IBM SmartCard Security Kit for Notebooks

Quick Reference Manual

Software Version 1.0 for Windows® 95 and 98

OPTIONS by IBM

P/N 10L7334

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

Contents

The following information should be recorded and retained for future reference.

CD Part Number	_____
CD Version #	_____
	FRU Part Number
Smart Card Reader	_____
Smart Card	_____
Tag	_____

Spare Smart Cards are available to replace lost or stolen cards. An order form is included in the Administrator Manual located on the Software CD.

Part 1: Installing Your SmartCard Security Kit

The Read First insert 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 manual is contained on the SmartCard Security Kit CD. The CD-ROM contains an Administrator Manual and a User Manual in a format that can be viewed online or printed for offline reading. Before installing your SmartCard Security Kit, please read the manual and become familiar with its contents. A copy of the Read First document and this Quick Reference manual are also located on the software CD. Refer to the README.TXT file on the software CD for the latest information.

The SmartCard Security 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. Refer to the Smart Card Install Utility for instructions on how to generate diskettes for software installation.

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 on the CD 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. Again, refer to the User Manual on the CD 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 PIN for all Smart Cards is **1234**. However, you must replace this PIN with another PIN of your choice (either four, six, or eight digits in length) during the installation. The Administrator PIN is also preset to **1234** and should be changed by the Administrator as soon as possible.

Important: Before installing any of the SmartCard Security Kit hardware or software, you should update your system with the latest BIOS and device drivers. In most cases, your system was manufactured before there was support for devices like Smart Card readers. Contact your system support organization to obtain the latest updates for your system. IBM ThinkPad customers can find updates posted on the following web site:

http://www.pc.ibm.com/support?page=IBM+ThinkPad

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.

You can use any one of the following methods to view the IBM SmartCard Security Kit on line help files from Windows Explorer, My Computer, or from your Windows 95/98 desktop:

- In Windows Explorer or My Computer, select a file or folder, and click the right mouse button.
- Click the right mouse button on the **Start** menu.
- In any local or mapped network drive, or on your desktop, select a file or folder, and click on the **File menu.**

Then, select either **SCsecurity Administrator Help** or **SCsecurity User Help**.

Inserting the IBM Smart Card Reader

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

Using your Smart Card

Before inserting your Smart Card into your Smart Card Reader, assure that the gold contacts are facing up and inserted into the reader first. Insert the Smart Card between the bottom of the reader and the reader flap. Avoid inserting or removing the Smart Card during a system power ON/OFF sequence.

Part 2: Instructions for Administrators

The first part of this manual addresses the administrator who will set up the administrator software and administer the IBM SmartCard Security Kit.

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.

As you go through the Administrator Setup, you decide what security settings best fit your organization. Choose your security settings based on the type of organization you are administering and your file security plan. There are three typical ways to set up security:

- FOR A SINGLE USER

  An individual user of the IBM SmartCard Security Kit can set up the administrator software and the user software on one machine. The user also acts as the administrator of Emergency Access.

- FOR AN ORGANIZATION

  A security administrator can tailor the IBM SmartCard Security Kit to a particular organization's needs.

  To implement Smart Card security for an organization having multiple notebooks with the SmartCard Security Kit installed, an administrator should set up the administrator software on the administrator's computer and then distribute the customized Administrator Preference software to users, using diskettes or a network folder.

- FOR AN ORGANIZATION WITH DISTINCT INTERNAL GROUPS

  A large organization with multiple groups can designate an adminstrator for each group. Each administrator can then separately install the administrator software and tailor the SmartCard Security Kit software to that particular group's needs. Each group will have its own Emergency Access key and trustees. Detailed information and step-by-step instructions for Administrator Setup are found in the Administrator Manual located on the Software CD.

How Emergency Access Works

The Emergency Access feature provides the ability to recover the encrypted files of any user in an organization when the user's Smart Card is not available.

