80141505-001

User Manual

SmartPIN L100

Rev. B

Revised: 8/26/2016

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.

Revision History

Revision	Description and Reason for Change	Date	By
A	Release to Production	6/3/2016	JH
B	Removed certain items, clarified MTBF.	8/26/2016	JH, KT

TABLE OF CONTENTS1 ..... INTRODUCTION 6

1 Introduction

ID TECH's SmartPIN L100 provides a compact, rugged, secure keypad interface for POS systems in which PIN and/or manual-entry capability are required. The device's 16-key layout and built-in LCD make it ideal for kiosks and other unattended applications. When paired with ID TECH's Spectrum Pro insert reader, the SmartPIN L100 provides a complete, EMV-ready chip-and-PIN, chip-and-signature, debit/PIN, and MSR solution that meets ADA, ANSI, and ISO standards for PIN Entry Devices.

For development of applications that communicate with the SmartPIN L100, please ask your ID TECH representative about the ID TECH Universal SDK for L100 (Windows), which contains libraries (DLLs), C# source code, a demo app, and documentation for a C# API on Windows. By using the Universal SDK (which also works with other ID TECH products, such as the Spectrum Pro insert reader), you can save time developing host applications that talk to the L100 via USB or RS-232 and take advantage of many convenience methods (including encryption libraries) exposed via the high-level-language API.

Low-level access to L100 via firmware commands can be achieved via USB-HID or RS-232 (serial connection). This manual documents the various low-level commands that can be used to control the L100 and provides essential information you'll need for establishing a serial connection to the device.

2 Features

- PCI 4 certified
- 4 x 4 key layout (0-9, *, #, Cancel, Clear, Enter, Blank), plus 64x128-pixel liquid crystal display
- 3 function keys adjacent to the LCD
- One tri-color LED on the back of the unit to display unit status

- Meets ADA, ANSI, and ISO standards for a PIN Entry Device
- Audio feedback
- Size and mounting compatible with (mechanical drop-in replacement for) Hypercom Artema Compact and the Verifone UX100
- Built-in gasket for watertight mounting
- IP65 rated for dust and water resistance
- IK09 rated for intrusion resistance
- Removal Detection and tamper-resistant
- Secure schemes for authorized activation, installation, and injection of keys
- Low power consumption when PIN pad is in sleep mode
- Support for TDES encryption
- Master/Session & DUKPT key management
- Spectrum Pro (standard version) and L100 (standard version) can work either as two standalone products or be paired together (no special CA certification download required)
- Supports multiple key slots, using the same key storage hardware and firmware design in Spectrum Pro, which can store fifteen (15) DUKPT keys and twelve (12) 2048-bit RSA public keys as X.509 certificates
- Encrypted text and clear text entry
- RoHS and REACH compliant
- 1 year manufacturer warranty
- Minimum 2,000,000 keystroke operations
- Meets Interac standard for Canadian Market
- When connected to ID TECH Spectrum Pro, supports full functions required by Spectrum Pro, such as Mutual Authentication with Host through Spectrum Pro, Remote Key Injection through Spectrum Pro, Firmware Download through Spectrum Pro, Key Pairing (for both PIN Debit and Chip & PIN), etc.
- Firmware is easily upgraded in the field via the serial communication interfaces

3 Applicable Documents

ISO/IEC 7813 – Identification cards, Physical Characteristics
ISO/IEC 7811 – Identification cards, Recording Techniques, Magnetic Stripe

4 Abbreviations

ANSI	American National Standard Institute
APACS	Association for Payment Clearing Service
API	Application Programming Interface
CPU	Central Processing Unit
DC	Direct Current
DES	Data Encryption Standard
DUKPT	Derived Unique Key Per Transaction, Key management
EMI	Electromagnetic Interference

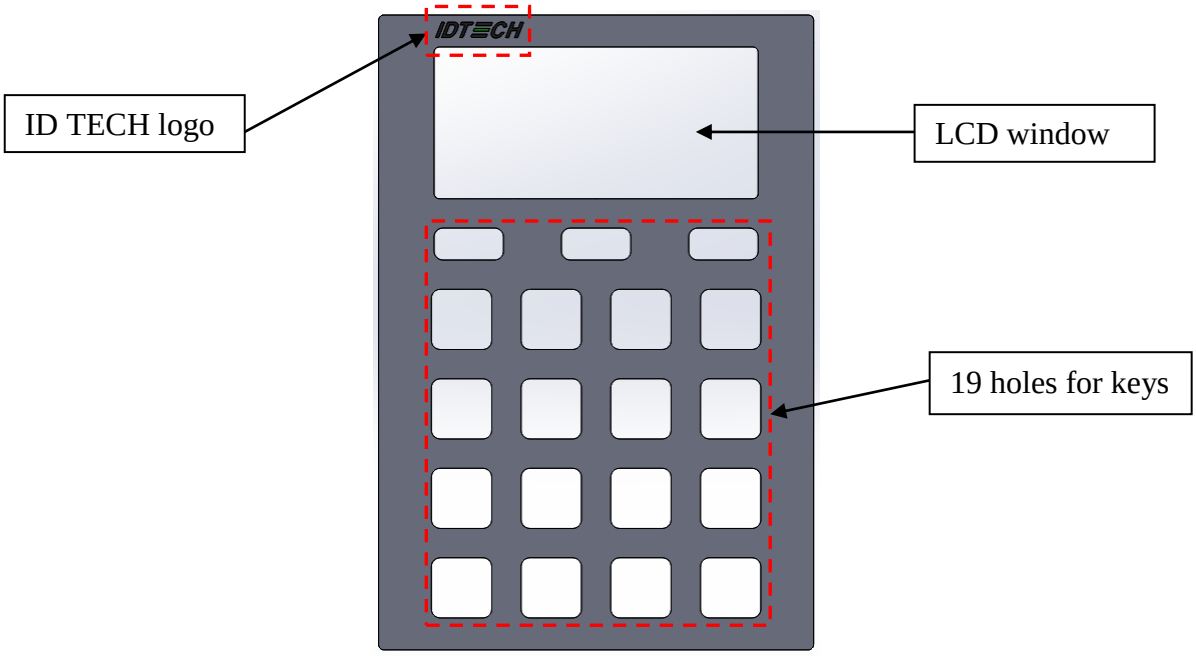
EMV	Europay, MasterCard, Visa
ESD	Electrostatic Discharge
GND	Signal Ground
Host	A PC or like device with local Application Software for controlling connected SmartPAY terminals
IEC	International Electrical Congress
ISO	International Organization for Standardization
JPOS	Java for Retail Point-of-Sale
KSN	Key Serial Number
LCD	Liquid Crystal Display
mA	MilliAmperes
MAC	Message Authentication Code
MK/SK	Master Key/Secession Key, Key management
MTBF	Mean Time Between Failures
mV	MilliVolts
OPOS	OLE for Retail Point-of-Sale
PC	Personal Computer or similar hardware device
PCB	Printed circuit board
PCI	Payment Card Industry
PED	PIN Entry Device
PIN	Personal Identification Number
TDES	Triple Data Encryption Standard

5 Specifications

5.1 Components

5.1.1 Faceplate

Color: Silver gray
Finish: Brushed finish



5.1.2 LCD

There are four lines of 20 characters each in the liquid crystal display. With 128 dots to a character, this means there are 4*20*128 (or 10,240) dots in the LCD.

One tri-color LED on the back of the unit to display unit status

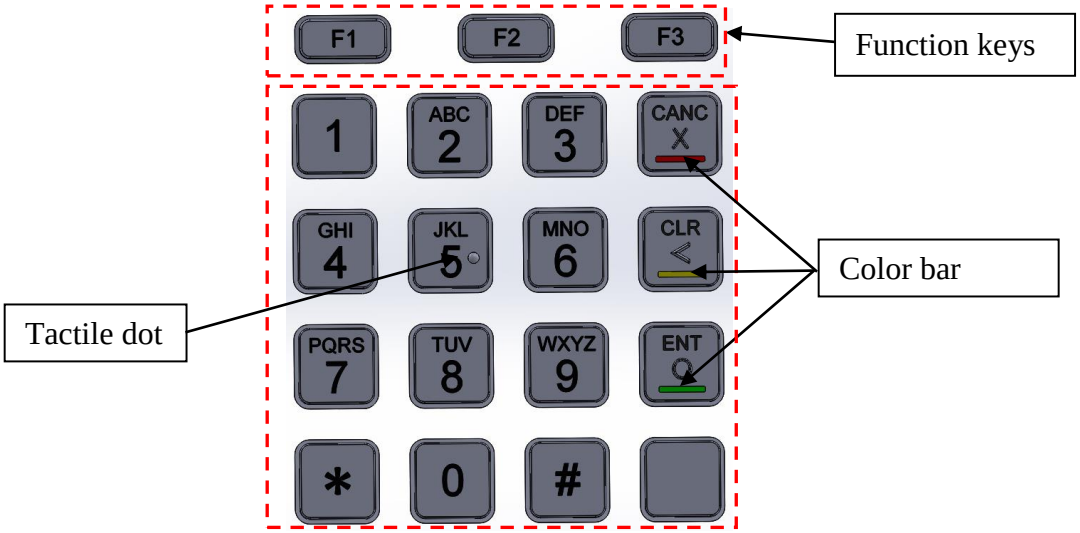
5.1.3 LED

There is one tri-color (red, yellow, green) LED on the back of the unit to display unit status. Looking at the back of the L100, with the top (LCD end) up, the LED is just to the left of the DB-9 connector opening.

Any given color of LED light can have multiple meanings, depending on the context; for details, see the table under **LCD & Beeper State from Deactivation State to Activation State** further below.

5.1.4 Keys

Color: Silver gray
Finish: Brushed finish
Layout: Alphabetical characters printed on the keys
Operation keys have engraved, colored bar and symbols: Cancel (red), Clear (yellow), Enter (green)
3 Function Keys are etched or engraved with “F1” “F2” and “F3” respectively
Tactile identifier on the numeral key 5
Meets ADA standard (which requires embossed symbols to be between 0.6 and 0.9 mm in height).



