



IBM SmartCard Security Kit for Notebooks

OPTIONS
by IBM

Administrator Reference Manual

Software for Windows 95 and 98
Version 1.0

Copyright

Copyright © 1998 Gemplus and 1998 by International Business Machine, Inc. All Rights Reserved. Some algorithms used in this product are copyright by RSA Data Security, Inc., a Security Dynamics Company and used with its permission. No part of this work may be reproduced in any form or by any means—graphic, electronic, or mechanical—including photocopying, recording, taping, or storage in an information system, without the prior written consent of the copyright owner.

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, Comcrypt, Concrypt, PASSCODE, PINPAD, SecurID Protected, SecurID Ready, SecurESS, SecurPC, SecurSight, SecurSSO, and SecurVPN are trademarks, of Security Dynamics Technologies, Inc.

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

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

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

Netscape Navigator is a trademark of Netscape Communications.

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

Software Version 1.0 for Windows 95 and 98.
October, 1998

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.

© Copyright GEMPLUS and International Business Machines, 1998.

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

© Copyright International Business Machines Corporation 1998. All Rights Reserved.

Note to U.S. Government Users - Documentation related to restricted rights - Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

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: SmartCard 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

Contents	vii
Preface	10
Introduction	11
Document Conventions	13
Getting Support and Service	14
Additional Technical Support Resources	14
Step 1. Problem Solving	14
Step 2: Preparing for the Call	15
Part I	16
Welcome to the IBM SmartCard Security Kit	17
What is the IBM SmartCard Security Kit?	17
Features of the IBM SmartCard Security Kit Administration Module	18
Administrator Overview.....	20
IBM SmartCard Security Kit's Security Components	20
Administrator Setup Overview	20
Some Considerations.....	21
Security Suggestion.....	21
Security Plans — Three Examples	22
Implementing the IBM SmartCard Security Kit for a Single User	22
Implementing the SmartCard Security Kit for an Organization	22
Implementing IBM SmartCard Security Kit for a Large Organization.....	23
How Emergency Access Works	23
Emergency Access Passphrase Suggestions	25
Installation	27
Compatibility with Windows 3.1 and Windows NT.....	28
Migrating to the IBM SmartCard Security Kit	28

Hardware and Software Requirements	28
Installation Scenario.....	29
Before Installing.....	29
Making diskettes from the CD-ROM	29
Installation Steps of the Administration Security Software.....	31
Using the Installer.....	31
Step 1 a: Installing the Administrator Software From the CD-ROM	33
Step 1 b: Installing the Administrator Software From Diskette	33
Part II.....	36
IBM SmartCard Security Kit Administration Setup	37
Before You Begin.....	37
Emergency Access Authority.....	38
Emergency Access Authority Confirmation	39
Emergency Key Protection	40
Generating the Security Key.....	45
Testing Emergency Access	47
Seeing Emergency Access Information	47
Distribute the Customized Administrator File Disk	47
Part III.....	50
Administrator’s Tasks.....	51
Using the SmartCard Administration control panel	52
Change User PIN.....	52
Change User Information	52
Administration Options	53
Grant Access to the Computer	53
Overview of IBM SmartCard Security Kit Contextual Menu.....	53
Emergency Access to the Data.....	54
SCsecurity Emergency Contextual Menu	54
SCsecurity Administrator <u>H</u> elp.....	58
Security Log File	59
De-installing the Administration Software	61
What to do Before De-installing	61
Uninstalling the Administration Software.....	62
Glossary	63
Index	69
IBM Smart Card Order Form	71

Preface

This manual contains instructions for installation and setup of the IBM® SmartCard Security Kit hardware and software for Microsoft® Windows® 95 and 98. The complete User's and Administration manual are contained on the SmartCard Security Kit CD. The CD-ROM disk contains an administrator manual and a user manual in a format that can be viewed on-line or printed for off-line reading. Before installing your SmartCard Security Kit, please read the manual and become familiar with its contents.

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

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

The user then sets up the individual aspects of the software, such as the encryption options. Refer to the User Reference manual on the CD-ROM for a complete description of the options available to the user.

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

Introduction

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

It also ensures the privacy of files stored on the notebook's hard drive. The IBM SmartCard 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 95/98 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 95/98 applications. Files on hard drives, mapped network folders, and removable disks can be encrypted.

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

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

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

The IBM SmartCard Security Kit's setup is a two-step process. The administrator customizes the SmartCard Security Kit for the secure protection features. Then, the user sets up the encryption software. These manuals take you through the process, step-by-step.

IBM SmartCard Security Kit complies with the following 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

Document Conventions

Before 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, for example, **d**:\setup)

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

Select **setup.exe** file from the IBM SmartCard 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 **S**mart Card key from the **E**ncrypt menu.

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

Enter the user name in the **N**ame field and click **OK**.

The terminology in this Administration 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 whenever necessary to prevent potential problems such as data loss.

Getting Support and Service

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

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

Additional Technical Support Resources

On-line technical support is available during 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.

<i>On-line Technical Support</i>	
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.

<i>Support 24 hours a day, 7 days a week</i>	
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 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 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 de-installing 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 disks 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 SmartCard Security Kit
2. Option number: 10L7333
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 part of the this Administration Reference manual describes the features of the IBM SmartCard Security Kit, the organization of a security system and explains the installation and setup of the Administration software.

1

Welcome to the IBM SmartCard Security Kit

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

- **What is the IBM SmartCard Security Kit?** – how the IBM SmartCard Security Kit fits into the Windows 95/98 environment and protects your data
- **Administrator Overview** – how to plan for and implement the IBM SmartCard Security Kit
- **Security Plans** – how the IBM SmartCard 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 SmartCard Security Kit?

The IBM SmartCard 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 SmartCard Security Kit is a utility program that appears as **File** menu options in Microsoft's Windows 95/98 environment.

In addition, the SmartCard 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 or her valid Personal Identification Number (PIN) to access the desktop. The same smart card is also used to safely store the SmartCard Security Kit encryption key and the Private/Public key pair used for digital signatures.

Features of the IBM SmartCard Security Kit Administration Module

Powerful Encryption Technology

The SmartCard 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 95 and 98

The IBM SmartCard Security Kit integrates with Windows 95/98 through the user's desktop, the **Start** menu, and the **File** menu in My Computer, Windows Explorer, and Find File. Special SmartCard Security Kit move and copy menu options are available, when a file or folder is transferred, using the right mouse button.

Solid Protection Against Unauthorized Access


The SmartCard Security Kit uses a smart card containing a Personal Identification Number (PIN), an encryption key, a Digital Signature Public/Private Key pair, reserved Digital Certificate Space and provision for a Security Dynamic compatible SoftID “seed”.

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

File Security

The IBM SmartCard 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 or her Smart Card PIN, any file encrypted with that user's “smart card encryption key” can still be decrypted. This is because the user's “smart card key” does not change, only the PIN changes.

AutoCrypt

The AutoCrypt feature works behind the scenes. When the user adds a folder to the AutoCrypt List, the folder's contents are automatically encrypted. The IBM SmartCard 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 95/98 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 95/98 applications. Files on hard drives, mapped network folders, and removable disks can be encrypted.

Sharing Encrypted Files

The IBM SmartCard 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 SmartCard Security Kit installed.

