USER MANUAL

SecureKey™ M100/M130
Encrypted Keypad with Optional Encrypted MSR

80120502-001-H
August 8, 2014
<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>First draft release for internal review</td>
<td>03/14/11</td>
</tr>
<tr>
<td>A</td>
<td>Initial Release</td>
<td>05/14/11</td>
</tr>
</tbody>
</table>
| B        | -Modified output format and added example data  
-Added instruction to change the initial key in the demo software  
-Modified commands to change XML output field settings | 06/22/11   |
| C        | -Added #6 configuration for firmware v1.04 and above  
-Added more explanation on the data output format | 12/08/11   |
| D        | -Added Admin menu command  
-Added new manual entry format for firmware v1.14 and above  
-Added Appendix A: Setting Configuration Parameters and Values | 09/19/12   |
| E        | -Added many sections  
-Major update to configuration settings | 11/05/12   |
| F        | Removed some parts related to security level 1 and 2  
Change hash data to 20 bytes for manual entered data  
Many additions, corrections, and deletions to increase accuracy, make more complete, etc. | 3/27/2013  
4/03-12/2013 |
| G        | Add handling shifted ABA track; mod-10 in configuration  
8F add sending serial # in enumeration in AE; add ETrk3=  
Correct the field 9 description in section 9.3  
Remove XML; PIN Pad encryption to PIN Key | 5/15/2013- 
7/31/2013  
9/30/2013 |
| H        | '0' and '1' bit set command; Security Code → Secure Code;  
Add enhanced encryption only for several settings;  
Corrected ADR and ZIP identifier digit pg 28  
Corrected Clear/Mask status definition pg 29  
Correct Appendix A commands for command ID 10, 13, 3E, 84.  
Remove command ID 60  
Corrected 8F setting | 2/7/2014- 
8/6/2014 |
Table of Contents

1.0 Introduction ........................................................................................................................................ 5
2.0 Product Configurations ......................................................................................................................... 5
3.0 Features ................................................................................................................................................... 6
4.0 Terms and Abbreviations ....................................................................................................................... 7
5.0 Applicable Documents ........................................................................................................................... 7
6.0 Function & Operation ............................................................................................................................ 9
   6.1 Function Keys Operation: ..................................................................................................................... 9
   6.2 Admin Menu ...................................................................................................................................... 9
   6.3 Help Mode ....................................................................................................................................... 10
7.0 Configuration ....................................................................................................................................... 11
   7.1 Setup Command Structure ................................................................................................................. 11
   7.2 Communication Timing ....................................................................................................................... 12
   7.3 Default Settings ................................................................................................................................. 12
   7.4 General Selections ............................................................................................................................. 12
       7.4.1 Change to Default Settings ....................................................................................................... 12
       7.4.2 MSR Reading Settings .............................................................................................................. 12
       7.4.3 Decoding Method Settings ....................................................................................................... 13
7.5 Review Settings ..................................................................................................................................... 13
7.6 Review Serial Number .......................................................................................................................... 13
7.7 Controlling Keyed-in Options ............................................................................................................. 13
       7.7.1 Configuration byte 8F controls Keyed in options ................................................................... 13
       7.7.2 Configuration byte 8E Setting Admin Level Options ............................................................... 14
7.8 Message Formatting Selections ............................................................................................................ 14
       7.8.1 Preamble Setting ....................................................................................................................... 14
       7.8.2 Postamble Setting ...................................................................................................................... 14
7.9 Magnetic Track Selections ................................................................................................................... 14
       7.9.1 Track Selection ........................................................................................................................... 14
7.10 Set MSR Data Terminator [53 21] ....................................................................................................... 15
7.11 Security Settings ................................................................................................................................ 15
       7.11.1 Encryption Settings .................................................................................................................. 15
7.12 Review KSN (DUKPT Key management only) ...................................................................................... 15
7.13 Review Security Level ........................................................................................................................ 16
7.14 Control Credit Card Output when Card Swiped Lifted ........................................................................ 16
7.15 Encrypted Output for Decoded Data .................................................................................................... 16
       7.15.1 Encrypt Functions ..................................................................................................................... 16
       7.15.2 Security Related Function ID .................................................................................................. 16
       7.15.3 Security Management .............................................................................................................. 19
       7.15.4 MSR Data Masking .................................................................................................................. 19
1.0 Introduction

ID TECH SecureKey M series is an encrypted numeric keypad with an optional Magnetic Swipe Reader (MSR). The Secure keypad allows the retailers to not only encrypt credit card data at the magnetic reader but it also encrypts a manually entered credit card number. The SecureKey M series has 15 keys (10 Numeric, 5 functional) with a 2x20 backlit LCD.

SecureKey M series keypads encrypt the data using TDES or AES algorithm format with DUKPT key management. For encrypted card reader settings and operations, please refer to 80096504-001 SecureMag User Manual.

SecureKey M series is available in USB-Keyboard and USB-HID interface.

2.0 Product Configurations

SecureKey M series include 2 main models:
- SecureKey M100: Encrypted Keypad
- SecureKey M130: Encrypted Keypad with Magstripe Card Reader

Currently we offer the following configurations:

TDES encryption default
1. IDKE-504800B SecureKey M100 IDT Encryption Format, TDES
2. IDKE-534833B SecureKey M130 IDT Original Encryption Format, TDES
3. IDKE-534833BE SecureKey M130 IDT Enhanced Encryption Format, TDES

AES encryption default
4. IDKE-504800AB SecureKey M100 IDT Encryption Format, AES
5. IDKE-534833AB SecureKey M130 IDT Original Encryption Format, AES
6. IDKE-534833ABE SecureKey M130 IDT Enhanced Encryption Format, AES
3.0 Features

- Encrypted numeric keypad with 2x20 LCD and optional encrypted MSR
- 1,000,000 swipe, industry proven Magnetic Stripe Reader
- 20,000,000 key operations for each key
- Meets FCC Class B & CE regulatory requirements
- Plug-n-Play operation for USB-Keyboard and USB-HID interface
- Keypad is encrypted using DUKPT and TDES/AES encryption.
- Optional encrypted MSR with DUKPT and TDES/AES encryption
- Works with Windows 95/98, WINME 2000, XP, Vista, & Windows 7
4.0 Terms and Abbreviations

AAMVA American Association of Motor Vehicle Administration
ABA American Banking Association
AES Advanced Encryption Standard
ANSI American National Standard Institute
ASIC Application Specific Integrated Circuit
BPI Bits per Inch
CE European Safety and Emission approval authority
DES Data Encryption Standard
DUKPT Derived Unique Key Per Transaction
ESD Electrostatic Discharge
GND Signal Ground
HOST A Personal Computer or Similar Computing Device
HID Human Interface Device
IPS Inches per Second
ISO International Organization for Standardization
JIS Japanese Industrial Standard
KSN Key Serial Number
LRC Longitudinal Redundancy Check Character.
MAC Message Authentication Code
MSR Magnetic Stripe Reader
MTBF Mean Time Between Failures
OTP One Time Programmable
PAN Primary account number
PCI Payment Card Industry
PID USB Product ID
POS Point of Sale
P/N Part Number
RoHS Restrictions of Hazardous Substances
T1,T2,T3 Track 1 data, Track 2 data, Track 3 data
TDES Triple Data Encryption Standard
USB Universal Serial Bus
VID USB Vendor ID

Note: many unusual words used in this document are defined in Appendix A Setting Configuration Parameters and Values table on page 45.

5.0 Applicable Documents

ISO 7810 – 1985 Identification Cards – Physical
ISO 7811 - 1 through 6 Identification Cards - Track 1 through 3
ISO 7812 Identification Cards – Identification for issuers Part 1 & 2
ISO 7813 Identification Cards – Financial Transaction Cards
ISO 4909 Magnetic stripe content for track 3
ANSI X.94 Retail Financial Services Symmetric Key Management
USB ORG USB Specification Rev. 2.0
6.0 Function & Operation

On power-on the device will go into its data capture mode. In data capture mode the device will prompt the user to enter data.

The device will display “Key is not injected!” if the device is not key-injected with encryption enabled after a key is pressed. The evaluation unit is injected with the ID TECH demo key by default and the data can be decrypted using the ID TECH SecureKey demo software.

6.1 Function Keys Operation:

Clear:
- Pressing the “Clear” key allows users to remove all entered data at the current level. The current transaction would not be cancelled.

BS:
- Pressing the “BS” (backspace) key allows users to remove the entered data one character at a time.

#Admin:
- Pressing the “#Admin” key when the screen displays “Swipe or Hand-Key Card Number” or “Enter Card Number then press Enter” allows user to enter the Admin Menu. Pressing the “#Admin” key in other screens puts the device in the Help Mode.

Cancel:
- Pressing the “Cancel” key once allows users to remove all the input in the current as well as the previous level. The device then goes back to the previous prompt of the current transaction. If the “Cancel” key is pressed twice, the current transaction would be cancelled and the device goes back to the initial mode.

6.2 Admin Menu

When the “Admin” key is pressed, the screen will display "Select manual config 1-6" to prompt the user to select one of six manual entry modes.

Manually-Keyed Configuration Options (Firmware Version v1.14 or below)

<table>
<thead>
<tr>
<th>Configuration #1</th>
<th>Configuration #2</th>
<th>Configuration #3</th>
<th>Configuration #4</th>
<th>Configuration #5</th>
<th>Configuration #6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Number, Expiration Date</td>
<td>Card Number, Expiration Date, Zip Code</td>
<td>Card Number, Expiration Date, Street Number of the Address, Zip Code</td>
<td>Card Number, Expiration Date, Zip Code, Secure Code</td>
<td>Card Number, Expiration Date, Address, Zip Code, Secure Code</td>
<td>Card Number, Expiration Date, Address, Secure Code</td>
</tr>
</tbody>
</table>

Manually-Keyed Configuration Options (Firmware Version v1.16 or above)
**Configuration #1**: Card Number, Expiration Date  
**Configuration #2**: Card Number, Expiration Date, Zip Code  
**Configuration #3**: Card Number, Expiration Date, Street Number of the Address, Zip Code  
**Configuration #4**: Card Number, Expiration Date, Secure Code, Zip Code  
**Configuration #5**: Card Number, Expiration Date, Secure Code, Address, Zip Code  
**Configuration #6**: Card Number, Expiration Date, Secure Code

When the user selects the key corresponding to a manual mode, and then selects enter, the mode will be configured and the unit will return to the data capture mode.  
If the user selects more than one key, then the last key selected will be used to select the mode.  
If a invalid key is selected the unit will display "**error**" then "**Select manual config 1-6**"

### 6.3 Help Mode

If the user selects the Admin key while in Admin mode, the unit enters the Help Mode. In the Help Mode, the unit displays short text messages of the various manual entry configurations with a 3 seconds pause between each message. Hitting any key in the Help Mode makes the unit return to the Admin Menu.
7.0 Configuration

The reader must be appropriately configured to your application. Configuration settings enable the reader to work with the host system. Once programmed, these configuration settings are stored in the reader’s non-volatile memory (so they are not affected by the cycling of power).