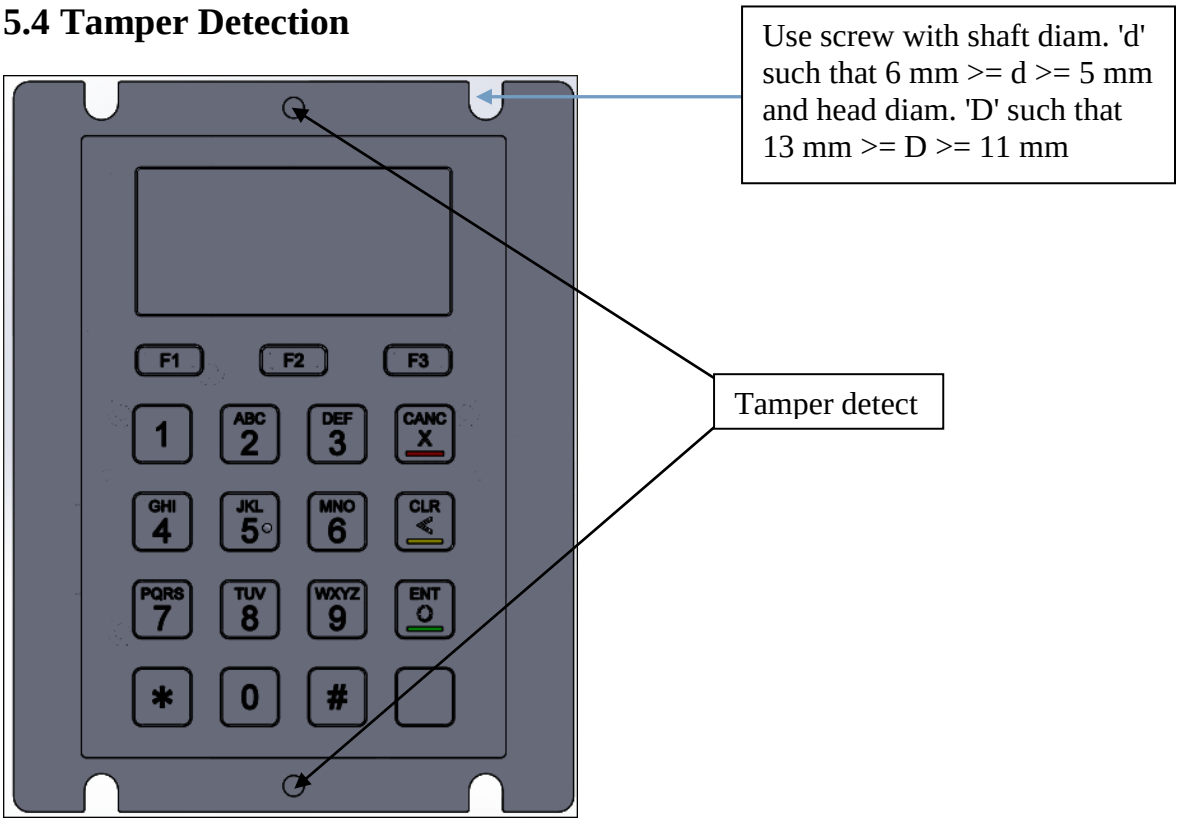
5.2 Size & weight

Size: 107.5 mm *140 mm *29 mm
Weight: 526 g

5.3 Mounting

Use the provided cutouts to mount the device using standard #10 screws or equivalent (shaft diameter 5 mm or 0.19 inch). Note: The head of the screw should be greater than 11 mm, less than 13 mm. For best results, use a washer (with outside diameter greater than 0.43 in. or 11 mm, less than 0.5 in. or 13 mm) under the screw head.

5.4 Tamper Detection



5.5 Drop Test

Unit can withstand 4-ft drop to concrete on 6 surfaces and 4 corners (3 cycles) with no damage and still maintain functionality.

5.6 Dust and Water Resistance

All front face components are designed for direct liquid spray, and/or splashed or spilled liquids. The unit passes IP65 ratings.

5.7 Salt spray test

Faceplate, metal keys, mounting plate pass the salt spray test.

5.8 IK Test

The front face is impact resistant to meet IK9 rating (10 joules of impact energy, equivalent to dropping a 5kg object from 20 cm height).

5.9 Key Life

The L100 is designed for a minimum of 2,000,000 keystroke operations per key.

6 Electronic Design

6.1 Power Supply

The SmartPIN L100 is able to support 3 different modes:
RS232 – Requires power supplied by an external A/C power adapter (5VDC).
UART - RJ45 cable connecting directly to the Spectrum Pro insert reader, also requires an external A/C power adapter (5VDC)
USB – Connected directly to the host which will provide power through the USB interface

6.2 USB - Power supplied through USB port Power Management

**why is the background gray?
Power management includes several parts
1. System voltage supply
   - An LDO chip is used to convert 5V external voltage to 3.3V, which is the common voltage for all chips and components used in this device.
2. Battery
   - A battery supplies the power for the SRAM to keep the keys in storage.

6.2.1 Low Power Mode

**Under USB section?
In low power mode, voltage of all peripherals is cut off and could be woken up by key press and communication from PC.

6.3 Reliability & Environmental

MTBF：425010 hrs
（FR=2352 FITs, BasicR=0.979）
FR is failure rate. FITs, which is failures per billion hours.
MTBF, the Mean Time between Failures, in hours.
BasicR (Reliability), the probability that the circuit, taken as a purely Serial configuration, will operate without failure for the mission time. For example, if the BasicR = 0.837438, then the circuit has a probability of 0.837438 (or 83.74%) of working without a failure for the mission time duration.

6.3.1 Electro-Static Discharges (ESD)

The electronics can survive electrostatic discharges of 6kV contact, and 12kV air discharge, per ID TECH ESD testing procedure, with no loss of communications.

Environmental Temperature range:

Operating	-25 to 70° C	(-13 to 158° F) [non-condensing]
Storage	-30 to 80° C	(-22 to 176° F) [non-condensing]

Relative humidity
Maximum 95% (non-condensing)

6.4 Agency Certifications

FCC CLASS B & CE
PCI 4.1

7 Base Functionality

7.1.1 PIN Pad function

- PIN MK/SK, DUKPT Key Management
- TDES Encryption (keystrokes are not sent in the clear)
- 4 x 4 key layout with 0-9 numerical keys, *, #, Cancel, Clear, Enter, Blank, and 3 additional Function keys adjacent to the bottom of the LCD screen: F1, F2, F3 (function defined by application)
- Supports clear text entry
- PCI-PTS 4.x certified

7.1.2 Interface function

- USB-HID and RS232 interfaces connect via one DB9 connector on the back of the PIN pad that plugs into the appropriate interface cable.
- The unit supports both USB-HID and RS232 interfaces for the regular host.

RS232 :

- Baud rates supported: 2400, 4800, 9600, 19200, 38400, 115200 bps
- Data bits: 8
- Parity: Odd, Even, or None
- The COM default settings are initialized to: 38400, 8, 1, & None

USB-HID:

- PID: 0x1050
- VID: 0x0ACD

7.1.3 Key injection function

- Compatible with FutureX SKI 9000 HSM for PIN Key Injection.
- Can communicate with HSM using the key injection protocol for unattended products.

7.1.4 Low-Power Modes

Sleep Mode

While RS232 interface is used, Sleep Mode is controlled by a timeout , after the unit is idle for a specified time (default is 120s).While USB interface is used， Sleep Mode is controlled by the suspend signal and resume signal of USB. Sleep Mode is used for battery-operated and solar-powered systems. It reduces power consumption to a much lower level (1 mA USB, 8 mA RS232) than full-power mode (200 mA), but leaves the device capable of being woken up by key press or communication from the host.

Stop Mode (20 µA)

Stop Mode is controlled by the application through a specific command. Stop Mode reduces power consumption to the lowest possible level (20 µA). A unit in Stop Mode can only be woken up by a physical key press.

7.1.5 Bootloader function

The firmware can be upgraded via USB/RS-232 port (Baud rate is 115200).
For detailed information, please refer to document P/N 80000420-001, *Bootloader Firmware Specification (V52).doc*.

7.2 NGA Commands & Responses format

Device uses NGA protocol commands and responses in general communication. The format is as below.

<STX> <Len_Low><Len_High> <Command Body / Response Body / Notification Body> <CheckLRC> <CheckSUM> <ETX>

Where:

- <STX> is 0x02 and <ETX> is 0x03
- <Len_Low><Len_High> is length of <Command Body / Response Body / Notification Body>
- <CheckLRC> is LRC (8-bit XOR) of all data bytes in <Command Body / Response Body / Notification Body>
- <CheckSUM> is SUM (8-bit SUM) of <Command Body / Response Body / Notification Body>
- Response Body is <Response Status> + [<Response Data>]
  - <Response Status>: status of the response. 1 byte.
    NAK: 0x15
    ACK: 0x06
  - <Response Data>: main response string.
    - If <Response Status> is ACK: More bytes needed.
    - If <Response Status> is NAK: Response data is Error codes (2 bytes).

Next section lists <Command Body>, <Response Body>, and <Notification Body> detailed.