Secure File Transfer

The IBM SmartCard Security Kit can create a self-decrypting encrypted file that can be read on an unprotected system.

Secure Screen Saver

The secure screen saver blocks access to your system if the smart card is removed from the reader. Access is available after entering the proper password when the smart card is reinserted in 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 (we refer to them as "trustees") hold a part of the key file. While each trustee holds a key file, only a minimum number of trustee key files are required to decrypt user files.

Remote Administration

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

Administrator Overview

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

IBM SmartCard Security Kit's Security Components

- **Administrator preferences** determine how the SmartCard 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 Administration software
- Set up emergency access.
 - Set Emergency Access for a Single User*OR*
 - Split Emergency Access among trustees
 - Assist in Trustee Key Disk creation
- Customize Administrator Preferences
- Back up special administrator files

Distribute the customized Administrator preference file to users, through disks 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 administration 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 SmartCard 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 (say, 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 disks look like.

The SmartCard 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. Emergency Access decrypts files encrypted with either the user's "smart card key" or shared passphrase, including self-extracting files.

Security Plans — Three Examples

The IBM SmartCard 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 SmartCard Security Kit setup consists of two parts:

- **Administrator Setup** – for installation of emergency recovery of files, creation of the passphrases, and enforcement of organizational security policy, by designing your users' file security plan
- **User Setup** – for installing encryption and decryption software

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 file security plan. The following examples illustrate three typical ways to set up the software:

- for a single user
- for an organization
- for an organization with distinct internal groups

Implementing the IBM SmartCard Security Kit for a Single User

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

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

1. Set up the administrator software on the designated administrator system.
2. Set up the user software on the users system.

Implementing the SmartCard Security Kit for an Organization

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

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

1. Set up the administrator software on the administrator's station.
2. Distribute the customized administrator files (also called User Preference Files) to users, through disks or a network folder.

Implementing IBM SmartCard 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 SmartCard 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 SmartCard Security according to the procedures in "Implementing the SmartCard Security Kit for an Organization" on page 22. Each group's name must be unique. Each group's administrator then distributes the customized administrator files through disks 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 the ones 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 SmartCard Security public/private key pair for access to encrypted files. The administrator places the public key portion on the Customized Administrator Disk, copies the disk, and distributes them to users. The Emergency Access Key is the private key portion and is protected by either a single passphrase or multiple trustee passphrases. For our purposes, the SmartCard 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 disks (Trustee Key Disks), each held by a different person (a trustee) and each protected by its own passphrase.

If the Emergency Access key is split among multiple trustees, a minimum ("threshold") number of trustees must be present to activate it. For example, an organization might have seven trustees and a threshold of four. The presence of any four of the seven trustees is required to decrypt a user's files. The number of trustees can be as large as 255. The threshold number can be the total number, although most security plans call for a smaller threshold number.

If a user's smart card is lost, the administrator can copy the user's encrypted files into a directory accessible to the administrator. Emergency decryption requires passphrases to activate the Emergency Access key. Either the administrator enters the single Emergency Access passphrase or the threshold number of trustees insert their Trustee Key Disks 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 59.

Emergency Access Passphrase Suggestions

Good passphrase composition is vital for ensuring the security of data. Review the following ideas for creating strong passphrases:

- Use at least 10 characters: the IBM SmartCard 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, such as: the name of your spouse, child, or parent; your home or work street name, number, or city; your birthday, telephone number, social security number, etc.
- Choose 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	Good Passphrases
Abcdefghi	*4 score & 7 years ago*
Qwerty	>>I R8 her Hily!<<
Junior Johnson	Jr. wakes up like this (-o)

2

Installation

The IBM SmartCard Security Kit protects your computer from intrusion and keeps your data private. The IBM SmartCard 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 SmartCard Security Kit also enables you to share encrypted files with others – even if they do not have the IBM SmartCard Security Kit installed on their computer.

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

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

- **Compatibility with Windows 3.1 and Windows NT** – explains the compatibility level with the other Microsoft operating systems.
- **Migrating to the IBM SmartCard Security Kit** – instructions for users of other encryption software.
- **Before Installing the Software** – Explains what has to be done before installing the software.
- **Minimum Hardware and Software Requirements** – list the minimum hardware and software requirement for using the IBM SmartCard Security Kit.
- **Installing the Administration Security Software** – how to install the IBM SmartCard Security Kit, step-by-step.

Compatibility with Windows 3.1 and Windows NT

This product is intended for Windows 95 and Windows 98 **only**. It is not intended for Windows 3.1, or Windows NT.

To share files with Windows 3.1 or NT 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 SmartCard 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 SmartCard Security Kit installed.

Migrating to the IBM SmartCard Security Kit

IMPORTANT: If you have any other secure access or data encryption software installed, you must first **decrypt all encrypted files** and uninstall that program before installing the IBM SmartCard Security Kit.

Files encrypted with other security programs **cannot** be decrypted by the IBM SmartCard Security Kit.

Hardware and Software Requirements

Before installing the IBM SmartCard Security Kit, you must have the following computer and software:¹

- An IBM or IBM-compatible notebook 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;
- A 1.44Mb 3.5-inch floppy drive;
- Access to a CD-ROM drive;
- Microsoft Windows 98 or Windows 95.

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 this CD. In most cases, your system was manufactured before there was support for devices like Smart Cards. Refer to your systems support organization to obtain the latest updates for your system.

To obtain updates, IBM ThinkPad customers can logon to:

http://www.pc.ibm.com/us/support/thinkpad/thinkpad_support.html

¹ From this point on, we refer to Windows 95 and Windows 98 simply as Windows unless necessary.

Installation Scenario

The following installation scenarios are possible:

1. One person acting as administrator AND user.

Install **all** the components as they appear on the Installer program on one computer.

IMPORTANT: Read all instructions to insure proper installation.

For the Administrator software, see the section “Installation Steps of the Administration Security Software” later in this manual.

2. One person acting as administrator for several users.

Install the Administration software **only** on the administrator’s computer.

Install for each user the following components: DCOM, Smart Card Components, Smart Card Driver, and User Software. The instructions for installing the User Software are located in the User’s manual.

Before Installing

Note: The IBM SmartCard Security Kit should not be installed on a file server.

Before doing the installation, save all documents, backup important files and quit **ALL** running applications including anti-virus programs.

Making diskettes from the CD-ROM

IMPORTANT: If you need to create diskettes from the CD-ROM, do the following steps:

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

1. Have a box of blank formatted 1.44 floppies at hand.
2. Locate a computer that has both a CD-ROM drive and a floppy drive
3. Insert the CD-ROM in the drive
3. Start the Install program to launch the Installer.
The splash screen is displayed.
4. Click on the **Continue** button, the main screen of the Installer appears.

OR

Click on **Exit** to quit the Installer.

5. For each software item that you want to make diskettes, click on the **Floppies** button for that item.

The dialog box displayed prompts you to select a drive.

6. Click the **Create Floppy** button to create the disk
7. Insert a disk into the floppy drive and click the **OK** button to create the disk.
The dialog box mentions how many floppies are needed.
Ensure that you label each diskette appropriately for proper installation.

