SmartPIN K100 3.X
Technical Reference Manual

80114510-001-C
February 14, 2017

International Technologies & Systems Corporation
10721 Walker Street, Cypress, CA 90630-4720; Tel: (714) 761-6368; Fax: (714) 761-8880
www.idtechproducts.com

Revision History

Rev.	Date	Description of Changes	By
A	4/19/2016	Release to Revision A	JH
A	6/8/2016	New engineering drawings. Miscellaneous edits. Include USB VID & PID. Expanded explanation of Get Numeric Entry.	KT
A	6/17/2016	Include tamper-protection info (Sections 3.10, 6.4, 6.5).	KT
B	6/22/2016 11/30/2016	Added USB descriptor info. Removed "sleep mode."	KT
C	2/8/2017 2/14/2017	Add 75 46 28 (Get All Key) command. Update 78 46 25 (Get Key Status) command.	KT

ID TECH

10721 Walker Street, Cypress, CA90630 Voice: (714) 761-6368 Fax: (714) 761-8880

The information contained herein is provided to the user as a convenience. While every effort has been made to ensure accuracy, ID TECH is not responsible for damages that might occur because of errors or omissions, including any loss of profit or other commercial damage, nor for any infringements or patents or other rights of third parties that may result from this information's use. The specifications described herein were current at the time of publication, but are subject to change at any time without prior notice.

LIMITED WARRANTY
ID TECH warrants to the original purchaser for a period of 12 months from the date of invoice that this product is in good working order and free from defects in material and workmanship under normal use and service. ID TECH's obligation under this warranty is limited to, at its option, replacing, repairing, or giving credit for any product that returned to the factory of origin with the warranty period and with transportation charges and insurance prepaid, and which is, after examination, disclosed to ID TECH's satisfaction to be defective. The expense of removal and reinstallation of any item or items of equipment is not included in this warranty. No person, firm, or corporation is authorized to assume for ID TECH any other liabilities in connection with the sales of any product. In no event shall ID TECH be liable for any special, incidental or consequential damages to purchaser or any third party caused by any defective item of equipment, whether that defect is warranted against or not. Purchaser's sole and exclusive remedy for defective equipment, which does not conform to the requirements of sales, is to have such equipment replaced or repaired by ID TECH. For limited warranty service during the warranty period, please contact ID TECH to obtain a Return Material Authorization (RMA) number & instructions for returning the product.

THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE. THERE ARE NO OTHER WARRANTIES OR GUARANTEES, EXPRESS OR IMPLIED, OTHER THAN THOSE HEREIN STATED. THIS PRODUCT IS SOLD AS IS. IN NO EVENT SHALL ID TECH BE LIABLE FOR CLAIMS BASED UPON BREACH OF EXPRESS OR IMPLIED WARRANTY OF NEGLIGENCE OF ANY OTHER DAMAGES WHETHER DIRECT, IMMEDIATE, FORESEEABLE, CONSEQUENTIAL OR SPECIAL OR FOR ANY EXPENSE INCURRED BY REASON OF THE USE OR MISUSE, SALE OR FABRICATIONS OF PRODUCTS WHICH DO NOT CONFORM TO THE TERMS AND CONDITIONS OF THE CONTRACT.

ID TECH and Value through Innovation are trademarks of International Technologies & Systems Corporation. USB (Universal Serial Bus) specification is copyright by Compaq Computer Corporation, Intel Corporation, Microsoft Corporation, and NEC Corporation. Windows is a registered trademark of Microsoft Corporation.

Table of Contents

1.0 Introduction

ID TECH’s SmartPIN K100 3.X is a PCI 3.X certified, ruggedized PIN-entry device designed for use in vending and ATM environments. The 4x4, 16-key layout is a familiar format seen on other unattended payment devices and is specifically designed to meet applicable ADA, ANSI, and ISO standards. The unit's IP65 rating makes it ideal for outdoor environments.

This document provides technical information for integrating the K100 into typical deployment environments. In addition to physical and electrical information, this document presents firmware API specifications for communicating with the K100 via (for example) USB-HID.

The low-level (firmware) commands are applicable using either the USB-HID or RS232 interface.