During installation, the administrator creates a public/private key pair for access to encrypted files. The administrator provides to the individual users, the public key portion which is required during the user software installation procedure. 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 IBM 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 placed in the trust of member(s) of the organization. This distribution can occur in one of two ways:

- The Emergency Access key is kept whole and is protected by a single passphrase.

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.

Each encrypted file bears the name of the user who encrypted it. The name appears when a file is decrypted with the Emergency Access key. This enables the administrator to verify that a user who requests emergency decryption is the same user who encrypted the file. For more information, see the Administrator Manual located on the software CD.

Administrator Setup

This section describes how to set up the administrator's software and preferences. Prepare to set up the administrator software by reviewing the Administrator Manual on the CD-ROM.

Your trustees must be present to set up IBM SmartCard Security Kit's Emergency Access if you are splitting the Emergency Access key.

Before You Begin

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

All trustees (those who hold Emergency Access key files) must be present during setup. Each trustee must have a formatted, floppy disk to store their part of the Emergency Access key.

During administrator software setup, you create files that will be required during user software installation. If you choose to copy the files onto a floppy disk, label the disk *IBM SmartCard Security Kit User Setup Disk*.

After you have set up the administrator software, have a floppy disk available for backing up the administrator preference files. Label this diskette *Administrator Preferences Backup Disk*. **This backup disk must be created and strictly guarded.**

Setting Up Emergency Access

After you have installed the IBM SmartCard Security Kit administrator software, your next step is to set up Emergency Access. You will generate an Emergency Access key, specify the name of the administrator who manages Emergency Access, and choose whether to keep the Emergency Access key whole or to split it into parts. (For more information, refer to the Administrator Manual on the CD-ROM.) If you split the Emergency Access key, all trustees must be present, each with a blank formatted floppy disk.

Setting Up the SmartCard Security Kit Emergency Access Key

To set up Emergency Access, you first enter information into the Emergency Access Authority dialog box. This information will provide a contact if the user ever needs Emergency Access to their files. Before saving, carefully review the information you entered. To change these names later, you will have to re-install the IBM SmartCard Security Kit Emergency Access software.

CAUTION: If you re-install the Emergency Access software, you will be unable to decrypt files that were encrypted with user disks customized by any previous installation, unless you save the old key during uninstallation or re-installation. **Each installation is protected by a different key.**

Configuring the Emergency Access key:

Select **Single passphrase** to protect the Emergency Access key with a single passphrase accessible only to the administrator, or select **Split among trustees** if you want more than one person to protect the Emergency Access key.

You will then specify the number of trustees to hold the different parts of the protection for the Emergency Access key. Next, you will specify the minimum number of Emergency Access key parts (number of Trustees) necessary to decrypt user files. Note that this number can be *less than* the total number of trustees, thus making Emergency Access possible even when a trustee is sick or traveling.

Now that you have chosen how the Emergency Access key will be protected, you will perform the steps to create the key, beginning with the generation of a random number "seed." This seed adds randomness to the cryptography process, making your copy of the IBM SmartCard Security Kit absolutely unique. The IBM SmartCard Security Kit uses your keystrokes and mouse movements to generate a personalized "Emergency Access key".

Protecting the Emergency Access Key

At this point, you create a passphrase for the Emergency Access key or a passphrase for each trustee's key file.

The Emergency Access key passphrase you enter will unlock the "Emergency Access key" which will decrypt any IBM SmartCard Security Kit-encrypted file, so you must craft the passphrase carefully.

If you are splitting the Emergency Access key among trustees, you will need a formatted disk (one for each trustee) and all trustees must be present to create a Trustee Key Disk for each trustee. Each trustee will be required to insert a blank formatted floppy disk and enter a passphrase known only to him or her.

Backing Up Administrator Preference Files

Now that you have set up the IBM SmartCard Security Kit's administrator features, you are prompted to back up the administrator preference files. The administrator preference files are copied onto the floppy disk that you previously labeled *Administrator Preference Backup Disk*.

CAUTION: The administrator preference files contain the configuration information for the administration of the IBM SmartCard Security Kit and for emergency file access.

