MASTER/SESSION
KEY AND FIT LOADER
FOR INTELLIPIN
SOFTWARE INSTALLATION AND OPERATION MANUAL

Manual Part Number: 99875098 Rev 5

OCTOBER 2008

MAGTEK®

REVISIONS

Rev Number	Date	Notes
1	27 Apr 98	Initial Release
2	11 May 00	All references to IntelliPIN Plus changed to IntelliPIN
3	23 Aug 00	Software license added, deleted Limited Warranty.
4	12 May 03	Editorial throughout; Front Matter: Added ISO Line To Logo, changed License Agreement to generic version. Sec 1 through Sec 4: Added or changed all screen captures.
5	15 Jul 04	Title Page: Added "Master/Session" to title and changed title in header throughout to reflect this change.

SOFTWARE LICENSE AGREEMENT

IMPORTANT: YOU SHOULD CAREFULLY READ ALL THE TERMS, CONDITIONS AND RESTRICTIONS OF THIS LICENSE AGREEMENT BEFORE INSTALLING THE SOFTWARE PACKAGE. YOUR INSTALLATION OF THE SOFTWARE PACKAGE PRESUMES YOUR ACCEPTANCE OF THE TERMS, CONDITIONS, AND RESTRICTIONS CONTAINED IN THIS AGREEMENT. IF YOU DO NOT AGREE WITH THESE TERMS, CONDITIONS, AND RESTRICTIONS, PROMPTLY RETURN THE SOFTWARE PACKAGE AND ASSOCIATED DOCUMENTATION TO ABOVE ADDRESS ATTENTION: CUSTOMER SUPPORT.

TERMS, CONDITIONS AND RESTRICTIONS

MagTek, Incorporated (the "Licensor") owns and has the right to distribute the described software and documentation, collectively referred to as the "Software".

LICENSE: Licensor grants you (the "Licensee") the right to use the Software in conjunction with MagTek products.

LICENSEE MAY NOT COPY, MODIFY OR TRANSFER THE SOFTWARE IN WHOLE OR IN PART EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT. Licensee may not decompile, disassemble or in any other manner attempt to reverse engineer the Software. Licensee shall not tamper with, bypass or alter any security features of the software or attempt to do so.

TRANSFER: Licensee may not transfer the Software or license to the Software to another party without prior written authorization of the Licensor. If Licensee transfers the Software without authorization, all rights granted under this Agreement are automatically terminated.

COPYRIGHT: The Software is copyrighted. Licensee may not copy the Software except for archival purposes or to load for execution purposes. All other copies of the Software are in violation of this Agreement.

TERM: This Agreement is in effect as long as Licensee continues the use of the Software. The Licensor also reserves the right to terminate this Agreement if Licensee fails to comply with any of the terms, conditions or restrictions contained herein. Should Licensor terminate this Agreement due to Licensee's failure to comply, Licensee agrees to return the Software to Licensor. Receipt of returned Software by the Licensor shall mark the termination.

LIMITED WARRANTY: Licensor warrants to the Licensee that the disk(s) or other media on which the Software is recorded to be free from defects in material or workmanship under normal use. THE SOFTWARE IS PROVIDED AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Because of the diversity of conditions and PC hardware under which the Software may be used, Licensor does not warrant that the Software will meet Licensee specifications or that the operation of the Software will be uninterrupted or free of errors.

IN NO EVENT WILL LICENSOR BE LIABLE FOR ANY DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE. Licensee's sole remedy in the event of a defect in material or workmanship is expressly limited to replacement of the Software disk(s) if applicable.

GOVERNING LAW: If any provision of this Agreement is found to be unlawful, void or unenforceable, that provision shall be removed from consideration under this Agreement and will not affect the enforceability of any of the remaining provisions. This Agreement shall be governed by the laws of the State of California and shall insure to the benefit of MagTek, Incorporated, its successors or assigns.

ACKNOWLEDGMENT: LICENSEE ACKNOWLEDGES THAT HE HAS READ THIS AGREEMENT, UNDERSTANDS ALL OF ITS TERMS, CONDITIONS AND RESTRICTIONS AND AGREES TO BE BOUND BY THEM. LICENSEE ALSO AGREES THAT THIS AGREEMENT SUPERSEDES ANY AND ALL, VERBAL AND WRITTEN, COMMUNICATIONS BETWEEN LICENSOR AND LICENSEE OR THEIR ASSIGNS RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT.

QUESTIONS REGARDING THIS AGREEMENT SHOULD BE ADDRESSED IN WRITING TO MAGTEK, INCORPORATED, ATTENTION: CUSTOMER SUPPORT, AT THE ABOVE ADDRESS OR E-MAILED TO support@magtek.com

TABLE OF CONTENTS

SECTION 1. FEATURES

The Key and FIT Loader is a Windows program that consists of two separate modules. One module loads Keys into the IntelliPIN and the other loads FITs (Financial Institution Tables).

Keys and FITs can be loaded by an operator and loaded or modified by an administrator. For security requirements, the operator and administrator have separate passwords for entry.

The program can be used with any IntelliPIN model interface: RS-232, USB, Keyboard Wedge, and Standalone. The Standalone model requires an RS-232 interface cable (P/N 30019304) for loading the information, but the IntelliPIN can operate in the Standalone mode after the FITs have been loaded.

KEY LOADER

When the IntelliPIN is used in the Interactive mode, a number of keys need to be downloaded in order to encrypt the PIN block and other messages. The Key Loader can be used to download the Master Key, Session Key, Working Keys and other transaction-related information into the IntelliPIN.

FIT LOADER

When the IntelliPIN is used in the Offline (standalone) Mode, certain parameters must be stored in the unit to compute the offset and PVV values. These parameters can be loaded from a Program Card or downloaded from a PC using this FIT Loader program. These parameters are stored in a Financial Institution Table (FIT). In the Offline Mode, the FIT parameters must be stored in the IntelliPIN. This program eliminates the need for Program Cards since all of the FIT parameters can be downloaded from this program. An Activate Card may be required to begin daily operation.

REFERENCE DOCUMENTS

The following IntelliPIN documents are related to the Key and FIT Loader program:

- IntelliPIN, PINPad with Magnetic Stripe Reader, Installation and Operation Manual, (99875066)
- IntelliPIN, Programming Reference Manual, (99875047)
- IntelliPIN, Installation Instructions, (99875076)
- MTD, MagTek Device Drivers for Windows, Programming Reference Manual (99875125)

1

REQUIREMENTS

The following are required for operating the program:

- PC with Windows 95, 98, ME, NT, 2000, or XP
- Any IntelliPIN (300151XX) and hardware interfaces
- Key and FIT Loader Program for IntelliPIN, (30037369)

SECURITY

The program has unique security features:

- A password is required to operate the program. The information is saved and then encrypted on a floppy disk.
- Program information is encrypted with a hidden key and the Administrator password, which prevents information from being used on any other computer with a different Administrator password.
- Any information entered cannot be stored on a hard disk. Information can be stored only on removable media.

SECTION 2. INSTALLATION

The installation consists of loading the program disk, opening the program, and selecting passwords for the operator and administrator.