7.3 LCD & Beeper State & LED

7.3.1 Note

Item	Define
Device is in a Deactivation State	Tamper Switch Or Battery Error
Important Data - No	At least one of Public Key, Firmware Key , Check Value, and/or Numeric Key was not loaded
Important Data - Have	Loaded Public Key, Loaded Firmware Key, Loaded Check Value, and Loaded Numeric Key

7.3.2 LCD & Beeper State from Deactivation State to Activation State

PK – Public Key (Manufacture Key)
FK – Firmware Key
NK – Numeric Key
CV – Check Value
DTV – Date & Timer Value

Device State	Definition	LCD Display Message	Beeper State	LED auxiliary indicator
Deactivation	Device - Removal Security Chip - De-activation No **PK**, **FK**, **CV**, **NK**, and **DTV**	Line0: Fatal Error Other line: Battery/SDI1/SDI2/ Other Other lines are used to describe the cause to de-activation	Always beeping, quick	Steady Red
Load Important Data State	Device - Removal Activation Need Load PK, FK, CV, NK, and DTV	Load Check Value &Related Key	Always beep(slow)	Steady Red
Activation1	Activation **PK**, **FK**, **CV**, **NK**, and **DTV** are loaded successfully No DUKPT Key or Master Key	Ready	Not beeping	If not set user passwords: Blink Yellow If set user passwords: If legally Removal State: Steady Yellow If legally Install State: Steady Green
Load Key	Activation	Refer to	Refer to Key	If not set user

State	**PK**, **FK**, **CV**, **NK**, and **DTV** are loaded successfully Want load DUKPT Key or Master Key	XX DUKPT Key Loading … Master Key Loading…	Loading Note	passwords: Blink Yellow If set user passwords: If legally Removal State: Steady Yellow If legally Install State: Steady Green
Suspend for Get PIN	Activation **PK**, **FK**, **CV**, **NK** and **DTV** are loaded successfully GET PIN more than 120 times /hour by MKSK	Line0: SUSPEND Other lines: Get PIN Other lines are used to describe the cause to suspend	Not beeping	If not set user passwords: Blink Yellow If set user passwords: If legally Removal State: Steady Yellow If legally Install State: Steady Green
Activation2	Activation **PK**, **FK**, **SCV**, **NK**, and **DTV** are loaded successfully At least DUKPT Key or MKSK is loaded successfully	Ready	Not beeping	If not set user passwords: Blink Yellow If set user passwords: If legally Removal State: Steady Yellow If legally Install State: Steady Green

7.3.3 Other LCD State for PIN function

State	LCD Display Message	Note
Checking Firmware	Firmware Checking…	
Get Encrypt PIN	Line0:xxxxxxxx Line1:xxxxxxxx Line2:xxxxxxxx Line3:***……	
Get Numeric	Line0:xxxxxxxx Line1:xxxxxxxx Line2:xxxxxxxx Line3: xxxxxxxx…	The Message and Plaintext Numeric Display is defined by Command.

Get Numeric	Line0:xxxxxxxx Line1:xxxxxxxx Line2:xxxxxxxx Line3:***……	The Message and Star Display is defined by Command.
Suspend	Line0: SUSPEND Line1: PWD ERR	Removal Detection Password Error 3 times continuously
Modify default password	Please input one password ******** → Please input new password ******** → Please input new password again ******** → Please input another password ******** → Please input new password ******** → Please input new password again ********	Modify 2 groups default passwords to user passwords.
Input Removal Detection Enable/Disable user passwords	Please input one new password ******** Please input another new password ********	Enter 2 groups user psaawords.
State	LCD Display Message	Note
Checking Firmware	Firmware Checking…	
Get Encrypt PIN	Line0:xxxxxxxx Line1:xxxxxxxx Line2:xxxxxxxx Line3:***……	
Get Numeric	Line0:xxxxxxxx Line1:xxxxxxxx Line2:xxxxxxxx Line3: xxxxxxxx…	The Message and Plaintext Numeric Display is defined by Command.
Get Numeric	Line0:xxxxxxxx	The Message and Star Display is

	Line1:xxxxxxxx Line2:xxxxxxxx Line3:***……	defined by Command.
Suspend	Line0: SUSPEND Line1: Get PIN	Get Encrypted PIN under MKSK more than 120 times in a hour
Modify default password	Please input one Please input new password Please input new password again Password1 → → ******** ******** ******** Please input another Please input new password Please input new password again Password2 → → ******** ******** ********	modify 2 groups default passwords to user passwords.
Input Removal Detection Enable/Disable user passwords	Please input one new password Password1 ******** Please input another new password Password2 ********	Enter 2 groups user psaawords.

7.3.4 Beeper Tone

Name	Tone Note
Normal Tone	beep tone once
Complete Tone	beep short tone 2 times
Invalid Tone	beep short tone 3 times

7.3.5 Keypad Note

F1	F2		F3
1	2	3	Cancel
4	5	6	Backspace
7	8	9	Enter
*	0	#	Blank

7.4 Device Operation Process

7.4.1 Activation/Removal of Device

7.4.1.1 Set User Activation/Deactivation password

**Change Help with Blank
The SmartPIN L100 comes with two default Removal Detection passwords that need to be reset with user-generated passwords before the Removal Detection feature can be activated. The following steps will instruct you how to set the passwords.

Step 1 Power up the PINPad. After the device beeps its **normal tone** and the LCD screen displays its version message, press **Cancel**, **Clear**, **Enter**, **Blank**, **Clear**, and **Enter** (6 keys) or **Cancel**, **Clear**, **Enter**, **Blank**, **Cancel,** and **Blank** (6 keys). The interval between keys cannot exceed 5 seconds.

If the Log of Fix and Removal full, the device will beep short tone twice – pause – short tone once and will quit the "Want Fix / Removal Device" state.

If two groups "User Activation Password" has already been set into the device. The device will beep once and will enter "Want Fix / Removal Device" state. User can skip section 1 or go to section 2 to active/deactive removal detection.

Step 2 Modifying Activation passwords
For the new unit comes from manufacture, the default Activation Key Password A is 12345678 and the other default Activation Key Password B is 87654321. All passwords need to be numeric.

Step 2.1 When the LCD screen displays "Please input one/another password", enter Default Password A (12345678) and the device will beeper its **complete.** (When the first numerical key is pressed, the device will stop beeping).
Step 2.2 When the LCD screen displays "Please input new password", enter new password 1. The device will beep short tone twice. (New passwords cannot be the same as the Default Loading Key Passwords.)

Step 2.3 When the LCD screen displays “Please input new password again”, re-enter new password 1 and the device will beep short tone twice.
If the password is modified successfully, the device beeps short tone twice and the new password 1 is now a user activation password.
Step 2.4 The PINPad will continue beeping. The LCD screen will display “Please input another password”. Then enter the default password B (87654321).
Step 2.5 When the LCD screen displays “Please input new password”, enter new password 2 for first times, and device will beep **short tone twice**. (New password cannot be the same as default password.)
Step2.6 When LCD displays “Please input new password again”, re-enter new password 2 and the device will beep short tone twice.

If two groups passwords have been modified to “User Activation Passwords” successfully, The LCD screen will display prompt message to enter section1 or section2 (needn’t re-enter key sequence and enter new passwords directly) according to the key sequence entered before.
If entry timeout, the device will quit the “Want Fix / Removal Device” state.
Time Intervals for Entry:
The interval between Password 1 and Password 2 can be no more than 20 seconds.
The interval between the two keys of a password can be no more than 10 seconds.
Any key will have a short tone to show registration.

7.4.1.2 Activate Removal Detection

Power the unit, and immediately after the device beep tone once and the LCD screen displays its version message, press **Cancel**, **Clear, Enter, Blank, Clear,** and **Enter** (6 keys). The interval between keys cannot exceed 5 seconds

Enter the password 1 which was set in the section 1. If the password 1 was entered successfully, the unit will beep twice.

Enter the password 2 which was set in the section1. If the password 2 was entered successfully, the unit will beep twice.

After the two passwords are entered correctly in two steps above, the LCD screen displays the menu as follows: to use “*” and “#”, select “Enable PINPAD” or “Enable CR”. Press “Enter” to confirm.

Select “Enable PINPAD” to activate removal detection of SmartPIN L100

If the PINPAD Device is not fixed and **IN Removal State**: PINPad will beep short tone twice- pause – short tone 3 times, and will quit “Want Fix / Removal Device” state.

If the PINPAD Device is fixed and **IN Removal State**: The device will beep short tone twice. It means the removal detection of PINPad is activated. The PINPad saves 2 records for Active Fixed Device, and will quit “Want Fix / Removal Device” state.

If the PINPAD Device is fixed and **IN Fixed State**: The device will beep short tone three times and quit “Want Fix / Removal Device” state.

Select “Enable CR” to active the removal detection of Spectrum Pro

If the PINPAD Device is not fixed or **IN Removal State**: The device will beep short tone twice – pause – short tone 3 times, and will quit “Want Fix / Removal Device” state.

If the user enters an incorrect User Activation Password, the device will beep short tone twice – pause- short tone once and then user need to re-enter password.

If the user presses incorrect User Activation Password 3 times, the device will beep its Invalid Tone and suspend for 3 minutes. After the device finishes suspension, the device will quit "Want Fix / Removal Device" state.

Interval limits:
The interval between Password 1 and Password 2 cannot be more than 2 Minutes.
The interval between the two keys of a password cannot be more than10 Seconds.

7.4.1.3 Deactivate Removal Detection

Power the unit and after the device beep tone once and the LCD screen displays its version message, press **Cancel, Clear, Enter, Blank, Cancel,** and **Blank**. The interval between keys cannot exceed 5 seconds.

Enter the password 1 which was set in the section 1. If the password 1 was entered successfully, the unit will beep twice.

Enter the password 2 which was set in the section1. If the password 2 was entered successfully, the unit will beep twice.

After the two passwords entered correct in two steps above, the LCD screen displays the menu as follows: to use "*" and "#", select "Disable PINPAD" or "Disable CR". Press "Enter" to confirm.

Select "Disable PINPAD" to deactive SmartPIN L100

If PINPAD Device is fixed and **IN Fix State**: Device beeps short tone twice. This means PINPad removal detection is deactivated successfully, save 2 records for Deactive Removal Device, and quit "Want Fix / Removal Device State". Now PINPad can be removed securely with no data erased.

If PINPAD Device is Fixed and **IN Removal State**: Device beeps **Device is Removal State Tone** and quit "Want Fix / Removal Device State".

Select "Disable CR" to deactive Spectrum Pro

If PINPAD Device is not fixed or **IN Removal State**: PINPad beeps short tone twice- pause- short tone 3 times, and quits "Want Fix / Removal Device" state.

If the user enters an incorrect User Activation Password, the device will beep short tone twice – pause- short tone once and then user need to re-enter password.