Emergency functionality is impossible without these crucial files!

Consider storing multiple backup copies in different secure locations.

Administrator's Tasks

This section explains how to recover files, how to access the security log, and how to regain complete security after file recovery.

Emergency Access

The IBM 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 or shared passphrase, including self-extracting files.

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

Note: Emergency decryption can only be done on a system that has the SmartCard Security Kit administrator software installed. To move the encrypted file to a different system, copy the encrypted files to a floppy disk using the **Copy Here Without Decrypt** or the **Move Here Without Decrypt** menu option.

1. Select the files to be decrypted from Windows Explorer or the My Computer window.
2. Right-click the mouse button, select **SCsecurity Emergency**, and choose **Emergency Decrypt**.

What happens next depends on how your organization has set up the Emergency Access key. If your Emergency Access key is protected by a single passphrase, enter the Emergency Access key passphrase.

If the Emergency Access key is split into parts on Trustee Key Disks, assemble the threshold number of Emergency Access trustees with their Trustee Key Disks. Each trustee must insert their Trustee Key Disk and enter their secret passphrase.

File Recovery

Your attempt to decrypt a file is recorded in the security log file. Then, the Confirm User Name dialog box appears which enables you to verify that the user who requested emergency decryption is the same user who encrypted the file. In the Confirm User Name dialog box, select one of the following options:

- **Recover this file** decrypts the current file and 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 selections that have not already been skipped.
- **Skip this file** leaves the current file encrypted and automatically searches for the next encrypted file.

Security Log File

When you recover a file, a description of that event is noted in a security log file on the machine where Emergency Access was done. The log file, **emrgdcrt.log**, is a plain text file. It is hidden in the same directory where Emergency Access is installed. New entries are added to the end of the log.

Part 3: Instructions for Users

The remaining pages address the user who sets up and uses the IBM SmartCard Security Kit user software. Refer to the complete User Manual which is contained on the SmartCard Security Kit CD. Much of this information also appears in the online Help file.

User Setup

You can use any one of the following methods to access the IBM SmartCard Security Kit choices from Windows Explorer, My Computer, or from your Windows 95/98 desktop:

- In Windows Explorer or My Computer, select a file or folder, and click the right mouse button.
- Click the right mouse button on the **Start** menu.
- In any local or mapped network drive, or on your desktop, select a file or folder, and click on the **File menu.**

Using the IBM SmartCard Security Kit

To use your system, you must first log on using your personalized Smart Card and PIN. Logging on gives you access to your system and establishes a communication path between your system and your Smart Card. The SmartCard Security software now has access to the "secret key" stored on your Smart Card which it needs to encrypt and decrypt files.

After you have logged on, you can access the security menus in the following ways:

- In Windows Explorer, select a file or folder in the Contents window on the right, and choose **File** from the menu bar or click the right mouse button.
- Select a file in My Computer, and choose **File** from the menu bar or click the right mouse button.
- Select a file on your desktop, and right-click on the file.

With the IBM SmartCard Security Kit installed on your computer, encrypting or decrypting files is simple. You can manually encrypt files on your hard disk, floppy disks, or network and removable drives. Also, AutoCrypt automatically encrypts files in folders on your hard drive or in mapped folders, and any files you save to the AutoCrypt folder.

Overview of IBM SmartCard Security Kit Menu Options

Encrypt or Decrypt

- **Use Smart Card Key...** encrypts or decrypts one or more selected files or folders with the key stored on your Smart Card.
- **Use Shared Passphrase...** encrypts or decrypts one or more selected files with a passphrase that you share with others for secure file exchange.

AutoCrypt

- **Add Folder to AutoCrypt List…** adds the selected folder and all its subfolders to the AutoCrypt List. The security software then automatically encrypts all files in the selected folder and its subfolders. The security software also automatically encrypts new files and the contents of new subfolders as they are added to the AutoCrypt folder. AutoCrypt folders are identified with a **Locked Folder** icon (has a lock in front of the standard folder).
- **Remove Folder from AutoCrypt List…** removes the selected folder and all its subfolders from the AutoCrypt List and decrypts all files inside. No further automatic encryption will take place in the selected folder. The locked folder icon is changed to the standard folder icon.
- **Edit AutoCrypt List…** displays the AutoCrypt List dialog box and enables you to add and remove folders from the AutoCrypt List.