Installation Steps of the Administration Security Software

 **To install the SmartCard Security Kit Administrator Software from the CD-ROM:**

The following software must be installed:

- Administration Software

Using the Installer

An install utility will be loaded to make it easier to install the various components of your SmartCard Security Kit.

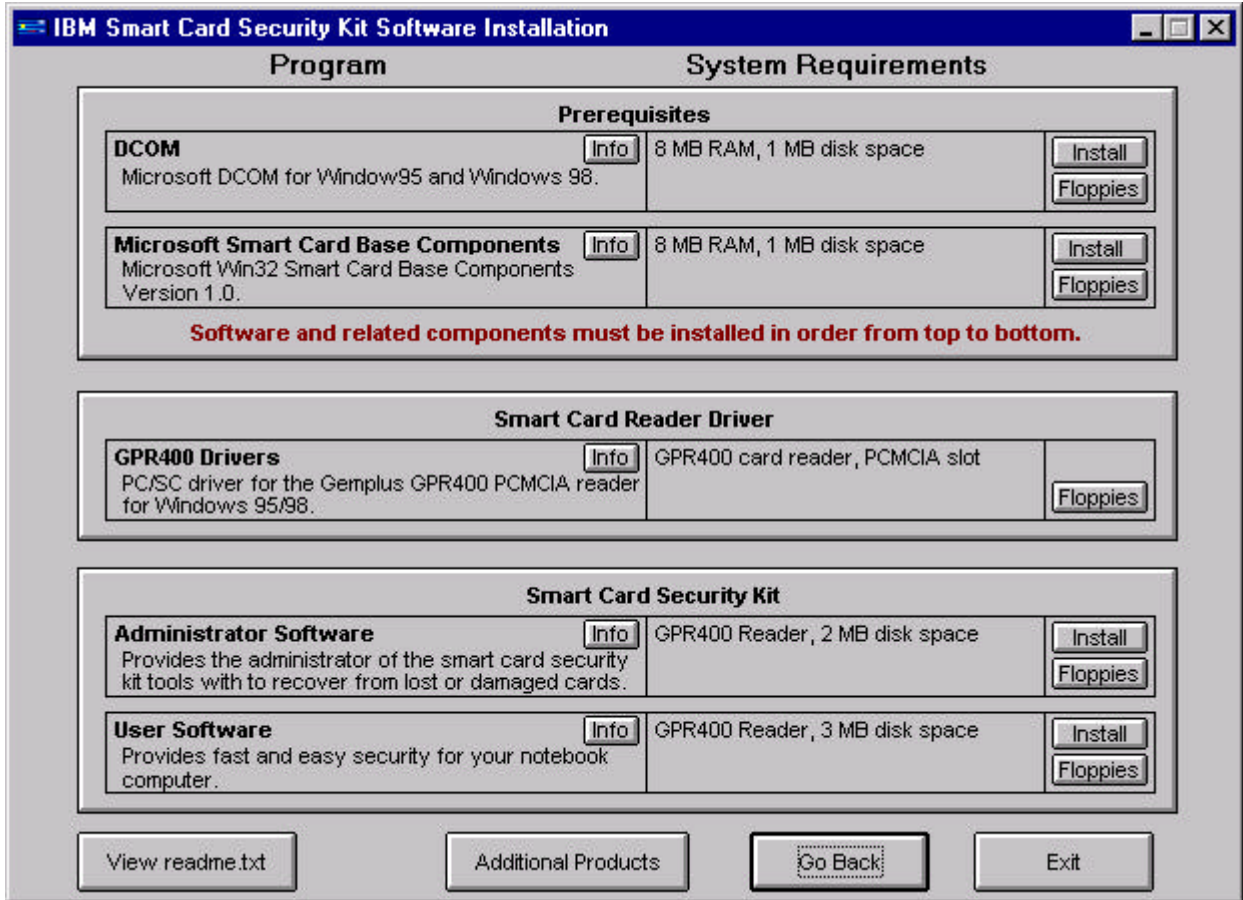
A welcome screen will appear to explain how to use the installer from the CD-ROM or how to make diskettes for the different software modules. Click on **Continue** to go to the Install screen.

Use this dialog box to install all the necessary components into your laptop computer.

Click on the **Info** button located near the middle of the dialog box to get additional information on the components that will be installed.

The SmartCard Security Kit software is divided into separate Administration and User installations. The Administration software should be installed by the Security Administrator, usually only on the administrator's system.

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



NOTE: The correct installation sequence of the software is a critical element in the installation process. Please read the instructions carefully and follow them closely to avoid difficulties. The User Software installation process will not allow the User software to be installed unless the Prerequisite software is installed correctly.

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

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

1. Start Window 95 or 98, and insert the CD-ROM in the drive.
2. Click on **Start**, select **Settings**, and click on **Control Panel**.
3. Double click on **Add/Remove Programs**.
4. In the Install/Uninstall tab, select **Install**.
5. Use the **Browse** button to locate the Setup file.
6. Select Setup, click **Open** then **Finish**.

An installation program will be loaded to make it easier to install the various components of your SmartCard Security Kit and associated software. The Installation welcome screen will appear and explain how to install the application software.

7. Click **Continue** to go to the Install menu.
8. Locate the **Administration** software entry and click the **Install** button to begin writing the Administration Software to your hard drive.
9. A dialog box requesting confirmation appears. Click **OK** to continue.
10. Read the instruction on screen. Click **Next**.
11. Read the License Agreement. Do not continue **if you do not agree with the terms of the license**. If you click the **Yes** button the installation will proceed.
12. If desired, select another location (directory) where the files will be installed using the **Browse** button.
13. Click **Next** to begin the actual installation.

When you see the Welcome to the SmartCard Security Kit dialog box, the SmartCard Security files have been copied successfully.

14. Choose **OK** or press ENTER.
15. Go to Chapter 3, IBM SmartCard Security Kit Administration Setup.

Step 1 b: Installing the Administrator Software From Diskette

1. Start Window 95 or 98, and insert the Administration diskette in the drive.
2. Click on **Start**, select **Settings**, and click on Control Panel.
3. Double click on **Add/Remove Programs**.
4. In the Install/Uninstall tab, select **Install**.
5. Use the **Browse** button to locate the Setup file.
6. Select Setup, click **Open** then **Finish**.

An installation program will be loaded to make it easier to install the various components of your SmartCard Security Kit and associated software. The Installation welcome screen will appear and explain how to install the application software.

7. Click **Continue** to the Install menu.
8. A dialog box requesting confirmation appears. Click **OK** to continue.
9. Read the instructions on screen. Click **Next**.
10. Read the License Agreement. Do not continue **if you do not agree with the terms of the license**. If you click the **Yes** button the installation will proceed.
11. If desired, select another location (directory) where the files will be installed using the **Browse** button.
12. Click **Next** to begin the actual installation.
13. When you see the “Welcome to the SC Security Administrator Setup” dialog box, the SmartCard Security files have been copied successfully.
14. Choose **OK** or press Enter.
15. Go to Chapter 3, IBM SmartCard Security Kit Administration Setup.

Part II

This chapter addresses the setup of the IBM SmartCard Security Kit Administration Software.