If the user enters the incorrect User Activation Password 3 times, the device will beep short tone twice – pause - short tone once, and suspend for 3 Minutes. After the device finishes suspension, the device will quit "Want Fix / Removal Device" state.

Interval limits:
The interval between Password 1 and Password 2 cannot be more than 2 minutes.
The interval between the two keys of a password cannot be more than 10 seconds.

7.4.2 Bootloader Detailed Process

7.4.2.1 Detailed Description

1. When device enters into Bootloader, device is in "Waiting State", and LCD Display "Bootloader…" is in Line 0. In this State, device only receives Get Version Command. The Response is Bootloader Version.

2. Device can receive Get Version command and all Data Blocks commands:

- If Device received Get Version command successfully, it should response "Bootloader" characters.
- If Device received a Data Block command successfully, it should verify the Block Data format, and versify Version and Signature.:
- If verification is OK, Device will Copy the Block Data into Application Area and response ACK.
- If verification is Error, response NAK with Error Code , then waiting for this block again. If one data block continuously failed 3 times, Device Erase all Application, and response NAK with Error Code, then waiting for the first data block in bootloader state.

If Bootloader Timeout (30 seconds), if the application is not modified, Device will return to old application; otherwise Device will Erase all Application and exist in Bootloader state.

7.4.2.2 Enter into Bootloader

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

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	0F	00	78 46 7A 49 52 46 57 00 00 00 00 00 00 00 00	4E	70	03
Output Hex String: 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.

7.4.3 PIN Pad and MSR Pairing Solution

7.4.3.1 Step1: Host sends Pairing MSR KSN from MSR device

Command Body is
75 46 10 00 + [20 bytes ASCII KSN]

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02		00	75 46 10 00 + [20 bytes ASCII KSN]			03
Output Hex String:						

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02	51	00	06 + [80 bytes TR-31 Block Version B Encrypted PAN Encryption Key], or 15 + failure information (see below)			03

Response Body:
06 + [80 bytes TR-31 Block Version B Encrypted PAN Encryption Key] or
15 07 00 – No BDK of Pairing MSR Key, Or
15 07 03 – Pairing Failed, Or
15 07 04 –MSR Pairing Key Other Error

Note:
BDK of Pairing MSR Key will generate a Pairing DUKPT Key according to the KSN.
PAN Encryption Key is a random number.
Encrypted PAN Encryption Key Array is encrypted by Pairing DUKPT Key.

7.4.3.2 Step2: The host passes the MAC to the PIN Pad

Command Body is
75 46 10 01 + [20 bytes ASCII KSN] +
[6 bytes ASCII MAC]

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02		00	75 46 10 01 + [20 bytes ASCII KSN] + [6 bytes ASCII MAC]			03

Response Body:
06 (Verify OK, PIN pad device save the new PAN Encryption Key) or
15 07 03 – Pairing Failed, Or
15 07 04 –MSR Pairing Key Other Error

7.4.4 General Group (Task)

7.4.4.1 Get Firmware Release Version

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	03	00	78 46 01	3F	BF	03
Output Hex String: 0203007846013fbf03						
Command Body is: 78 46 01						

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02	25	00	06 <Firmware Version String>	3A	74	03
Return Hex String: 022500064944205445434820536d61727450494e204c313030204669726d776172652056312e30303a7403 <STX> <length byte low><length byte high> <ACK>ID TECH SmartPIN L100 Firmware V1.00 <LRC><SUM> <ETX>						

7.4.4.2 Enter into Bootloader

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	03	00	78 46 7A 49 52 46 57 00 00 00 00 00 00 00 00	4E	70	03
Output Hex String:						
Command Body is: 78 46 7A 49 52 46 57						

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

7.4.4.3 Get Serial Number

Command Body is 78 46 02

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	03	00	78 46 01	3C	C0	03
Output Hex String: 0203007846023cc003						

Response Body is
06 + 10 bytes ASCII code Serial Number Or 15 62 00 – No Serial Number

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02	0B	00	06 <10-digit serial number>			03
Response Hex String: 020b000636313654353638393432673903 <STX><len low><len high><ACK><10-byte serial number><LRC><SUM><STX> The LRC and SUM will obviously depend on the model number.						

7.4.4.4 Get Model Status

Command Body is 78 46 20

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	03	00	78 46 20	1E	DE	03
Output Hex String: 0203007846201ede03						

Response Body is 06 + Model Status

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02	0D	00	06 <model status>			03
Response Hex String: 020d0006494450422d3630323430304d79cb03 <STX><len low><len high><ACK><model number><LRC><SUM><STX> In this example, the model number is IDPB-602400M.						

7.4.4.5 Reset

Warm reboot. Command Body is 78 46 49

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	03	00	78 46 49	77	07	03
Output Hex String: 020300784649770703						

Response Body is 06 (and LRC and SUM are 06)

Note:
Device will Reset (restart; warm reboot) after it responds ACK.
This is the Highest Priority Command in device except for Key Loading State.

7.4.4.6 Get Status for Key

Command Body is 78 46 25

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	03	00	78 46 25	1B	E3	03
Output Hex String: 0203007846251be303						

Response Body:
06 <2-byte Block Length> <KeyStatusBlock1> <[KeyStatusBlock2]> … <[KeyStatusBlockN]>,
Or
15 <Error Code>

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02			06 <Block Length Low><Block Length High> <KeyStatusBlock1> <[KeyStatusBlock2]> … <[KeyStatusBlockN]>			03

Response Hex String Example:
026300061800000000001000000030000000400000006000000070000000800000008000100
080002000800030008000400080005000800060008000700080008000800090008000a000800
0b000a0000000a03e8000c0000000d0000001400000128000000ce2a03
Where:

- <Block Length> - 2 bytes (LenL, LenH)
- KeyStatusBlock format is <Key Index and Key Name> <key slot> <key status>
  - <Key Index and Key Name> - 1 byte. Please see following table.

Key Name	Key Index and Key Name
Host-PINPAD Master DUKPT Key	0x00
PIN DUKPT Key	0x01
PIN Pairing DUKPT Key	0x03
Data Pairing DUKPT Key	0x04
CR-PINPAD Master DUKPT Key	0x06
CR-PINPAD MAC DUKPT Key	0x07
PIN Master Key	0x08
Pairing MSR BDK Key	0x0D

LCL-KEK(HSM DUKPT KEY)(HSM DUKPT KEY)	0x14
PIN Session Key	0x28

- <key slot> - 2 bytes. Range is 0 – 9999 (If key has not Slot, the value is 0x00 0x00, if key slot is 1000, the value is 0x03 0xE8)
- <key status> - 1 byte:
  - 0 – Not Exist
  - 1 – Exist

0xFF – Key Stop (Only Valid for DUKPT Key)

7.4.4.7 Get Key Status

Command Body is 78 46 30

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	03	00	78 46 30	0E	EE	03
Output Hex String: 0203007846300eee03						

Response Body is 06 + PIN DUKPT Status + PIN Master Key Status + PIN Session Key Status + Account DUKPT Key Status + AccountDUKPT Key Status + RKI-KEK (Admin DUKPT Key)

Where:

Key	Status	Note
PIN DUKPT Key	0: None. 1: Exist 0xFF: STOP	
PIN Master Key	0: None 1: At least Exist a Master Key	
PIN Session Key	0: None. 1: Exist	
Account/MSR DUKPT Key	0: None. 1: Exist 0xFF: STOP	Does not support this key. Always 0
Account/ICC DUKPT Key	0: None. 1: Exist 0xFF: STOP	Does not support this key. Always 0
RKI-KEK (Admin DUKPT Key)	0: None. 1: Exist	

	0xFF: STOP	

If unit has not been key-injected, response looks like
020700060000000000000060603

7.4.4.8 Set Remote Key Injection Timeout

Command Body is 78 53 01 01 02 <Timeout_H> <Timeout_L>

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	07	00	78 53 01 01 02 00 C0	E9	8F	03

Output Hex String: 020700785301010200c0e98f03

In this example, the timing value is 0x00C0 or 192 (decimal) seconds.

Timeout_H Timeout_L needs to be in the range 120 seconds ~ 3600 seconds

Response Body is 06
(Full response string: 02010006060603)

7.4.4.9 Get Remote Key Injection Timeout

Command Body is 78 52 01 01

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	04	00	78 52 01 01	2A	CC	03

Output Hex String: 020400785201012acc03

Response Body is 06 78 01 01 02 <Timeout_H> <Timeout_L>

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02	07	00	78 52 01 01 02 00 C0	BC	42	03

Output Hex String: 020700067801010200c0bc4203

In this example, the timing value is 0x00C0 (192 seconds).

7.4.4.10 Set Date & Time

Command Body is 78 53 01 50 06 <Date Time>

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	0B	00	78 53 01 50 06	39	F3	03

Output Hex String (example): 020b007853015006160520103056 39f303

Where: <Data Time> is 6 bytes data – Year, Month, Date, Hour, Minute, Second

Item	Value Area (BCD Code)
Year	00~99
Month	01~12
Date	01~31
Hour	00~23
Minute	00~59
Second	00~59

Response Body is simply 06.

Note:

- If current Date/Time is 2014/08/23 15:24:59, <Date Time> should be 14 08 23 15 24 59 (BCD Code).
- The command always valid in Activation IDLE State.
- 2000/01/01 00:00:00 is the base time; device will reject attempts to set this value.

7.4.4.11 Get Date & Time

Command Body is 78 52 01 50

16 05 20 10 26 01

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	04	00	78 52 01 50	7B	1B	03

Output Hex String: 020400785201507b1b03

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02	0B	00	06 78 01 50 06 16 05 10 13 16 19	36	42	03

Output Hex String: 020b000678015006160510131619364203

Which is STX, 2 length bytes, ACK + 78 01 50 06 + <Data Time>

Where: <Data Time> is 6 bytes data – Year, Month, Date, Hour, Minute, Second

Note:
The command is always valid in Load Important Data State & Activation IDLE State.