PROGRAM INSTALLATION

To begin the installation, insert the CD (P/N 30037369) into the appropriate drive. The installation program will automatically start. If the installation program does not begin automatically, select *Run* from the *Start* menu. Within the open field, type x:\setup, where x: is the drive letter of your CD ROM drive. Click *OK* to begin installation.
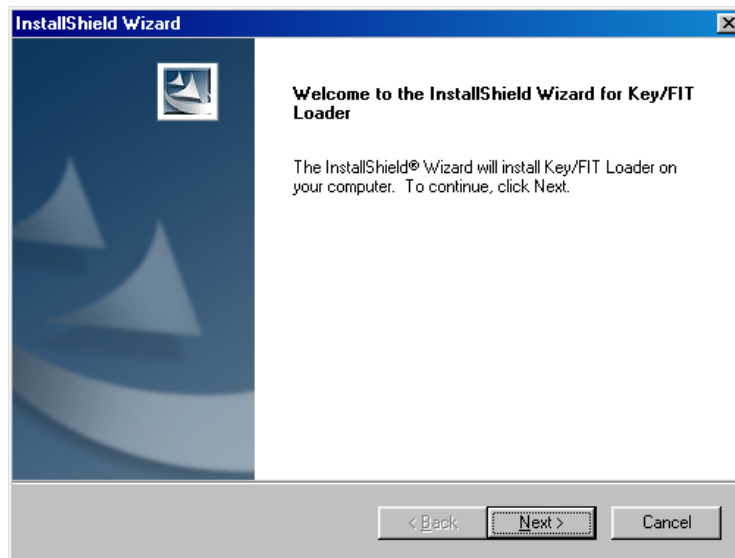
Click *Next*.
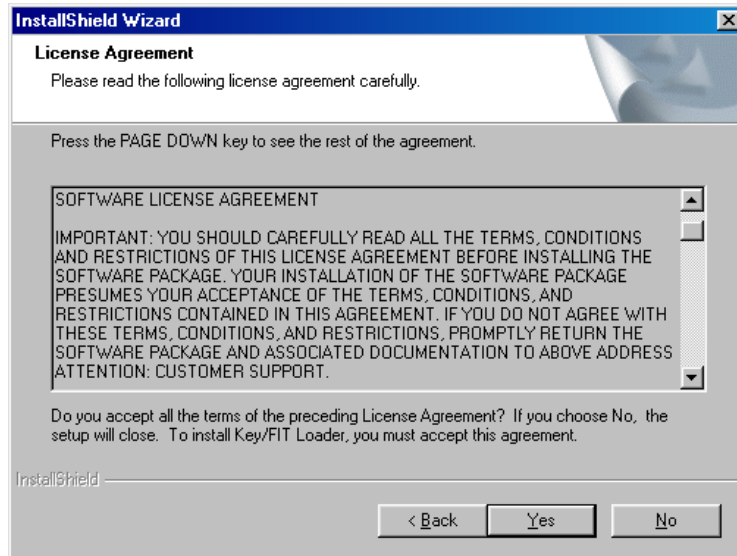
Review the license agreement and click *Yes* if you agree to the terms.

Select the *Destination Folder*. Either accept the default installation location or click *Browse* to define another location. Click *Next* when ready.
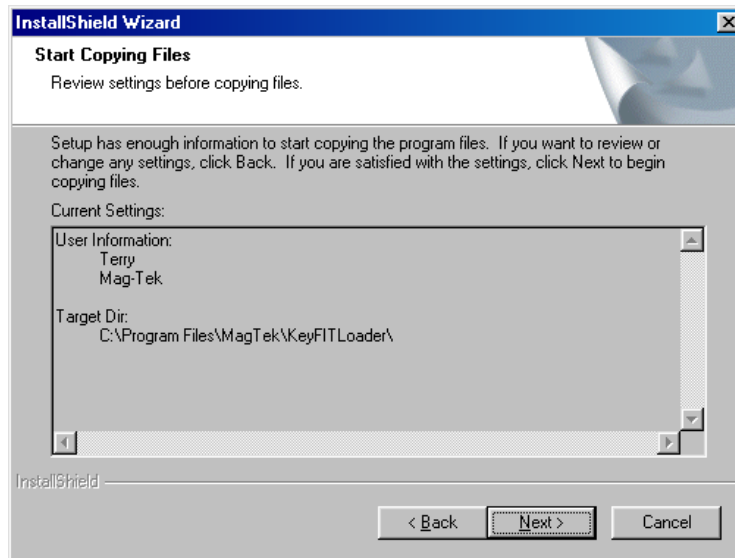
If the summary information is correct, click *Next* to install the program.

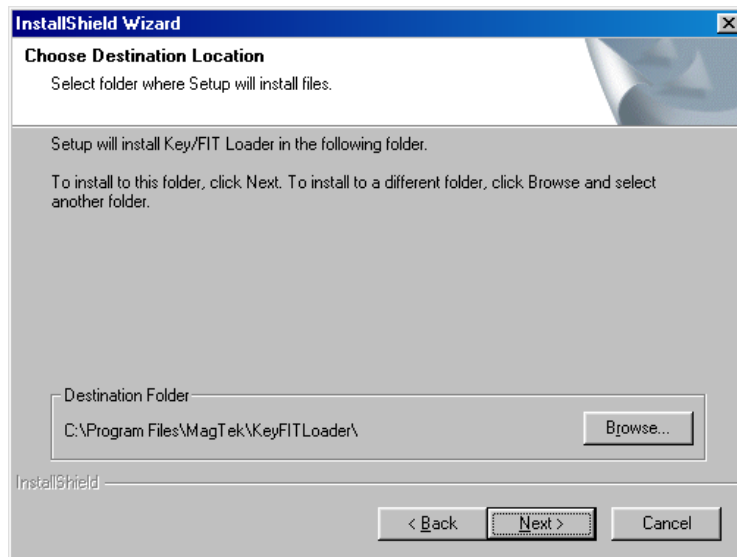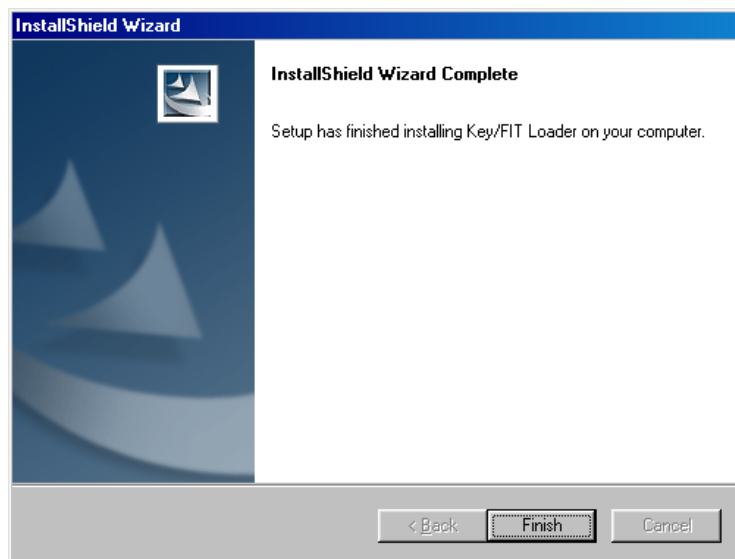Click *Finish* and remove the CD from the drive.

MTD Driver Installation

The Key/FIT Loader program requires the MTD Drivers to be installed in order to communicate with the various IntelliPIN versions. If the MTD Drivers are not already installed, you may obtain them from the MagTek web site (www.magtek.com) or you can order a CD (P/N 30037385) from MagTek. When you are installing the MTD Drivers, you will only need to select the IntelliPIN as the driver to install. Be sure to indicate the proper device interface (RS-

5

232, USB, or Keyboard Wedge) so it will match the IntelliPIN model you will be using. Refer to the MTD Drivers Programming Manual (99875125) for complete installation information.

SECTION 3. PROGRAM OPERATION

STARTING THE PROGRAM

When the program starts, two passwords of up to 8 alphanumeric characters must be entered. There are two authorization levels of security for using this program. The Administrator has the authority to modify any of the parameters and update the IntelliPIN. The Operator only has authority to load data from a previously saved disk and download the information to the IntelliPIN.

In order to prevent the information that is stored on the disk from being accessed on another system, the Administrator Password is used in the encryption process. Since the Administrator Password is used to encrypt data that is stored on the disk, it is not recommended to change the Administrator Password after a backup disk has been created.

PASSWORD SELECTION

Select the passwords for the Administrator and for the Operator as follows:

1. The first time the program is opened, the Password dialog box will appear. Select **Administrator**. Use the Tab key to place the cursor in the **New** box.

2. The maximum number of alphanumeric characters for the password is 8 characters. Type in a password of 4 to 8 characters.