7.1 Setup Command Structure

Commands sent to keypad/reader

a. Setting Command:
   \(<\text{STX}><\text{S}><\text{FuncID}><\text{Len}><\text{FuncData}>…<\text{ETX}><\text{CheckSum}>\)

b. Read Status Command:
   \(<\text{STX}><\text{R}><\text{FuncID}><\text{ETX}><\text{CheckSum}>\)

c. Function Command:
   \(<\text{STX}><\text{FuncID}><\text{Len}><\text{FuncData}>…<\text{ETX}><\text{CheckSum}>\)

Response from SecureKey

a. Setting Command
   Host
   Setting Command → SecureKey
   \(\leftarrow<\text{ACK}>\) if OK
   or
   \(\leftarrow<\text{NAK}>\) if Error

b. Read Status Command
   Host
   Read Status Command → SecureKey
   \(\leftarrow<\text{ACK}>\) and <Response> if OK
   or
   \(\leftarrow<\text{NAK}>\) if Error

c. Other Commands
   Host
   Other Command → SecureKey
   \(\leftarrow<\text{ACK}>\) and <Response> if OK
   or
   \(\leftarrow<\text{NAK}>\) if Error

Where:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(&lt;\text{STX}&gt;)</td>
<td>02h</td>
</tr>
<tr>
<td>(&lt;\text{S}&gt;)</td>
<td>Indicates setting commands. 53h</td>
</tr>
<tr>
<td>&lt;R&gt;</td>
<td>Indicates read setting commands. 52h</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>&lt;FuncID&gt;</td>
<td>One byte Function ID identifies the particular function or settings affected.</td>
</tr>
<tr>
<td>&lt;Len&gt;</td>
<td>One byte length count for the following data block &lt;FuncData&gt;</td>
</tr>
<tr>
<td>&lt;FuncData&gt;</td>
<td>data block for the function</td>
</tr>
<tr>
<td>&lt;ETX&gt;</td>
<td>03h</td>
</tr>
<tr>
<td>&lt;CheckSum&gt;</td>
<td>Check Sum: The overall Modulo 2 (Exclusive OR) sum (from &lt;STX&gt; to &lt;CheckSum&gt;) should be zero.</td>
</tr>
<tr>
<td>&lt;ACK&gt;</td>
<td>06h</td>
</tr>
<tr>
<td>&lt;NAK&gt;</td>
<td>FD for USB KB interface 15 for all other interface</td>
</tr>
</tbody>
</table>

7.2 Communication Timing
The SecureKey takes time to process a command. During that processing time, it will not respond to a new command.

The typical delay for the reader to respond to a command is 20ms, the maximum delay for the reader to respond can be as much as 40ms. Caution must therefore be taken to maintain a minimum delay between two commands.

7.3 Default Settings
The SecureKey is shipped from the factory with the default settings already programmed. In the following sections, the default settings are shown in **boldface**.

For a table of default settings, see Appendix A.

7.4 General Selections
This group of configuration settings defines the basic operating parameters of SecureKey.

7.4.1 Change to Default Settings

<STX><S><18h><ETX><CheckSum>

This command does not have any <FuncData>. It returns most settings to their default values.

7.4.2 MSR Reading Settings
Enable or Disable the SecureKey swipe reader. If the swipe reader is disabled, no data will be sent out to the host.

<STX><S><1Ah><01h><MSR Reading Settings><ETX><CheckSum>

MSR Reading Settings:

“0” MSR Reading Disabled
“1” MSR Reading Enabled
7.4.3 Decoding Method Settings

The SecureKey can support four kinds of decoded directions. 

<STX><S><1Dh><01h><Decoding Method Settings><ETX><CheckSum>

Decoding Method Settings:
“0” Raw Data Decoding in Both Directions,
“1” Decoding in Both Directions.
“2” Moving stripe along head in direction of encoding.
“3” Moving stripe along head against direction of encoding.

With the bi-directional method, the user can swipe the card in either direction and still read the data encoded on the magnetic stripe. Otherwise, the card can only be swiped in one specified direction to read the card. Raw Decoding just sends the card’s magnetic data in groups of 4 bits per character. The head reads from the first byte of each track, starting from the most significant bit. The data starts to being collected when the first 1 bit is detected. No checking is done except to verify track has or does not have magnetic data.

7.5 Review Settings

<STX><R><1Fh><ETX><CheckSum>

This command does not have any <FuncData>. It activates the review settings command. SecureKey sends back an <ACK> and <Response>.

<Response> format:
The current setting data block is a collection of many function-setting blocks <FuncSETBLOCK> as follows:

<STX><FuncSETBLOCK1>…<FuncSETBLOCKn><ETX><CheckSum>

Each function-setting block <FuncSETBLOCK> has the following format:

<FuncID><Len><FuncData>

Where:
<FuncID> is one byte identifying the setting(s) for the function.
<Len> is a one byte length count for the following function-setting block <FuncData>
<FuncData> is the current setting for this function. It has the same format as in the sending command for this function.
<FuncSETBLOCK> are in the order of their Function ID<FuncID>

7.6 Review Serial Number

<STX><R><4Eh><ETX><CheckSum>

This command is to get device serial number.

7.7 Controlling Keyed-in Options

7.7.1 Configuration byte 8F controls Keyed in options

bit 0: if 0: output in original keyed output; 1: output in enhanced keyed-in output
bit 1: if 0: allow empty CVV entry; 1: require 3 or more CVV digits
bit 2: if 0: allow empty ZIP entry; 1: require 5 or more ZIP digits
bit 3: if 0: allow empty ADR entry; 1: require 1 or more ADR digits
bit 4: if 0: do mod-10 check on keyed-in PAN; 1: don’t check PAN mod-10
bits 5-7: reserved all zero
Note: bits 1 through 3 are only applicable if the reader is configured for Manually-Keyed Configuration Options greater than 1 and only apply to firmware version 1.16 and above.

7.7.2 Configuration byte 8E Setting Admin Level Options
The reader can be configured to set the manually Keyed-in Configuration option in two ways first selecting the Admin key then a number from 1 to 6. For the meaning of these numbers see section 6.2 admin menu.

7.8 Message Formatting Selections

7.8.1 Preamble Setting
Characters can be added to the beginning of a string of data. These can be special characters for identifying a specific reading station, to format a message header expected by the receiving host, or any other character string. Up to fifteen ASCII characters can be defined.

<STX><S><D2h><Len><Preamble><ETX><CheckSum>

Where:
<Len>= the number of bytes of preamble string
<Preamble> = {string length}{string}
NOTE: String length is one byte, maximum fifteen <0Fh>.

7.8.2 Postamble Setting
The postamble serves the same purpose as the preamble, except it is added to the end of the data string, after any terminator characters.

<STX><S><D3h><Len><Postamble><ETX><CheckSum>

Where:
<Len> = the number of bytes of postamble string
<Postamble> = {string length}{string}
NOTE: String length is one byte, maximum fifteen <0Fh>.

7.9 Magnetic Track Selections

7.9.1 Track Selection
There are up to three tracks of encoded data on a magnetic stripe.
This option selects the tracks that will be read and decoded.
Track_Selection Settings:

“0” Any Track this is the only setting supported

Note: If any of the required multiple tracks fail to read for any reason, no data for any track will be sent.

7.10 Set MSR Data Terminator [53 21]

The <Terminator Setting> byte is any one byte except 0x00:

The default is 0x0D, which is Carriage Return (CR). If 0x00 is set the reader will send no terminator.

Example to set to send Line Feed (LF=0x0A) after the last MSR data

The terminator value 30 is special it will send out two characters CRLF or OD and OA

A Value of 0x00 means do not send any MSR data terminator.

7.11 Security Settings

7.11.1 Encryption Settings

Encryption type output.

Encryption Settings:

“1” Enable TDES Encryption

“2” Enable AES Encryption

7.12 Review KSN (DUKPT Key management only)

This command is to get DUKPT key serial number and counter.

Response:

Example:

06 02 51 0A 62 99 49 01 45 00 00 00 18 03 B7

Note: the response was somewhat different before V1.25
7.13 **Review Security Level**

<STX><R><7Eh><ETX><CheckSum>

This command is to get the current security level.

Response:
<STX><7E><01><33h><ETX><CheckSum>

7.14 **Control Credit Card Output when Card Swiped Lifted**

<STX><S><AFh><01h><Control Settings><ETX><CheckSum>

Control Settings:

- 01h Disallow Credit Card swiped while lifted
- 00h Allow to send credit card data unencrypted when on shifted track

If a credit card is swiped, while the card is lifted, it is possible to get a good card read, where track 1 data is shifted into track 2 or track 3 and/or where track 2 data is shifted into track 3. Since the credit card data is always normally encrypted, this potentially allows the credit card data to be sent without encryption exposing the card contents. By default this is allowed. This feature was added in V1.23.

7.15 **Encrypted Output for Decoded Data**

7.15.1 Encrypt Functions

When a card is swiped through the Reader, the track data will be TDEA (Triple Data Encryption Algorithm, aka, Triple DES) or AES (Advanced Encryption Standard) encrypted using DUKPT (Derived Unique Key Per Transaction) key management. DUKPT key management uses a base derivation key to encrypt a key serial number that produces an initial encryption key which is injected into the Reader prior to deployment. After each transaction, the encryption key is modified per the DUKPT algorithm so that each transaction uses a unique key. Thus, the data will be encrypted with a different encryption key for each transaction.

7.15.2 Security Related Function ID

Security Related Function IDs are listed below. Their functions are described in other sections.

<table>
<thead>
<tr>
<th>Characters</th>
<th>Hex Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PrePANID</td>
<td>49</td>
<td>First N Digits in PAN which can be clear data</td>
</tr>
<tr>
<td>PostPANID</td>
<td>4A</td>
<td>Last M Digits in PAN which can be clear data</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>MaskCharID</td>
<td>4B</td>
<td>Character used to mask PAN</td>
</tr>
<tr>
<td>EncryptionID</td>
<td>4C</td>
<td>Security Algorithm</td>
</tr>
<tr>
<td>Device Serial Number ID</td>
<td>4E</td>
<td>Device Serial Number (Can be write once. After that, can only be read)</td>
</tr>
<tr>
<td>DisplayExpirationDateID</td>
<td>50</td>
<td>Display expiration data as mask data or clear data</td>
</tr>
<tr>
<td>KSN and Counter ID</td>
<td>51</td>
<td>Review the Key Serial Number and Encryption Counter format v1.22) 51 0A KSN</td>
</tr>
<tr>
<td>Session ID</td>
<td>54</td>
<td>Set current Session ID</td>
</tr>
<tr>
<td>Key Management Type ID</td>
<td>58</td>
<td>Select Key Management Type</td>
</tr>
<tr>
<td>HashOptID</td>
<td>5C</td>
<td>to include or not hash data</td>
</tr>
<tr>
<td>SecurityLevelID</td>
<td>7E</td>
<td>Security Level (Read Only)</td>
</tr>
<tr>
<td>EncryptOptID</td>
<td>84</td>
<td>which tracks to encrypt: note force</td>
</tr>
<tr>
<td>EncryptStrID</td>
<td>85</td>
<td>original or enhanced swipe encrypt structure</td>
</tr>
<tr>
<td>MaskOptID</td>
<td>86</td>
<td>which tracks to mask</td>
</tr>
<tr>
<td>EnFmtID</td>
<td>88</td>
<td>for XML</td>
</tr>
<tr>
<td>T3ExpDatePosID</td>
<td>89</td>
<td>offset to date on ISO4049 track 3</td>
</tr>
<tr>
<td>KeyedOptID</td>
<td>8F</td>
<td>original or enhanced keyed-in encrypt structure</td>
</tr>
<tr>
<td>Equip2ID</td>
<td>AE</td>
<td>unusual special settings control</td>
</tr>
<tr>
<td>CustSet2ID</td>
<td>AF</td>
<td>check for cc tracks shifted due to swipe while card lifted</td>
</tr>
</tbody>
</table>

Feasible settings of these new functions are listed below.