7.4.4.12 Get All Fix/Removal Records

Command Body is 78 52 01 51

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	04	00	78 52 01 51	7A	1C	03

Output Hex String: 020400785201517A1C03

Response Body is 06 + < Fix/Removal Records Number> (<Record Block>…) < Illegal Removal Records Number> (<Record Block>…)

Where:
< Fix/Removal Records Number> is Number of Fix/Removal Record Block. If it is 0, there is not <Record Block>
< Illegal Removal Records Number> is Number of Illegal Removal Record Block. If it is 0, there is not <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) or 0x30 (Illegal Removal)
<State> is 0x30 (Fix) or 0x31 (Removal) or 0x32 (Illegal Removal)
Year, Month, Date, Hour, and Minute need be ASCII code.

Note:
The Max Records is 40.
After response this command, all Records are deleted.

7.4.4.13 Enter Stop Mode

Command Body: 78 46 72 01

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	04	00	78 46 72 01	4D	31	03

Output Hex String: 020400784672014D3103

Response Body is 06.

Note:

1. Sets device enter to Stop Mode. In this mode, LCD display and backlight are off. Stop Mode reduces power consumption to the lowest possible level. A unit in Stop Mode can only be woken up by a physical key press.
2 .Stop Mode cannot be reached from Bootloader mode, Diagnosis mode, Get PIN, Get Numeric, Get Function Key, Get PIN for Pro, Display and Get Key for Pro and Active PINpad, Active/Deactive Passwords, load cert, load key and load important data for PINpad mode.

7.4.4.14 Set Enter Sleep Mode Time

Enter Sleep Mode timeout period (the period after which the unit, if idle, goes to sleep); default is 120 seconds.

Command Body: 78 46 71 <TimeH> <TimeL>

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	05	00	78 46 71 <TimeH> <TimeL>	62	5C	03

Output Hex String: 020500784671012C625C03

<TimeH><TimeL>:
Enter sleep mode time. After TimeH*256+TimeL seconds, device enters Sleep Mode.

Response Body is 06.

Note:

1. The Sleep Mode is controlled by a timeout after the unit is idle for a specified time.
Sleep Mode reduces power consumption to a much lower level but the device remains capable of being woken up by key press or communication from the host.

2. Bootloader mode, Diagnosis mode, Get PIN, Get Numeric, Get Function Key, Get PIN for Pro, Display and Get Key for Pro and Active PINpad, Active/Deactive Passwords, load cert, load key and load important data for PINpad cannot enter sleep mode.

7.4.5 Other PIN Pad Group (Task)

7.4.5.1 Get Encrypted PIN

Command Body: 75 46 07 <KeyType><PAN (Account#)><LCD len><LCD Command format>

Where:

- <Key Type>- 1 byte.
  - 0x00- MKSK-TDES , External Plaintext PAN
  - 0x01- DUKPT-TDES, External Plaintext PAN
  - 0x10 MKSK-TDES , External Ciphertext PAN
  - 0x11 DUKPT-TDES, External Ciphertext PAN

[<PAN (Account#)>] - external account, ASCII code for digital (0x30 – 0x39):
<Key Type> is 0x00 or 0x01, the PAN is Plaintext (Removal detection enable valid), 16 bytes.
<Key Type> is 0x10 or 0x11, the PAN is Ciphertext: Removal detection enable valid, Ciphertext PAN is encrypted by PAN Encryption Key from pairing, uses PAN Encryption Key as Key, use 8 bytes 0 as IV, TDES and CBC encrypt the Plaintext PAN Format (24 bytes) to get 24 bytes Encrypted PAN.
<LCD len> - 1 byte. The length of LCD Command format.
<LCD Command format> - 1~20 bytes ASCII code Display Message.

Response Body:
1. 0x06 if operation is successful, or 0x15 Error Code if it is not successful.
2. Waiting for entering PIN. And:
If Get Encrypted PIN with DUKPT Key under Triple DES: 06 + 20 ASCII code KSN + 16 ASCII code Encrypted PIN block
If Get Encrypted PIN with MKSK: 06 + 16 ASCII code Encrypted PIN block

Note:
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 no 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 implement Pairing successfully, but the Encrypted PAN is error, response 15 07 02
  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

- If related key was not loaded, response 15 04 00
- If PIN DUKPT Key was STOP, response 15 73 00
- If MKSK algorithm was used more than 120 times in a hours, response 15 72 00

Wait 30 Seconds, The Pin Len default is 4~12

Per 10 Seconds, if the PIN length was not zero, the PIN would be clear

While you press numeric key, **Device** will increase display "*" on LCD if Total PIN length is smaller than 12. Line 1 display:

If Enter 2 numeric: **

If Enter 12 numeric: **********

While you press Backspace key, **Device** will decrease display "*" on LCD if Total PIN length is not 0.

While you press Cancel key, **Device** will display cursor on LCD if Total PIN length is not 0, or **Device** will quit the work state.

While Cancel Command was sent, **Device** will quit the work state.

7.4.5.2 Get Numeric with Display Message

Command Body is 75 46 08 & <256 bytes Encrypted Display Message>

Where:

<256 bytes Encrypted Display Message> is encrypted Plaintext Display Message by Numeric Key using RSA-2048 algorithm.

Plaintext Display Message format is: <Len> <Flag> <Display Message String>

<Len> - 1 bytes, is the length of Display Message String

<Flag> - 1 byte, is Display Option of Line2

0:

While you press numeric key, **Device** will increase the display space devoted to this numeric on LCD if Total numeric length is smaller than 16.

While you press Backspace key, **Device** will decrease the display space devoted to the last numeric on LCD if Total numeric length is not 0.

1:

While you press numeric key, **Device** will increase display “*” on LCD if Total numeric length is smaller than 16.

While you press Backspace key, **Device** will decrease display “*” on LCD if Total numeric length is not 0.

<Display Message String> - 1~16 bytes, need be ASCII code.

Note: The Display Message will display in Line1 of LCD.

Response Body:

1. 0x06 if command is successful, or 0x15 Error Code if it is not successful.
2. Waiting for enter Numeric.And 06 + n ASCII code Numeric (n is 1~16).

For Example: enter into 7 numeric keys: 2 5 7 8 9 0 6, response is 06 32 35 37 38 39 30 36.

Note:

Wait 30 Seconds, The Numeric Len is 1~16

Per 10 Seconds, if the Numeric length was not 0, the Numeric will be clear and will display cursor on LCD.
While you press numeric key, **Device** will increase display numeric on LCD if Total length is smaller than MaxLen. . Line 1 display:
If Enter 2 numeric (12): 12 or **
If Enter 16 numeric (1234567890123456): 1234567890123456 or **********

While you press Backspace key, **Device** will decrease display numeric on LCD if Total numeric length is not 0.
While you press Cancel key, **Device** will display cursor on LCD if Total numeric length is not 0, or **Device** will quit the work state.
While Cancel Command was sent, **Device** will quit the work state.

7.4.5.3 DisplayMessage and Get Numeric Key

Command Body is 75 46 22 & <echo_flag> <max_len> <min_len> <256 bytes Encrypted Display Message>
Where:
<echo_flag>:
0 - display numeric for numeric key on LCD
1 - display "*" for numeric key on LCD
< max_len> - the max length for numeric. Max length cannot be beyond 16
< min_len> - the max length for numeric. Max length cannot be less than 1
<256 bytes Encrypted Display Message> is encrypted Plain text data by numeric key using RSA-2048 algorithm. The plain text of <256 bytes Encrypted Display Message> format is:
<LCD Message len><LCD Message Data>

Response Body:
1. 0x06 if operation is successful, or 0x15 Error Code if it is not successful.
2. Waiting for entering Numeric. And 06 + <len><keys0><keys1>...<keys16>
For example: enter into 7 numeric keys: 2 5 7 8 9 0 6, response is 06 07 25 78 90 6F FF FF FF FF FF FF FF FF FF FF FF FF

Note:
Wait 30 Seconds, The Numeric Len is 1~16
Per 10 Seconds, if the Numeric length was not 0, the Numeric would be clear and will display cursor on LCD.
While you press numeric key, **Device** will increase display numeric on LCD if Total length is smaller than MaxLen. Line 1 display:
If Enter 2 numeric (12): 12 or **
If Enter 16 numeric (1234567890123456): 1234567890123456 or **********
While you press Backspace key, **Device** will decrease display numeric on LCD if Total numeric length is not 0.
While you press Cancel key, **Device** will display cursor on LCD if Total numeric length is not 0, or **Device** will quit the work state.
While Cancel Command was sent, **Device** will quit the work state.

7.4.5.4 DisplayMessage and Get Amount

Command Body is 75 46 23 & <flag> <max_len> <min_len> <256 bytes Encrypted Display Message>
Where:
<flag> - 1 byte, Reserved
< max_len>- the max length for numeric. Max length cannot be beyond 15
< min_len>- the max length for numeric. Max length cannot be less than 1
<256 bytes Encrypted Display Message> is encrypted Plain text data by numeric key using RSA-2048 algorithm. The plain text of <256 bytes Encrypted Display Message> format is:
<LCD Message len><LCD Message Data>

Response Body:
1. 0x06 if command is successful, or 0x15 Error Code if it is not successful.
2. Waiting for entering Numeric. And 06 + <len><keys0><keys1>...<keys14>
For example: enter into 7 numeric keys: 2 5 7 8 9 0 6, amount is 25789.06, response is 06 07 25 78 90 6F FF FF FF FF FF FF FF FF FF FF FF FF

Note:
Wait 30 Seconds, The Numeric Len is 1~16
Per 10 Seconds, if the Numeric length was not 0, the Numeric would be clear and will display cursor on LCD.
While you press numeric key, **Device** will increase display numeric on LCD if Total length is smaller than MaxLen. Line 1 display:
If Enter 2 numeric (12): 0.12
If Enter 15 numeric (12345678901245): 1234567890123.45
While you press Backspace key, **Device** will decrease display numeric on LCD if Total numeric length is not 0.
While you press Cancel key, **Device** will display cursor on LCD if Total numeric length is not 0, or **Device** will quit the work state.
While Cancel Command was sent, **Device** will quit the work state.

