialog box. A verification message will appear.
2. Select **OK** on this message box.

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 **Shut Down**. 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 in Windows NT, this shuts down the computer and turns off the power.*

Changing a Password

NOTE: Administrators should not change users' passwords on the domain controller.

Users should change their own passwords using the **Smart Card Security** dialog box. This will ensure that the home domain account password on the smart card is synchronized with the domain controller.

Administrators can always have the users' passwords expire or force users to change their passwords at the next login. The password expired or the password change condition will be detected and users will be prompted for a password change.

Users will only be able to change passwords for currently logged accounts. Password changes will always occur on the *primary domain controller*. This will ensure proper updating on all *backup domain controllers*. If the logged account is a home domain account, the change will also be made on the smart card.

To ensure that passwords are synchronized between domain accounts and smart card accounts, passwords should not be changed when smart card functionality is not available. For this reason the **Change Password** function is disabled, when smart card security is suspended.

Users can change a password, once they are logged in to an account. To do this:

1. Press Ctrl+Alt+Del.
2. Select **Change Password** on the **SCsecurity Options** dialog box.
3. Enter the existing password, the new password and confirm the new password in the appropriate text boxes on the **Change Password** dialog box and select **OK**.

Task Manager

Selecting **Task Manager** on the **SCsecurity Options** dialog box invokes the Windows NT Task Manager.

Smart Card Options

Smart Card Options include the following:

- Change PIN
- Change Profile
- Card Backup
- Suspend Security
- Disable Security
- Card Diagnostics

Not all of the above options are available at all times. Options become available to administrators and/or users as explained below:

Administrators

When an administrator is logged in to a smart card account and presses Ctrl+Alt+Del:

- **Change PIN**, **Card Backup**, **Suspend Security** and **Card Diagnostics** will be enabled.
- **Change Profile** and **Disable Security** will be disabled.

When an administrator selects **Smart Card** on the **SCsecurity Login** screen.

- **Change PIN**, **Change Profile** and **Card Diagnostics** will be enabled.
- **Card Backup**, **Suspend Security**, **Disable Security** and **Card Diagnostics** will be disabled.

Users

When a user is logged in to a smart card account and presses Ctrl+Alt+Del:

- **Change PIN** and **Card Diagnostics** will be enabled.
- **Change Profile**, **Card Backup**, **Suspend Security** and **Disable Security** will be disabled.

When an user selects **Smart Card** on the **SCsecurity Login** screen:

- **Change PIN, Change Profile** and **Card Diagnostics** will be enabled.
- **Card Backup**, **Suspend Security**, **Disable Security** and **Card Diagnostics** will be disabled.

Emergency Windows NT Administrator Session

During an **Emergency Windows NT Administrator Login**, only **Disable** will be available. When security is disabled, all smart services are disabled.

Smart Card Options are defined below.

Changing PINs

Administrators should change the Admin PIN on each smart card at the first opportunity, usually when granting access to a computer. Users should also change their PINs at the first opportunity. The default Administrator PIN is 1234.

Both users and administrators have the option to change the PIN of the currently inserted smart card and to change their own PINs.

Only administrators can unblock users' PINs. Administrators' PINs cannot be unblocked.

To change a PIN:

1. Select **Change PIN** on the **Smart Card Options** dialog box. The **Smart Card Options (PIN Maintenance)** dialog box will appear.
2. Enter the PIN in the **PIN** field and select the either **Admin** or **User** to indicate if you are an administrator or user.
3. Select **Change**.
4. Enter and confirm the new PIN in the appropriate fields.

If **Admin** is selected in Step 1, the new PIN will replace the administrator's PIN on the currently inserted smart card. If **User** is selected, the user's PIN will be replaced.

Unblocking a PIN

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

Only administrators can unblock users' PINs. Administrator's PINs cannot be unblocked.

To unblock a user's PIN:

1. Insert the user’s smart card into the smart card reader.
2. Press Ctrl+Alt+Del. The **SCsecurity Options** dialog box will appear.
3. Select **Smart Card**. The **Smart Card Options** dialog box will appear.
4. Select **Change PIN** to access the **Smart Card Options (PIN Maintenance)** dialog box.
5. Enter the administrator’s PIN for the currently inserted smart card and select **Admin**.
6. Select **Unblock**.
7. Enter and confirm the new PIN in the appropriate fields and select **OK**.

The new PIN will replace the user’s blocked PIN.