<table>
<thead>
<tr>
<th>Characters</th>
<th>Default Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PrePANID</td>
<td>04h</td>
<td>00h ~ 06h Allowed clear text from start of PAN Command format: 02 53 49 01 04 03 LRC</td>
</tr>
<tr>
<td>PostPANID</td>
<td>04h</td>
<td>00h ~ 04h Allowed clear text from end of PAN Command format: 02 53 4A 01 04 03 LRC</td>
</tr>
<tr>
<td>MaskCharID</td>
<td>‘*’</td>
<td>20h ~ 7Eh Command format: 02 53 4B 01 3A 03 LRC</td>
</tr>
<tr>
<td>DisplayExpirationDataID</td>
<td>‘0’</td>
<td>‘0’ Display expiration data as mask data ‘1’ Display expiration data as clear</td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| EncryptionID                      | ‘0’   | ‘0’ Clear Text  
‘1’ Triple DES  
‘2’ AES  
Command format:  
02 53 4C 01 31 03 LRC          |
| SecurityLevelID                   | ‘1’   | ‘0’ ~ ‘3’  
Command format:  
02 52 7E 03 LRC          |
| Device Serial Number ID           | 00, 00, 00, 00, 00, 00, 00, 00, 00, 00 | 10 bytes number:  
Set Serial Number:  
02 53 01 4E 09 08 37 36 35 34 33 32 31 30 03 LRC  
Get Serial Number:  
02 52 4E 03 LRC          |
| KSN and Counter ID                | 00, 00, 00, 00, 00, 00, 00, 00, 00, 00 | This field includes the Initial Key  
Serial Number in the leftmost 59  
bits and a value for the Encryption  
Counter in the right most 21 bits.  
Get DUKPT KSN and Counter:  
02 52 51 03 LRC          |
| Session ID                        | 00, 00, 00, 00, 00, 00, 00, 00, 00, 00 | This Session ID is an eight bytes  
string which contains any hex data.  
This filed is used by the host to  
uniquely identify the present  
transaction. Its primary purpose is to  
prevent replays. It is only be used at  
Security Level 4. After a card is read,  
the Session ID will be encrypted,  
along with the card data, a supplied as  
part of the transaction message. The  
clear text version of this will never be  
transmitted.  
New Session ID stays in effect until  
one of the following occurs:  
1. Another Set Session ID command  
is received.  
2. The reader is powered down.  
3. The reader is put into Suspend  
mode.          |
| Key Management Type ID            | ‘1’   | Fixed key management by default.  
‘1’: DUKPT Key          |
| HashOptID                         | ‘7’   | hash all encrypted tracks          |
| SecurityLevelID                   | ‘3’   | Security Level (Read Only)          |
| EncryptOptID                      | 0     | which tracks to encrypt          |
EncryptStrID | ‘1’ | to use original or enhanced swipe encryption format
---|---|---
MaskOptID | 7 | which tracks may be sent masked
EnFmtID | 023034 |
T3ExpDatePosID | 34 | offset to track 3 expire date position
KeyedOptID | 0 or 1 | to use original or enhanced keyed in encryption format.
Equip2ID | 00 (any) | if bit 4 is set high, the USB enumeration will include the reader’s serial number.
CustSet2ID | 00H (or 01H) | bit0=0 send unencrypted as other type card; bit0=1 disallow a credit card shifted 1 or 2 tracks

### 7.15.3 Security Management

This reader is intended to be a secure reader. Security features include:

- Can include Device Serial Number
- Can encrypt track 1, track 2, and track 3 data for bank cards and other cards
- Provides clear text confirmation data including card holder’s name and a portion of the PAN as part of the Masked Track Data for bank cards
- Optional display expiration date
- Security Level is settable

The reader features configurable security settings. Before encryption can be enabled, Key Serial Number (KSN) and Base Derivation Key (BDK) must be loaded before encrypted transactions can take place. The keys are to be injected by certified key injection facility.

### 7.15.4 MSR Data Masking

For ABA cards needing to be encrypted, encrypted data, hash data and clear text data maybe sent.

**Masked Area**

The data format of each masked track is ASCII.

- The clear data includes start and end sentinels, separators, first N, last M digits of the PAN, card holder name (for Track1).
- The rest of the characters should be masked using mask character.

Set PrePANClrData (N), PostPANClrData (M), MaskChar (Mask Character)

N and M are configurable and default to 4 first and 4 last digits. They follow the current PCI constraints requirements (N ≤ 6, M ≤ 4 maximum).

Mask character default value is ‘*’.

- Set PrePANClrDataID (N), parameter range 00h ~ 06h, default value 04h
- Set PostPANClrDataID (M), parameter range 00h ~ 04h, default value 04h
- MaskCharID (Mask Character), parameter range 20h ~ 7Eh, default value 2Ah
- DisplayExpirationDateID, parameter range ‘0’~’1’, default value ‘0’

8.0 Descriptor
The USB version of the reader can be operated in two different modes:
- HID ID TECH mode (herein referred to as “HID mode”)
- HID with Keyboard Emulation (herein referred to as “KB mode”).

When the reader is operated in the HID mode, it behaves like a vendor defined HID device. A direct communication path can be established between the host application and the reader without interference from other HID devices.
8.1 Descriptor Tables

Device Descriptor:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Des type</td>
<td>01</td>
<td></td>
</tr>
<tr>
<td>bcd USB</td>
<td>00 02</td>
<td>USB 2.0</td>
</tr>
<tr>
<td>Device Class</td>
<td>00</td>
<td>Unused</td>
</tr>
<tr>
<td>Sub Class</td>
<td>00</td>
<td>Unused</td>
</tr>
<tr>
<td>Device Protocol</td>
<td>00</td>
<td>Unused</td>
</tr>
<tr>
<td>Max Packet Size</td>
<td>08</td>
<td></td>
</tr>
<tr>
<td>VID</td>
<td>0A CD</td>
<td></td>
</tr>
<tr>
<td>PID</td>
<td>26 10 26 20</td>
<td>HID ID TECH StructureHID Keyboard</td>
</tr>
<tr>
<td>BCD Device Release</td>
<td>00 01</td>
<td></td>
</tr>
<tr>
<td>i-Manufacture</td>
<td>01</td>
<td></td>
</tr>
<tr>
<td>i-Product</td>
<td>02</td>
<td></td>
</tr>
<tr>
<td>i-Serial-Number</td>
<td>00</td>
<td>Changes to 3 if USB serial number enabled</td>
</tr>
<tr>
<td># Configuration</td>
<td>01</td>
<td></td>
</tr>
</tbody>
</table>

Configuration Descriptor:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>09</td>
<td></td>
</tr>
<tr>
<td>Des type</td>
<td>02</td>
<td></td>
</tr>
<tr>
<td>Total Length</td>
<td>22 00</td>
<td></td>
</tr>
<tr>
<td>No. Interface</td>
<td>01</td>
<td></td>
</tr>
<tr>
<td>Configuration Value</td>
<td>01</td>
<td></td>
</tr>
<tr>
<td>iConfiguration</td>
<td>00</td>
<td></td>
</tr>
<tr>
<td>Attributes</td>
<td>80</td>
<td>Bus power, no remove wakeup</td>
</tr>
<tr>
<td>Power</td>
<td>32</td>
<td>100 mA</td>
</tr>
</tbody>
</table>

Interface Descriptor:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>09</td>
<td></td>
</tr>
<tr>
<td>Des type</td>
<td>04</td>
<td></td>
</tr>
<tr>
<td>Interface No.</td>
<td>00</td>
<td></td>
</tr>
<tr>
<td>Alternator Setting</td>
<td>00</td>
<td></td>
</tr>
<tr>
<td># EP</td>
<td>01</td>
<td></td>
</tr>
<tr>
<td>Interface Class</td>
<td>03</td>
<td>HID</td>
</tr>
<tr>
<td>Sub Class</td>
<td>01</td>
<td></td>
</tr>
<tr>
<td>Interface Protocol</td>
<td>01</td>
<td></td>
</tr>
<tr>
<td>iInterface</td>
<td>00</td>
<td></td>
</tr>
</tbody>
</table>
**HID Descriptor:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>09</td>
<td></td>
</tr>
<tr>
<td>Des type</td>
<td>21</td>
<td>HID</td>
</tr>
<tr>
<td>bcdHID</td>
<td>11 01</td>
<td></td>
</tr>
<tr>
<td>Control Code</td>
<td>00</td>
<td></td>
</tr>
<tr>
<td>numDescriptors</td>
<td>01</td>
<td>Number of Class Descriptors to follow</td>
</tr>
<tr>
<td>DescriptorType</td>
<td>22</td>
<td>Report Descriptor</td>
</tr>
<tr>
<td>Descriptor Length</td>
<td>37 00</td>
<td>HID ID TECH format</td>
</tr>
<tr>
<td></td>
<td>3D 00</td>
<td>HID Other format</td>
</tr>
<tr>
<td></td>
<td>52 00</td>
<td>HID Keyboard format</td>
</tr>
</tbody>
</table>

**End Pointer Descriptor:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>07</td>
<td></td>
</tr>
<tr>
<td>Des Type</td>
<td>05</td>
<td>End Point</td>
</tr>
<tr>
<td>EP Addr</td>
<td>83</td>
<td>EP3 – In</td>
</tr>
<tr>
<td>Attributes</td>
<td>03</td>
<td>Interrupt</td>
</tr>
<tr>
<td>MaxPacketSize</td>
<td>40 00</td>
<td></td>
</tr>
<tr>
<td>bInterval</td>
<td>01</td>
<td></td>
</tr>
</tbody>
</table>