3. Use the Tab key to move the cursor to the **Confirm** box, and retype the password for confirmation.

4. Select **Operator** from the Password dialog box. Use the Tab key to place the cursor in the **New** box.

5. The maximum number of characters for the password is 8 characters. Type in a password of 4 to 8 characters.

6. Use the tab key to move the cursor to the **Confirm** box, and retype the password.

MAIN SCREEN SELECTIONS

Information is derived from the Main Screen from three sources: the drop-down menus, the toolbar, and the status bar in the lower left corner. These sources are described below.
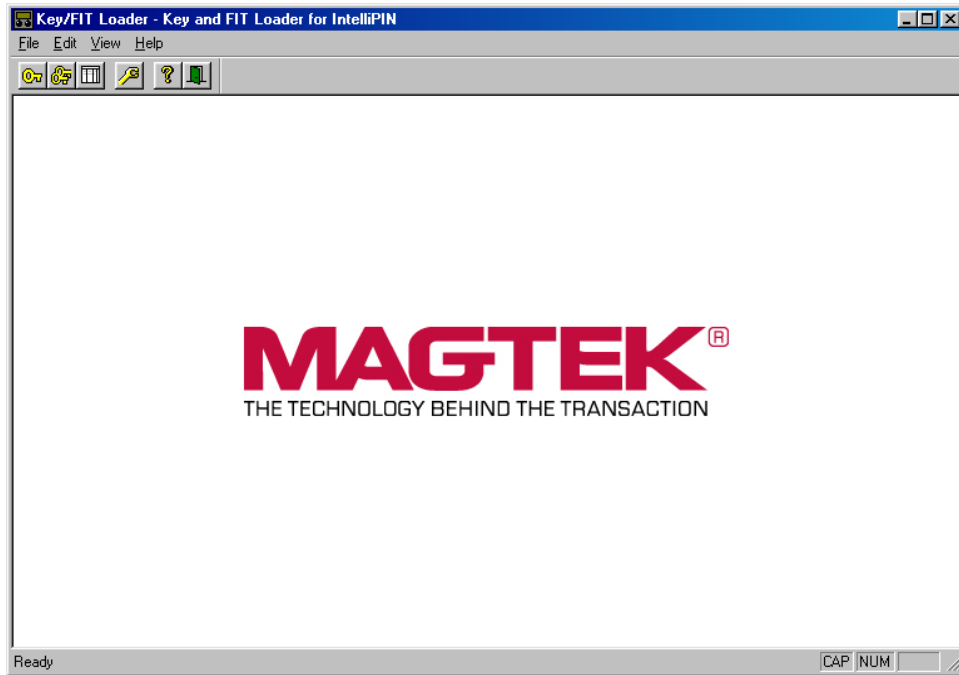
Drop-Down Menus

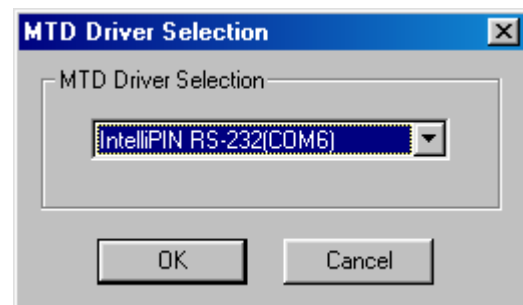The Drop-down menus are File, Edit, View, and Help. They are as follows:

File - contains Port Setup, Change Password, (Admin only) Change Mode Administrator/Operator, and Exit. The Port Setup must match the IntelliPIN setup.
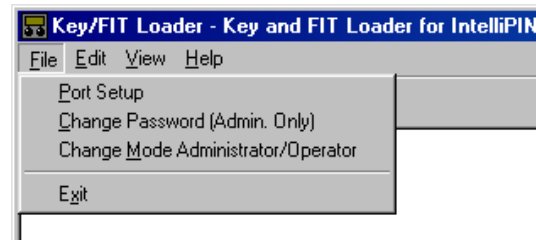
Port setup allows you to define the MTD device. Use the pulldown menu to select the appropriate IntelliPIN. Click *OK* if correct.

Edit - contains <u>K</u>eys…, <u>F</u>IT Table…, and Multi-Master Key. Key Design is described in Section 4. FIT Loading is described in Section 5.

View - displays and removes the tool bar and status bar from the screen.

Help - contains <u>C</u>ontents, <u>S</u>earch and <u>A</u>bout Fit Loader. Contents is a Table of Contents for the Help file. Search contains an alphabetical Contents list, an Index and a Find dialog box. About FIT Loader lists the program version, the IntelliPIN Firmware Number, Revision Level, Sub Revision Level, and copyright information.

Toolbars

The toolbar buttons perform the following functions:

This button, the "Key," brings up one of two Key Design boxes, depending on whether the Administrator or the Operator is signed on. The mode is selected by password after the opening screen. These dialog boxes are described in Section 4.

This is the Multi Master Key button. It brings up dialog box that presents all 10 Multi-Master Keys.

This button, the "Table," brings up one of two FIT Table boxes, depending on whether the Administrator or the Operator function is selected by password. These dialog boxes are described in Section 5.

This button, the "Wrench," brings up the MTD Selection Box.

This button, the "Question Mark," brings up the Table of Contents including menus for Contents, Index, Find, Print, and Glossary.
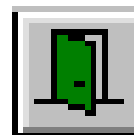
This button, the "Door," exits the program. Before exiting, a prompt to save documents will appear.

9

Status Bar

The Status Bar in the lower left corner of the screen describes the Toolbar buttons as the cursor is pointed to each one. These descriptions of the buttons (from left to right) are as follows:

- Ready - The program is ready for operation; select a function from the Toolbar or menu.
- Invokes Keys dialog - See Section 4 for a description of the Keys loading operation.
- Invokes Multi Master Key Dialog – See section 4 for a description of the Multi Master Key entry operation.
- Invokes FIT table dialog - See Section 5 for a description of the FIT Table operation.
- Port Setup – Brings up the MTD device selection window.
- Contents - Contents of the Help menu.
- Quit the application; prompts to save documents – click to exit program

CHANGE PASSWORD

As previously stated, changing the Administrator password is not recommended, because the Administrator Password is used to encrypt data that is stored on the disk. However, it may be necessary to change the Administrator or Operator password. To change a password, select Administrator on the Login dialog box. Then select *File* and *Change Password* from the Main Screen. The following reminder will appear:
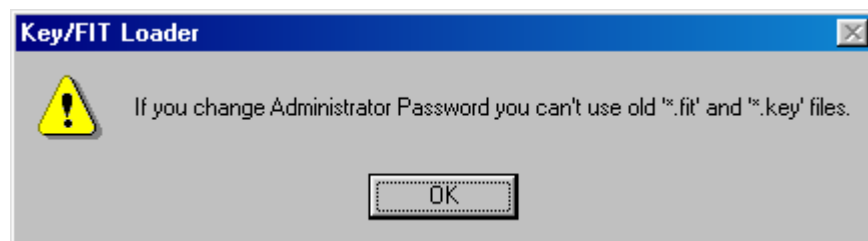
Click *OK* to continue. When the *Password Design* window appears, select Administrator or Operator in the *Mode* pulldown box. Then enter the present (old) password. If that is valid, you will be prompted to enter the *New* password. You must enter it one more time to confirm entry. Click *OK* when done.

SECTION 4. KEY DESIGN AND LOADING

When ready to enter or inject keys, click the *Key* icon on the toolbar. When in the Administrator mode, the full function Key Design dialog box will be shown.

ADMINISTRATOR KEY DESIGN AND LOADING

If the Administrator mode has been selected and Administrator Password entered, the screen shown below will appear when the *Key* icon is selected. The Administrator/Operator mode may be changed by clicking *File* and *Change Mode* and entering the password for the required mode.

Other dialog boxes will be shown as the individual items are selected. If you wish to enter or change the Master Key, click the *Enter* button in the Master Key section. This will bring up the key entry dialog box for the Master Key. The key can be entered in plain text or as components. You also have the option of entering a single-length key (left entry only) for single DES encryption or a double-length key (enter both left and right portions) for Triple DEA encryption. The KCV will be presented when you click the *Accept* button. Click *OK* when the key is complete.