Changing a User’s Profile

Administrators are able to modify the user profile stored on the smart card. To do so:

1. Insert the user’s smart card in the smart card reader.
2. Press Ctrl+Alt+Del. The **SCsecurity Options** dialog box will appear.
3. Select **Smart Card**. The **Smart Card Options** dialog box will appear.
4. Select **Profile**. The **Smart Card Options (PIN Request)** dialog box will appear.
5. Enter both the User PIN and the Admin PIN in the appropriate text boxes.
6. Select **OK**. The **Smart Card Options (Profile Maintenance)** dialog box will appear.
7. Enter the following information in the appropriate text boxes:
   - Full name of the user as it appears on the NT account.
   - User name.
   - User’s Password.
   - Domain name. The domain name can be typed in the Domain text box or selected from the drop-down list.

The administrator can also enable the Suspend Security feature at this time, by selecting t**he User can suspend smart card security**.

NOTE: The first time the **Profile** option is selected, the **PIN Request** dialog box will appear. However, as long as the **Smart Card Options** dialog box remains open, it will not re-appear every time.

Suspending Smart Card Security

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

If they have the right (see “Changing a User’s Profile” on page 48), users will be able to suspend smart card security, once they are logged in. Suspending smart card security makes it possible to insert a different smart card into the smart card reader.

To suspend security, users:

1. Press Ctrl+Alt+Del. The **SCsecurity Options** dialog box will appear.
2. Select **Smart Card**.
3. Select **Suspend Security**. The **Card Diagnostics** window will appear.

The following points should be noted:

- Security only remains suspended for the current user 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, the user must first lock the workstation, then follow the procedure for unlocking the workstation, explained above.

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, users:

1. Press Ctrl+Alt+Del. The **SCsecurity Options** dialog box will appear.
2. Select **Smart Card**.
3. Select **Card Diagnostics**. The **Card Diagnostics** window will appear.

The information that is displayed includes:

- Computer system and platform
- Whether a user is logged in
- Type, version number and serial number of the inserted smart card
- Type of smart card reader
- Number of times the user's or administrator's PIN can be entered before it is blocked
- Number of items stored on the smart card

Using the Backup Restore Utility

The **Backup Restore Utility** is accessible during the user session. To access this, administrators:

1. Press Ctrl+Alt+Del. The **SCsecurity Options** dialog box will appear on the screen.
2. Select **Smart Card**.
3. Select **Card Backup**. The **PIN Request** dialog box will appear.
4. Enter both the administrator's PIN and the user's PIN in the appropriate text boxes.
5. Select **OK**.

To backup the contents of a user's card:

1. Enter your administrator PIN in the **Admin PIN** field.
2. Select the **Backup Restore Utility** button.
3. Click **Execute**.

4. **To create a new backup file:** Select **New** from the **File** menu. A new backup file will be opened. To save the contents of a card to the backup file, click **Save Card** or select **Save Card** from the **Card** menu. The Admin PIN Validation box will appear. Enter the admin PIN for the card. Click **Verify**. The User's PIN Verification box will appear. Enter the user PIN for this card. Click **Verify**.

   The backup information for the new backup file will appear on the list. To save this backup file, select **Save** from the **File** menu. Select the file location and enter the file name. To save the file, click **Save**. The Admin PIN Validation box will appear. Enter the admin PIN. Click **Verify**. Click **Exit** to return to the SCsecurity Administrator Options.

5. **To add information to a backup file**: Select **Open** from the **File** menu. Select a backup file (.sci) and click **Open**. The Admin Validation box will appear. Insert the smart card into the reader and enter the admin PIN for the card. Click **Verify** to open the backup file. The backup information for the card will be listed.

   To add a card to the backup file: Insert the smart card into the reader. The Admin PIN Validation box will appear. Enter the admin PIN for the card. Click **Verify**. The User's PIN Verification box will appear. Enter the user PIN for this card. Click **Verify**.

   To save the backup file, select Save from the File menu. Enter the admin PIN. In the **Backup Restore Utility**, click **Exit** to return to the SCsecurity Administration Options.

   To delete information from a backup file: Select **Open** from the File menu. Select a backup file (.sci) and click **Open**. The Admin Validation box will appear. Insert the smart card into the reader and enter the Admin PIN for the card. Click **Verify** to open the backup file. The backup information for this file will be listed. Select the name of the user to be removed from the backup file. Click **Delete**. The user name and the associated information will be removed from the backup file.

   To save changes to the backup file, click **Save** from the **File** menu. Click **Exit** to return to the SCsecurity Administration Options.

6. **To restore the backup information to the card**: Select the name of the user. Click **Restore** or select **Restore Card** from the **Card** menu to restore this information to the card. The Admin PIN Validation box will appear. Enter the Admin PIN for the card. Click **Verify**. The User's PIN Verification box will appear. Enter the user PIN for this card. Click **Verify**.