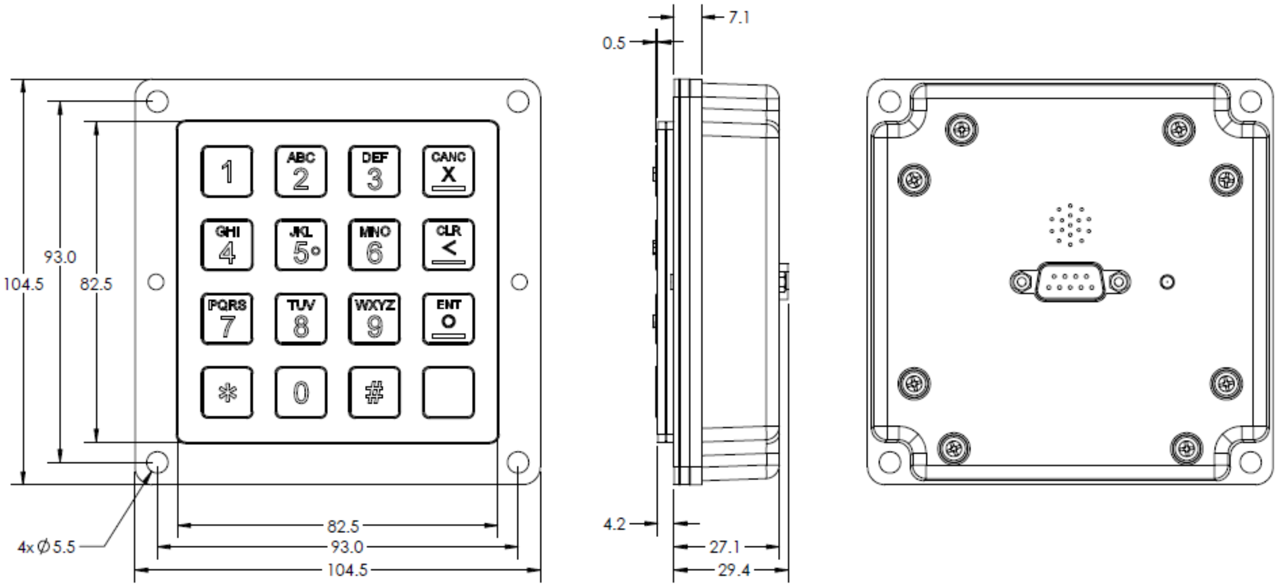
- For RS232 interface, the default COM parameters are: 38400, 8, 1, none.
- For USB, the VID is 0xACD and the PID is 0x0850.

2.0 Features

- PCI 3.X Certified
- 4x4 keypad layout
- LED on back of unit for unit status
- Meets ADA, ANSI, and ISO standards for PIN Entry Devices
- Optional audible feedback
- Drop in replacement for the SmartPIN K100 2.X
- Gasket for watertight mounting
- IP65 rating
- Removal detection and tamper responsive
- Low Power consumption mode
- Supports TDES encryption with DUKPT key manangement
- Supports serial communication via RS232 or USB-HID

3.0 Physical Specification

3.1 Physical Specification



Materials & Finish

Keys: Material: Stainless steel with brushed finish
Key Embossing (ADA compliant) tactile symbol
Numeric keys, 12 each, includes * and # (or ↓ and ↑)
Operation Keys (4 each)
Key graphics are etched or engraved
The operation keys (CANC, CLR, ENT) have engraved color bars near the bottom of the key surface
The operation keys also have raised symbols (X, < , & O)
Sequence from top to bottom:
CANCEL (red), CLEAR (yellow), ENTER (green), [blank] (no color)

Faceplate Brushed finish, stainless steel

3.2 Operating Environment

Minimum Temperature Range
Operating: -40 to 80° C (non-condensing)
Non-operating: -40 to 80° C (non-condensing)

Relative Humidity Range:
Operating: maximum 95% (non-condensing)
Non-operating: maximum 95% (non-condensing)

3.3 Electrical

Power is supplied to the unit in the following manner:
RS232 interface – uses A/C power adapter, 5VDC +/- 10%
USB interface – Hub/PC supplied power
Operation current: <100mA

3.4 Output Connections

The RS-232 Output complies with the standard RS-232 Pin-out as listed below:

Pin number	RS-232
1	-
2	RD
3	TD
4	-
5	GND
6	-
7	RTS
8	CTS
9	-

3.5 Audio Feedback

Audio feedback is available through a non-oscillating beeper for keystrokes and operation alerts. The beeper device provides a single pulse for audio feedback recognition of each key press. The beeper can be given a time and frequency command to produce modulated tones. The beeper is capable of producing a 75db sound level at 1 foot.