This same Key Entry dialog box will be shown for any of the other keys. Click the *Enter* button in the appropriate section to activate the Key Entry dialog box. When entering the Session Key or Working Keys you will also be able to select *Encrypted* as one of the mode for key entry.

OPERATOR KEY LOADING

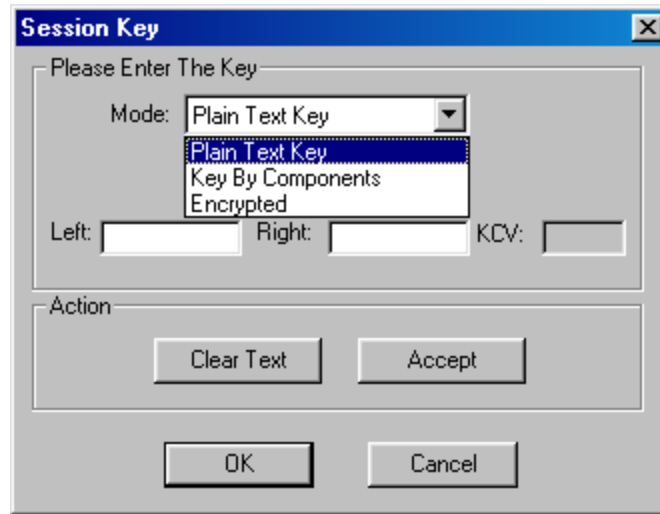The Operator can load files from a disk and download (inject) files to the IntelliPIN. The Key and FIT files are first created in the Administrator's Key Design dialog box. If the Operator mode has been selected and Operator Password entered, the screen shown below will appear when the *Key* icon is selected.

If you attempt to open a file but do not have the correct Administrator password, the system will indicate "Bad File".
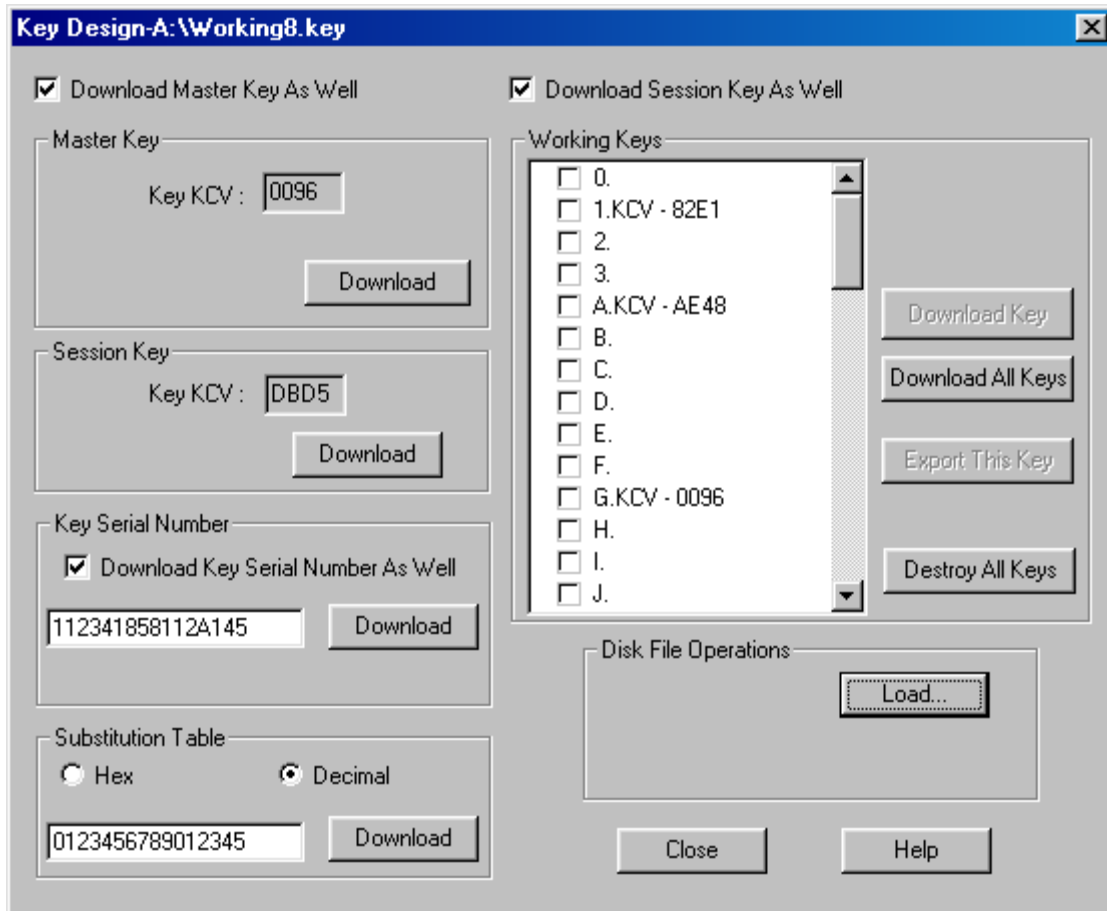
Fewer options are available to the Operator because only the Administrator has the ability to enter or change information. The Operator only has the ability to retrieve and inject keys.

To load and download a file perform the following steps:

1.   Select **Load** from **Disk File Operations**.

2.   From the list of files select the file to be loaded and click **Open**.

3.   The parameters of the opened file will appear on the Key Design Operator's screen similar to the one above.

4.   Enter or change the Key Serial Number if required as defined by the Administrator. (Each IntelliPIN may have its own Key Serial Number.) Download the Key Serial Number if required.

5.   Download the keys by clicking the **Download** buttons as required for the Master Key, Session Key, and Working Keys. (Download operations are described in detail at the end

of this section.) If all Keys are to be downloaded at one time, click **Download All Keys**. Ensure that **Download Master Key As Well** is selected if the Master Key is to be injected.

6.   While the keys are being injected, a bar graph will show progress. When the bar graph goes away, all keys have been injected and the IntelliPIN can be disconnected. The next IntelliPIN can be connected and the process can begin again. Be sure to click the *Download Master Key As Well* and the *Download Key Serial Number As Well* check boxes so that all keys will be properly injected into the next IntelliPIN.

KEY ENTRY

A Key consists of a string of 16 or 32 hexadecimal digits (0-9, A-F). Before entering any of the Key characters, select one of the three methods of entering a key:

1) Plain text key (for all keys)

- The Key is entered in the clear and therefore should only be done in a secure location.

2) Key by components (for all keys)

- A complete Key is entered by more than one person, each knowing only a portion (component) of the Key.
- A KCV is presented for each component to validate correct entry after the *accept* button is checked.
- After all Key components have been entered, click OK. The final KCV will be shown on the Key design dialog box.

3) Encrypted (only for Session Key and Working Keys)

- The Key is entered in its Encrypted Form; the resulting KCV will show the true KCV.
- The Session Key is encrypted under the Master Key; the Working Keys are encrypted under the Session Key.
- The corresponding encrypting key must be the same as when the key was originally encrypted.
- Key Parity can be used to ensure that the encrypted key has been correctly entered and is being decrypted under the proper key. If the Key Parity is bad, it may indicate that the key being used in the Key & FIT Loader Program is not the same as the original encrypting key.

16

KEY CHECK VALUE (KCV)

Since the keys which are stored in the IntelliPIN can never be viewed from outside, a Key Check Value (KCV) is used to determine which key has been defined. The KCV can also be used, especially when entering keys as components, to verify that the key has been entered properly. The KCV is computed by encrypting a string of binary zeros under the selected key. The resulting 4-digit number is known as the KCV.

MASTER KEY

The Master Key is used to encrypt other information that is transmitted to and from the IntelliPIN. The Master Key is required for both the Interactive Mode and the Offline Modes.