   To save changes to the backup file, click **Save** in the **File** menu. The Admin PIN Validation box will appear. Enter the admin PIN for the card. Click **Verify**. Click **Exit** to return to the SCsecurity Administration Options.

   If your workstation is locked after you restore backup information to a new card, you will only be able to unlock it with the card that was used at login. To use the new card, you will need to log off and log on with the new card.

CAUTION: After the contents of a card are restored to a card, the new card will only be valid if the user profile exists in the Windows NT network.

NOTE: If the contents of a card are restored using the Backup Restore Utility, the user PIN will be reset to 1234, the default user PIN.

Overview of the IBM Smart Card Security Kit Administrator Contextual Menu

SCsecurity Emergency

- **Emergency Decrypt...** provides a method to decrypt files.
- **Change Emergency Key Protection...** lets the administrator change the Emergency Access Method.
- **Emergency Access Info...** displays the Emergency Access Information dialog.
- **About...** displays copyright information, software version, etc.

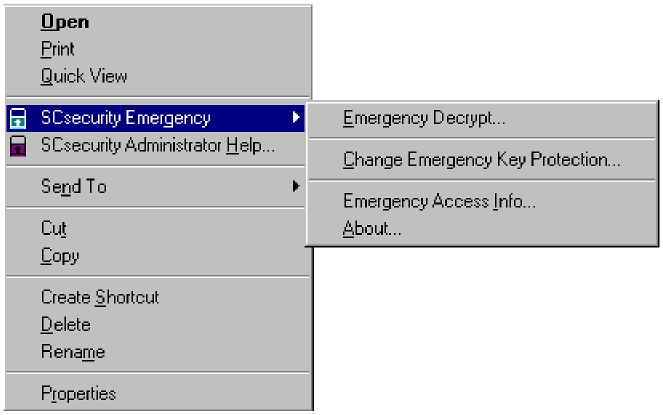
SCsecurity Administrator Help... provides information on the IBM Smart Card Security Kit Administrator features, procedures, menu options, and dialog boxes.

Using Emergency Access

The Smart Card Security Kit's Emergency Access feature provides a way to decrypt and recover a user's encrypted files when a user's smart card is not available, using the SCsecurity Emergency contextual menu. Emergency Access decrypts files encrypted with either the user's "smart card key" or shared passphrase.

SCsecurity Emergency Contextual Menu

Right click on a selected file, then select SCsecurity Emergency to see the contextual menu which includes the following choices: Emergency Decrypt..., Change Emergency Key Protection, Emergency Access Info..., and About.



Emergency Decryption

Under some conditions, the administrator may have to copy the files to be recovered to another system. The procedure is as follows:

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 File recovery will be done, 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**.

The next step depends on how your organization chooses to set up the Emergency Access key. Use one of the following methods:

If the Emergency Access Key Is Protected by a Single Passphrase

To decrypt a user's files when the Emergency Access key is protected by a single passphrase:

1. Enter the Emergency Access key passphrase, and choose **OK** or press ENTER.

   A dialog box opens with the name of the first encrypted file to be recovered.

2. Choose **OK** or press ENTER to decrypt the file(s).

   The Confirm User Name dialog box opens with the name of the first encrypted file to be recovered and the name of the user who encrypted the file. Go to “Confirming Emergency Access” to learn more about this dialog box.

If the Emergency Access Key is split into several keys:

To decrypt a user's files when the Emergency Access key is split into parts:

1. Assemble the threshold number of emergency access trustees with their trustee key diskettes.

   The threshold number of trustees was chosen when emergency access was first installed and refers to the minimum number of trustees needed to access the emergency access key.

2. Choose **OK** or press ENTER.
3. Instruct a trustee to do the following:
   - Insert a Trustee Key Diskette.
   - Choose **OK**.
   - Type a passphrase.
   - Choose **OK**.

4. Repeat step **3** with each of the remaining trustees until the threshold number is reached.

   When the required number of Trustee Key Diskettes and passphrases has been entered, a dialog box opens with the name of the first encrypted file to be recovered.

5. Choose **OK** or press ENTER to decrypt the file(s).

   The Confirm Emergency Access dialog box opens.

Confirming Emergency Access

Your attempt to decrypt the file is added to the security log file (see "Security Log File" on page 60). Then, the Confirm User Name dialog box enables you to verify that the user who requested emergency decryption is the same user who encrypted the file.