3.6 Battery

The battery provides power to maintain the contents of cryptographic keys while power to the unit is off. For maximum security, the battery power is cut off during a “tamper event” condition, which causes the erasure of the cryptographic key(s). The battery is not in use when the unit is powered by an external source.

3.7 Operation LED

The Op-LED is a surface mount, tri-color LED, which is visible from the back of the housing (using a light pipe). It is molded into the housing. The LED provides operating information for the PIN Pad. The following chart gives operation status meanings. The blink rate is about 12 times per minute with an LED-on period of about 2.5 second.

LED State	**Operating Condition**
Off	No power
Steady Green	Powered on, with keys injected, communication established
Blinking Green	Powered on, with Keys injected, no communication
Steady Yellow	Powered on, no keys, communication established
Blinking Yellow	Powered on, no keys, no communication established
Steady Red	Powered on & PIN pad is not functional
Blinking Red	Powered on, Tampering detected, keys erased

3.8 Reliability

ESD: Passes 8kV contact and 8kV air discharge

Drop Test: Withstands 3 ft drop to concrete, 6 surfaces & 4 corners, no functional damage

MTBF: Minimum calculated MTBF value of 120,000 power on hours

Key Stroke: The Key operational life is greater than 2,000,000 key stroke operations any one key.

3.9 Peripheral Device Pairing

Unit has the ability to pair with other peripheral payment devices to complete MSR-Debit transactions

3.10 Tamper Protection Features

The unit incorporates anti-tamper features, consisting of small buttons on the left and right edges of the housing (and two internal buttons, not accessible from the outside). When these buttons are depressed and the unit has been anti-tamper enabled via software commands (see Activate Fix Device), any sudden release of tension on the buttons causes the unit to deactivate. (Also, *cryptographic keys will be erased*.) Thus, unauthorized removal of the unit (theft, disassembly, etc.) will cause deactivation and make it impossible for sensitive data to be accessed or for the unit to be (re)used by an unauthorized user.

4.0 USB Descriptors

4.1 USB Descriptor Info

The USB version of the K100 can be operated in USB-HID mode.

When the K100 is operated in HID mode, it behaves like a vendor-defined USB-HID device. A direct communication path can be established between the host application and the reader without interference from other HID devices. You can identify the device in Windows using the Devices and Printers utility (Microsoft). In Linux, you can run *lsusb* or *usb-devices* from the shell to get device info.

Detailed USB-HID descriptor information follows.

4.1.1 Device Descriptor

Field	**Value**	**Description**
Length	12	
Des type	01	
bcd USB	00 02	USB2.0
Device Class	00	Unused
Sub Class	00	Unused
Device Protocol	00	Unused
Max Packet Size	40	
VID	0A CD	
PID	08 50	HID ID TECH StructureHID PINPAD
BCD Device Release	00 02	
i-Manufacture	00	
i-Product	00	
i-Serial-Number	00	Changes to 3 if USB serial number enabled
# Configuration	01	

4.1.2 Configuration Descriptor

Field	**Value**	**Description**
Length	09	
Des type	02	
Total Length	29 00	
No. Interface	01	
Configuration Value	01	
iConfiguration	00	
Attributes	E0	Bus power
Power	64	200mA

4.1.3 Interface Descriptor

Field	**Value**	**Description**
Length	09	
Des type	04	
Interface No.	00	
Alternator Setting	00	
# EP	02	
Interface Class	03	HID
Sub Class	01	
Interface Protocol	00	
iInterface	00	

4.1.4 HID Descriptor

Field	**Value**	**Description**
Length	09	
Des type	21	HID
bcdHID	00 01	
Control Code	00	
numDescriptors	01	Number of Class Descriptors to follow
DescriptorType	22	Report Descriptor
Descriptor Length	1C 00	HID ID TECH format

4.1.5 End Point 1 Descriptor

Field	**Value**	**Description**
Length	07	
Des type	05	End Point
EP Addr	81	EP1 In
Control Code	03	Interrupt
MaxPacketSize	40 00	64 bytes
bInterval	02	

4.1.6 End Point 2 Descriptor

Field	**Value**	**Description**
Length	07	
Des type	05	End Point
EP Addr	02	EP2 Out
Control Code	03	Interrupt
MaxPacketSize	40 00	64 bytes
bInterval	01	