3

IBM SmartCard Security Kit Administration Setup

This chapter describes how to set up the IBM SmartCard Security Kit administrator's software and preferences. Your trustees must be present to set up the IBM SmartCard 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
- **Seeding the Random Key** – how to create the random encryption key that protects the files.
- **Customizing the User Setup** – how to copy options to the user's computer.
- **Backing Up Administrator Preference Files** – how to store the administrator preference files
- **Testing and Duplication** – how to confirm administrator setup

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, floppy disk to store a part of the Emergency Access key.

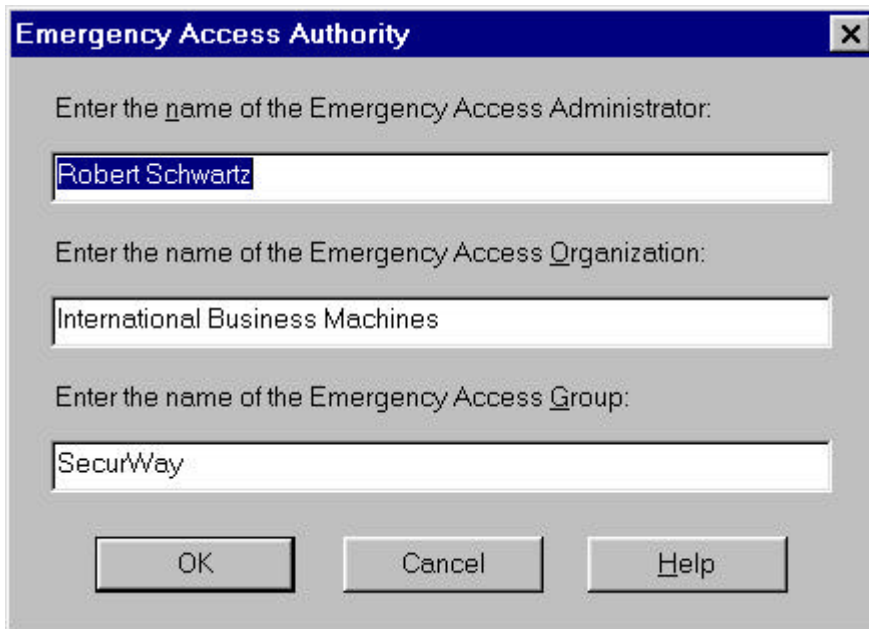
During administrator software setup, you create Administrator files which are copied to a location of your choice. These files will be used during user setup.

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

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



Emergency Access Authority



The Emergency Access Authority window appears:

 **Fill in the Emergency Access Authority window as follows:**

1. Type the name of Emergency Access Administrator in the top text box, and press TAB.
2. Type the name of Emergency Access Organization in the middle text box, and press TAB.

3. Type the name of Emergency Access Group in the bottom text box, and press OKAY.

If the information is correct, press the OK button. If not, press the Tab key to move back up to the first field.

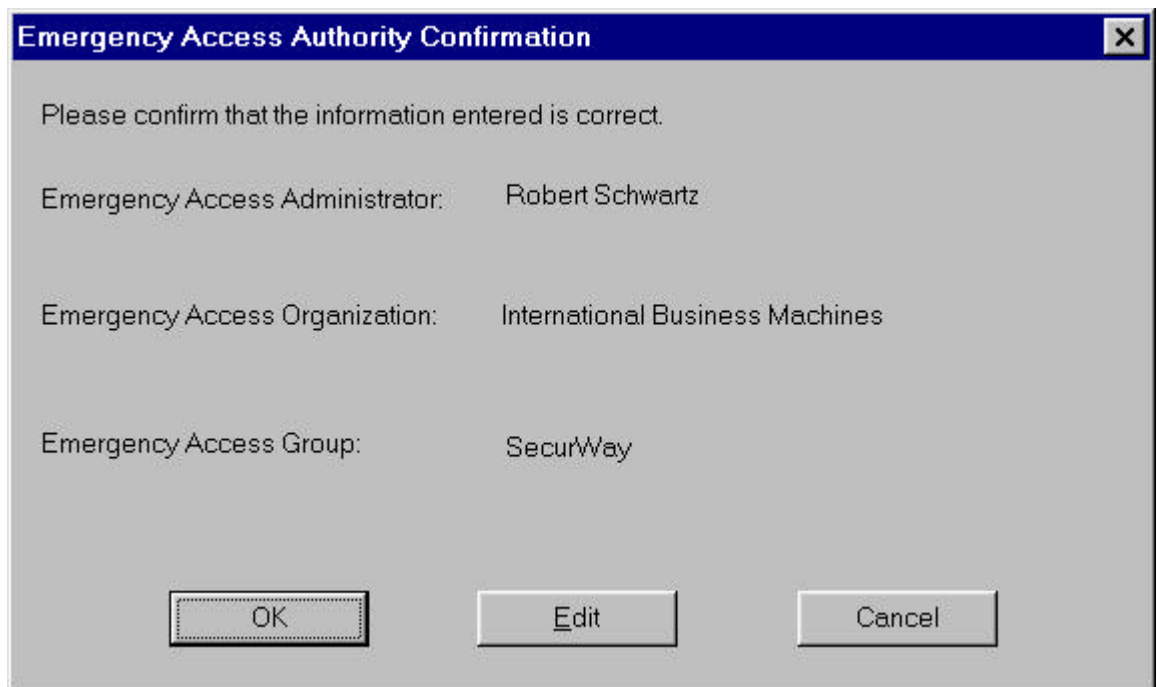
After clicking on the OK button or pushing the RETURN key, the Emergency Access Authority Confirmation dialog appears.

Emergency Access Authority Confirmation

This dialog provides the opportunity to correct or change any of the three fields filled previously.

In this confirmation dialog box, carefully review the information you entered. To change these names later you will have to re-install the IBM SmartCard Security Administration software.

CAUTION: If the Administration software is re-installed, you will be unable to decrypt files that were encrypted with customized Administrator files from any previous installation. **Each installation generates a different protection key.**

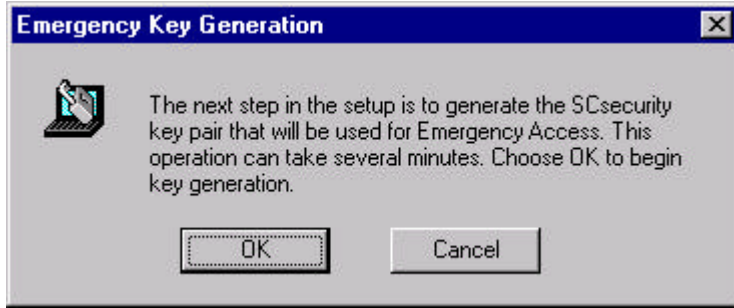


If the information entered is correct, click on the OK button or push the ENTER key.