7.4.5.5 Get Function Key

Command Body is 75 46 0B

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	03	00	75 46 0B	38	C6	03
Output Hex String: 02030075460B38C603						

Response Body: 06 + 1 byte ASCII code Func Key or 2 bytes ASCII code Func Key.

Note:
Wait 3 minutes.
While you press Backspace key, **Device** Sends “B”
While you press Cancel key, **Device** Sends “C”
While you press Enter key, **Device** Sends “E”
While you press ‘*’ key, **Device** Sends “*”
While you press ‘#’ key, **Device** Sends “#”
While you press Blank key, **Device** Sends “?”
While you press F1 key, **Device** Sends “F””1”
While you press F2 key, **Device** Sends “F””2”
While you press F3 key, **Device** Sends “F””3

7.4.5.6 Cancel Command

Command Body is 75 46 09

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	03	00	75 46 09	3A	C4	03
Output Hex String: 0203007546093AC403						

Note: Use this command to Cancel “Get Func Key” & “Get Encrypted PIN” & “Get Numeric” & “Get Amount”

Response Body is always 15 18 00

7.4.5.7 Beeper Control

Open / Close Beeper:
Command Body is 75 46 01 01 <On/Off>

<On/Off> - 0x00 : Off
- 0x01 : On

Beep according to 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 1000 (0x03E8), <Fre1> <Fre2> <Fre3> <Fre4> will be 0x45 0x38 0x30 0x33.

According to the datasheet of Beeper of SmartPIN C100:
Frequency will be more than 1000Hz and less than 20000Hz.
4000Hz tone will generate the First Max Decibels sound.
6000Hz tone will generate the Second Max Decibels sound.
<Dur1> <Dur2> is is the first and second nibble for the first byte of Duration.
<Dur3> <Dur4> is is the first and second nibble for the second byte of Duration.
If the Duration is 200 (0x00C8), <Fre1> <Fre2> <Fre3> <Fre4> will be 0x43 0x38 0x30 0x30.
Duration need be more than 16ms and less than 65535 ms.

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

7.4.5.8 Set PIN Len

Command Body is 75 53 01 01 02 MinLen MaxLen

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	07	00	75 53 01 01 02 MinLen MaxLen			03
Output Hex String: 0207007553010102040A2ADA03 MinLen need be 4~12 MaxLen need be 4~12 MinLen need be same or less than MaxLen						

Response Body is 06

7.4.5.9 Get PIN Len

Command Body is 75 52 01 01

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	04	00	75 52 01 01	27	C9	03
Output Hex String: 0204007552010127C903						

Response Body is 06 75 01 01 02 MinLen MaxLen

7.4.5.10 Set Numeric Len

Command Body is 75 53 01 02 02 MinLen MaxLen

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	07	00	75 52 01 02 02< MinLen><MaxLen>	3E	E4	03

Output Hex String: 02070075520102020810 3EE403

MinLen need be 1~16
MaxLen need be 1~16
MinLen need be same or less than MaxLen

Response Body is 06

7.4.5.11 Get Numeric Len

Command Body is 75 52 01 02

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	04	00	75 53 00	24	CA	03

Output Hex String: 0204007552010224CA03

Response Body is 06 75 01 02 02 MinLen MaxLen

7.4.5.12 Default PINpad Group All Setting

Command Body is 75 53 00

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	03	00	75 53 00	26	C8	03

Output Hex String: 02030075530026C803

Response Body is 06

Below Setting should be reset to default value:

Function Name	Default Value
PIN Length	Min is 4, Max is12
Numeric Length	Min is 1, Max is16

7.4.5.13 Review PINpad Group All Setting

Command Body is 75 52 00

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	03	00	75 52 00	27	C7	03
Output Hex String: 02030075520027C703						

Response Body is 06 75 02 01 02 <Min PIN Length> <Max PIN Length> 02 02 <Min Numeric Length> <Max Numeric Length>

7.4.6 LCD Group (Task)

7.4.6.1 Clear Display

Command Body is 8A 46 01 <Control>

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	0C	00	8A 46 01 <Control>	EA	46	03
Output Hex String: 0204008a4601ff32d003 <Control> 0:First Line 1:Second Line 2:Third Line 3:Fourth Line 0xFF: All Screen						

Response Body is 06

7.4.6.2 Save Prompt Display

Command Body is 8A 46 24 <Prompt> <Message>
<Prompt> - Prompt number 0 – 9
<Message> - display message 20 char MAX ((ASCII Code – 0x20~0x7F))

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	0C	00	8A 46 24 <Prompt> <Message>	EA	46	03

Output Hex String: 020c008a4624022a2a2a2a2a2a2a2aea4603

Example shows Prompt 2, Message "********"

Response Body is 06

7.4.6.3 Display Prompt

Command Body is 8A 46 25 <Line> <Prompt>

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02		00	8A 46 25 <Line> <Prompt>			03

Output Hex String: 0205008a46250001e8f603

Response Body is 06

7.4.6.4 Display Message

Command Body is 8A 46 26 <Line> <1~20 Message>
<Line> - Display line number 0 Or 1 or 2 or 3
<1~20 Message > - Message (ASCII Code – 0x20~0x7F)

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX

02	17	00	8A 46 26 <Line> <1~20 Message>	D2	F6	03

Output Hex String: 0217008a462600536d61727450494e204c313030205265616479d2f603

<Line> - Display line number 0 Or 1 or 2 or 3
<1~20 Message > - Message (ASCII Code – 0x20~0x7F)

The example above sets the message "SmartPIN L100 Ready"

Response Body is 06

7.4.6.5 Default LCD Group All Setting

Command Body is 8A 53 00

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	03	00	8A 53 00	D9	DD	03

Output Hex String: 0203008a5300d9dd03

Response Body is 06

Default values:

Function Name	Default Value
Back Light of LCD On/Off	OFF

7.4.6.6 Review LCD Group All Setting

Command Body is 8A 52 00

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	03	00	8A 52 00	D8	DC	03

Output Hex String: 0203008a5200d8dc03

Response Body is 06 8A 04 01 <Back Light Control>

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02	05	00	06 8A 04 01 <Back Light Control>05 01 <TimerValue>	88	96	03
Output Hex String: 020500068a040101889603						

7.4.6.7 Set Back light of LCD On/Off

Command Body is 8A 53 01 04 01 <Control>
Where <Control> is:
- 0: OFF
- 1: ON

Response Body is 06

7.4.6.8 Get Back light of LCD On/Off

Command Body is 8A 52 01 04

Response Body is 06 8A 01 04 01 <Control>

7.4.7 RS232 Task Commands

7.4.7.1 Set BaudRate

Command Body is 70 53 01 41 01 ASCIIChar

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	06	00	70 52 01 41 01 <Speed>	54	3C	03
Output Hex String: 0206007053014101365 43c03 This example shows Speed as 0x36, the code for 19200 (see table below).						

BaudRate	ASCIIChar
2400	0x32
4800	0x33
9600	0x34
19200	0x36

38400	0x37
115200	0x39

Response Body is 06

7.4.7.2 Get BaudRate

Command Body is 70 52 01 41

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	04	00	70 52 01 41	62	04	03

Output Hex String: 02040070520141620403

Response Body is 06 70 41 01 <ASCIIChar>:

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	05	00	06 70 41 01 <Speed>	01	EF	03

Output Hex String: 020500067041013701ef03

BaudRate	ASCIIChar
2400	0x32
4800	0x33
9600	0x34
19200	0x36
38400	0x37
115200	0x39

7.4.7.3 Set StopBits

Command Body is 70 53 01 45 01 ASCIIChar

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	06	00	70 53 01 45 01 31	57	3B	03

Output Hex String: 02060070530145013157 3b03

StopBits	ASCIIChar
1	0x31
2	0x32

Response Body is 06

7.4.7.4 Get StopBits

Command Body is 70 52 01 45

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	04	00	70 52 01 45	66	08	03
Output Hex String: 02040070520145660803						

Response Body is 06 70 45 01 + <ASCIIChar>

7.4.8 Exchange Certificates

32 – Gets Certificates

CR/Host gets PINPAD certificates for encryption/decryption and signature/validation purpose.

Command:

Task ID	'65' or '75'
	'46'
Function ID	'32'
Length	0
Data	none

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Complete • Wrong parameter • Any hardware problems • Invalid Manufacturing system data [Note] • Invalid certificate • No nonce generated • AT-HOST checks failed • Wait • Number of retries over limit
Task ID	'56' or '57'
	'46'
Function ID	‘32’
Length	Length of data
Data	If PINPAD command checks pass, else data not present. • Length of CERT_ PEK • CERT_PEK • Length of CERT_ PSK • CERT_ PSK

33 – Sends Certificates

CR /Host send PINPAD certificates for encryption/decryption and signature/validation purpose.

Command:

Task ID	'65' or '75'
	'46'
Function ID	'33'
Length	Length of data
Data	• Length of CERT_HEK or CEK • CERT_HEK or CEK • Length of CERT_HSK or CSK • CERT_HSK or CSK

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Complete • Wrong parameter • Any hardware problems • Invalid Manufacturing system data [Note] • Invalid certificate • No nonce generated • AT-HOST checks failed • Wait • Number of retries over limit
Task ID	'56' or '57'
	'46'
Function ID	‘33’
Length	0
Data	none

7.4.9 8.5.17 Asymmetric Key Loading

36 – Sets Key: Master and Working Key

Description:
1. Working key includes PIN DUKPT Key / PIN Master Key / Data Pairing DUKPT Key / PIN Pairing DUKPT Key /MAC DUKPT Key.
2. This command should be issued after Card Reader and PINPAD or PINAD and HOST have exchanged certificates.