4.1.7 Report Descriptor

Value	Description
05 02	Usage Page (Simulation Controls)
09 26	Usage (Driving Control)
A1 01	Collection (Application)
05 0C	Usage Page (Consumer Devices)
15 00	Logical Minimum
26 FF 00	Logical Maximum
75 08	Report Size
95 40	Report Count
81 03	Input
09 00	Usage (Cnst,Var,Abs)
75 08	Report Size (Undefined)
95 40	Report Count
91 03	Feature
C0	End Collection

5.0 Command / Response Communications

The command/response protocol uses the following format:

```
<02> <Len_L> <Len_H> <Command Body / Response Body> <CheckLRC> <CheckSUM> <03>
```

Where:
<Len_L> <Len_H> is length of <Command Body / Response Body>
<CheckLRC> is LRC of <Command Body / Response Body> (exclusive OR of command body)
<CheckSUM> is SUM of <Command Body / Response Body> (8-bit sum of command body)

If Command has an error, the <Response Body> will be <NAK> with <Error Code>. The <Error Code> can be found in a later section of this document.

6.0 PIN Pad Task Commands

6.1 Get Encrypted PIN

1. Get Encrypted PIN with DUKPT Key under Triple DES or Single DES mode using Plaintext PAN (Primary Account Number):
Command Body is 75 46 07 01 & 16 bytes ASCII (Plaintext PAN)
Response Body:
06 + 20 ASCII code KSN + 16 ASCII code Encrypted PIN block

2. Get Encrypted PIN with MKSK using Plaintext PAN:
Command Body is 75 46 07 00 & 16bytes ASCII (Plaintext PAN)
Response Body: 06 + 16 ASCII code Encrypted PIN block

3. Get Encrypted PIN with DUKPT Key under Triple DES or Single DES mode using Encrypted PAN:
Command Body is 75 46 07 11 & 24bytes data (Encrypted PAN)
Response Body:
06 + 20 ASCII code KSN + 24 ASCII code Encrypted PIN block

4. Get Encrypted PIN with MKSK using Encrypted PAN:
Command Body is 75 46 07 10 & 24 bytes data (Encrypted PAN)
Response Body: 06 + 24 ASCII code Encrypted PIN block

Note

- Wait 3 Minutes (max); the Pin Len default is 4~12
- Per 20 seconds, if the PIN length was not zero, the PIN would be clear, and SmartPIN K100 Sends "C"
- While you press numeric key, SmartPIN K100 Sends "*"
- While you press Backspace key, SmartPIN K100 Sends "B"
- While you press Cancel key, SmartPIN K100 Sends "C"
- If Get Encrypted PIN using Plaintext PAN:
    - If the Plaintext PAN is error, response 15 07 02
- If Get Encrypted PIN using Encrypted PAN:
    - If there is not BDK of Pairing MSR Key, response 15 07 00
- If there is BDK of Pairing MSR Key, but not implement Pairing successfully, response 15 07 01
- If implemented Pairing successfully, but the Encrypted PAN is error, response is 15 07 02
- If there is Internal Account (from MSR), according to there is PIN DUKPT Key or not, the command is valid or response 15 04 00

15 07 00 –No BDK of Pairing MSR Key
15 07 01 – Have BDK of Pairing MSR Key, Not Pairing with MSR (No PAN Encryption Key)
15 07 02 – PAN is Error
15 07 03 – Pairing Failed
15 07 04 –MSR Pairing Key Other Error

6.2 Get Numeric Entry

Command Body is 75 46 08

Wait 3 Minutes, The Pin Len default is 1~16
While you press numeric key, SmartPIN K100 Sends numeric value: ASCII 0x30 through 0x39 (zero to 9) as appropriate.
While you press CLR (backspace) key, SmartPIN K100 Sends "B" (0x42).
While you press Cancel key, SmartPIN K100 Sends "C"
While you press Enter key, SmartPIN K100 Sends the entire accumulated keyed-in sequence. For example, if the keyed-in sequence was 0-1-2-3-4-5-6-7-8-9, the device will respond to Enter with:

020b0006**30313233343536373839**071303

The data (shown above in **boldface**) contains ASCII 0x30 through 0x39.

6.3 Get Function Key

Command Body is 75 46 0B

Wait 3 Minutes
While you press Back key, SmartPIN K100 Sends "B"
While you press Cancel key, SmartPIN K100 Sends "C"
While you press Enter key, SmartPIN K100 Sends "E"
While you press # key, SmartPIN K100 Sends "#"
While you press * key, SmartPIN K100 Sends "*"
While you press ? key, SmartPIN K100 Sends "?"