When the IntelliPIN is used in the Interactive Mode, the Master Key can be used to encrypt the Session Key. The Master Key can either be a single-length key (64 bits or 8 bytes) or a double-length key (128 bits or 16 bytes). When a double-length Master Key is required, both the Left Half and the Right Half must be entered. A double-length key is sometimes referred to as "triple DES" since there are 3 DES processes involved: 1) encrypt under left half; 2) decrypt result under right half; 3) encrypt result under left half.

Whenever the Master Key is downloaded (injected) into the IntelliPIN, all other keys in the IntelliPIN will be deleted since the Master Key was used to encrypt the other keys.

When used in one of the Offline Modes, the IntelliPIN uses the Master Key to decrypt the information loaded either from Program Cards or from the Key & FIT Loader Program. The data on the Program Cards and the FIT information stored in the Key & FIT Loader database are encrypted under this Master Key. In this case, the Master Key must be the same key as used on the MCAT to generate the Program Cards.

MASTER KEY DESIGN

To design, load, and download the Master keys, perform the following steps:

1.   In the Administrator's Key Design box, click the **Download Master Key As Well** box and the **Download Session Key As Well** box if these keys are to be downloaded to the IntelliPIN.

                                            Note

                *When the Master Key is downloaded, all other keys in the IntelliPIN are
                erased. The Master Key should be downloaded only the first time the
                IntelliPIN is loaded unless a new Master Key is to be used.*

17

2.   Select **Enter**, and when the Master Key dialog box appears, select the mode, **Plain Text Key** or **Key By Components**, as described above.
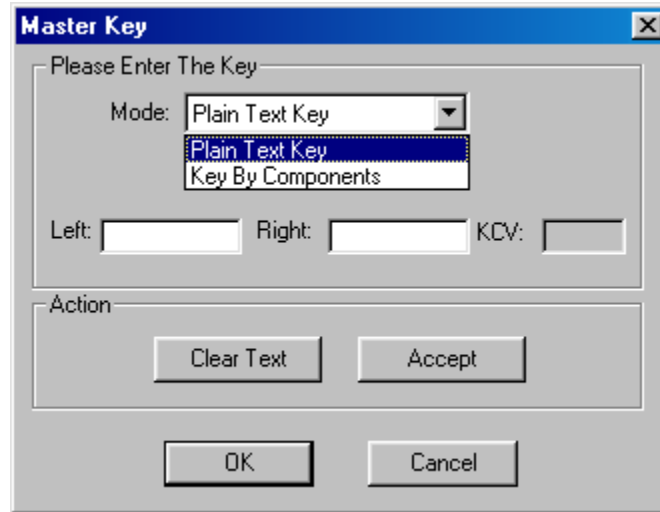
3.   Each of the 8 bytes of a key is entered using two hexadecimal characters. Enter the 16-character key, then click the *Accept* button if only a single-length key will be used.

4.   If a double-length key (described above) is to be entered, press Tab on the keyboard to move to the right key field

5.   Enter the 16-character key, as above, then click **Accept.** Click **OK** if the KCV is correct. The program then returns to the Key Design screen.

6.   If only the Master Key is to be downloaded, click **Download** in the Master Key section. When the bar graph display goes away, the operation is complete.

SESSION KEY

The Session Key can be used to encrypt information that is used on each session or transaction. It is also used to encrypt the Working Keys. It is only used in the Interactive Mode. To design, load, and download the Session Key, perform the following steps:

1. In the Administrator's Key Design box, click the **Download Master Key As Well** box and the **Download Session Key As Well** box if these keys are to be downloaded to the IntelliPIN.

2. Select **Enter** in the Session Key section, and when the Session Key dialog box appears, use the **Mode** pull down arrow, then select **Plain Text Key**, **Key By Components**, or **Encrypted**, as described above.
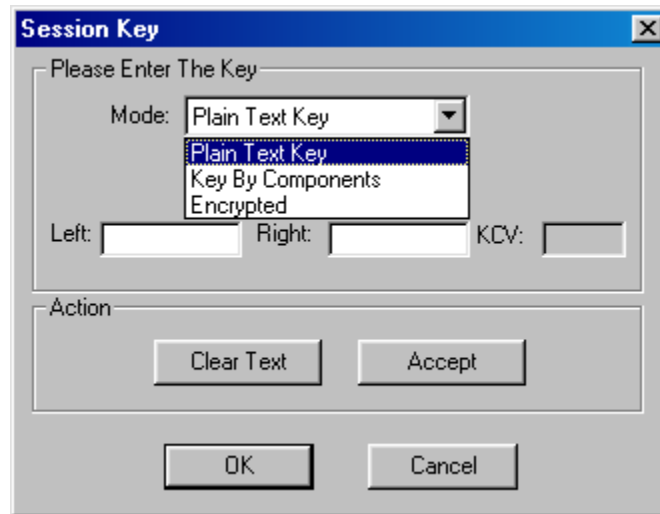
3. Enter the key as described above for the Master Key.

4. If only the Session Key is to be downloaded, ensure the **Download Master Key As Well** is unchecked. Click **Download** in the Session Key section.
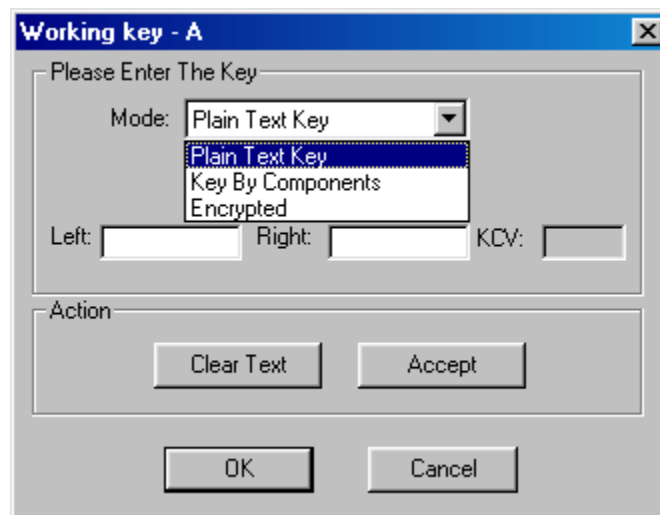
Note

> *Even though the Master Key is not being downloaded, it must still be entered in the Key and FIT Loader database. This is required because the Session Key is encrypted under the Master Key before it is sent to the IntelliPIN.*

WORKING KEYS

The Working Keys are used to encrypt a PIN to ensure a secure transmission to the host security module. They are only used in the Interactive Mode. Any of the 56 working keys can be defined and sent to the IntelliPIN.

To design, load, and download the Working keys, perform the following steps:

1.   In the Administrator's Key Design box, click the **Download Master Key As Well** box and the **Download Session Key As Well** box if these keys are to be downloaded to the IntelliPIN.

2.   In the Working Keys section, select the required Working Key box, then click **Enter**, and when the Working Key dialog box appears, select the **Mode**, **Plain Text Key**, **Key By Components** or **Encrypted**, as described above.

3.   Enter the keys as described above for the Master Key.

4.   Load the other Working Keys, as required, in the same manner. The Program will return to the Key Design dialog box

5.   If only one Working Key is to be downloaded, click the box next to the specified Working Key, then with the red check mark click **Download Key** in the Working Keys section. If all Keys are to be downloaded, click **Download All Keys**.

Note

Even if the Session Key is not being downloaded, it must still be entered in the Key and FIT Loader database. This is required because the Working Keys are encrypted under the Session Key before they are sent to the IntelliPIN.

Export This Key

Working Keys can be exported to individual files. Each key is saved as either 16 or 32 hexadecimal digits with a default file name (WORK followed by four KCV numbers), which can be changed to any valid file name. These exported files can then be used as part of the Load Working Key command (96) that will later be transmitted to the IntelliPIN for PIN block encryption operations. This feature allows the Working Keys to be safely stored for later retrieval by an application program.

Destroy All Keys

This function allows all of the keys in the IntelliPIN to be removed. This operation might be selected when an IntelliPIN is being sent to another location and all keys are to be removed from that IntelliPIN for security purposes.