**Report Descriptor: (USB-HID Setting)**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>06 00</td>
<td>Usage Page (MSR)</td>
</tr>
<tr>
<td>FF</td>
<td></td>
</tr>
<tr>
<td>09 01</td>
<td>Usage (Decoding Reader Device)</td>
</tr>
<tr>
<td>A1 01</td>
<td>Collection (Application)</td>
</tr>
<tr>
<td>15 00</td>
<td>Logical Minimum</td>
</tr>
<tr>
<td>26 FF</td>
<td>Logical Maximum</td>
</tr>
<tr>
<td>00</td>
<td></td>
</tr>
<tr>
<td>75 08</td>
<td>Report Size</td>
</tr>
<tr>
<td>09 20</td>
<td>Usage (Tk1 Decode Status)</td>
</tr>
<tr>
<td>09 21</td>
<td>Usage (Tk2 Decode Status)</td>
</tr>
<tr>
<td>09 22</td>
<td>Usage (Tk3 Decode Status)</td>
</tr>
<tr>
<td>09 28</td>
<td>Usage (Tk1 Data Length)</td>
</tr>
<tr>
<td>09 29</td>
<td>Usage (Tk2 Data Length)</td>
</tr>
<tr>
<td>09 2A</td>
<td>Usage (Tk3 Data Length)</td>
</tr>
<tr>
<td>09 38</td>
<td>Usage (Card Encode Type)</td>
</tr>
<tr>
<td>95 07</td>
<td>Report Count</td>
</tr>
<tr>
<td>81 02</td>
<td>Input (Data, Var, Abs, Bit Field)</td>
</tr>
<tr>
<td>09 30</td>
<td>Usage (Total Sending Length)</td>
</tr>
<tr>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>05 01</td>
<td>Usage Page (Generic Desktop)</td>
</tr>
<tr>
<td>09 06</td>
<td>Usage (Keyboard)</td>
</tr>
<tr>
<td>A1 01</td>
<td>Collection (Application)</td>
</tr>
<tr>
<td>05 07</td>
<td>Usage Page (Key Codes)</td>
</tr>
<tr>
<td>19 E0</td>
<td>Usage Minimum</td>
</tr>
<tr>
<td>29 E7</td>
<td>Usage Maximum</td>
</tr>
<tr>
<td>15 00</td>
<td>Logical Minimum</td>
</tr>
<tr>
<td>25 01</td>
<td>Logical Maximum</td>
</tr>
<tr>
<td>75 01</td>
<td>Report Size</td>
</tr>
<tr>
<td>95 08</td>
<td>Report Count</td>
</tr>
<tr>
<td>81 02</td>
<td>Input (Data, Variable, Absolute)</td>
</tr>
<tr>
<td>95 01</td>
<td>Report Count (1)</td>
</tr>
<tr>
<td>75 08</td>
<td>Report Size</td>
</tr>
<tr>
<td>81 01</td>
<td>Input Constant</td>
</tr>
<tr>
<td>95 05</td>
<td>Report Count</td>
</tr>
<tr>
<td>75 01</td>
<td>Report Size</td>
</tr>
<tr>
<td>05 08</td>
<td>Usage Page (LED)</td>
</tr>
<tr>
<td>19 01</td>
<td>Usage Minimum</td>
</tr>
<tr>
<td>29 05</td>
<td>Usage maximum</td>
</tr>
<tr>
<td>91 02</td>
<td>Output (Data Variable Absolute)</td>
</tr>
<tr>
<td>95 01</td>
<td>Report Count</td>
</tr>
<tr>
<td>75 03</td>
<td>Report Size</td>
</tr>
<tr>
<td>91 01</td>
<td>Output (Constant)</td>
</tr>
<tr>
<td>95 06</td>
<td>Report Count</td>
</tr>
<tr>
<td>75 08</td>
<td>Report Size</td>
</tr>
<tr>
<td>15 00</td>
<td>Logical Minimum</td>
</tr>
<tr>
<td>25 66</td>
<td>Logical Maximum (102)</td>
</tr>
<tr>
<td>05 07</td>
<td>Usage Page (key Code)</td>
</tr>
<tr>
<td>19 00</td>
<td>Usage Minimum</td>
</tr>
</tbody>
</table>

**Report Descriptor: (USB KB Interface)**
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29 66</td>
<td>Usage Maximum (102)</td>
</tr>
<tr>
<td>81 00</td>
<td>Input(Data, Array)</td>
</tr>
<tr>
<td>06 2D</td>
<td>Usage Page (ID TECH)</td>
</tr>
<tr>
<td>FF</td>
<td></td>
</tr>
<tr>
<td>95 01</td>
<td>Report Count</td>
</tr>
<tr>
<td>26 FF</td>
<td>Logical maximum (255)</td>
</tr>
<tr>
<td>00</td>
<td></td>
</tr>
<tr>
<td>15 01</td>
<td>Logical Minimum</td>
</tr>
<tr>
<td>75 08</td>
<td>Report Size (8)</td>
</tr>
<tr>
<td>09 20</td>
<td>Usage (Setup data byte)</td>
</tr>
<tr>
<td>95 08</td>
<td>Report Count (8)</td>
</tr>
<tr>
<td>B2 02</td>
<td>Feature (Data Var, Abs)</td>
</tr>
<tr>
<td>01</td>
<td></td>
</tr>
<tr>
<td>C0</td>
<td>End Collection</td>
</tr>
</tbody>
</table>
9.0 Data Output Format
For ID TECH standard data format, there are two different structures, the original and the enhanced output format. The default is the enhanced encryption output format.

<STX><DataLenL><DataLenH><Card Data><CheckLRC><CheckSum><ETX>

<STX> = 02h, <ETX> = 03h
<DataLenL><DataLenH> is a two byte length of <Card Data>.
<CheckLRC> is a one byte Exclusive-OR sum calculated for all <Card Data>.
<CheckSum> is a one byte Sum value calculated for all <Card Data>.

9.1 ID TECH Swipe Data Original Encryption Output Format

<table>
<thead>
<tr>
<th>Field</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>STX (02)</td>
</tr>
<tr>
<td>1</td>
<td>Data Length low byte</td>
</tr>
<tr>
<td>2</td>
<td>Data Length high byte</td>
</tr>
<tr>
<td>3</td>
<td>Card Encode Type (note 1 page 29 paragraph 9.4.1)</td>
</tr>
<tr>
<td>4</td>
<td>Track 1-3 Status (note 2 page 29 paragraph 9.4.2)</td>
</tr>
<tr>
<td>5</td>
<td>T1 data length</td>
</tr>
<tr>
<td>6</td>
<td>T2 data length</td>
</tr>
<tr>
<td>7</td>
<td>T3 data length</td>
</tr>
<tr>
<td>8</td>
<td>T1 clear/mask data - (Track 1 data)</td>
</tr>
<tr>
<td>9</td>
<td>T2 clear/mask data - (Track 2 data)</td>
</tr>
<tr>
<td>10</td>
<td>T3 clear data - (Track 3 data)</td>
</tr>
<tr>
<td>11</td>
<td>T1 and T2 encrypted data</td>
</tr>
<tr>
<td>12</td>
<td>T1 hashed (20 bytes each) (if encrypted and hash tk1 allowed)</td>
</tr>
<tr>
<td>13</td>
<td>T2 hashed (20 bytes each) (if encrypted and hash tk2 allowed)</td>
</tr>
<tr>
<td>14</td>
<td>KSN (10 bytes)</td>
</tr>
<tr>
<td>15</td>
<td>CheckLRC</td>
</tr>
<tr>
<td>16</td>
<td>CheckSum</td>
</tr>
<tr>
<td>17</td>
<td>ETX (03)</td>
</tr>
</tbody>
</table>
### 9.2 ID TECH Swipe Data Enhanced Encryption Output Format

<table>
<thead>
<tr>
<th>Field</th>
<th>Field Decryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>STX (02)</td>
</tr>
<tr>
<td>1</td>
<td>Data Length low byte</td>
</tr>
<tr>
<td>2</td>
<td>Data Length high byte</td>
</tr>
<tr>
<td>3</td>
<td>Card Encode Type (note 1 page 29 paragraph 9.4.1)</td>
</tr>
<tr>
<td>4</td>
<td>Track 1-3 Status (note 2 page 29 paragraph 9.4.2)</td>
</tr>
<tr>
<td>5</td>
<td>T1 data length</td>
</tr>
<tr>
<td>6</td>
<td>T2 data length</td>
</tr>
<tr>
<td>7</td>
<td>T3 data length</td>
</tr>
<tr>
<td>8</td>
<td>Clear/mask data sent status (note 3 page 29 paragraph 9.4.3)</td>
</tr>
<tr>
<td>9</td>
<td>Encrypted/Hash data sent status (note 4 page 29 paragraph 9.4.4)</td>
</tr>
<tr>
<td>10</td>
<td>T1 clear/mask data - (Track 1 data)</td>
</tr>
<tr>
<td>11</td>
<td>T2 clear/mask data - (Track 2 data)</td>
</tr>
<tr>
<td>12</td>
<td>T3 clear/mask data - (Track 3 data)</td>
</tr>
<tr>
<td>13</td>
<td>T1 encrypted data - (Track 1 encrypted data)</td>
</tr>
<tr>
<td>14</td>
<td>T2 encrypted data - (Track 2 encrypted data)</td>
</tr>
<tr>
<td>15</td>
<td>T3 encrypted data - (Track 3 encrypted data)</td>
</tr>
<tr>
<td>16</td>
<td>T1 hashed (20 bytes each) (if encrypted and hash tk1 allowed)</td>
</tr>
<tr>
<td>17</td>
<td>T2 hashed (20 bytes each) (if encrypted and hash tk2 allowed)</td>
</tr>
<tr>
<td>18</td>
<td>T3 hashed (20 bytes each) (if encrypted and hash tk3 allowed)</td>
</tr>
<tr>
<td>19</td>
<td>Reader Serial Number (10 bytes) (optional)</td>
</tr>
<tr>
<td>20</td>
<td>KSN (10 bytes)</td>
</tr>
<tr>
<td>21</td>
<td>CheckLRC</td>
</tr>
<tr>
<td>22</td>
<td>CheckSum</td>
</tr>
<tr>
<td>23</td>
<td>ETX (03)</td>
</tr>
</tbody>
</table>
9.3 ID TECH Manual Entry Original Data Output Format (Default)

Note: This is the default for historical reasons, for new development, the enhanced data output format should normally be used see page 28 Section 9.4 ID TECH Manual Entry Enhanced Data Output Format (New)