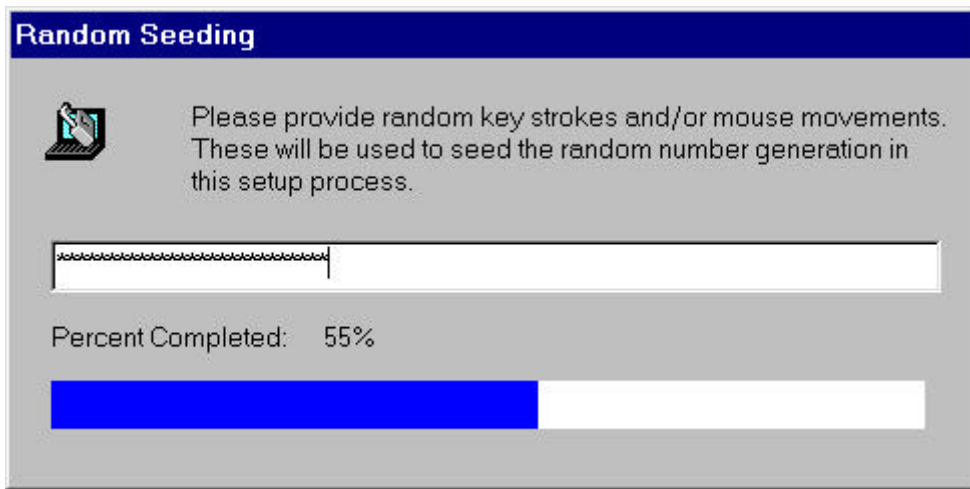
If the information entered is **NOT** correct, click on the EDIT button or push the E key.

Click on the CANCEL button or push the ESC key to cancel the installation.

Emergency Key Protection



At this point, you generate a random seed, create an emergency access key and provide a passphrase for the Emergency Access key or a passphrase for each trustee's key file.

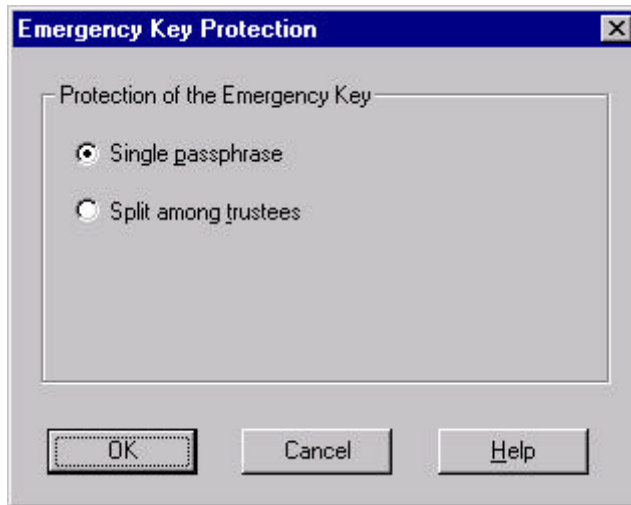


 **Choose one of the following options:**

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

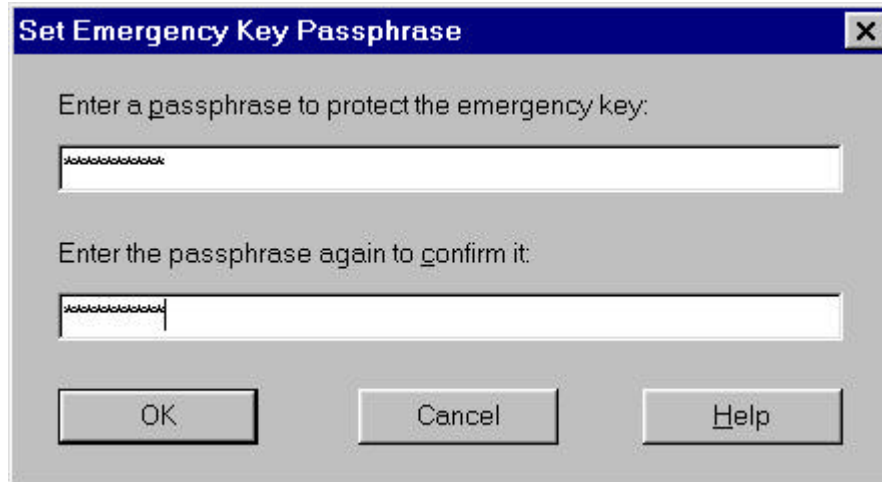
OR

- If you chose **split the Emergency Access Key** to split the protection among several trustees, go to **Option 2** on page 42.



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

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



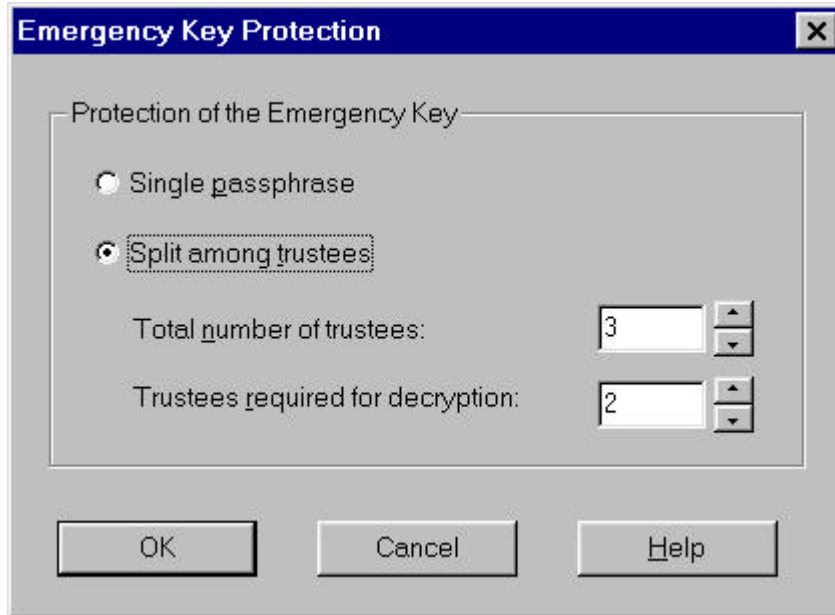
The Emergency Access key passphrase you enter will decrypt any IBM SmartCard Security Kit-encrypted file in your organization, so craft the passphrase carefully.

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.
The Emergency Key Generation dialog box opens.
3. Choose **OK** or press ENTER to generate the Emergency Access key pair.
The message “Successfully generated the SCsecurity key part” appears at the end of the process.
4. Choose **OK** or press ENTER.
5. Go to the section “Generating the Security Key”.

Option 2: Splitting the Emergency Access Key Among Trustees

The following dialog box reminds you to assemble disks to hold the number of Emergency Access key parts you specified.

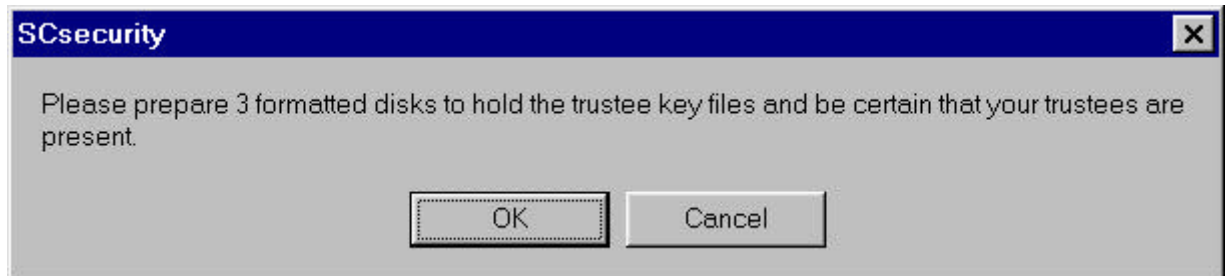


 **To protect the Emergency Access key with multiple passphrases:**

1. After you have gathered formatted disks (one for each trustee) and all trustees are present, choose **OK** or press ENTER to create a Trustee Key Disk for each trustee.