6.4 Get All Key

Command Body is 75 46 28

This commands allows echoing any key.

Wait 3 Minutes
While you press 0~9 key, PIN pad Sends "0~9"
While you press * key, PIN pad Sends "*"
While you press # key, PIN pad Sends "#"
While you press ? key, PIN pad Sends "?"
While you press Back key, PIN pad Sends "B"
While you press Cancel key, PIN pad Sends "C"
While you press Enter key, PIN pad Sends "E".

6.5 Cancel Command

Command Body is 75 46 09
Note: Cancel "Get Fun key" & "Get Encrypted PIN" & "Get Numeric Entry"

Response Body is always 15 18 00

6.6 Beeper Control

1. Beeper on/off
Command Body is 75 46 01 01 <On/Off>
<On/Off> - 0x00: Off
- 0x00: On
2. Beeper frequency and duration
Command Body is 75 46 01 02 <Fre1> <Fre2> <Fre3> <Fre4> <Dur1> <Dur2> <Dur3> <Dur4>

<Fre1> <Fre2> is the first and second nibble for the first byte of frequency.
<Fre3> <Fre4> is the first and second nibble for the second byte of frequency.
If the frequency is 1000Hz (0x03E8), <Fre1> <Fre2> <Fre3> <Fre4> will be 0x45 0x38 0x30 0x33.

<Dur1> <Dur2> is the first and second nibble for the first byte of duration.
<Dur3> <Dur4> is the first and second nibble for the second byte of duration.
If the duration is 200ms (0x00C8), <Fre1> <Fre2> <Fre3> <Fre4> will be 0x43 0x38 0x30 0x30.
duration need be more than 16ms and less than 65535ms.

If Beeper is Off, response is15.
If Beeper is On:
If frequency is correct, response is 06.
If frequency is incorrect, response is 15.

6.7 Get Model Number

Command Body is 75 46 0A

Response Body is 06 & IDPA-902000 (RS232) Or
Response Body is 06 & IDPA-905000 (USB-HID)

6.8 Get Key Status

Command Body is 78 46 25
Response Body:
06 <Block Length> <KeyStatusBlock1> <[KeyStatusBlock2]> …<[KeyStatusBlockN]>, Or
15 <Error Code>

Where:

- <Block Length> is 2 bytes, format is Len_L Len_H, is KeyStatusBlock Number
- <KeyStatusBlockX> is 4 bytes, format is <Key Index and Key Name> <key slot> <key status>:
    - <Key Index and Key Name> is 1 byte. Please refer to following table and <80000426-001 KeyNameIndex Database – V51.xls>
    - <key slot> is 2 bytes. Range is 0 – 9999
    - <key status> is 1 byte.
        - 0 – Not Exist
        - 1 – Exist
        - 0xFF – (Stop. Only Valid for DUKPT Key)

Key Index and Key Name Table

KeyNameIndex	**Key Name**	**Value**	**Key Slot**
0x14	LCL Key Encryption Key (Master Key or KEK)	0x14	LCL Key Encryption Key (Master Key or KEK)
0x01	PIN DUKPT Key	0x01	PIN DUKPT Key

0x0C	RKI-KEK DUKPT Key	0x0C	RKI-KEK DUKPT Key
0x08	PIN Master Key	0x08	PIN Master Key
0x0D	Pairing BDK Key(PINPAD)	0x0D	Pairing BDK Key(PINPAD)

6.9 Get Real Time

Command Body is 75 46 51
Response Body is 06 + Year/Month/Date Hour:Minute:Second

6.10 Get all Fix/Removal Records

Command Body is 75 46 52
Response Body is 06 + <Records Number> (<Record Block>…)
Where:

- <Records Number> is Number of Record Block. If it is 0, there is no <Record Block>
- <Record Block> has the following format of <UserID> <State> <-> <4 bytes Year> <2 bytes Month> <2 bytes Date> <-> <2 bytes Hour> <2 bytes Minute> </>
- Where:
  - <UserID> is 0x31 (User1) or 0x32 (User2)
  - <State> is 0x30 (Fix) or 0x31 (Removal)
  - Year, Month, Date, Hour, and Minute need be ASCII code.

Note:
The Max Records is 20.
After response this command, all Records are deleted.