The default manual entry data output format does not include clear/masked data in the manual entry output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Field Decryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>STX (0x02)</td>
</tr>
<tr>
<td>1</td>
<td>Data Length low byte</td>
</tr>
<tr>
<td>2</td>
<td>Data Length high byte</td>
</tr>
<tr>
<td>3</td>
<td>card type always 85—keyed in (note 1 page 29 paragraph 9.4.1)</td>
</tr>
<tr>
<td>4</td>
<td>always 0</td>
</tr>
<tr>
<td>5</td>
<td>always 0</td>
</tr>
<tr>
<td>6</td>
<td>always 0</td>
</tr>
<tr>
<td>7</td>
<td>always 0</td>
</tr>
<tr>
<td>8</td>
<td>Status (1 byte) bit set if field is present in output (range 0-7)</td>
</tr>
<tr>
<td></td>
<td>bit 7 bit 6 bit 5 bit 4 bit 3 bit 2 bit 1 bit 0</td>
</tr>
<tr>
<td></td>
<td>0 0 0 0 0 SessionID EXP ADR ZIP</td>
</tr>
<tr>
<td>9</td>
<td>Length of unencrypted key-in data</td>
</tr>
<tr>
<td>10</td>
<td>Encrypted card data (max: 180 bytes) PAN=EXP=CVV</td>
</tr>
<tr>
<td>11</td>
<td>Hash data (20bytes)</td>
</tr>
<tr>
<td>12</td>
<td>EXP one byte length+ASCII Expiration date (len: 1+4 bytes)</td>
</tr>
<tr>
<td>13</td>
<td>ADR one byte length+ASCII Street number (max: 1+20 bytes)</td>
</tr>
<tr>
<td>14</td>
<td>ZIP one byte length+ASCII Zip code (max: 1+10 bytes)</td>
</tr>
<tr>
<td>15</td>
<td>Reader Serial Number (10 bytes) (optional)</td>
</tr>
<tr>
<td>16</td>
<td>KSN (10 bytes)</td>
</tr>
<tr>
<td>17</td>
<td>CheckLrc</td>
</tr>
<tr>
<td>18</td>
<td>CheckSum</td>
</tr>
<tr>
<td>19</td>
<td>ETX (0x03)</td>
</tr>
</tbody>
</table>

Encrypted data sent status:
- Data Length low byte/high byte should be in length of characters.
- Data include encrypted card key-in PAN=EXP (YYMM) and 3-4 digit security code (CVV). The format should be:
  (Security level 3) PAN=YYMM=[CVV]

Each field is separated by delimiter ‘=’, this should always present even CVV is not keyed-in.
- Format of the fields: EXP, ADR and ZIP is:

<table>
<thead>
<tr>
<th>1 byte field length in hex</th>
<th>Data</th>
</tr>
</thead>
</table>

The length byte ASCII not including length
9.4 ID TECH Manual Entry Enhanced Data Output Format (New)

The new manual entry output format is supported in firmware v1.14 and above. Command to enable the new manual entry format is 53 8F 01 01

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>STX (0x02)</td>
</tr>
<tr>
<td>1</td>
<td>Data Length low byte</td>
</tr>
<tr>
<td>2</td>
<td>Data Length high byte</td>
</tr>
<tr>
<td>3</td>
<td>Card Encode Type always C0 ABA format (note 1 page 29 paragraph 9.4.1)</td>
</tr>
<tr>
<td>4</td>
<td>Field 4 see description (0x17 track2 only) or 37 track 2 and track 3 (page 29 paragraph 9.4.2)</td>
</tr>
<tr>
<td>5</td>
<td>T1 data length always 0</td>
</tr>
<tr>
<td>6</td>
<td>Length of unencrypted manual input data PAN; EXP [and CVV]</td>
</tr>
<tr>
<td>7</td>
<td>Length of unencrypted manual input additional data ZIP and/or ADR</td>
</tr>
<tr>
<td>8</td>
<td>Field 8 see description (page 29 paragraph 9.4.3)</td>
</tr>
<tr>
<td>9</td>
<td>Field 9 see description (page 29 paragraph 9.4.4)</td>
</tr>
<tr>
<td>10</td>
<td>Keyed-in data presented as track-2=&quot;PAN=EXP[:CVV]?LRC &quot;</td>
</tr>
<tr>
<td>11</td>
<td>T3 clear additional keyed-in data in ASCII presented as track 3 [1ADR=][0ZIP=]</td>
</tr>
<tr>
<td>12</td>
<td>Encrypted Track-2 data</td>
</tr>
<tr>
<td>13</td>
<td>T2 hashed (20 bytes each)</td>
</tr>
<tr>
<td>14</td>
<td>Device serial number(10 bytes)( optional)</td>
</tr>
<tr>
<td>15</td>
<td>KSN (10 bytes)</td>
</tr>
<tr>
<td>16</td>
<td>LRC</td>
</tr>
<tr>
<td>17</td>
<td>Check Sum</td>
</tr>
<tr>
<td>18</td>
<td>ETX (0x03)</td>
</tr>
</tbody>
</table>

Note:
- Data Length low byte/high byte should be in length of characters.
- Field 11 includes encrypted PAN, EXP (YYMM) and 3-4 digit (CVV). The format should be:
  1) ;PAN=YYMM[:CVV]?LRC
     ‘;’—start sentinel
     ‘=’—field separator between PAN and EXP
     ‘:’—field separator between EXP and CVV if there is a CVV
     ‘?’—end sentinel
- The format of the fields ADR and ZIP is:

<table>
<thead>
<tr>
<th>1 byte field identifier</th>
<th>ASCII Data</th>
<th>field terminator ‘=’</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘1’—ADR; ‘0’—ZIP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
9.4.1  Note 1: Card Encode Type
Card Encode Type starts with 0: original encryption format
Card Encode Type starts with 8: enhanced encryption format

<table>
<thead>
<tr>
<th>Value</th>
<th>Encode Type Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 / 80</td>
<td>ISO/ABA format</td>
</tr>
<tr>
<td>01 / 81</td>
<td>AAMVA format</td>
</tr>
<tr>
<td>03 / 83</td>
<td>Other</td>
</tr>
<tr>
<td>04 / 84</td>
<td>Raw; un-decoded format</td>
</tr>
<tr>
<td>85</td>
<td>manual entry mode (default)</td>
</tr>
<tr>
<td>C0</td>
<td>manual entry enhanced mode</td>
</tr>
</tbody>
</table>

9.4.2  Note 2: Track 1-3 status byte
Field 4:
Bit 0: 1 — track 1 decoded data present
Bit 1: 1 — track 2 decoded data present
Bit 2: 1 — track 3 decoded data present
Bit 3: 1 — track 1 sampling data present
Bit 4: 1 — track 2 sampling data present
Bit 5: 1 — track 3 sampling data present
Bit 6, 7 — Reserved for future use (always 0)

9.4.3  Note 3: Clear/mask data sent status
Field 8 (Clear/mask data sent status) and field 9 (Encrypted/Hash data sent status) will only be sent out in enhanced encryption format.

Field 8: Clear/masked data sent status byte:
Bit 0: 1 — track 1 clear/mask data present
Bit 1: 1 — track 2 clear/mask data present
Bit 2: 1 — track 3 clear/mask data present or additional data present (in manual entry mode)
Bit 3: 1 — reserved for future use (always 0)
Bit 4: 0 — TDES encryption; 1 — AES encryption
Bit 5: 0 — reserved for future use (always 0)
Bit 6: 1 — PIN Key encryption
Bit 7: 1 — reader serial number present

9.4.4  Note 4: Encrypted/Hash data sent status
Field 9: Encrypted data sent status
Bit 0: 1 — track 1 encrypted data present
Bit 1: 1 — track 2 encrypted data present
Bit 2: 1 — track 3 encrypted data present
Bit 3: 1 — track 1 hash data present
Bit 4: 1 — track 2 hash data present
9.4.5 Description:

Track 1, Track 2 and Track 3 Unencrypted Length

This one-byte value is the length of the original Track data. It indicates the number of bytes in the Track masked data field. It should be used to separate Track 1, Track 2 and Track 3 data after decrypting Track encrypted data field.

Track 1 and Track 2 Masked

Track data masked with the MaskCharID (default is ‘*’). The first PrePANID (up to 6 for BIN, default is 4) and last PostPANID (up to 4, default is 4) characters can be in the clear (unencrypted).

Track 1, Track 2 and Track 3 Encrypted

This field is the encrypted Track data, using either TDES-CBC or AES-CBC with initial vector of 0. If the original data is not a multiple of 8 bytes for TDES or a multiple of 16 bytes for AES, the reader right pads the data with 0.

The key management scheme is DUKPT. For DUKPT, the key used for encrypting data is called the Data Key. Data Key is generated by first taking the DUKPT Derived Key exclusive or’ed with 0000000000FF000000000000FF0000 to get the resulting intermediate variant key. The left side of the intermediate variant key is then TDES encrypted with the entire 16-byte variant as the key. After the same steps are preformed for the right side of the key, combine the two key parts to create the Data Key.

Encrypted Data Length

Original Structure
Track 1 and Track 2 data are encrypted as a single block. In order to get the number of bytes for encrypted data field, we need to get Track 1 and Track 2 unencrypted length first. The field length is always a multiple of 8 bytes for TDES or multiple of 16 bytes for AES. This value will be zero if there was no data on both tracks or if there was an error encoding both tracks. Once the encrypted data is decrypted, all padding bytes need to be removed. The number of bytes of decoded track 1 data is indicated by track 1 unencrypted length field. The remaining bytes are track 2 data, the length of which is indicated by track 2 unencrypted length field.

Enhanced Structure
Track 1, 2 and 3 data are encrypted separatedly. In order to get the number of bytes for each track encrypted data field, the field length is always a multiple of 8 bytes for TDES or multiple of 16 bytes for AES. This value will be zero if there was no data on a track. Once the encrypted
data is decrypted, all padding bytes need to be removed. The number of bytes of decoded track n data is indicated by track n unencrypted length field.

**Track 1, Track 2 and Track 3 Hashed**

SecureKey reader uses SHA-1 to generate hashed data for track 1 to track 3 unencrypted data. It is 20 bytes long for each track. This is provided with two purposes in mind: One is for the host to ensure data integrity by comparing this field with a SHA-1 hash of the decrypted Track data, prevent unexpected noise in data transmission. The other purpose is to enable the host to store a token of card data for future use without keeping the sensitive card holder data. This token may be used for comparison with the stored hash data to determine if they are from the same card.

**Original Encryption Format Swipe Output**

028801001F372300%*5150********7903^PAYPASS/MASTERCARD^***************?*;5150********7903=***************?*5150********7903=***************?*
8871B640F379F3BD8D057A13F8145439B28D80BE8A43F3440D85928F576065EEE1BA54CAADFF67D552C20CBF1A9F34B63402B967998FC7C80487C8A6D
BFD4697985BD37E865FEEF6A48930751DC971FDFC6BC198924B7EF6F0D0007AA731C31F574608EB85E7751DA48970F96BE8BECDB94D672D746C2CC75176FA6E0C9E6FEFE0B154A0959B6299490125000000000197F6903

Key Value: F5 BF 6B E8 55 AB 92 3A DE 7E 77 40 D8 46 F9 DE
KSN: 62 99 49 01 25 00 00 00 00 1A

Decrypted Data:

Data in ASCII Format
%B5150710200107903^PAYPASS/MASTERCARD^090910140000631??;5150710200107903=090910140000631?