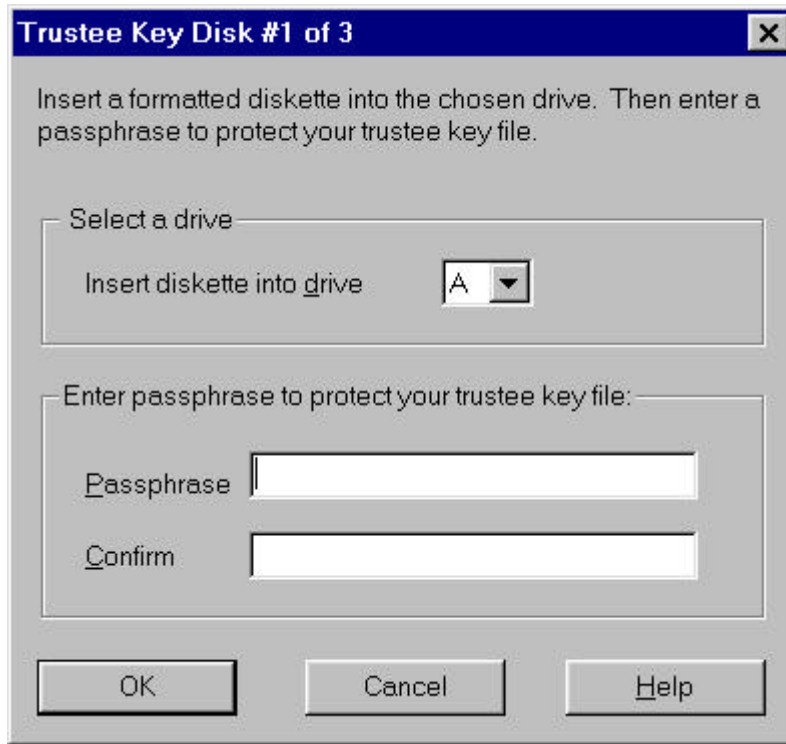
Each of the next dialog boxes prompts each trustee to place a trustee key file on a Trustee Key Disk.

2. Instruct one trustee to do all of the following steps:
 - Insert a blank floppy disk to create a Trustee Key Disk.

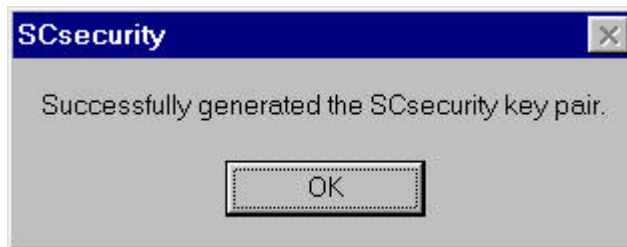


- Type a passphrase, and press TAB. The passphrase must have a minimum of eight characters.
- Type the passphrase again.
- Choose **OK**.

The following dialog box prompts each new trustee.



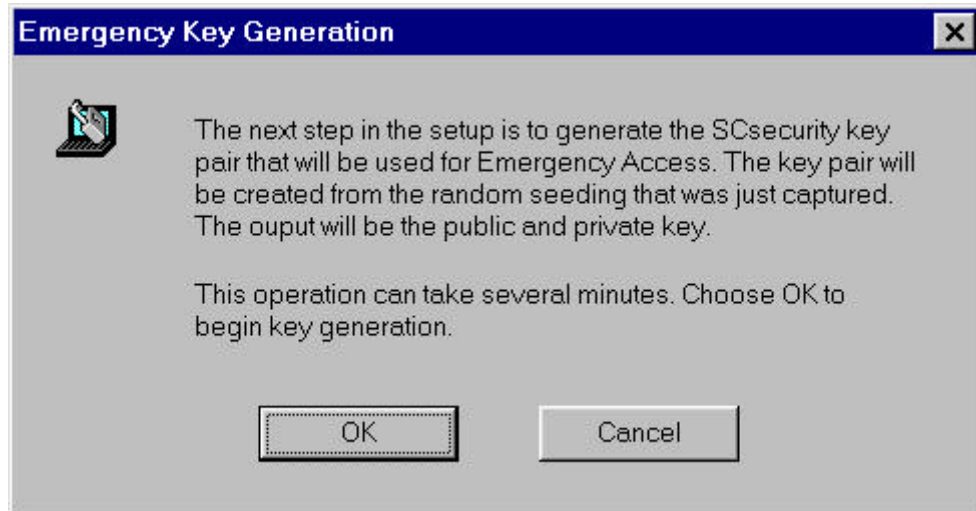
3. Choose **OK**, and repeat step 2 with each of the remaining trustees.
The Emergency Access Key Generation dialog box opens.
4. Choose **OK** or press ENTER to generate the Emergency Access key pair.
The following message box appears at the end of the process.



5. Choose **OK** or press ENTER.

Generating the Security Key

The information dialog appears.



To perform the steps necessary to create the key, beginning with the generation of a random number “seed.” The SmartCard Security Kit uses your keystrokes and mouse movements to generate a personalized “secret key” for its use. This random seed adds randomness to SmartCard Security Kit’s cryptography process, making your copy of the IBM SmartCard Security Kit absolutely unique. This has to be done only once—unless the SmartCard Security Kit has to be reinstalled for whatever reason.

3. Move your mouse, press any keys or do both until the process is complete.

An asterisk (*) will appear for each keystroke. When random seeding is finished, the following dialog box appears.

IMPORTANT: Move the mouse cursor over the dialog box to generate the seed correctly.



The next step in the setup is to generate the SCsecurity key pair that will be used for Emergency Access. This operation can take several minutes. Choose OK to begin key generation.

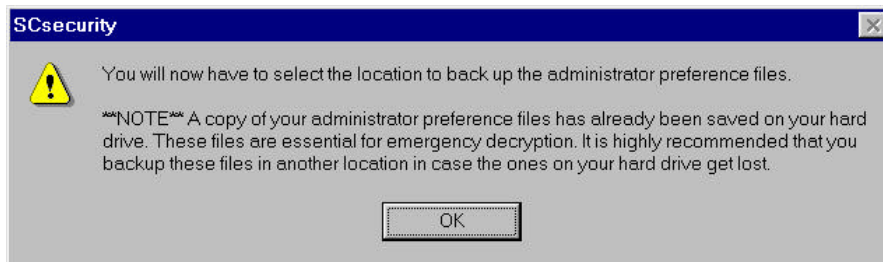
4. Choose **OK** or press ENTER.

The message “Successfully generated the SCsecurity key pair” appears when the random key is generated correctly. Choose **OK** or press ENTER.