6.11 Set PIN Length

Command Body is 75 53 01 01 02 MinLen MaxLen

Response Body is 06

MinLen need be 4~12
MaxLen need be 4~12
MinLen need be same or less than MaxLen

6.12 Get PIN Length

Command Body is 75 52 01 01

Response Body is 06 75 01 01 02 MinLen MaxLen

7.0 General Task Commands

7.1 Restart Command

Command Body is 78 46 49

Response Body is 06

7.2 Get Firmware Version

Command Body is 78 46 01 – Get Release Version

Response Body is 06 & some bytes ASCII codes

7.3 Enter into Bootloader

Command Body is 78 46 7A 49 52 46 57 00 00 00 00 00 00 00 00

Response Body is 06 - Device has the function, Or
15 – Device does not have the function.

7.4 Activate Fix Device (via Password)

The K100 incorporates anti-tamper features that must be activated via passwords. PCI requirements stipulate that two users, with two different passwords, should have to work in concert to remove/replace/relocate an in-service keypad. This section, and the section following this one, explains how to activate the K100's anti-tamper functionality, and how to remove/replace/relocate the device (for maintenance) after anti-tamper functionality has been enabled.

To activate anti-tamper functionality once the unit is in place (securely mounted, with anti-tamper buttons along the left and right edges of the housing depressed):

Step1. Power On device, after device beeps **Normal Tone**, please press **Cancel**, **Back**, **Enter**, **Help**, **Back**, and **Enter** key (6 keys). The interval between the two keys need be at most 5 seconds.

- If Log of Fix and Removal is full, Device Beeps **Invalid Tone** and quit “Want Fix / Removal Device State”.
- If there is at least a Default Activation Password in device.
  - Device enters into “Want Fix / Removal Device State”.
  - Device beeps always, the User need modify passwords. Please do Step2
- If there are two User Activation Passwords in device.
  - Device beeps **Normal Tone** and enters into “Want Fix / Removal Device State”.
  - The User can press password.

Step2. Modify Activation passwords

- One Default Activation Key Password is 123456. Another Default Activation Key Password is 654321. All passwords need be numeric key.

- The process is:
  - Step2.1 Press Default Loading Key Password once and device will beep **Complete Tone**. (If the first numeric key is pressed, Device will stop Always beeps).
  - Step2.2 Press New Password first times, and device will beep **Complete Tone**. (New Password need not be same as Default Loading Key Password.)
  - Step2.3 Press New Password second time, and device will beep **Complete Tone**.
  - If the password is modified successfully, Device beeps **Complete Tone** and the New Password is a User Loading Key Password.
- If another Password is Default Loading Key Password, beeper will beep always. Then User need not Re-Power on device (unplugging device) and can do above Process (Step2.1 ~ Step 2.3) to modify another Default Password.
- If 2 Password all be modified to User Activation Password; device quits “Want Loading Key State”.
- Interval limits:
  - The Interval between Password1 and Password2 is 20 seconds.
  - The Interval between the two keys of a password is 10 seconds.
- Any key will have a short tone to be the acknowledgement tone.

Step3. Press User Activation Key Password

- If the User presses 2 User Loading Key Passwords
  - A User Password is pressed correctly, Device beeps **Normal Tone**
  - Another User Password is pressed correctly, Device beeps **Normal Tone**
- Device confirms 2 User Passwords correct:
  - If Device is not Fixed and **IN Removal State**: Device beeps **Device is Removal Tone** and quit “Want Fix / Removal Device State”.
  - If Device is Fixed and **IN Removal State**: Device beeps **Complete Tone**, **Active Fix Device** successfully, save 2 Records for Active Fixed Device, and quit “Want Fix / Removal Device State”.
  - If Device is Fixed and **IN Fixed State**: Device beeps **Device IN Fixed State Tone** and quit “Want Fix / Removal Device State”.
- If the User presses at least an incorrect User Activation Password, Device beeps **Invalid Tone** and the User can presses again.
- If the User presses incorrect User Activation Password 3 times, Device beeps **Invalid Tone** and Suspend 3 Minutes. After Device finished suspend, Device quit “Want Fix / Removal Device State”.
- Interval:
  - The Interval between Password1 and Password2 is 2 Minutes.
  - The Interval between the two keys of a password is 10 Seconds.

7.5 Activate Removal of Device (Legally, via Password)

Step1. Power On device, after device beeps **Normal Tone**, please press **Cancel**, **Back**, **Enter**, **Help**, **Cancel**, and **Help** (6 keys). The interval between the two keys need be at most 5 seconds.