SCsecurity Features

- Disable/Enable Automatic Decryption. With the **Disable Automatic Decryption** and **Enable Automatic Decryption** features, you can choose whether to allow your files to automatically decrypt. At times, you might not want a file to decrypt automatically, such as when you perform a backup. The SmartCard Security Kit installation, and restarting your computer, sets the default to automatic decryption.
- **About** displays copyright information, software version and additional information.

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

Additional IBM SmartCard Security Kit menu options enable you to move and copy files without decrypting them. To see the move and copy menu options:

1. Select an encrypted file or AutoCrypt folder from Windows Explorer.

2. Hold down the right mouse button, and drag the file or folder to a new location.
3. Release the right mouse button and view the menu options:
   - **Move Here Without Decrypt** moves an encrypted file to a new location without decrypting.
   - **Copy Here Without Decrypt** copies an encrypted file to a new location without decrypting.

SCsecurity User Help

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

AutoCrypt Folders

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

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

Note: If a file is located in the AutoCrypt folder, you can choose not to decrypt the file, using the **SCsecurity Features**, **Disable Automatic Decryption** menu option. There might be times, such as when you perform a backup, when you will not want a file to decrypt automatically (see "Disabling and Enabling Automatic Decryption").

Adding a Folder to the AutoCrypt List

To automatically encrypt all files in a folder on a hard drive or mapped network drive: In Windows Explorer, right mouse click on the selected folder, then select **AutoCrypt**, and choose **Add Folder to AutoCrypt List.**

Note: Folders in Network Neighborhood cannot be added to the AutoCrypt List. To add a network folder to the AutoCrypt List, you must first map the drive on which it resides, using **Map Network Drive** in the **Tools** menu.

The files within the selected folders are now encrypted. The folders and all subfolders are now AutoCrypt folders and are part of the AutoCrypt List. Individual file names do not change when a folder becomes an AutoCrypt folder. The folder's icon changes to display a locked folder; any file placed inside becomes encrypted (except for special files, as noted in "Files You Cannot Encrypt").

Removing a Folder from the AutoCrypt List

The **Remove Folder from AutoCrypt List** feature removes a folder and its subfolders from the AutoCrypt List. All encrypted files will be decrypted, and any file added in the future to the removed folder will not be automatically encrypted. The folder's icon changes to display a standard folder.

To remove a folder and its subfolders from the AutoCrypt List: In Windows Explorer, right click on the selected folder(s), select **AutoCrypt**, and choose **Remove Folder from AutoCrypt List.**

Editing the AutoCrypt List

You can display and edit the AutoCrypt List which lists all AutoCrypt folders. From the Edit AutoCrypt List dialog box, you can add or remove folders from the list.

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

Encrypting Files with your Smart Card Key

You can encrypt individual files with your "Smart Card Key" by right clicking on the selected file, and then choosing the **Use Smart Card Key** menu option. When a file is encrypted, it will have a **(!)** added to the file name, just before the file name extension.

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

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

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

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

Encrypting Files with a Shared Passphrase

With the IBM SmartCard Security Kit, you can share encrypted files with others. File encryption for the purpose of sharing the file is similar to the file encryption methods described earlier. Any Windows or IBM SmartCard Security Kit user who knows the shared passphrase can decrypt shared passphrase files. Files encrypted with your Smart Card Key require your Smart Card to decrypt the file. Thus, a recipient of such encrypted files would be unable to decrypt them.

Shared Passphrase Encryption

To send an encrypted file, use the following procedure.

To encrypt a file with a shared passphrase:

Right click the desired file, select **Encrypt**, and choose **Use Shared Passphrase**.