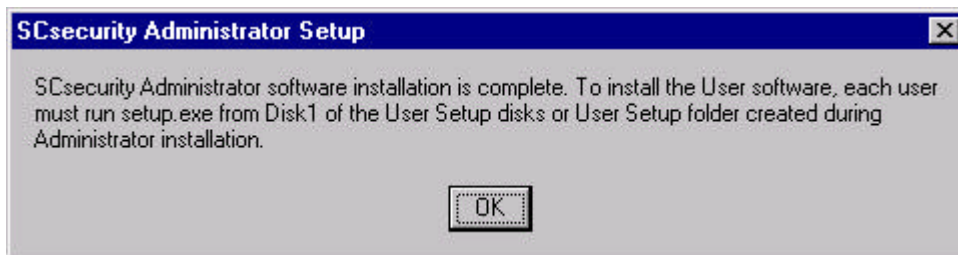
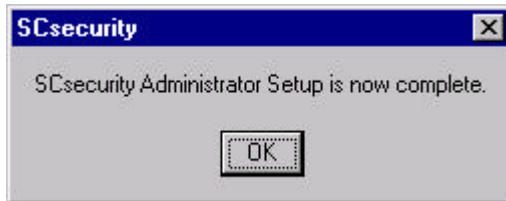


At this time, you are prompted to back-up the administrator file containing the public key (pkfile) to your hard disk. . Choose **OK** or press ENTER.

IMPORTANT: The file is copied to the administrator's hard drive automatically. The pkfile should also be copied to a floppy disk as a back up. This back-up floppy should be kept in a secure location at the Administrator's office.



Each user must now install the SmartCard Security Kit user software from the CD-ROM or from floppies if diskettes were created beforehand. A copy of the customized Administrator files will be required for user installation. Choose **OK** or press ENTER.



Testing Emergency Access

Before making multiple copies of your organization's master Administrator Files disk 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 for instructions.
3. Decrypt the test file.
Use the Emergency Access procedure "To decrypt a user's files with the Emergency Access Key" on page 54.

Seeing 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 disks (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.

Distribute the Customized Administrator File Disk

If the test was successful, make the appropriate number of copies from the master IBM SmartCard Security Kit Customized Administration File disk and distribute them to users for installation. Alternatively, you can copy the disk contents to a directory on your network and instruct users to where to find the files for use during user installation.

The 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 SmartCard Security Kit user manual (**user.pdf**) and the Adobe Acrobat Reader setup program (**ar32e301.exe**) on a network drive for reference during user installation.

Part III

This remaining part addresses the features of the IBM SmartCard Security Kit Administration Software.

4

Administrator's Tasks

This chapter explains how to recover files, how to access the security log, and how to regain complete security after file recovery. Topics include:

- **Emergency Access** – how to recover files
- **Changing Emergency Access Key Protection** – how to update Emergency Access
- **Security Log File** – information about emergency recovery attempts

Using the SmartCard Administration control panel

The SmartCard Administration icon, located in the Windows control panel, lets the user change four settings:



- Change user pin
- Change user information
- Administration options
- Grant access to computer

Select one of the four options and press the Execute button or click on the Finish button to close the dialog box without doing any additional functions. This dialog box remains open until the Finish button is clicked.

Administrators should change the Admin PIN on each Smart Card at the first opportunity. A good time to do this is when granting access for the smart cards on individual systems.

Change User PIN

Clicking on the Change user PIN radio button displays a dialog box so that the PIN can be modified. Enter the old (current) PIN, press the Tab key to change field, enter the new PIN, press the Tab key again to change field, confirm the PIN by entering it again.

Press the Enter key or click on the Ok button to validate the change or press the Esc key, or click on the Cancel button to nullify the change.

Change User Information

Enter the following user information to change the information for personalizing the card:

- | | |
|-------------------------|--|
| Full Name: | Enter your first name and last name |
| User Name: * | Enter the user name where the computer is connected. |
| User Domain: * | Enter the user domain where the computer is connected on a Local Area Network (LAN). |
| User Password: * | Enter the LAN password |
| Confirm: * | Confirm the password |

Press the Enter key or click on the Ok button to validate the change, or press the Esc key or click on the Cancel button to null the change.

* Optional Windows field, not required for operation of the SmartCard Security Kit.

Administration Options

Clicking on this radio button displays a dialog box that allows the administrator to:

- Unlock the smart card should the user enter the wrong PIN more than three times in a row.
 - Administrator must enter his PIN in the edit box provided.
 - Click on the Change (unblock) Logon PIN radio button
 - Enter New User PIN
 - Confirm New User PIN
- Click on the Change Admin PIN radio button to change the Administrator PIN.
 - Enter current Admin PIN in the Edit box provided
 - Press the Tab key and enter the new Admin PIN
 - Press the Tab key again to change field, and confirm the Admin PIN by entering it a second time.

Press the Enter key or click on the Ok button to validate the change, or press the Esc key or click on the Cancel button to nullify the change.

Grant Access to the Computer

This dialog is used to authorize a specific smart card to be used on the computer. The dialog box displays the serial number of the smart card to be authorized.

To grant access to the computer, the administrator must provide the Admin PIN.

Click the Grant button to provide access, or click on the Cancel button to finish the dialog without granting access.

Overview of IBM SmartCard Security Kit Contextual Menu

SCsecurity Emergency

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

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

Emergency Access to the Data

The SmartCard 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, via the SCsecurity Emergency contextual menu. Emergency Access decrypts files encrypted with either the user’s “smart card key” or shared passphrase, including self-extracting files.

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.

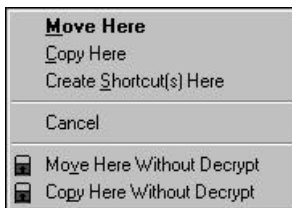
Emergency Decryption

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 floppy disk 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 has 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 disks.
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 Disk.
 - 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 Disks 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 59). 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 SmartCard 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 SmartCard 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 SmartCard Security Kit software enables the administrator and trustees to change the Emergency Access protection method using the Change Emergency Key Protection... menu item. The SmartCard 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 Customized Administrator File Disk 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 Disks.
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 floppy disk.

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 disks, except that the threshold number of trustees must insert their disks 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 Disk), 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, do 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 42 of this 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 42 of this manual.

Important: Always back up the emergency preference file (**emerpref!!!**), safeguard the disk, and memorize the passphrase you chose.

Emergency Access Inf...

displays the Emergency Access Information dialog 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.

SCsecurity Administrator Help...

Provides information on the IBM SmartCard Security Kit features, procedures, menu options, dialog boxes, etc.

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, **emrgdcr.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

De-installing the Administration Software

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

- **What to do before Uninstalling** – What must be done to ensure a safe de-installation.
- **De-installing the Security Software** – how to de-install the IBM SmartCard Security Kit software..

What to do Before De-installing

Before de-installing the IBM SmartCard Security Kit Administration software, make sure **all** encrypted files have been decrypted. The users **must** decrypt all files before uninstalling the SmartCard Security Kit.

To preserve the option of restoring the Emergency Access software with its unique key, you must retain any administrator preference files (**emrgpref.!!!** and **manalist.!!!**).

CAUTION: If the administrator preference files (**emrgpref.!!!** and **manalist.!!!**) are destroyed or lost, there is no way to recover files encrypted with the IBM SmartCard Security Kit. Make sure to have backup copies of these files on a floppy disk or another suitable media.

Uninstalling the Administration Software

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

Important: If other users use the SmartCard 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 for additional information about the AutoCrypt List feature.