- If Log of Fix and Removal is full, Device Beeps **Invalid Tone** and quit “Want Fix / Removal Device State”.
- If there is at least a Default Activation Password in device.

    - Device enters into “Want Fix / Removal Device State”.
    - Device beeps always, the User need modify passwords. Please do Step2
- If there are two User Activation Passwords in device.
    - Device beeps **Normal Tone** and enters into “Want Fix / Removal Device State”.
    - The User can press password.

Step2. Modify Loading Key passwords

- One Default Loading Key Password is 123456. Another Default Loading Key Password is 654321. All passwords need be numeric key.
- The process is:
    - Step2.1 Press Default Loading Key Password once and device will beep **Complete Tone**. (If the first numeric key is pressed, Device will stop Always beeps).
    - Step2.2 Press New Password first times, and device will beep **Complete Tone**. (New Password need not be same as Default Loading Key Password.)
    - Step2.3 Press New Password second time, and device will beep **Complete Tone**.
    - If the password is modified successfully, Device beeps **Complete Tone** and the New Password is a User Loading Key Password.
- If another Password is Default Loading Key Password, beeper will beep always. Then User need not Re-Power on device (unplugging device) and can do above Process (Step2.1 ~ Step 2.3) to modify another Default Password.
- If 2 Password all be modified to User Activation Password, device quit “Want Loading Key State”.
- Interval:
    - The Interval between Password1 and Password2 is 2 Minutes.
    - The Interval between the two keys of a password is 10 Seconds.
- Any key will have a short tone to be acknowledged tone.

Step3. Press User Activation Key Password

- If the User presses 2 User Loading Key Passwords
    - A User Password is pressed correctly, Device beeps **Normal Tone**
    - Another User Password is pressed correctly, Device beeps **Normal Tone**
- Device confirms 2 User Passwords correct:
    - If Device is Fixed and **IN Fixed State**: Device beeps **Complete Tone**, **Active Removal Device** successfully**,** save 2 Records for Active Removal Device, and quit “Want Fix / Removal Device State”. Then device can be removal legally and secure data are not erased.
    - If Device is Fixed and **IN Removal State**: Device beeps **Device IN Removal State Tone** and quits “Want Fix / Removal Device State”.
- If the User presses at least an incorrect User Activation Password, Device beeps **Invalid Tone** and the User can presses again.
- If the User presses incorrect User Activation Password 3 times, Device beeps **Invalid Tone** and Suspend 3 Minutes. After Device finished suspend, Device quits “Want Fix / Removal Device State”.
- Interval:
    - The Interval between Password1 and Password2 is 2 Minutes.
    - The Interval between the two keys of a password is 10 Seconds.

8.0 RS232 Task Commands

8.1 Note

1. If the device is connected with RS232 Cable, the settings will be saved in system and be valid after it response ACK to host.
2. If the device is connected with USB Cable, the settings only be saved in system and be valid when the device is connect with RS232 Cable.