Data in HEX Format
2542353135303731303230303130373930335E504159504153534D41535445524152445E30393039313031343030
3030303036333313F3F3B353135303731303230303130373930333D30393039313031343030303036333313F3000000000000

**Enhanced Encryption Format Swipe Output**

028C01801F372300039B%*5150********7903^PAYPASS/MASTERCARD^***************?*;5150********7903=***************?*;5150********7903=***************?*
C5E75008986207CBFC9B1DA19F6EFF392E26C04C3BC76121C480A3B6FC122EDCE85B813682D4C3628002507B424831A0D6196BDF563F182147055DF7F5CB7EA2226764915B3A1B41190105132DB237068A9F56407F7FB69F39A429B7EB1911F574608EB85E57751DA48970F96B0E8BECDB94D672D746C2CC75176FA6E0C9E6FEFE0B154A0959B62994901250000000001B777703

Key Value: 32 68 28 A3 E4 F5 84 48 09 D2 8A B5 EB B8 AA 74
KSN: 62 99 49 01 25 00 00 00 00 1C
Decrypted Data:

Data in ASCII Format
%B5150710200107903^PAYPASS/MASTERCARD^090910140000631??
;5150710200107903=090910140000631?0

Data in HEX Format
2542353135303731303230303130373930335E504159504153532F4D4153544552434152445E30393
039313031343030303633313F3F00
3B3531353037313032303031303739303333D30393039313031343030303633313F300000000000

Manual Entry Format (default)
029C00850000000000718A1F6300C7241C9933DE31A01AB0C6021563FFC7B4810D94DA8863CE5
EC84B37EA79A87D96572047CFCF1068F0430393039053130373231053930363330629949012500
0000001D095B03

Key Value: B8 C7 3E 0A 17 58 09 5A 7A 86 44 6F 9B 57 76 FF
KSN: 62 99 49 01 25 00 00 00 00 1D

Decrypted Data:

Data in ASCII Format
515710200107903=0909=356

Data in HEX Format
35313537313032303031303739303333D303930393D333536
Manual Entry Format (new)
029200C0170018000292;515071******7903=0909?*FBCE9EFFF7500011FA447DC93C11F3816BC7A37EED3C8D0464AB280F610A7035448E0888CDF683D6C5C32DBE629949003700006000161DB103

Masked manually entered data: ;515071******7903=0909?*

Key Value: D1 3F 0B D8 47 AA 1D 27 C1 1C F8 4C D8 66 6A 2E
KSN: 62 99 49 00 37 00 00 60 00 16

Decrypted Data:
Data in ASCII Format
;5150710200107903=0909?0

Data in HEX Format
3B353135303731303230303130373930333D303930393F30

Note: To use this format set configuration byte 85 to 31 and 8F to 1.
10.0 MSR Settings

10.1 Setting Command
The setting data command is a collection of one or more function setting blocks and its format is as the following:

Command: \texttt{<STX><S><FuncSETBLOCK1>…<FuncBLOCKn><ETX><LRC>}
Response: \texttt{<ACK>} or \texttt{<NAK>} for wrong command (invalid funcID, length or value)

Each function-setting block \texttt{<FuncSETBLOCK>} has following format:

\texttt{<FuncID><Len><FuncData>}

The setting command will function with any one, any group or all the setting in one command.

Where:
\texttt{<FuncID>} is one byte identifying the setting(s) for the function.
\texttt{<Len>} is a one byte length count for the following function-setting block \texttt{<FuncData>}.  
\texttt{<FuncData>} is the current setting for this function. It has the same format as in the sending command for this function.

10.2 Bit Setting and Clearing Commands
This is a special type of setting command. For an 'S' (53) command that is setting only one configuration byte, the first byte of the command (the 'S' or 53) can be replaced with a '0' (31) to clear individual bits or a '1' (31) to set individual bits without changing the other bits in that configuration byte. These commands allows one to set or clear one or more bits of a configuration setting.  
A command to clear one bit of a configuration setting is '0'.

Example:
30 30 01 80 will clear the highest bit in configuration byte 10
31 30 01 80 will set the highest bit in configuration byte 10
31 30 01 81 will set the lowest and highest bits of configuration byte 10

This simplifies the setting commands for those not familiar with hexadecimal values; there is no need to read the setting before writing the setting; and it reduces the chance of changing another setting when setting a bit value.

Limitations
It can only be used on a one byte configuration setting.  
This cannot be used on special fields like the security level, that is no 30 7E 01 02  
This cannot be used to simultaneously turn some bits on and some bits off, so no changing 31 to 32 which is necessary to change TDES to AES.
### 10.3 Get Setting

This command will send current setting to application.

**Command:** `<STX> <R> <ReviewID> <ETX> <LRC 1>`

**Response:** `<ACK> <STX> <FuncID> <Len> <FuncData> <ETX> <LRC 2>`

<FuncID>, <Len> and <FuncData> definition are same as described above.

Note: ReviewID (value 0x1F) will return all funcID-s.

### 10.4 Security Management

The MSR reader is intended to be a secure reader. Security features include:

- Can include Device Serial Number
- Can encrypt track 1, track 2 and track 3 data for all bank cards (ETrk1 and ETrk2 will be empty if non bank card is swiped).
- Provides clear text confirmation data including card holder’s name and a portion of the PAN as part of the Masked Track Data (for bank cards)
- Optional display expiration date (for bank cards)
- Configurable Security Level

The reader supports five Security Levels. This allows customer to select the security profile needed for the application. The Security Level can be raised by command, but can never be lowered:

**Level 0**

Security Level 0 is a special case. It signifies that all DUKPT keys have been used. In this case the unit is at the end of its useful life. This level is set automatically by the reader when it runs out of DUKPT keys. The life time of DUKPT keys is one millions. Once reach the end of keys’ life time, user should inject DUKPT keys again.

**Level 1**—not applicable because encryption required

Reader properties are as configured from factory having the lowest level of default settings. There is no encryption process, no key serial number transmitted with decoded data. The reader has read operation and decoded track data is sent in default format. Encrypt type TDES and AES cannot be selected under Level 1.

**Level 2**—not applicable because encryption required

Key Serial Number and/or Initially Loaded Device Key have been injected. The encryption process is not activated and decoded track data is sent in default format. Key Serial Number and Initially Loaded Device Key can be set only once after manufacture.

**Level 3**

Both Key Serial Number and Initially Loaded Device Keys are injected and encryption is on. The encryption process is activated. The output of level 3 will be different from level 1 and level 2. Clear data output cannot be selected under Level 3. The output format in this level is more rigidly fixed so many track formatting output options are not supported, see function ID table for limitations.
• Level 4
When the reader is at Security Level 4, a correctly executed Authentication Sequence is required before the reader sends out data for a card swipe. Commands that require security must be sent with a four byte Message Authentication Code (MAC) at the end. Note that data supplied to MAC algorithm should NOT be converted to ASCII-Hex; rather it should be supplied in its raw binary form. Calculating MAC requires knowledge of current DUKPT KSN, this could be retrieved using Get DUKPT KSN and Counter command. The output format in this level is more rigidly fixed so many track formatting output options are not supported, see function ID table for limitations.

10.5 Encryption Management

The Encrypted swipe read supports TDES and AES encryption standards for data encryption. Encryption can be turned on via a command. TDES is the default.

If the reader is in security level 3, for the encrypted fields, the original data is encrypted using the TDES/AES CBC mode with an Initialization Vector starting at all binary zeroes and the Encryption Key associated with the current DUKPT KSN.

10.6 Check Card Format

• ISO/ABA (American Banking Association) Card
  Encoding method
  Track1 is 7-bit encoding.
  Track1 is 7-bit encoding. Track2 is 5 bits encoding. Track3 is 5-bit encoding.
  Track1 is 7-bit encoding. Track2 is 5 bits encoding.
  Track2 is 5-bit encoding.
  If only track3 and it is 5 bit encoding, ISO4909 and has PAN
  Additional checks
  Track1 2\textsuperscript{nd} byte is ‘B’.
  There is at least one ‘=’ in track 2 and the position of ‘=’ is between 12\textsuperscript{th} ~ 20\textsuperscript{th} character.
  Total length of track 2 is above 19 characters.
  Total of 4 digits after the separator character for expiration date or a second separator to indicate no expiration date
  Card number range in PAN will be used to identify bank card.

• AAMVA (American Association of Motor Vehicle Administration) Card
  Encoding method
  Track1 is 7 bits encoding. Track2 is 5 bits encoding. Track3 is 7 bits encoding.

• Others (Customer card)

10.7 MSR Data Masking

For ABA Card Data (Card type 0)
For cards that need to be encrypted, both encrypted data and clear text data are sent.
Masked Area

The data format of each masked track is ASCII.
The clear data include start and end sentinels, separators, first N, last M digits of the PAN, card holder name (for Track1). Optional expiration date may be revealed.
The rest of the characters should be masked using mask character.

Mask character default value is ‘*’.
11.0 SecureKey Decryption Demo Software

SecureKey demo software is available to demonstrate the MSR data decryption. Please see the below screenshots:

This demo software can be used for USB-HID or USB KB interface. For USB KB interface, please make sure the cursor is placed in the “manual command” window before swiping a card.

The following demo software screenshots are shown for reference and might not reflect the latest demo software version.
The demo software uses the IDTECH demo key 0123456789ABCDEFFEDCBA9876543210 to decrypt the swiped or entered data by default. To change the decryption key, click on “input initial key”

11.1 Card Swipe Data, IDTECH Original Encryption Format

Type 52 85 on the manual command screen to see the current SecureKey setting and press “Send Command”
Check the 5th byte of the response, if it’s “30”, the SecureKey is in IDTECH original encryption format, for example 06 02 85 01 30 03 85
If the 5th byte is “31”, the SecureKey is in IDTECH enhanced encryption format.