You will then be asked to enter and verify a shared passphrase. During encryption, a separate file is created to store the encrypted data for each file. The original files will not be erased unless you checked the **Delete original file(s)** option.

- If you do not check the **Encrypt as self-extracting Windows file (.exe)** checkbox, the encryption software changes the file name and icon, and adds the extension of **.s!!** to indicate that the file has been encrypted with a shared passphrase. You can send this file to another person that has the IBM SmartCard Security Kit installed.

- You may want to share a file with a Windows user who does not have the IBM SmartCard Security Kit installed. For this person, you can encrypt the file as a self-extracting file which provides a way for a Windows user to decrypt it.

Simply, select the **Encrypt as self-extracting Windows file (.exe)** checkbox. The encryption software changes the file extension to **.exe** to show that it has been encrypted as an executable file. After receiving the file, the Windows user double-clicks on the file, enters the shared passphrase, and the file will decrypt itself.

Note: To maintain compatibility with Windows 3.1 users, IBM SmartCard Security Kit creates a file with an eight-character name. You might want to rename the file in advance with this in mind.

Before the recipient can decrypt the file, the originator must communicate the passphrase in a secure manner.

Decrypting Files with your Smart Card Key

Decrypting files is as straightforward as encrypting them. Manually encrypted file names include the characters: **(!)**. After decrypting, the files are renamed to their original names. (For example, the file **myfile(!).doc** becomes **myfile.doc**.) This name change reflects the decrypted state of the files.

You cannot decrypt files in an AutoCrypt folder. You must move files out of the AutoCrypt folder to decrypt them.

With the IBM SmartCard Security Kit, you decrypt a file automatically when opening it from any Windows 95/98 application. Windows 95/98 enables you to open a data file in its associated application by double-clicking on the file in Windows Explorer or My Computer. The IBM SmartCard Security Kit extends this capability to encrypted files.

Decrypting Files with a Shared Passphrase

Read the following instructions for information on decrypting files.

Shared Passphrase Decryption

When someone sends you a file with the **.s!!** extension, you can decrypt the file if you know the shared passphrase used to encrypt it. Right click on the encrypted file, select **Decrypt**; then select **Use Shared Passphrase**. Provide the shared Passphrase when requested to decrypt the file.

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

Decrypting a Self-Extracting, Encrypted File

To decrypt a file that has been encrypted as a self-extracting file, double-click on the file, then enter the shared passphrase used for encryption.

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

Special SmartCard Security Kit Features

Read the following instructions for information on using special SmartCard Security Kit features.

Identifying Encrypted Files

You can use the following methods to identify encrypted files.

Property Sheets

You can look at a file's property sheet to determine whether or not a file is protected by IBM's SmartCard Security Kit. The property sheet for an encrypted file or AutoCrypt folder will have an IBM SmartCard Security Kit tab labeled **Encryption**.

AutoCrypt Folder Icon

On your computer, you can have two types of folders, AutoCrypt folders and non-AutoCrypt folders. An AutoCrypt folder displays a "locked folder" icon. A folder not protected by IBM SmartCard Security Kit has a standard folder icon. As with files, folders have IBM SmartCard Security Kit property sheet tabs labeled **Encryption**.

File Naming Conventions in the IBM SmartCard Security Kit

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

1. All encrypted files in AutoCrypt folders and subfolders retain their original names. Moving or copying files into or out of AutoCrypt folders (without using IBM SmartCard Security Kit's special menu items) does not change their names, regardless of whether or not they are encrypted.
2. All files encrypted outside of AutoCrypt folders have the "**(!)**" characters just before the file name extension; for example, **plan.doc** becomes **plan(!).doc** when encrypted outside of an AutoCrypt folder.

In short, a file is encrypted with your Smart Card key if and only if the file is in an AutoCrypt folder or has "**(!)**" before the last period in its name. For information about naming conventions of files encrypted with a shared passphrase, see "Encrypting Files with a Shared Passphrase" on page 17.