To confirm Emergency Access:

1. In the Confirm User Name dialog box, choose one of the following options:
   - **Recover this file** decrypts the current file. The Smart Card Security Kit software then automatically searches for the next encrypted file.
   - **Recover all files with this user name** decrypts the current file and all other files with the same user name in the selection that have not already been decrypted or skipped.
   - **Skip this file** leaves the current file encrypted. The Smart Card Security Kit software then automatically searches for the next encrypted file.
2. Choose **OK** or press ENTER.

   The software completes the emergency decryption process.

Changing Emergency Access Key Protection

The Smart Card Security Kit software enables the administrator and trustees to change the Emergency Access protection method using the Change Emergency Key Protection... menu item. The Smart Card Security Kit software's public/private key pair remains the same. Only its configuration and the passphrases used to protect the key change. You do not need to change anything on your User Setup Diskette or do any updates of user software.

To change the Emergency Access key configuration:

1. Assemble the person or people who now protect the Emergency Access key.
   - If a single passphrase protects the Emergency Access key, the individual holding the passphrase must be present.

     OR
   - If multiple trustees protect the Emergency Access key, gather the threshold number of trustees (the minimum number needed to access the Emergency Access key – for example, 4 trustees out of 10), with their Trustee Key Diskettes.

2. Assemble the person or people who will protect the Emergency Access key, according to the new protection method.

   - If a single passphrase will protect the Emergency Access key, the individual who will hold that passphrase must be present.

     OR

   - If multiple trustees will protect the Emergency Access key, they must all be present, each with a diskette.

3. From the **SCsecurity Emergency** contextual menu, choose the **Change Emergency Key Protection**... item.

   The Change Emergency Key Protection dialog box opens.

   NOTE: What happens next depends on the configuration of the Emergency Access key. The following instructions assume that the Emergency Access key is currently protected with a single passphrase. The procedure for changing the Emergency Access key protection is the same if the Emergency Access key is split into parts on diskettes, except that the threshold number of trustees must insert their diskettes and enter passphrases during step **5**.

   ---

4. In the Change Emergency Key Protection dialog box, choose **OK** or press ENTER.

   If the Emergency Access key is whole, the Emergency Access Passphrase dialog box prompts you for a passphrase.

5. Enter the current Emergency Access key passphrase, and choose **OK** or press ENTER.

6. Select the new Emergency Access key protection method:

   - If the Emergency Access key will be protected with a single passphrase, select **Single passphrase**, and choose **OK** or press ENTER.

     OR

   - If the Emergency Access key will be protected by trustees (each with their own Trustee Key Diskette), select **Split among trustees**. Enter the number of trustees, and the threshold number of trustees required to be present for file decryption. Then, choose **OK** or press ENTER. The dialog box expands.

To complete setting up the new protection method, perform one of the following steps:

- If you chose to protect the Emergency Access key with a single passphrase, go to "Option 1: Protecting the Emergency Access Key with a Single Passphrase" described on page 36 of this Administrator Reference Manual.

  OR

- If you chose to protect the Emergency Access key by splitting it among trustees, go to "Option 2: Splitting the Emergency Access Key Among Trustees" described on page 36 of this Administrator Reference Manual.

IMPORTANT: Always back up the emergency preference file (**emerpref.!!!**), safeguard the diskette, and memorize the passphrase.

Emergency Access Info...

displays the Emergency Access Information dialog box that can also be accessed by clicking on the More button in the Emergency Access group box of the Encrypt or Decrypt dialogs. The dialog contains the following information:

- 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.

About...

displays copyright information, software version, etc.

Using SCsecurity Administrator Help...

The Help function provides information on the IBM Smart Card Security Kit features, such as procedures, menu options, and dialog boxes. It follows the form of a normal Windows-type help file. Subjects can be accessed from an index or by keying in search words. Related topics are hyperlinked within the Help system so that the reader can move from topic to topic gaining a deeper understanding with each screen.

Security Log File

When you recover a file using emergency recovery procedures, a description of that event is noted in a security log file on the machine where Emergency Access is installed. The log file, **emrgdcrt.log,** is a plain text file. You may have to change your viewing options to see hidden files. It is hidden in the same directory where Emergency Access is installed. New entries are added to the end of the log.