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

The SmartCard 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 SmartCard Security Kit software:**

1. Log on to the Desktop.
2. Close all other programs and any SmartCard 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 SmartCard Security Kit Uninstall program to remove the IBM SmartCard Security Kit administrator software from the hard drive. The Add/Remove Programs Properties sheet opens.

4. Choose **Smart Card Security Kit Administrator** from the program list, then click **Remove**.
A confirmation dialog box opens.
5. Choose **Yes** or press ENTER.
Windows removes the SmartCard Security Kit Administrator software from the hard drive. The SmartCard Security Kit software displays a message confirming the SmartCard Security Kit software was uninstalled.
6. Choose **OK** or press enter to reboot your machine and complete uninstall.
Windows restarts.

Glossary

The following terms are used throughout this manual.

administrator software	The part of the IBM SmartCard Security Kit used to configure and maintain administrative control over the SmartCard Security Kit User Setup.
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 who customizes User Setup. These settings are placed in files and backed up at the end of Administrator Setup.
Administrator Setup	The setting up of administrator software, including emergency file access, and user software configuration.
Algorithm	A set of steps the SmartCard Security Kit takes to encrypt and decrypt data securely.
Attack	An intentional attempt to bypass access controls, violate privacy, corrupt services, or simply to break security plans.
AutoCrypt	The SmartCard Security Kit feature that automatically encrypts and decrypts files in folders (and subfolders) the user or administrator has chosen to keep secure.
clear text	Readable text. Text that is not encrypted. Plain text.
Cryptography	The practice and study of encryption and decryption. The encoding of data so that only authorized individuals have access to it.
Customized User Setup Disks	The group of disks or files initialized during Administrator Setup that is used to set up the SmartCard Security Kit's user software.
Decryption	The reverse of encryption. Decryption returns data to its original state, making it readable again.
Emergency Access	The SmartCard Security Kit feature that enables trusted individuals to gain access to files without the password of the

user who encrypted the files.

Cryptography	The practice and study of encryption and decryption. The encoding of data so that only authorized individuals have access to it.
Customized User Setup Disks	The group of disks or files initialized during Administrator Setup that is used to set up the SmartCard Security Kit's user software.
Decryption	The reverse of encryption. Decryption returns data to its original state, making it readable again.
Emergency Access	The SmartCard 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.
Key	A very large number the SmartCard Security Kit uses to encrypt and decrypt a file.
Key generation	The creation of a key for encryption and decryption.
Organization	A collection of individuals who share the same administrator.
Passphrase	A string of character used to gain authorized access to a computer and its data. Passphrases are usually longer than passwords, and therefore, more secure.
Pkfile (User preference file)	The user preference file (pkfile) contains your organizations public key and Emergency Access information. The IBM SmartCard Security Kit uses the information in this file combined with your PIN protected smart card to generate your "dynamic" user preference file, at the time you log onto the computer.
Plain text	Readable text. Text that is not encrypted. Clear text.
Privacy	The protection of a message such that only intended recipients can read a message.
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 SmartCard Security Kit "secret key."
RC4® Symmetric Cipher	The technology behind file encryption. RC4 uses randomly seeded keys to encrypt files.
Random seed	A unique number that the IBM SmartCard Security Kit uses to create a key.
RSA Public Key Cryptosystem™	The technology behind Emergency Access. The IBM SmartCard Security Kit public key is the key exchanged between the administrator and the users of the IBM SmartCard Security Kit. It enables the emergency decryption of files.

secret key	The key generated during User Setup. This key personalizes each user's version of the IBM SmartCard Security Kit. The "secret key" is stored in the SmartCard and is protected by the user PIN. The user's "secret key" is used to encrypt and decrypt a file.
secret passphrase	The SmartCard Security Kit uses the user's "secret key" to encrypt or decrypt files when the Use Smart Card key menu option is selected.
secure single sign-on	Automatic and secure sign-on to host systems, network environments, and application programs.
security log file	A file found in the SmartCard 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.
Screen lock	The SmartCard 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.
trustee	One person out of a group of people entrusted to authorize Emergency Access to the user's encrypted files.
Trustee Key Disk	A disk 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 preference file (pkfile)	The user preference file (pkfile) contains your organization's public key and Emergency Access information. The IBM SmartCard Security Kit uses the information in this file, combined with your PIN-protected smart card, to generate your "dynamic" user preference file, at the time you log on to your system.
User Setup	Installing and setting up the SmartCard Security Kit user software on a computer.
User Setup Disks	The disks that hold the SmartCard Security Kit user software. These disks must be customized by the administrator before users make use of them.
user name	A unique name used to log on to a computer or network service.

to access information.

Index

A

About.....	58
administrator overview	20
Administrator Setup	
and security plans.....	22
single user.....	22
testing	47
administrator software	
single user setup.....	22
uninstalling	61

C

Change Emergency Key Protection... ..	57
configuration	28
Customized User Setup.....	38

D

default Personal Identification Number	10
--	----

E

Emergency Access	21, 54
how it works	23
security suggestions.....	21
Emergency Access Info.....	58
emergency access passphrase	38, 39, 41
emergency key	
changing protection	56
defined.....	23
distributed access	21
feature.....	11, 19
single passphrase.....	42
emergency key disks	<i>See also</i> trustee key disks
creating	43
security suggestion	21
emergency key files	
trustee	38
emergency key passphrase	
suggestions.....	25

emrgdcert.log	59
---------------------	----

F

filename compatibility.....	28
-----------------------------	----

G

generating a random seed	45
--------------------------------	----

H

hardware requirements	28
-----------------------------	----

I

IBM Web site	14
installation	
hardware.....	27
software.....	27

M

Master Customized User Setup	38
migrating	
user	28

P

passphrase	
suggestions	25
Personal Identification Number	
default	10

R

random seed.....	45
recommended configuration	28
recovering	
encrypted files	21, 54

S

SCsecurity Administrator Help	58
SCsecurity Emergency contextual menu	54, 57
security	
plans	22
suggestions	21
security log file	59
single user	
Administrator Setup	22
software requirements	28

T

trustee	11, 19
and changing emergency key protection	56
how Emergency Access works	23
participation	21
passphrase suggestions	25
Trustee	23
trustee key disk	43

U

uninstall	
-----------	--

administrator software	61
previous versions	28
Uninstall	
SmartCard Security Kit Administration software	62
upgrading	
user	28
user name	
confirming	55
recover all files	56
User Setup	22
User Setup	38
User Setup Disks	
copying	47
user software	
setting up	27

W

Web site	14
Windows 3.1	
filename compatibility	28
Windows 95	18, 28
Windows 98	18, 28
Windows NT	
compatibility	28



IBM Smart Card ORDER FORM

Fax order form along with PO to **Gemplus @ (215) 654-8922**

or

Call **(215) 654-8444** for credit card orders

Order Date:		Sales Rep:	Gemplus
Customer:		Requested By:	
Application:		PO NUMBER:	

BILL TO:

SHIP TO:

Order Placed By:		Attention:	
Phone:		Fax:	
Type of Payment (Select one: Net 30 days, or C.O.D.)		Ship Via (Select one: UPS Red or Blue, Fed-X, or Mail)	
Tax Exempt? Yes / No If yes, YOU MUST PROVIDE TAX 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

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