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

Files You Cannot Encrypt

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

The IBM SmartCard Security Kit will not encrypt these files:

- files already encrypted
- IBM SmartCard Security Kit program files
- systems files
- files with any of the following extensions: **.bat**, **.bin**, **.cfg**, **.com**, **.dll**, **.drv**, **.exe**, **.fon**, **.fot**, **.grp**, **.ico**, **.ini**, **.ovl**, **.pif**, **.sys**, **.ttf**, **.vbx**, **.386**, **.vxd**, **.lnk**
- most files in the **\Windows** folders and its subfolders. (Not encrypting these protects the wide range of configuration files with different names that are stored in these directories.) There are exceptions to this exclusion. The IBM SmartCard Security Kit will encrypt files in the folders **\Windows\Temp**, **\Windows\Desktop**, and each user's **\Desktop** subfolder (**\Windows\Profiles*User name*\Desktop**), as long as the files do not contain the reserved extensions listed above.

Files Encrypted with Another Smart Card

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

Note: When viewing the property sheet of a file encrypted with another user's Smart Card, you might get an error message. However, you will still be able to read the property sheet.

Moving and Copying Encrypted Files without Decrypting

1. Select an encrypted file or AutoCrypt folder from the Contents window on the right-hand side of Windows Explorer.
2. Hold down the right mouse button, and drag the file or folder to a new location.
3. Release the right mouse button and view the menu options:
   - **Move Here Without Decrypt** moves an encrypted file to a new location without decrypting it.

- **Copy Here Without Decrypt** copies an encrypted file to a new location without decrypting it.

Uninstalling the Software

Note: Be sure to follow the uninstall instructions in the Read First insert shipped with your SmartCard Security Kit.

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

IBM recommends that you use the standard Windows 95/98 **Add/Remove Programs** option to uninstall the IBM SmartCard Security Kit user software.

As with most Windows 95/98 programs, it is recommended that you exit all other applications prior to uninstalling IBM SmartCard Security Kit. During the uninstall process, a dialog box warns you that only files encrypted with your Smart Card, **and** located in the AutoCrypt List can be decrypted during uninstall. If other users share your system, there may be files in the AutoCrypt List that cannot be decrypted during uninstall or after uninstall. Uninstall continues to remove all the items on the uninstall checklist. There may be some items left that you will need to remove manually.

Note: You can also use the Start menu **Run** command to run the IBM SmartCard Security Kit Uninstall program to remove the IBM SmartCard Security Kit from the hard drive.

Part 4: Overview of Digital Signature and Digital Certificates

Your IBM SmartCard Security Kit includes GemSAFE™ software from Gemplus. GemSAFE provides DIGITAL SIGNATURE and CERTIFICATE support using the Smart Card that is included in your SmartCard Security Kit.

For specific details about the available GemSAFE functions, refer to the GemSAFE manuals located on your software CD. The CD also has a white paper that will help you understand the fundamentals of Smart Card security when you are using the Web or e-mail. The latest documentation can be found on the GemSAFE Web site: http://www.gemplus.com/GemSAFE

GemSAFE is a smart card-based solution which is designed to primary secure electronic mail (e-mail) communication and Web sessions on the Internet.

This solution combines the privacy, tamper-detection (integrity) and proof of origin (authentication) functionality provided by cryptographic algorithms with the simplicity, portability and convenience of Smart Cards.

Using GemSAFE

The GemSAFE Smart Card securely stores your personal secret information and thus prevents someone from usurping your identity. In fact, your password must be presented before you can use your private keys. The advantage of using GemSAFE rather than software-only solutions is that your keys are always stored in your Smart Card.

The latest standards such as SSL3 (for Web access) or S/MIME (for e-mail) enable inter-operability (that, is compatibility) of security services between any browser interface and any Web server. For example, although S/MIME is designed to exchange secure e-mails, you can also use the same mail application to send regular (unsecured) e-mails.

However, your personal keys and certificate can be easily tampered with if you save them on your PC using this protocol.