Command:

Task ID	'65’ or '75’
	‘46’
Function ID	'36’
Length	Length of data

Data	• Length Key remaining • Key remaining • Length success code • Success code(’Y’ = Keys delivered successfully; ‘N’ = Error sending keys) • Length of SKT • SKT (HOST Key Token or CR Key Token) • Length of Encrypted key ASN.1 structure • Encrypted key ASN.1 structure • Length of Host nonce • Host nonce • Length SIGN2-HOST or CR • SIGN2-HOST or CR

Note: SING2: RSASSA_PSS_SHA256 (Key remaining || Success code || SKT || Encrypted key ASN.1 structure || CR_NONCE || HOST_NONCE || 2)

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Complete • Wrong parameter • Not Authenticated • No nonce generated • AT-HOST checks failed • TR34 checks failed • Wait • Number of retries over limit
Task ID	'56' or '57'
	‘46’
Function ID	‘36’
Length	Length of data
Data	• Length Key Verification ASN.1 structure • Key Verification ASN.1 structure, DER format • Length of PINPAD/CR nonce • PINPAD/CR nonce • Length of SIGN3-CR or PINPAD • SIGN3-CR or PINPAD

Encrypted key ASN.1 structure:: = Sequence
{
    Encrypted key ASN.1 structure version = 1 (INTEGER)
    Keys:: = Set

```
    {
        Keyinfo:: = Sequence
        {
            TR31Key = (PRINTABLESTRING)
            KeyType = (INTEGER)
            Ksn = (OCTET STRING) -- If keyType is not DUKPT, 00000000000000000000
            KeySlot = (INTEGER)
            KeyName = (PRINTABLESTRING)
            KCV = (OCTET STRING) -- 2 bytes
        }
    }
}
```

Example 1 of Encrypted key ASN.1 structure-one key:

30819702010131819130818E13704130313132423154 4E303045303130304B5331384646464632323232323232323232363030303030303046354146313134393433793345424336333832324141444233443336383842394436444543454234232343132373244304330464141383833314342434445314444453545383202010204040AFFFF2222222226000002010013045465737404 02F873

Example 2 of Encrypted key ASN.1 structure-multiple keys:

3082029B02010131820294307613584130303838423154 4E3030453030303038303130413932323647374635363230303539393444638383339314231324242353832333746304235424137424133463934383344463634444343333637443939394639434635020102040AFFFF2222222265222222020100130453524544040254 8C307C13584130303838 4B30444E3030453030303031444543354144304538313131433344373443436373833413344393242413431453330373636443436464131334341444339374245423343444433830463041393046363037410201010 40A00000000000000000000020100130A546573744B6579312D3504 02E6D8307F13584130303838423154 4E3030453030303032354645444438433946323136343739443944334434414246313946303035444342333944454636453246383843414536353537434546323443454533333037433541423339413602010 2040AFFFF000000004300000002010113 0D546573742042444B204B65793104029504307913584130303838423154 4E3030453030303034334445363334303036423331393242394231464546393945353638314245383530353442313146373845394332443843414135303031464541394146353541343244414535344402010 2040AFFFF22222226702222202010113075049 4E204B6579040 2F95D30819F13784230313230423154 4E3030453031303 04B533138464646463030303030303030303030303045303030303030304646463843394233943363939433543413732413943443142413135424336424624238423231303337334332364142434545373134443743314333464230324244532333130413941354536373138020102040AFFFF0000000000E000000201031 30D7669702D64656D6F2D7465737404 02616F

Note: SING3: RSASSA_PSS_SHA256 (Key Verification ASN.1 structure || CR_NONCE || HOST_NONCE || 2)
2 means Padding method is PSS

```
Key Verification ASN.1 structure:: = Sequence
{
    Key Verification ASN.1 structure version = 1 (INTEGER)
    Keys:: = Set
    {
        Keyinfo:: = Sequence
```

```
        {
            KeyName = (PRINTABLESTRING)
            ErrorCode = (INTEGER) --‘0’ signifies a successful load
            ErrorMessage = (PRINTABLESTRING)
        }
    }
}
```

Example of success-one key “Test” key: 30120201013110d300b13045465737402010013 00
Example of success-multiple keys:
3061020101315c30141 30d7669702d64656d6f2d7465737402010013 00300e13075 0494e204b6
5790201001300301413 0d546573742042444b204b65793102010013 00301113 0a546573744b6
579312d3502010013 00300b13045352454402010013 00

3C – Set Working Key

Description:
Working key includes PIN/PIN Master /PIN Pairing/ Data Pairing/ MAC Key.
This command should be issued after the Card Reader and PINPAD have established the CR_PINPAD_MASTER_DUKPT_KEY.
Note:
Yellow: Optional block-KeyIndex
Green: Optional block-KeySlot
Red: Optional block-KSN/KeyID

KBH for PIN DUKPT Key:
B0136B1TX00E0300010800010208000 0KS18FFFF0000000000000000

MK/SK PIN Master Key:
B0112K0TB00E020001080008 02080000

DATA Pairing DUKPT Key:
B0136B1TX00E0300010800040208000 0KS18FFFF0000000000000000

PIN Pairing DUKPT Key:
B0136B1TX00E0300010800030208000 0KS18FFFF0000000000000000

MAC Key:
B0136B1TX00E0300010800050208000 0KS18FFFF0000000000000000
Command:

Task ID	'65’ or '75’
	‘46’
Function ID	'3C’
Length	Length of data

Data	• Length of Encrypted key ASN.1BLK • Encrypted key ASN.1 BLK, using TR31_B • Length MASTER_DUKPT_KEY_KSN • MASTER_DUKPT_KEY_KSN

Encrypted key ASN.1 structure:: = Sequence
{
    Encrypted key ASN.1 structure version = 1 (INTEGER)
    Keys:: = Set
    {
        Keyinfo:: = Sequence
        {
            TR31Key = (PRINTABLESTRING)
            KeyType = (INTEGER)
            Ksn = (OCTET STRING) -- If keyType is not DUKPT, 00000000000000000000
            KeySlot = (INTEGER)
            KeyName = (PRINTABLESTRING)
            KCV = (OCTET STRING) -- 2 bytes
        }
    }
}

Response 1:

Result byte	If success, return ACK. If failed , return NAK <Error Code>
Task ID	'67' or '56' or '57'
	'46'
Function ID	'3C'
Length	Length of data
Data	KCV ASN.1 structure

KCV ASN.1 structure:: = Sequence
{
    KCV ASN.1 structure version = 1 (INTEGER)
    Keys:: = Set
    {
        Keyinfo:: = Sequence
        {
            KeyName = (PRINTABLESTRING)
            ErrorCode = (INTEGER) --'0' signifies a successful load
            ErrorMessage = (PRINTABLESTRING)
            KCV = (OCTET STRING) -- 3 bytes, algorithm refer to x9.24
        }
    }

}

7.5 Error Codes

Error Code	Definition
0x0100	Log is full
0x0400	Related Key was not loaded
0x0500	Key Same
0x0501	Key is all zero
0x0502	TR-31 format error
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
0x0705	No Internal MSR PAN (or Internal MSR PAN is erased timeout)
0x0F00	Encryption Or Decryption Failed
0x1800	Response for Cancel (Get PIN, Get Numeric, Get FunKey) command
0x1900	Response for Cancel Key Press in Get PIN / Numeric State
0x3005	Removal detection not active.
0x30FF	Slave Chip is not connect
0x5500	No RKI-KEK (Admin DUKPT Key)
0x5501	RKI-KEK (Admin DUKPT Key) STOP
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
0x5509	Remote Key Injection Timeout (Latest Command is Timeout)
0x550A	MAC Error
0x550B	Key Usage Error
0x550C	Mode Of Use 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
0x6A01	Unsupported Command – Protocol and task ID are right, but command is invalid – In this State
0x6B00	Unknown parameter in command – Protocol task ID and command are right, but parameter is invalid
0x6C00	Unknown parameter in command – Protocol task ID and command are right, but length is out of the requirement.
0x7200	MKSK Suspend or press passwords Error Suspend
0x7300	PIN/MSR/ICC/ RKI-KEK (Admin DUKPT Key) is STOP (21 bit 1)
0x7400	Device is Busy
0x7500	Device is in diagnose mode
0x7600	Device is in Transparent Transmission mode
0x8100	Timeout
0x8200	Wrong operate step
0x0100	Log is full

7.6 LCD Foreign Language Mapping Table

ID	Message ID	English	French	Spanish	Chinese
0	MSG_NULL				
1	MSG_AMOUNT	AMOUNT	MONTANT	CANTIDAD	金额
2	MSG_AMOUNT_OK	AMOUNT OK?	MONTANT OK	MONTO CORRECTO?	确定金额
3	MSG_APPROVED	APPROVED	APPROUVE	APROVADO	通过
4	MSG_CALL_YOUR_BANK	CALL YOUR BANK	APPE VOTRE BANQE	LLAME A SU BANCO	请联系您的银行
5	MSG_CANCEL_OR_ENTER	CANCEL OR ENTER	ANNULE OU ENTRER	CANCEL O ENTRAR	取消或确定
6	MSG_CARD_ERROR	CARD ERROR	ERREUR CARTE	ERROR DE TARJETA	读卡错误
7	MSG_DECLINED	DECLINED	REFUSE	DECLINADO	卡被拒
8	MSG_ENTER_AMOUNT	ENTER AMOUNT	ENTRER MONTANT	INGRESE MONTO	输入金额
9	MSG_ENTER_PIN	ENTER PIN:	ENTRER PIN:	ENTRAR NPI:	请输入密码
10	MSG_INCORRECT_PIN	INCORRECT PIN	NIP INCORRECT	NPI INCORRECTO	密码错误
11	MSG_ICC_MSR1	SWIPE OR INSERT	PASSER OU INSERT	MOVER O INSERT	请刷卡或插卡
12	MSG_ICC_MSR2	CARD	CARTE	TARJETA	卡
13	MSG_INSERT_CARD	INSERT CARD	INSERT CARTE	INSERTAR TARJETA	请插卡
14	MSG_USE_CHIP_READER	USE CHIP READER	UTI LECTEUR CHIP	USO CHIP LECTOR	使用芯片卡
15	MSG_NOT_ACCEPTED	NOT ACCEPTED	PAS ACCEPTE	DENEGADO	无法接受
16	MSG_PIN_OK	PIN OK?	PIN OK	PIN CORRECTO?	确定密码
17	MSG_PLEASE_WAIT	PLEASE WAIT...	ATTENDRE...	POR FAVOR ESPERE	等候中
18	MSG_PROCESSING_ERROR	PROCESSING ERROR	ERREUR DE TRAITE	ERROR PROCESANDO	处理错误
19	MSG_USE_MAGSTRIPE	USE MAGSTRIPE	USAGE MAGSTRIPE	USO DE MAGSTRIPE	使用磁条卡
20	MSG_TRY_AGAIN	TRY AGAIN	REESSAYER	VUELV INTENTARLO	请重试
21	MSG_ONLINE	GO ONLINE	GO LIGNE	GO LINEA	在线