To change the encryption format, go to “MSR Security” and select the original or enhanced encryption format

Swipe a card, the output and decrypted data will be shown on screen.
11.2 Key in data, IDTECH Format

Manually key in the card data on the device, the data will show on the demo as the following (shown is the default manual entry format)
## 12. Specifications

### Mechanical

<table>
<thead>
<tr>
<th>ITEM</th>
<th>SPECIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key switch Information</td>
<td></td>
</tr>
<tr>
<td>Total/ Pre-Travel</td>
<td>2.5 + 0.5 mm/ 1.5 + 0.4 mm</td>
</tr>
<tr>
<td>Operating Type</td>
<td>Tactile Type</td>
</tr>
<tr>
<td>Operating Force</td>
<td>55 + 7g</td>
</tr>
<tr>
<td>Tactile Feel Force</td>
<td>30 + 14g</td>
</tr>
<tr>
<td>Letter of Keycap</td>
<td>Traditional North American</td>
</tr>
<tr>
<td>Material of Key switch</td>
<td>Silicone Rubber (Rubber Key Pad)</td>
</tr>
<tr>
<td>Keyboard Information</td>
<td></td>
</tr>
<tr>
<td>Enclosure</td>
<td>Top &amp; Bottom Case</td>
</tr>
<tr>
<td>Material</td>
<td>High Impact ABS</td>
</tr>
<tr>
<td>Color</td>
<td>Black</td>
</tr>
<tr>
<td>Cable Information</td>
<td></td>
</tr>
<tr>
<td>Jacket Material</td>
<td>Polyester 0.075 mm</td>
</tr>
<tr>
<td>Conductors</td>
<td>Polyester 0.10 mm</td>
</tr>
<tr>
<td>Color</td>
<td>Upper circuit: 3M467+PET125S</td>
</tr>
<tr>
<td>Length</td>
<td>Lower circuit: 3M467+PET 100S</td>
</tr>
<tr>
<td>PC Connector</td>
<td>Acheson ED-725A 5~10 um</td>
</tr>
<tr>
<td>Keyboard Membrane Material</td>
<td>The auxiliary ports are only on the USB keyboard &amp;</td>
</tr>
<tr>
<td>Spacer</td>
<td>located horizontal to each other on the rear. USB</td>
</tr>
<tr>
<td>Back-up Plate</td>
<td>port plastic color is white.</td>
</tr>
<tr>
<td>Upper Circuit</td>
<td></td>
</tr>
<tr>
<td>Lower Circuit</td>
<td></td>
</tr>
<tr>
<td>Silver</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>USB-KB and USB-HID</td>
</tr>
</tbody>
</table>

### Electrical

<table>
<thead>
<tr>
<th>ITEM</th>
<th>SPECIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Rating</td>
<td>+5.0 VDC ±10%, 60ma Max (excludes ICC)</td>
</tr>
<tr>
<td>Type of Circuit</td>
<td>1 Circuit 1 Contact</td>
</tr>
<tr>
<td>Insulation Resistance</td>
<td>DC 100V 50 M Ω Min</td>
</tr>
<tr>
<td>Bounce</td>
<td>10 ms Max</td>
</tr>
<tr>
<td>Operating Life</td>
<td>20,000,000 keystrokes</td>
</tr>
<tr>
<td>Industry Requirements</td>
<td>FCC class B and CE</td>
</tr>
</tbody>
</table>

### Quality & Reliability

<table>
<thead>
<tr>
<th>ITEM</th>
<th>SPECIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>MI Requirement</td>
<td>The keyboard meets the FCC class B limits</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>ESD Immunity</td>
<td>The keyboard passes 0KV to 8 kV minimum without any data loss; passes 8KV to 15 kV minimum that may cause malfunctions. No internal components are destroyed and after reset, the keyboard functions normally.</td>
</tr>
<tr>
<td>MTBF</td>
<td>The main operating time between failures will be more than 60,000 hours</td>
</tr>
<tr>
<td>Drop</td>
<td>610 mm (24”) height</td>
</tr>
<tr>
<td></td>
<td>Drop: 4 corner, 4-sidelines, 2-sides front/back</td>
</tr>
<tr>
<td>Vibration</td>
<td>Vibration frequency 60 Hz/sec. 3 mm amplitude of an oscillation. X,Y,Z each axis at 2 hours</td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>0°C ~ 40°C</td>
</tr>
<tr>
<td>Storage Temperature</td>
<td>-20°C ~ + 40°C</td>
</tr>
</tbody>
</table>

### MagStripe Reader

<table>
<thead>
<tr>
<th>Number of tracks</th>
<th>Tracks 1 &amp; 2 or Tracks 2 &amp; 3 or Tracks 1, 2 &amp; 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>TDES or AES with DUKPT key management</td>
</tr>
<tr>
<td>Compatibility</td>
<td>ISO 7810 and 7811-1 through -6</td>
</tr>
<tr>
<td>Output data formatting</td>
<td>Standard output format</td>
</tr>
<tr>
<td>Operating Life</td>
<td>1,000,000 card swipes</td>
</tr>
<tr>
<td>Card speed range</td>
<td>3 to 60 IPS (Inches Per Second)</td>
</tr>
</tbody>
</table>
### 12.0 Appendix A  Setting Configuration Parameters and Values

Following is a table of default setting and available settings (value within parentheses) for each function ID.

<table>
<thead>
<tr>
<th>Function ID</th>
<th>Hex</th>
<th>Description</th>
<th>Default Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TrackSelectID</td>
<td>13</td>
<td>Track Selection</td>
<td>‘0’</td>
<td>Any Track 0-any</td>
</tr>
<tr>
<td>PollingInterval ID</td>
<td>14</td>
<td>Polling Interval</td>
<td>1 (1 ~ 255)</td>
<td>USB HID Polling Interval</td>
</tr>
<tr>
<td>TrackSepID</td>
<td>17</td>
<td>Track Separator</td>
<td>0x0D=CR/Enter</td>
<td>CR for RS232, Enter for KB any character supported except 00 which means none.</td>
</tr>
<tr>
<td>SendOptionID</td>
<td>19</td>
<td>Send Option</td>
<td>‘1’ (‘0’~’F’) ‘5’ for Port Powered IV</td>
<td>Sentinel and Account number control</td>
</tr>
<tr>
<td>DecodingMethodID</td>
<td>1D</td>
<td>Decoding Direction</td>
<td>‘1’ (‘0’~’3’)</td>
<td>Reading Direction 0x30 – Raw Data Decoding in Both Directions. 0x31 – Decode in Both directions. 0x32 – Moving Stripe Along Head in Direction of Encoding. 0x33 – Moving Stripe Along Head Against Direction of Encoding.</td>
</tr>
<tr>
<td>ReviewID</td>
<td>1F</td>
<td>Review All Settings</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>TerminatorID</td>
<td>21</td>
<td>Terminator</td>
<td>0x0D (any)</td>
<td>CR for RS232, Enter for KB; ‘0’ for CRLF</td>
</tr>
<tr>
<td>FmVerID</td>
<td>22</td>
<td>Firmware Version</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>USBHIDFmtID</td>
<td>23*</td>
<td>USB HID Fmt (HID rdr only)</td>
<td>‘0’ (‘0’, ‘8’)</td>
<td>‘0’ ID TECH Format; ‘8’ HIDKB format</td>
</tr>
<tr>
<td>ForeignKBID</td>
<td>24</td>
<td>Foreign KB</td>
<td>‘0’ (‘0’ ~0x3A)</td>
<td>Foreign Keyboard</td>
</tr>
<tr>
<td>CustSetID</td>
<td>30</td>
<td>Custom Customer Settings</td>
<td>00(00-07)</td>
<td>.0-Level 3/4 Non-CC send as Level 1 .1-Level3: No empty pkt when not enough sampling bits .2- Enhanced Secured Output will have SN after hash</td>
</tr>
<tr>
<td>Track1PrefixID</td>
<td>34</td>
<td>Track 1 Prefix</td>
<td>0 (any string)</td>
<td>No prefix for track 1, 6 char max</td>
</tr>
<tr>
<td>Track2PrefixID</td>
<td>35</td>
<td>Track 2 Prefix</td>
<td>0 (any string)</td>
<td>No prefix for track 2, 6 char max</td>
</tr>
<tr>
<td>Track3PrefixID</td>
<td>36</td>
<td>Track 3 Prefix</td>
<td>0 (any string)</td>
<td>No prefix for track 3, 6 char max</td>
</tr>
<tr>
<td>Track1SuffixID</td>
<td>37</td>
<td>Track 1 Suffix</td>
<td>0 (any string)</td>
<td>No suffix for track 1, 6 char max</td>
</tr>
<tr>
<td>Track2SuffixID</td>
<td>38</td>
<td>Track 2 Suffix</td>
<td>0 (any string)</td>
<td>No suffix for track 2, 6 char max</td>
</tr>
<tr>
<td>Track3SuffixID</td>
<td>39</td>
<td>Track 3 Suffix</td>
<td>0 (any string)</td>
<td>No suffix for track 3, 6 char max</td>
</tr>
<tr>
<td>KeyTypeID</td>
<td>3E*</td>
<td>data or pin key</td>
<td>0</td>
<td>0-data key; 5A-pin key</td>
</tr>
<tr>
<td>PrePANID</td>
<td>49</td>
<td>PAN to not mask</td>
<td>4 (0-6)</td>
<td># leading PAN digits to display</td>
</tr>
<tr>
<td>PostPANID</td>
<td>4A</td>
<td>PAN to not mask</td>
<td>4 (0-4)</td>
<td># of trailing PAN digits to display</td>
</tr>
<tr>
<td>MaskCharID</td>
<td>4B</td>
<td>mask the PAN with this character</td>
<td>‘*’ 20-7E</td>
<td>any printable character</td>
</tr>
<tr>
<td>CrypTypeID</td>
<td>4C*</td>
<td>encryption type</td>
<td>‘1’ (‘1’-‘2’)</td>
<td>‘1’ 3DES ‘2’ AES</td>
</tr>
<tr>
<td>SerialNumberID</td>
<td>4E*</td>
<td>device serial #</td>
<td>any 8-10 bytes</td>
<td>8-10 digit serial number; Can be set only once</td>
</tr>
<tr>
<td>DispExpDateID</td>
<td>50</td>
<td>mask or display expiration date</td>
<td>‘0’ ‘0’-‘1’</td>
<td>‘0’ mask expiration date; ‘1’ display expiration date</td>
</tr>
<tr>
<td>SessionID</td>
<td>54</td>
<td>8 byte hex not stored in EEPROM</td>
<td>None</td>
<td>always init to all ‘FF’</td>
</tr>
<tr>
<td>Mod10ID</td>
<td>55</td>
<td>include mod10 check digit</td>
<td>‘0’ (‘0’-‘2’)</td>
<td>‘0’ don’t include mod10, ‘1’ display mod10, ‘2’ display wrong mod10</td>
</tr>
<tr>
<td>KeyManageTypeID</td>
<td>58*</td>
<td>DUKPT</td>
<td>‘1’</td>
<td>‘1’ DUKPT</td>
</tr>
<tr>
<td>HashOptID</td>
<td>5C</td>
<td>‘7’ (‘0’-‘7’)</td>
<td>Send tk1-2 hash bit 0:1 send tk1 hash; bit 1:1 send tk2 hash; bit2:1 send tk3 hash.</td>
<td></td>
</tr>
<tr>
<td>HexCaseID</td>
<td>5D</td>
<td>‘1’ (‘0’-‘1’)</td>
<td>‘0’ send in lower case; ‘1’ send in upper case</td>
<td></td>
</tr>
<tr>
<td>T17BStartID</td>
<td>61</td>
<td>Track 1 7 Bit Start Char</td>
<td>‘%’ (any)</td>
<td>‘%’ as Track 1 7 Bit Start Sentinel</td>
</tr>
<tr>
<td>T16BStartID</td>
<td>62</td>
<td>T16B Start</td>
<td>‘%’ (any)</td>
<td>‘%’ as Track 1 6 Bit Start Sentinel</td>
</tr>
<tr>
<td>T15BStartID</td>
<td>63</td>
<td>T15B Start</td>
<td>‘,’ (any)</td>
<td>‘;’ as Track 1 5 Bit Start Sentinel</td>
</tr>
<tr>
<td>T27BStartID</td>
<td>64</td>
<td>Track 2 7 Bit Start Char</td>
<td>‘%’ (any)</td>
<td>‘%’ as Track 2 7 Bit Start Sentinel</td>
</tr>
<tr>
<td>T25BStartID</td>
<td>65</td>
<td>T25BStart</td>
<td>‘;’ (any)</td>
<td>‘;’ as Track 2 5 Bit Start Sentinel</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
<td>Start Character(s)</td>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------------</td>
<td>--------------------</td>
<td>--------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>T37BStartID</td>
<td>Track 3 7 Bit Start Char</td>
<td>‘%’ (any)</td>
<td>‘%’ as Track 3 7 Bit Start Sentinel</td>
<td></td>
</tr>
<tr>
<td>T36BStartID</td>
<td>Track 3 6 Bit Start</td>
<td>‘!’ (any)</td>
<td>‘!’ as Track 3 6 Bit Start Sentinel</td>
<td></td>
</tr>
<tr>
<td>T35BStartID</td>
<td>Track 3 5 Bit Start</td>
<td>‘;’ (any)</td>
<td>‘;’ as Track 3 5 Bit Start Sentinel</td>
<td></td>
</tr>
<tr>
<td>T1EndID</td>
<td>Track 1 End Sentinel</td>
<td>‘?’ (any)</td>
<td>‘?’ as End Sentinel</td>
<td></td>
</tr>
<tr>
<td>T2EndID</td>
<td>Track 2 End Sentinel</td>
<td>‘?’ (any)</td>
<td>‘?’ as End Sentinel</td>
<td></td>
</tr>
<tr>
<td>T3EndID</td>
<td>Track 3 End Sentinel</td>
<td>‘?’ (any)</td>
<td>‘?’ as End Sentinel</td>
<td></td>
</tr>
<tr>
<td>T1ERRSTAR TID</td>
<td>Track 1 error code</td>
<td>‘%’ (any)</td>
<td>start sentinel if track 1 error report</td>
<td></td>
</tr>
<tr>
<td>T2ERRSTAR TID</td>
<td>Track 2 error code</td>
<td>‘;’ (any)</td>
<td>start sentinel if track 2 error report</td>
<td></td>
</tr>
<tr>
<td>T3ERRSTAR TID</td>
<td>Track 3 error code</td>
<td>‘+’ (any)</td>
<td>start sentinel if track 3 error report</td>
<td></td>
</tr>
<tr>
<td>SecureLrcID</td>
<td>Secured output format track LRC option</td>
<td>‘1’ (‘0’-‘1’)</td>
<td>‘1’ to send track LRC in secured output data; ‘0’ don’t send track LRC</td>
<td></td>
</tr>
<tr>
<td>EquipFwID</td>
<td>feature option setting</td>
<td>any</td>
<td>Factory Reader firmware configuration setting</td>
<td></td>
</tr>
<tr>
<td>SyncCheckID</td>
<td>check for track sync bits-can allow poorly encoded cards to be read</td>
<td>‘2’ (‘0’-’2’)</td>
<td>check leading &amp; trailing sync bits ‘0’ 13 bits; ‘1’ 13 bits, but allow if valid through track LRC; ‘2’ 9 bits ABA; 13 bits IATA; 16 bits JIS</td>
<td></td>
</tr>
<tr>
<td>SecurityLevelID</td>
<td>Reader’s encryption level</td>
<td>‘1’ or ‘3’ (‘0’- ‘4’)</td>
<td>‘1’ no encryption; ‘2’ key loaded; ‘3’ encrypted reader; ‘0’ DUKPT exhausted; ‘4’ authentication required</td>
<td></td>
</tr>
<tr>
<td>EncryptOptID</td>
<td>encryption options, enhanced only</td>
<td>0 encrypt card type 0; (0-1F)</td>
<td>bit 0 encrypt trk1; bit 1 encrypt trk2; bit 2 forces encryption on track 3 and there would be no mask data; bit 3 encrypt trk3; bit 4 encrypt trk3 if card type 0 only and allow trk1, trk 2, trk3 masked data to be sent as well.</td>
<td></td>
</tr>
<tr>
<td>EncryptStrID</td>
<td>encrypt structure</td>
<td>‘0’</td>
<td>‘0’ original; ‘1’ enhanced</td>
<td></td>
</tr>
<tr>
<td>MaskOptID</td>
<td>clear / mask data options</td>
<td>7</td>
<td>bit 0 send clear/mask trk1 bit 1 send clear/mask trk2</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Code</td>
<td>Description</td>
<td>Value/Explanation</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>------</td>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>EnFmtID</td>
<td>88</td>
<td>encryption format defined in xml specification</td>
<td>\02\30\34</td>
<td></td>
</tr>
<tr>
<td>T3ExpDatePosID</td>
<td>89</td>
<td>track 3 expiration date position offset</td>
<td>0x34 ((0x34, 0x36))</td>
<td></td>
</tr>
<tr>
<td>AdminLvlID</td>
<td>8E</td>
<td>Admin Level</td>
<td>B, 15, 1F, 29, 33, 3D</td>
<td></td>
</tr>
<tr>
<td>KeyedOptID</td>
<td>8F*</td>
<td>Keyed Options</td>
<td>0-(any)</td>
<td></td>
</tr>
<tr>
<td>Equip2ID</td>
<td>AE</td>
<td>special settings</td>
<td>00 (any)</td>
<td></td>
</tr>
<tr>
<td>CustSet2ID</td>
<td>AF</td>
<td>sending credit card shifted by lifting card.</td>
<td>00H (or 01H)</td>
<td></td>
</tr>
<tr>
<td>PrefixID</td>
<td>D2</td>
<td>Preamble</td>
<td>0 (any 15)</td>
<td></td>
</tr>
<tr>
<td>PostfixID</td>
<td>D3</td>
<td>Postamble</td>
<td>0 (any 15)</td>
<td></td>
</tr>
</tbody>
</table>