KEY SERIAL NUMBER

The Key Serial Number is a 16-digit hexadecimal number, which is assigned to an IntelliPIN. It is used as part of the Activation Command (Request 58), which allows the IntelliPIN to perform Offset and PVV calculations for the host. The Key Serial Number must be encrypted under the Master Key and supplied to the IntelliPIN in order to activate the unit. The Administrator generates the Key Serial Number, which gets loaded into the IntelliPIN. The encrypted value of the Key Serial Number allows access to the encryption functions, which include Offset and PVV calculations.

The Activation Command is required at least once after Power up. (For security reasons, Commands 31, 32, 33, 34, 35, 36, and 57 are activated on power up.) The encrypted Key Serial Number is needed to activate the IntelliPIN. This allows the Administrator to provide a user with the encrypted number if necessary; the user does not need access to the Master Key.

An example can be found in the Programming Reference Manual, P/N 99875047.

SUBSTITUTION TABLE

The Substitution Table is used as part of the Offset Generation (Request 31) and PIN Verification (Request 32) commands. The values in the Substitution Table are used either to convert hexadecimal characters into decimal digits or to further scramble the output values. The Substitution Table must be defined if Request 31 or Request 32 is going to be used.

An example can be found in the Programming Reference Manual, P/N 99875047.

DOWNLOAD OPERATIONS

"Download" refers to sending information to the IntelliPIN. All operations performed by a *Download* button will modify the contents of the IntelliPIN.

Key Design

Individual keys can be downloaded or all keys can be sent at one time if the appropriate boxes are checked. Even if the Master Key has already been injected into the IntelliPIN, the Master Key will still have to be entered into the Key & FIT Loader database. This is because the Session Key is encrypted under the Master Key so both the program and the IntelliPIN must contain the same Master Key.

Disk File Operations

After the information has been entered into the Key & FIT Loader database, it can be saved on a floppy disk for later use. This may be necessary for archive purposes or for loading additional IntelliPINs with the same information. Because of the secure nature of the data, it is not permitted to store the data on a hard disk. Furthermore, the data is encrypted before storing it on the floppy disk. After the floppy disk has been created, the floppy disk should be stored in a secure location.

When saving a file, the extension is automatically appended. Just supply the root file name, for example, "BankData" or "Branch17". The extension for the Key Loader is ".key" and for the FIT Loader is ".fit".

When a file has been loaded from the disk, the file name will be shown at the top of the Key Design form. To define information that will be stored in another disk file, select **New** in the Disk File Operations section. When *New* is selected, a prompt will appear to save any existing data to a disk file. After the data has been saved, the form will be empty and new information can be defined. After all of the data has been entered, use **Save As...** to save this data to a new file.

SECTION 5. FIT TABLE LOADING AND MODIFYING

The FIT (Financial Institution Table) is used with the IntelliPIN model. The FIT consists of all of the parameters required to compute an Offset or PVV. The parameters include BIN, Type of encryption scheme, Validation Data, PIN encryption Keys, Decimalization Table, and Offset location.

ADMINISTRATOR FIT TABLE

To open the Administrator's FIT Table, select **Administrator** from the Password dialog box and enter the Administrator's password. Then select the **Table** icon from the Toolbox. Values and selections can be entered into individual fields by selecting a value from the pull-down list or by typing a value. Invalid entries are not allowed and will be replaced by the default.

BIN

A BIN (Bank Identification Number) consists of from 1 to 6 digits. The BIN is used to identify a group of Primary Account Numbers (PAN). When the first digits of a PAN match the digits in a BIN then all of the validation data for that BIN is applied to that account number. The pull-down menu lists all the BINS that are stored in the database. (Active for DES, VISA, Diebold.)

Type

Allows selection of the Type of encryption scheme to use for this BIN. The three options are: DES, VISA and Diebold. The DES requires a DES Key and a Decimalization Table to be entered so an Offset can be generated. The VISA generates a PVV (PIN Verification Value). Two keys and a PVKI (PIN Verification Key Indicator) are required for VISA. No Keys are required for Diebold, but an Algorithm Type must be specified. (Active for DES, VISA, Diebold.)

Offset Reference

The Offset is referenced from either the Field Separator or the End Sentinel. (Active for DES, and Diebold.)

4-digit PIN Length

If **Yes** is selected, the PIN length is limited to 4 digits. If **No** is selected, the PIN length can be from 4 to 12 digits. (Active for DES, VISA, Diebold.)

Key-entered PAN

The PAN (Primary Account Number) may be entered either from the Customer's card or manually (key-entered) from the keys on the PINPad. The PAN includes all the data between the Start Sentinel and the first Field Separator. The PAN length is usually from 13 to 19 digits. If Key-entered PANs are allowed, the MOD-10 check method must be defined. (Active for DES, VISA, Diebold.)

MOD-10

The Selections are: Check MOD-10 (The IntelliPIN will verify that the check digit is correct for the Key-entered PAN); Add MOD-10 (The IntelliPIN will automatically insert a check digit at the end of the PAN); and No MOD-10 (No check digit is required).
(Active for DES, VISA, Diebold.)

Validation Pad

The fill character that is used if the validation length is less than 16. (Active for DES only.)

Algorithm Type

One of the offset generation parameters required for the Diebold BIN Type. Selections are from 0 to 99. (Active for Diebold only.)

Validation Length

The number of digits of the PAN (up to 16) that will be used. The selections are 1 through 16. (Active for DES only.)

Validation Displacement

Validation Displacement: the number of digits on the right end of PAN that will be ignored. The selections are 0 through 15. (Active for DES only.)

Offset Length

The number of digits placed on the card in the Offset field. Selections are 4, 5, or 6. (Active for DES; PVV Length for VISA.)

Offset Displacement

The Offset Displacement is the number of characters from the Offset Reference. The selections are 0 through15. (Active for DES and Diebold.)

PVV Length

The PVV (PIN Verification Value) is stored on a customer card to verify the owner of a card when the PIN has been entered. The PIN length is 4, 5, or 6 digits. PINs can be verified at the ATM network switch or transmitted to the host for verification. The PVKI must also be specified. (Active for VISA only.)

PVKI

The PIN Verification Key Indicator (PVKI) is used to indicate which set of keys is being used for the PVV calculation. Selections are 1 through 6. The PVKI digit precedes the PVV on the customer's card. (Active for VISA only.)

DES Key

A DES key is required for generating an Offset. It requires 16 digits to be entered in the dialog box. (Double-length keys are not supported in the Standalone Mode.) An encrypted key, previously encrypted under the Master Key, may also be entered. For each successive BIN entered, the program will prompt: DES Key same as prior BIN? If the Key for this BIN is the same as the previous BIN, click **Yes**. (Active for DES only.)

Decimalization Table

The Decimalization Table is used to convert the result of an encryption from the hexadecimal values (0-9 and A-F) into decimal digits (0-9). For each successive BIN entered, the program will prompt: Decimalization Table same as prior BIN? If the Decimalization Table is the same as the previous BIN, click **Yes**. The Decimalization Table must be added before the Add button is pressed in FIT Table Operations (the Add button will be in place of the Update button). (Active for DES only.)

VISA Key 1

Two VISA Keys are required for generating a PVV. Requires 16 digits to be entered in the dialog box. For each successive BIN entered, the program will prompt: First Key same as prior BIN? If the Key is the same as the previous BIN, click **Yes**. (Active for VISA only.)

VISA Key 2

The second VISA Key required for generating a PVV. Requires 16 digits to be entered in the dialog box. For each successive BIN entered, the program will prompt: Second Key same as prior BIN? If the Key is the same as the previous BIN, click **Yes**. When complete, click **Add** under FIT Table Operations. (Active for VISA only.)

ADMINISTRATOR FIT OPERATIONS

Download Master Key

The check box, **Download Master Key As Well**, permits the Master Key to be downloaded to the IntelliPIN with the current BIN.   Once the Master Key is downloaded, the **Download Master Key As Well** checkbox is automatically cleared.