8.2 Set BaudRate

Command Body is 70 53 01 41 01 ASCIIChar

BaudRate	ASCIIChar
2400	2
4800	3
9600	4
19200	6
38400	7
115200	9

Response Body is 06

8.3 Get BaudRate

Command Body is 70 52 01 41

Response Body is 06 70 41 01 ASCIIChar

8.4 Set Parity

Command Body is 70 53 01 43 01 ASCIIChar

Parity	ASCIIChar
None	0
Odd	1
Even	2

Response Body is 06

8.5 Get Parity

Command Body is 70 52 01 43

Response Body is 06 70 43 01 ASCIIChar

8.6 Set StopBits

Command Body is 70 53 01 45 01 ASCIIChar

StopBits	ASCIIChar
1	1
2	2

Response Body is 06

8.7 Get StopBits

Command Body is 70 52 01 45

Response Body is 06 70 45 01 ASCIIChar

9.0 Error Codes

Error Code	Definition
0x0100	Log (Removal / Fix) is full
0x0300	Key Type (DES/TDES) of Session Key is not same as the related Master Key
0x0400	Related Key was not loaded
0x0401	Related Key was not loaded
0x0500	Key Same
0x0700	No BDK of Pairing MSR Key
0x0701	Have BDK of Pairing MSR Key, Not Pairing with MSR (No PAN Encryption Key)
0x0702	PAN is Error
0x0703	Pairing Failed
0x0704	MSR Pairing Key Other Error
0x0D00	This Key was loaded
0x0E00	Base Time was loaded
0x1800	Send "Cancel" command after send "Get Fun key" & "Get Encrypted PIN" & "Get Numeric"
0x1900	Press "Cancel" key after send "Get Fun key" & "Get Encrypted PIN" & "Get Numeric"
0x30FF	Security Chip is not connect
0x3000	Only Security Chip is deactivation for No Secure data. (Unit is In Removal Legally State)
0x3001	Only Security Chip is deactivation for ST Chip Firmware Check Error. (Unit is In Removal Legally State)
0x3002	Only Security Chip is deactivation for Security Chip Firmware Check Error. (Unit is In Removal Legally State)
0x3003	Only Security Chip is deactivation for Illegally Removal.
0x3101	Security Chip is activation. (Unit is In Removal Legally State)
0x5500	No RKI-KEK DUKPT Key
0x5501	RKI-KEK DUKPT Key STOP
0x5502	RKI-KEK DUKPT Key KSN is Error
0x5503	Get Authentication Code1 Failed
0x5504	Validate Authentication Code Error
0x5505	Encrypt Or Decrypt data failed
0x5506	Not Support the New Key Type
0x5507	New Key Index is Error
0x5508	Step Error

0x550F	Other Error
0x6000	Save or Config Failed / Or Read Config Error
0x6200	No Serial Number
0x6900	Invalid Command - Protocol is right, but task ID is invalid
0x6A00	Unsupported Command - Protocol and task ID are right, but command is invalid
0x6B00	Unknown parameter in command - Protocol task ID and command are right, but parameter is invalid
0x7200	Device is suspend (MKSK suspend or press password suspend)
0x7300	PIN DUKPT is STOP (21 bit 1)
0x7400	Device is Busy
0x8100	Timeout for "Get Fun key" & "Get Encrypted PIN" & "Get Numeric"

NOTES

- If Security Chip is not connect, Response Body is 15 30 FF
- If Security Chip is de-activation for No Secure data (Unit is In Removal Legally State), Response Body is 15 30 00
- If Security Chip is de-activation for ST Chip Firmware Check Error (Unit is In Removal Legally State), Response Body is 15 30 01
- If Security Chip is de-activation for Security Chip Firmware Check Error (Unit is In Removal Legally State), Response Body is 15 30 02
- If Security Chip is de-activation for Illegally Removal, Response Body is 15 30 03
- If Security Chip is activation (Unit is In Removal Legally State), Response Body is 15 31 01

- If Public Key is not loaded, while receiving below Commands, Response Body is 15 04 00
  - Load Firmware Key
  - Load Numeric Key
  - Load ST Chip Check Value
  - Load MAXQ Chip Check Value
- If Public Key is loaded, while receiving Load Public Key Command, Response Body is 15 0D 00

- If Firmware Key is not loaded, while receiving below Command, Response Body is 15 04 01
  - Load ST Chip Check Value
  - Load MAXQ Chip Check Value
- If Firmware Key is loaded, while receiving Load Firmware Key Command, Response Body is 15 0D 00

- If Firmware Check Value is loaded, while receiving Load Firmware Check Value Command, Response Body is 15 0D 00

- If Base Time was loaded, while receiving Load Base Time Command, Response Body is 15 0E 00

- If have not related Master Key after send “Load Session Key”, Response Body is 15 04 00

- If have not DUKPT Key after send "Get Encrypted PIN with DUKPT Key", Response Body is 15 04 00
- If have not MKSK Key after send "Get Encrypted PIN with MKSK", Response Body is 15 04 00

- If the type of Session Key is not same as related Master Key after send “Load Session Key”, Response Body is 15 03 00

- If timeout for "Get Fun key" & "Get Encrypted PIN" & "Get Numeric", Response Body is 15 81 00
- If Send "Cancel" command after send "Get Fun key" & "Get Encrypted PIN" & "Get Numeric", Response Body is 15 18 00
- If press "Cancel" key after send "Get Fun key" & "Get Encrypted PIN" & "Get Numeric", Response Body is 15 19 00

- If device check keys sequence to enter Key Loading Status or Fix / Removal Device Status, response 15 74 00 for any tasks commands. If Host receives this response, please wait some seconds before sending command.

- While any key is loading, it should be compared to other secure key according to the specification in ‘Key Compare Spec.doc’ file. If the same situation is occurring, device response is 15 05 00 and it will stop the loading process.