The log file records the following information for each decrypted file:

- date and time of decryption
- name of the encrypted file
- name of the user who encrypted the file
- name of the original decrypted file
- date the original file was created
- date the original file was last modified

Here is a sample excerpt from a log file:

```
Decryption time: 03/31/97  09:59
Encrypted file name: c:\documents\topsecret.txt
Encrypting person: Jean Kim
Decrypted file name: c:\documents\topsecret.txt
Creation time: 12/01/96 12:03
Last write time: 2/25/97 17:23
--------------------------
Decryption time: 03/31/97  10:05
Encrypted file name: a:\schedule(!).doc
Encrypting person: Chris Johannson
Decrypted file name: a:\schedule.doc
Creation time: 07/21/96 09:03
Last write time: 07/21/96 09:03
--------------------------
```

When the size of the log exceeds 100K (over 1000 entries), a warning is displayed.

You have the option of saving the log to another hidden file, clearing the log (deleting all entries), or continuing to append to the current log.

5

Uninstalling the Administration Software

This chapter explains how to remove the IBM Smart Card Security Administration software safely and easily without any loss of data.

- **What to do before Uninstalling SCsecurity Software** – What must be done to safely uninstall SCsecurity software.
- **Uninstalling SCsecurity Software** – How to uninstall the IBM Smart Card Security Kit software step-by-step.

What to do Before Uninstalling SCsecurity Software

To preserve the option of restoring users' files using the Emergency Access software with its unique key, you must retain the administrator preference file (**emerpref.!!!**).

CAUTION: If the administrator preference file (**emerpref.!!!)** is destroyed or lost, there is no way to recover files encrypted with the IBM Smart Card Security Kit. Make sure that you have backup copies of this file on a diskette or another suitable media.

Uninstalling the Administration Software

Uninstalling the Administration software removes the Smart Card Security Kit Administration software from your computer, as well as removing references to your Smart Card Security Kit files in the Windows registry and other locations.

IMPORTANT: If other users use the Smart Card Security Kit on this machine, there may be files in the AutoCrypt List that cannot be decrypted during uninstall or after uninstall. See the User Reference Manual for additional information about the AutoCrypt List feature.

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

The Smart Card Security Kit Uninstall dialog box opens. This dialog box warns you that only files encrypted by your smart card, **and** located in the AutoCrypt List can be decrypted automatically during the uninstall.

To uninstall Smart Card Security Kit software if you only have the Administrator software installed:

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.

To uninstall Smart Card Security Kit software if you have both the Administrator and User software installed (Stand-Alone):

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. Click **Find** to locate encrypted files. Decrypt files and close the Find dialog box.
6. The Remove Shared File? dialog box opens. Choose **Yes**.

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

7. Choose **OK** or press enter to reboot your machine and complete uninstall. Windows restarts.

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.

Algorithm A set of steps the Smart Card Security Kit takes to encrypt and decrypt data securely.

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.

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 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 (Administrator The administrator public key file (**pkfile**) containing the

Public Key File) administrator’s public key and Emergency Access information. The IBM Smart Card Security Kit uses the information in this file combined with the user’s PIN protected smart card to generate the user preference file.

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.

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 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 Smart Card key** menu option is selected.

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 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 is generated by the administrator. It is necessary for user installation.

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

GEMPLUS

IBM Smart Card

ORDER FORM

Fax order form along with PO or credit card number to Gemplus @ (215) 654-8882.
This is a secure fax line.
If you do not have access to a fax machine, please e-mail the order form to ussales@gemplus.com.

Order Date:		**Sales Rep:**	**GEMPLUS KIT GROUP**
Customer:		**Requested By:**	
Application:		**PO Number:**	
Card Number:		**Expire Date:**	**AE MC VISA**

BILL TO:

SHIP TO:

Order Placed By:		**Attention:**	
Telephone:		**Fax:**	
Type of Payment (Select one: Net 30 days, or C.O.D.)		**Ship Via:**	**FedEx** **USMail** **UPS Red** **UPS Blue** **UPS**
Tax Exempt? Yes / No If yes, YOU MUST PROVIDE TAX EXEMPT CERTIFICATE NUMBER		**Exempt Certificate Number:**	

Item #	**Gemplus Part Number**	**Description**	**Qty**	**Unit Price**	**Ship to Arrive**
1	**W-C3034199**	**IBM Smart Card #10L7341 Single Card**		**$39.99**	**Next Day ($ includes S&H)**
2	**W-C3034194**	**IBM Smart Card #10L7341 4 Pack**		**$69.99**	**2 weeks from receipt of PO**
3	**RPF14257**	**IBM INTL Smart Card #33L5028 4 Pack**		**$69.99**	**2 weeks from receipt of PO**
4	**RPF14258**	**IBM INTL Smart Card #33L5028 Single Card**		**$39.99**	**Next Day ($ includes S&H)**

For special orders contact Tom Hissam at (910) 343-9857.