Update/Add

Click the **Add** button when a new BIN is added and the FIT Table is completed. If information in a FIT is to be modified, *update* allows modification of an existing FIT. Select the FIT to be changed by using the pull-down arrow next to the BIN field and pointing the desired BIN number. At this point, any of the information for that FIT can be modified. When the changes are complete, click the *Update* button.

Delete

This will remove the selected FIT from the database. When the Save File operation is performed, this FIT will no longer be included. This operation does not remove a FIT from the IntelliPIN.

When Delete is pressed, a prompt will appear: The BIN will be deleted. Are you sure? Refer to Destroy FITs to remove FIT information from the IntelliPIN.

New BIN

After Add or Update is entered, click this button to begin a new BIN.

OPERATOR FIT TABLE

The Operator may load the Disk File, select and download FITs to the IntelliPIN, and delete FITs in the IntelliPIN. The Operator may also download the Master Key.
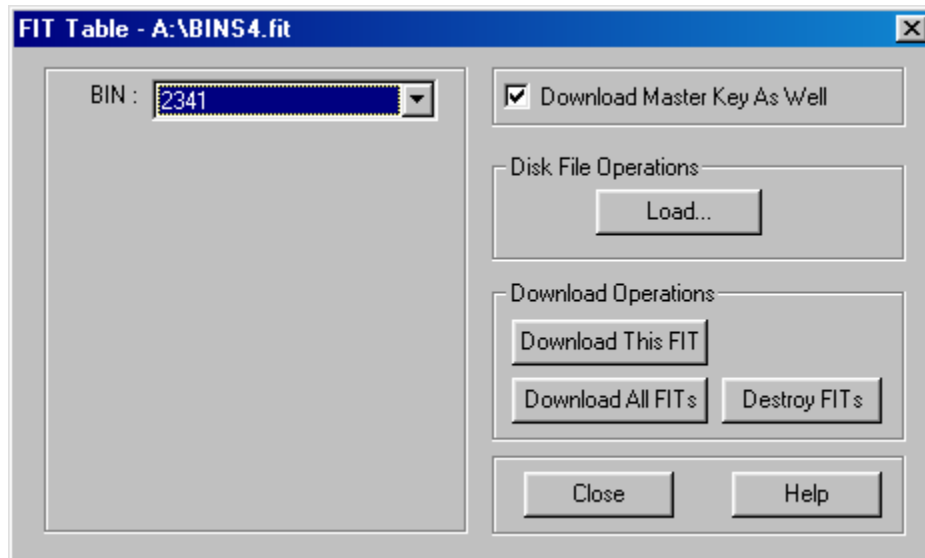
To perform these operations, follow the steps below.

Load Files

To load disks to the program, perform the following steps:

1.   Place the FIT file floppy disk into the PC.

2.   Open the program, and click the "**Table**" Toolbar button on the Main Screen and the FIT Table dialog box appears.

3.   Click **Load**, and the Open dialog box listing the files appears.

4.   Select the file to be loaded, and click **Open**.

27

5.   In the FIT Table dialog box, press the arrow on the BIN pull-down menu to see a list of available BINS.

Download

To download files from the program to the IntelliPIN, perform the following steps:

1.   Determine if the Master Key should be downloaded, and if it should be, ensure the box is checked.

2.   To download only a single FIT, select the FIT from the BIN pull-down menu, and press the **Download This FIT** button. The IntelliPIN display will briefly flash the added FIT, and a bar graph will be shown on the PC until the operation is complete.

3.   To download all FITs, press the **Download All FITs** button. The IntelliPIN display will briefly flash the added FITs, and a bar graph will be shown on the PC until the operation is complete.

Note

> *If a parity error in the key is detected by the IntelliPIN, the error*
> *"Key 1 parity is bad" will be shown. This probably indicates that*
> *the Master Key in the IntelliPIN is not the same as the one in the*
> *Key/FIT Loader program. The **Download Master Key As Well***
> *may have to be checked.*

4.   To remove the FITs from the IntelliPIN, press the **Destroy FITs** button, and a dialog box on the PC will ask for confirmation. When **Yes** is pressed, a bar graph will be shown on the PC until the operation is complete.

The **Done** button exits the FIT Table dialog box. The **Help** button opens the Help file.

DISK FILE OPERATIONS

New

When a file has been loaded from the disk, the file name will be shown at the top the FIT Table dialog box. To define information that will be stored in another disk file, click **New** in the Disk File Operations section. A prompt will then appear to save any existing data into a disk file. After the data has been saved, the dialog box will be empty and new information can be defined. After all of the data has been entered, click **Save As...** to save this data to a new file.

Load

This button will take the user to the list of files on the floppy. From there, the user may select the file to download, modify, or delete by double clicking on the file required. All information from the file will appear in FIT Table dialog box.

Save

This will save the all information in the database to the file name specified at the top of the FIT Table. After modification of information in the dialog box, update the disk file by clicking **Save** in the Disk File Operations section. It is recommended to use **Save** frequently; for example, save the data after each FIT has been completed.

Save As…

When **Save As** is clicked, the program will request a floppy disk if one is not inserted. Name the file, and click **Save**. The extension will be .fit.

CLEAR

Reset To Defaults

This allows clearing the currently displayed FIT information but it does not remove any FITs from the file. To remove the FIT entirely, use **Delete FIT** in the FIT Table Operations.   When the button is clicked, a confirmation dialog box will appear. If the confirmation is Yes, all fields are set to default values. Keys and the decimalization table will be clear. The BIN is not cleared.

Clear All FITs

This operation will remove all of the FITs from the Key & FIT Loader database. This might be useful when creating a different set of FITs for another institution. Be sure to save all existing information to a file before deleting all FITs.

DOWNLOAD OPERATIONS

After the information has been entered into the Key & FIT Loader database, it can be saved on a floppy disk for later use. This may be necessary for archive purposes or for loading additional IntelliPINs with the same information. Because of the secure nature of the data, the program does not permit storing the data on a hard disk. Furthermore, the data is encrypted before storing it on the floppy disk. After the floppy disk has been created, it should be stored in a secure location.

Download This FIT

This will download the current FIT to the IntelliPIN. The Master Key may have to be sent to the IntelliPIN. Until the Master Key has been entered, the Download dialog boxes will be shaded. When the buttons are clear, click to send. The IntelliPIN display will briefly flash the FITs being loaded and then return to the idle prompt.

This might be useful if only a single FIT is being added to the IntelliPIN. In this case, ensure the **Download Master Key As Well** button is not checked. If it is checked, any information already stored in the IntelliPIN will be destroyed and all FITs will have to be downloaded again.

Note

> *If a parity error in the key is detected by the IntelliPIN, the error "Key 1 parity is bad" will be shown. This probably indicates that the Master Key in the IntelliPIN is not the same as the one in the Key/FIT Loader program. The **Download Master Key As Well** may have to be checked.*

Download Master Key…

This allows entry and downloading of the Master Key to the IntelliPIN. When the Master Key is downloaded, all FITs in the IntelliPIN are erased. The Master Key should be downloaded only the first time the IntelliPIN is loaded unless a new Master Key is to be used.

This operation is useful to inject just a Master Key into the IntelliPIN before it is shipped to its final place of use. At that point, the other information such as keys and FITs can be downloaded.

Download All FITs

This operation will append to the IntelliPIN all of the FITs presently loaded into the Key and FIT Loader database. None of the FITs in the IntelliPIN will be removed; however, any FITs with identical BINs will be updated. To remove all of the FITs from the IntelliPIN, use the Destroy FITs selection.

Note

The IntelliPIN can only store up to 12 FITs.

Destroy FITs

Removes all FITs from the IntelliPIN. This is the only mechanism for removing obsolete FITs from the IntelliPIN. To remove a single FIT, it is necessary to remove all of them and Download all FITs again.

DONE

When **Done** is clicked, a dialog box will appear: Would you like to save FITs to a file? If **Yes** is selected, the program prompts for a file name. The program then exits the FIT Table dialog box.

HELP

Opens the Help file.