Traveling with your electronic identity in pocket, you can securely access online services with your personal Smart Card, protected by a PIN, from any machine in the world. In addition, your card also performs cryptographic algorithms, so that your private keys never leave the card. Simply plug your Smart Card into any reader connected to any Internet terminal equipped with the GemSAFE software. Therefore, GemSAFE provides secure Web access even if you do not have your computer with you.

GemSAFE was designed to be easily installed by users who simply connect the Smart Card reader to their system, install the software on Windows 98 or 95, and then activate the card. If the card was supplied without a preloaded personal certificate, users can recover a certificate online.

Connecting to the GemSAFE Web Site

Additional information and updates are available on the GemSAFE web site at

http://www.gemplus.com/GemSAFE

Digital Signatures

A digital signature provides proof of origin and tamper detection. It consists of sending additional information (known as a signature) along with the original data which proves to the recipient that the received data is word-for-word identical to the data the sender intended to send.

Digital signing of data is completely independent from data encryption. Data can be both signed and encrypted, signed only, encrypted only, and, of course, neither signed nor encrypted.

Since each person involved already has a private key (which is kept secret by its owner) and a corresponding public key (which everybody knows) for encryption purposes, a good system might consist of reusing these keys. The signature is calculated by the sender and sent along with the data to the recipient. Its value is a mathematical function of the sender's private key and the data to be sent. The construction of the algorithm is such that it is not possible to calculate this value without knowing the private key.

The recipient can verify that the data received corresponds to the data that was signed by the sender using another mathematical algorithm which relies upon the sender's public key, the signature, and the data received.

Using Digital Certificates

When the same key-pair is used for encryption and signature, this key-pair corresponds to a kind of online identity. You can use it to sign data (e-mails, expense claims, random challenges sent by Web servers, etc.) and decrypt data that is meant only for you (incoming e-mails, etc.). The GemSAFE solution means that this identity (the private key) is securely stored in a Smart Card and it never comes out. Any calculations that are performed using this key are done by the card itself.

The system relies on the fact that everybody knows a particular key-pair is linked to you. This is the purpose of digital certificates. A key pair without a corresponding digital certificate is effectively useless.

The Role of the Certificate Authority

By issuing a certificate, the Certification Authority (CA) basically states that "Public key 1234... corresponds to a private key that only Mr. Smith or Company XYZ has access to". Anybody who trusts the CA can, for example, encrypt an e-mail for Mr. Smith's eyes only, or verify a digital signature created by Company XYZ.

This binding of a real-world identity (Mr. Smith in this example) to a digital identity (Mr. Smith's key pair) is performed using a digital signature. The CA has its own key-pair which is used to sign the concatenation of Mr. Smith's public key and the name "Mr. Smith" (along with a host of other useful things such as the certificate's validity date, etc.).

Certification Authorities usually charge a fee for this binding task. In fact, depending on the company's policy, the CA might pay a visit to the person it is vouching for to verify that he or she is actually who he or she claims to be, or the CA might need a letter from this person's employer certifying that he or she works there. The CA might also offer other value-added services, such as a public directory of the certificates that it has issued.

To determine whether you can trust a particular CA, first look at the CA's policy statement to check that it performs a type of check that you find appropriate before issuing its certificate (e.g., guarantees and legal position provided by CA).

Second, recover a copy of the CA's public key so you can verify the CA's digital signatures. It is convenient to recover this public key within a certificate (since the certificate also provides validity dates and other relevant elements).

The certificate might be signed by the CA itself or by another CA whom you already trust. In the former case, the certificate cannot be independently verified and thus be validated by other means (for example, using the certificate's independently transmitted "fingerprint").

GemSAFE Security Features

The GemSAFE solution complements two key security standards:

- The SSL/TLS (Secure Socket Layer/Transport Layer Security) is a protocol between the server and the browser, which operates over the Internet.

- The S/MIME (Secure Multipart Internet Mail Encoding) is a message format designed to secure e-mail messages.

Note: TLS is the latest standardized version by the Internet Engineering Task Force (IETF) of SSL.