* These settings do not change with a default all command.

1. PrefixID and PostFixID are ignored on encrypted transaction unless the reader is a keyboard reader, then they are supported so that the host can recognize the reader’s output.
13.0 Appendix B  Guide to Encrypting and Decrypting Data

The encryption method used by SecureKey is called Cipher-block Chaining (CBC). With this method, each block of data is XOR’ed with the previous data block before being encrypted. The encryption of each block depends on all the previous blocks. As a result, each encrypted data block would need to be decrypted sequentially.

To encrypt the data, first generate an 8-byte random initialization vector which is XOR’ed with the first data block before it is encrypted. Then the data is encrypted with the device key using TDES algorithm. The result is again XOR’ed with the next 8-byte data block before it is encrypted. The process repeats until all the data blocks have been encrypted.

The host can decrypt the cipher text from the beginning of the block when the data is received. However, it must keep track of both the encrypted and clear text data. Or alternatively, the data can be decrypted backward form that last data block to the first, so that the decrypted data can replace the original data as the decryption is in process.

To decrypt the data using reverse method, first decrypt the last 8-byte of data using TDES decryption. Then perform an XOR operation with result and the preceding data block to get the last data block in clear text. Continue to decrypt the next previous block with the same method till it reaches the first block. For the first data block, the XOR operation can be skipped, since it is XOR’ing with 00h bytes.
14.0 Appendix C  Key Management Flow Chart
15.0 Appendix D  Example of IDTECH Raw Data Decryption

Original Raw Data Forward Direction:
01D67C81020408102D4481020408102042890A350854A2FB3EE4BA3D4065B67A9C391F58
2A42B99A858A90AF60852B14AA628A0D
028FC210842C18421084030092040B1581F24B56074404811160D

Original Raw Data Backward Direction:
01A28CAA51A9420DEA12A342B33A84A835F13872BCDB4C0578BA4EF9BE8A542158A1
228408102040810245681020481027CD60D
02D11024045C0D5A49F03515A0409201804210843068421087E20D

Note:

a. There is track number before each track. Track 1 is 01, Track 2 is 02, Track 3 is 03.
b. There is track separator after each track: 0D

Example of decryption of a two track ABA card with the original encryption format. For both Fix & DUKPT key management.

SecureKey Reader with default settings

Key for all examples is
0123456789ABCDEFFEDCBA9876543210

Original Encryption Format

Original encryption format (this can be recognized because the high bit of the fourth byte underlined (00) is 0.
02870041B331A0027D2E435CEE303F007E977B598B7E3C57C76F4445E309F6916C0321A
0F915B6E490813498839049FE5204762327C3C758C5BF82542DEEDD8D6AF88019149A702
FF2D43BD4AD60031FA450720B00D7808E15F3D5B29AE712C64A1212E9AF6F483BD4079
8A9FF2DDE77D046620B55BCE94A4D5534CF57E7E07629949011A00000000001871D03

STX, Length (LSB, MSB), card type, track status, length track 1, length track 2, length track 3
02 8700 04 1B 33 1A 00

Track 1 & 2 encrypted length 0x33+0x1A rounded up to 8 bytes =0x4D -> 0x50 (80 decimal)
Track 1 hashed
E15F3D5B29AE712C64A1212E9AF6F483BD40798A

Track 2 hashed
9FF2DDE77D046620B55BCE94A4D5534CF57E7E07

KSN
629949011A0000000001

LRC, checksum and ETX
87 1D 03

Key Value: 8A 60 A3 EB 80 87 63 52 B8 F5 05 CD A8 3C 33 70
KSN: 62 99 49 01 1A 00 00 00 00 01

Decrypted Raw Data:
01D67C81020408102D4481020408102042890A350854A2FB3EE4BA3D4065B67A9C391F58
2A42B99A858A90AF60852B14AA628A
028FC210842C18421084030092040B51581F24B5607440481116

-----------------------------------------

Security Level 4 Original Encryption Format
028F00041B331A0070756B86C0B670DAAA78EEA454F5A7BAFB5CDA91BA9A5B62BB49
F67CD21484D3138DB3468C80F3468688AE61E3FB25FEEEB630B81717CC405F8A73430FC
A6F98C4CEDE76A7AC0D909E2B25F7E77F7888306B57CB67A9BE15F3D5B29AE71
2C64A1212E9AF6F483BD40798A9FF2DDE77D046620B55BCE94A4D5534CF57E7E076299
49011A000000000002DD5D03

Key Value: 06 A9 B3 23 2A 69 B4 57 61 76 5E C3 CB A3 33 37
KSN: 62 99 49 01 1A 00 00 00 00 02
Session ID: AA AA AA AA AA AA AA AA

Decrypted Data:
01D67C81020408102D4481020408102042890A350854A2FB3EE4BA3D4065B67A9C391F58
2A42B99A858A90AF60852B14AA628A
028FC210842C18421084030092040B51581F24B5607440481116