APPENDIX A. GLOSSARY

Activate Card	An Activate Card can be used to ready the IntelliPIN for daily operation (when the prompt shows Unit is Shut Down). Activate Cards can be ordered from MagTek (P/N 96500059).
Administrator	The person who is able to modify entries in the Key & FIT Loader database. The Administrator Password is used to encrypt data on the disk.
Algorithm	A process used for security reasons to change plain, readable text into unreadable encrypted text.
Algorithm Type	One of the offset generation parameters required for the Diebold BIN type.
Baud Rate	Defines the speed of communication. To communicate with the IntelliPIN, the Key & FIT Loader program must be set up to match the configuration of the IntelliPIN.
BIN	A BIN (Bank Identification Number) consists of from 1 to 6 digits. The BIN is used to identify a group of Primary Account Numbers (PAN). When the first digits of a PAN match the digits in a BIN then all of the validation data for that BIN is applied to that account number.
Clear All FITs	This operation will delete all of the FITs from the Key & FIT Loader database. Use **Destroy FITs** to remove them from the IntelliPIN.
Clear Key	While in the Key Design dialog box, the current entry of the Key can be deleted.
COM	Designates the Communication Port on the PC. Selections include COM1 through COM4. In addition to the serial ports, the Keyboard port can also be selected.
Communication Parity	The Communication Parity specifies what kind of error checking will be used between the PC and the IntelliPIN.

CTS/DSR   These signals can be enabled to modify the Flow Control when using COM1-4 serial connections.

Decimalization Table   The Decimalization Table is used to convert the result of an encryption from the hexadecimal values (0-9 and A-F) into decimal digits (0-9).

Delete FIT   This will remove the selected FIT from the database.

DES   Data Encryption Standard. One of the BIN Types available for generating offset. This Type requires a DES Key and a Decimalization Table to be entered so an Offset can be generated.

Destroy FITs   This operation will remove all FITs from the IntelliPIN and the IntelliPIN will show Ready for program data.

Diebold   One of the BIN Types available for generating offset.

Disk File Operations   Loads previously saved files or saves the current database to a floppy disk. Because of the secure nature of the data, storing the data on a hard disk is not permitted.

Double-length Keys   A Key of 128 bits or 16 bytes. See Left Key and Right Key.

Download All FITs   This operation will append to the IntelliPIN all of the FITs presently loaded into the Key & FIT Loader database. Note: the IntelliPIN can only store up to 12 FITs.

Download Master Key   This operation replaces the existing Master Key and removes all other Key and FIT information from the IntelliPIN.

Download Operations   Download refers to sending information to the IntelliPIN. All operations in this group will modify the contents of the IntelliPIN.

Download This FIT   Only the currently displayed FIT will be sent to the IntelliPIN.

DSR/CTS   These signals can be enabled to modify the Flow Control when using COM1-4 serial connections.

Encrypted Key   A plain text key that has been coded for security.

34

End Sentinel

The last character encoded on the magnetic stripe. It can be used as a reference locator for the Offset.

Field Separator

A character encoded on the magnetic stripe that separates the PAN field, from other fields on the stripe. It can be used as a reference locator for the Offset.

Financial Institution Table

The Financial Institution Table (FIT) consists of all of the parameters required to compute an Offset or PVV. The parameters include BIN, Type, Validation Data, PIN Encryption Keys, Decimalization Table, and Offset location.

KCV

Key Check Value. Since the keys which are stored in the IntelliPIN can never be viewed from outside, a Key Check Value is used to determine which key has been injected.

Key by Components

A complete Key is entered by more than one person, each knowing only a portion (component) of the Key.

Key Check Value

See KCV

Key Design

The dialog box that permits key entry and downloading.

Key Loader

The Key Loader can be used to download the Master Key, Session Key, and Working Keys into the IntelliPIN.

Key Parity

Each byte of the key must contain an odd number of 1's. The Key Parity can be used to ensure that a Key has been correctly entered and, in the case of an encrypted key, that it is being decrypted under the proper key.

Key-entered PAN

Allows a PAN to be entered from the keypad as well as from a Customer's card. If Key-entered PANs are allowed, the MOD-10 method must be defined.

Key, Session

See Session Key.

Key, Working

See Working Keys.

Left Key

When the Master Key a single-length key (64 bits or 8 bytes), only the Left Key is entered.

Load Disk File   See Disk File Operations above.

Login   When the program starts, the Login dialog box requests a Password of up to 8 characters from either the Administrator or the Operator.

Master Key   The Master Key is used in encryption and decryption between the IntelliPIN and the host. Since there is no common key in either the IntelliPIN or the host at startup, the Master Key will be loaded in clear text; this should be done in a secure environment.

MCAT   MagTek Card Activating Terminal. Creates Program Cards used with the IntelliPIN.

MOD-10   If Key-entered PAN has been selected, this option will have to be specified. Modulo-10 is a numerical process that checks the validity of a PAN.

New Disk File   When New is selected, a prompt will appear to save any existing data into a disk file.

Offline Mode   The Offline Mode allows the IntelliPIN to operate without any communication from the PC.

Offset   The Offset is 4 to 6 digits in length and is often stored on the bank card. It is used to validate the owner of the card.

Offset Displacement   The Offset Displacement is the number of characters between the Offset Reference and the Offset.

Offset Length   Number of digits in the Offset. It can be from 4 to 6 digits.

Offset Reference   Referenced to the End Sentinel or Field Separator

Operator   The Operator cannot modify entries in the Key & FIT Loader database. The Operator Password is required to access files on a disk and download the data to the IntelliPIN.

PAN   The PAN or Primary Account Number uniquely identifies a bank card. This is usually a 16-digit number that is encoded on track 2 of the customer's card.

Parity, Communication	Parity is established in Port Setup, under File in the Main Screen. Parity can be Even, Odd, Mark, or None/Space.
Parity, Key	See Key Parity.
Password	When the program starts, the Login dialog box requests a Password of up to 8 characters from either the Administrator or the Operator.
PIN	Personal Identification Number.
Plain Text Key	A Key that is not encrypted. The Key is entered in the clear and therefore should only be done in a secure location.
Port	Designates the Communication Port on the PC. Selections include COM1 through COM4. In addition to the serial ports, the Keyboard port can also be selected.
Port Setup	The Port Setup defines the configuration of the communication to the IntelliPIN.
Program Card	A Program Card is used to load FIT information into the IntelliPIN. Program Cards can only be generated on an MCAT available from MagTek.
PVKI	The PIN Verification Key Indicator (PVKI) is used to indicate which set of keys is being used for the PVV calculation.
PVV	The PVV (PIN Verification Value) is stored on a customer card to verify the owner of a card when the PIN has been entered.
Remove FITs	There are a number of ways FITs can be removed from the program and from the IntelliPIN. Some of the operations simply remove a FIT from the Key & FIT Loader database but have no affect on the information in the IntelliPIN. **Destroy Fits** is the only way to remove FITs from the IntelliPIN.
Right Key	Second half of a double-length Master Key.
Save Disk File	If file has already been retrieved from the disk, its name will be shown on the title line of the form window. After modification of the information in the dialog box, update the disk file by clicking **Save** in the Disk File Operations section.

Session Key   The Session Key can be used to encrypt information that is used on
                            each session or transaction.

Type   Allows selection of Type of encryption scheme to use for the BIN.
                            The three options are: DES, VISA, and Diebold.

Type, Algorithm   One of the offset generation parameters required for the Diebold
                            BIN Type.

Update FIT   This selection allows modification of an existing FIT.

Validation Data   The Validation Data consists of a few parameters that specify what
                            information will be used in the encryption process. The Validation
                            Data includes: Validation Length; Validation Pad; and
                            Validation Displacement.

Validation Displacement   The number of digits on the right end of PAN that will be ignored.

Validation Length   The number of digits of the PAN (up to 16) that will be used.

Validation Pad   The fill character that is used if fewer than 16 PAN digits are
                            specified.

VISA   One of the BIN Types available for generating PVV.

Working Keys   The Working Keys are used to encrypt a PIN to ensure a secure
                            transmission to the host security module.

INDEX