The SSL Protocol

SSL is on online protocol which may provide privacy over the Internet as it allows client/server applications to communicate in a way that cannot be eavesdropped.

SSL offers the following features: message privacy, message integrity and mutual authentication.

Message Privacy

Message privacy is achieved through encryption. All traffic between an SSL server and an SSL client can be encrypted using a key and encryption algorithm negotiated during the SSL handshake. The SSL handshake (which takes place each time you start a secure Web session) identifies the server. It is automatically performed by your browser.

Message Integrity

The message integrity service ensures that SSL session traffic is not modified on the way to its final destination. SSL uses the combination of a shared secret and special mathematical functions (called hash functions) to provide the message integrity service.

Mutual Authentication

Mutual authentication is the process whereby the server convinces the client of its identity and the user convinces the server of its identity. These identities are coded in the form of public-key certificates (X509), and these certificates are exchanged during the SSL handshake.

To demonstrate that the entity representing the certificate is the legitimate certificate owner (i.e., that this entity has access to the private key which corresponds to the public key in the certificate) rather than a mere impostor, SSL requires that the certificate presenter must digitally sign data exchanged during the handshake (see *Digital Certificates*).

Note: Server authentication is systematically performed by the browser with the SSL protocol, whereas client authentication may or may not be systemically required by the server.

S/MIME

S/MIME is an offline message format standard implemented for use with the Netscape Messenger or Microsoft Outlook Express mail application, which is designed to encrypt and digitally sign electronic mail.

S/MIME offers users the following features:

- Encryption for message privacy
- Sender authentication with digital signatures
- Tamper detection
- Compatibility with any other S/MIME-compliant software

Private messaging

S/MIME's encryption helps ensure that your messages remain private. Both Netscape Messenger and Microsoft Outlook Express software support domestic and export-level public key and symmetric key encryption.

Sender Authentication and Tamper Detection

S/MIME authenticates the message sender by reading the sender's digital signature (the recipient can see who signed the message and view the certificate for additional detail).

Compatibility

Because S/MIME is an open standard, the mail software client can operate with other S/MIME-compliant clients (for example, if you are operating with Netscape Messenger, you can correspond with someone equipped with Microsoft Outlook Express, which is S/MIME-compliant).

Part 5: SoftID Support

Security Dynamics SoftID provides an easy, one-step process to positively identify network and system users and prevent unauthorized access. SoftID operates in conjunction with all Security Dynamics access control products.

SoftID uses the same algorithm as the SecurID hardware token and offers both automatic and manual authentication. When using the Smart Card version of SoftID, your Smart Card will be required for logging into secure systems.

You can visit Security Dynamics Web site at **http://www.securitydynamics.com** for product information and availablity of SoftID (Version 1.5) with Smart Card support.

Part 6: Help and Service Information

If you have questions about your new Options by IBM 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.

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 HelpCenter, 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 or after your warranty has expired, you might be charged a fee.

Marketing, installation, and configuration support through the HelpCenter will be withdrawn or made available for a fee, at IBM's discretion, 90 days after the option has been withdrawn from marketing. Additional support offerings, including step-by-step installation assistance, are available for a nominal fee.

During the warranty period, assistance for replacement or exchange of defective components is available. In addition, if your IBM option is installed in an IBM computer, you might be entitled to service at your location. Your technical support representative can help you determine the best alternative.

Step 1. Problem Solving

You may be able to solve the problem yourself. Before calling the HelpCenter, 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 the Read First document, 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.

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.

3. Uninstall and then reinstall the option. During the uninstall process, be sure to remove any files that were installed during the previous installation. Many IBM options include uninstall programs.

CAUTION: If you re-install the Emergency Access software, you will be unable to decrypt files that were encrypted with user disks customized by any previous installation, unless you save the old key during uninstallation or re-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
2. Option number
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 7: 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.

Notice

Any references in this publication to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Trademarks

IBM is a registered trademark of International Business Machines Corporation. Microsoft and Windows are registered trademarks of Microsoft Corporation.