22	MSG_TRANSACTION_ERROR	TRANSACTION ERR	ERREUR DE TRANS	ERROR DE TRANSAC	交易错误
23	MSG_TERMINATE	TERMINATE	RESILIER	TERMINAR	终止
24	MSG_ADVICE	ADVICE	CONSEILS	CONSEJOS	建议
25	MSG_TIMEOUT	TIME OUT	TIMEOUT	TIEMPO DE ESPERA	超时
26	MSG_PROCESSING	PROCESSING...	PROCESSUS...	PROCESANDO...	处理中。。。
27	MSG_PIN_TRY_EX	PIN TRY LIMIT EX	PIN TRY DEPASSE	TRY PIN SUPERADA	密码尝试次数过多
28	MSG_ISSUER_AUTH_FAIL	ISSUER AUTH FAIL	EMETTEUR FAIL	EMISOR FALLA	与发卡机构认证
29	MSG_CONTINUE_PROCESS	CONTINUE PROCESS	CONTINUERLA	CONTINUAR PROCES	继续处理
30	MSG_GET_PIN_ERROR	GET PIN ERROR	GET PIN ERROR	OBTENER PIN ERR	密码错误
31	MSG_GET_PIN_FAIL	GET PIN FAIL	GET PIN FAIL	OBTENER PIN FALL	获取密码错误
32	MSG_NOKEY_GET_PIN	NO KEY GET PIN	NO KEY GET PIN	NO CLAVE GET PIN	无法输入密码
33	MSG_CANCELLED	CANCELLED	ANNULE	CANCELADO	取消
34	MSG_LAST_PIN_TRY	LAST_PIN_TRY	LAST PIN TRY	LAST TRY PIN	最后一次密码尝试

Appendix A: Spectrum Pro Related Commands

Note:
The Length in the message blocks of following commands and responses all has the formatted as: 2 byte, little-endian.

CR gets PINPAD UID

Command:

Task ID	'65' or ‘56’
	‘46’
Function ID	'26'
Length	Length of data
Data	• Length of CR Unique identification number (UID), • CR Unique identification number (UID); • length of Symmetric or Asymmetric flag • Symmetric or Asymmetric flag 0 - Symmetric only 1- Asymmetric only 2- Both Symmetric and Asymmetric

Response:

Result byte	If success, return ACK. If failed , return NAK <Error Code>
Task ID	'56' or ‘65’
	‘46’
Function ID	‘26’
Length	Length of data
Data	• Length of PINPAD Unique identification number (UID), • PINPAD Unique identification number (UID), 8 bytes • length of Symmetric or Asymmetric flag • Symmetric or Asymmetric flag 0 - Symmetric only 1- Asymmetric only 2- Both Symmetric and Asymmetric

Get Nonce

Command:

Task ID	'65' or ‘56’
	‘46’
Function ID	'27'
Length	Length of data
Data	• Length of NONCE • CR NONCE, 16 bytes

Response:

Result byte	If success, return ACK. If failed , return NAK <Error Code>
Task ID	'56' or ‘65’
	‘46’
Function ID	‘27’
Length	Length of data
Data	• Length of NONCE • PINPAD NONCE, 16 bytes

NOTE:

1. This command must be used just before a command (that requires NONCE values) is issued.
2. NONCE is active after this command and will be used in checks and calculations. Once a NONCE is used (in a check or calculation), it is NOT allowed to use the same NONCE value again. So after one side completes a command that uses this NONCE, it will reset the NONCE value to indicate there is no active NONCE value.

Get DUKPT KSN

Command:

Task ID	'65' or '75' or ‘78’
	‘46’
‘Function ID	'3E’
Length	Length of data

Data	• Key Index, 1 byte 0x0 –Host-PINPAD Master DUKPT Key 0x1 –PIN DUKPT Key 0x3 –PIN Pairing DUKPT Key 0x4 –Data Pairing DUKPT Key 0x6– CR-PINPAD Master DUKPT Key 0x7–CR-PINPAD MAC DUKPT Key 0xA– RKL DUKPT Key 0xC–RKI-KEK (Admin DUKPT Key) 0x14 – HSM Key Encryption Key (Master Key or KEK) • Length Key Slot • Key Slot

Note:

Host to get the LCL-KEK (HSM DUKPT KEY) or Master DUKPT Key KSN or RKL DUKPT Key KSN from PINPAD or Card Reader to get the Master DUKPT Key KSN from PINPAD.

Response:

Result byte	If success, return ACK. If failed , return NAK <Error Code>
Task ID	‘56’ or ‘57’
	‘46’
Function ID	‘3E’
Length	Length of DUKPT KSN
Data	• DUKPT KSN

Activate and Deactivate Removal Sensor

Command:

Task ID	'76' or '56'
	‘46’
Function ID	'45'
Length	Length of data

Data	• Length of Operator ID • Operator ID • Length of Removal Sensor control • Removal Sensor control: Reactivate-0, Deactivate-1 • Length of Removal Sensor control timeout • Removal Sensor control timeout, in second • Length MAC-PINPAD • MAC-PINPAD

Response:

Result byte	If success, return ACK. If failed , return NAK <Error Code>
Task ID	'67' or '65'
Function ID	'45'
Length	Length of data
Data	If Card Reader command checks pass, else data not present. • Length of MAC -CR • MAC -CR

Note:

1. For command between PINPAD-CR and HOST-CR, and when this command is between PINPAD-CR, PINPAD is the master, and CR is the slave.

2. If the removal sensor is activated and removal sensor is not engaged, Reader will see the event as tamper event and erase all the sensitive information like all established / temporal keys, PAN and PIN, and set state to unauthenticated state.
If the removal sensor is deactivated and removal sensor is not engaged, the Reader won't erase any sensitive information but it will disable any PIN related operation. The state of Reader keeps the same. By default, card reader is at the status of deactivate removal sensor.

3. Operator ID is an 8-byte hexadecimal byte array. Because PinPad doesn't support account management (no Operator ID supported), it send all 0 as Operator ID1 to indicate this case and UID/HostID as the Operator ID2.

4. Sensor control timeout: A timeout within which the dual control need to be finished.

Handicap Assistant Signal

Output:

Result byte	ACK
Task ID	'57'
	‘46’
Function ID	‘50’
Length	0
Data	None

Note:
This command is used to respond with buzzer beeps for a key pressed, and it just responds when connected with host. This command applies to following commands:

Get Encrypted PIN
Get Numeric with Display Message
DisplayMessage and Get Numeric Key
DisplayMessage and Get Amount
Get Function Key

Display and Get Key (command only between CR-PINPAD)

Command:

Task ID	'25’
	‘46’
Function ID	'B0’
Length	Length of data

Data	• Display mode 1- Menu Display 2- Normal Display get function key 3- Display without key input ~~4- Normal Display get account number~~ ~~5- Normal Display get numeric key~~ 8- Language Menu Display 16- Clear Screen (Do Not Receive Input Data) • If Normal Display or Menu Display, Length of Total timeout for keypad entry. • If Normal Display or Menu Display, Total timeout for keypad entry, in second, little endian, default is 30 seconds. Note: Total timeout will cancel keypad entry and return error. • If Normal Display or Menu Display, Length of minor timeout during each keypad entry • If Normal Display or Menu Display, minor timeout during each keypad entry, in second, little endian, default is 10 seconds. Note: Minor timeout will erase all previous keypad entry. • Length Display Message Language • Display Message Language, 2 byte EN - English (default) ES - Spanish ZH - Chinese FR - French • Length Display Message Control (0-No Message display) • Display Message Control: repeatable combination of <Line><Message><0x1C> <Line> - Display line number (1-First Line, n-nth Line), Maximum 16 lines. The lower 7 bits is for line number. The MSB is to indicate following message is a Message String or Message ID. MSB – 0: Message String. MSR – 1: Message ID. <Message> - Message String or Message ID. Message String: character in the range of 0x20 – 0x7f, Maximum 16 characters Note: 1. For "Language Menu Display", external display should extend the Message String to full string. For example: EN – English ES – Espanol ZH – 中文 FR - Francais 2.For display Message, it is not allowed to have empty display message before max line. Message ID: 1 byte, check LCD Foreign Language Mapping Table <0x1C> - separator • Length Back Light On TimerValue, 2 bytes • Back Light On TimerValue in second, little endian (all 0-Back Light Off, all 0xff-Back Light always On) • Mask the keypad entry with '*', 1 byte 0 - Don't mask 1 - Mask Note: The flag works for "Normal Display get account number" and "Normal Display get numeric key".

Response:

Result byte	If success, return ACK. If failed , return NAK <Error Code>
Task ID	'52'
	'46'
Function ID	'B0'
Length	Length of data
Data	• Display mode 0 - Cancel (user presses cancel key on the key pad for mode 1, 4 and 5) 1 - Menu Display 2 - Normal Display get function key 3 - Display without key input ~~4 - Normal Display get account number~~ ~~5 - Normal Display get numeric key~~ 8- Language Menu Display 16- Clear Screen (Do Not Receive Input Data) If Mode byte is "Cancel", don't need to send below field, but MAC is required. • If Normal Display, Length of Key (for function key, length is 1) • If Normal Display, Key0...KeyN, ASCII format • If Menu Display, Length of Menu value • If Menu Display, Menu value, sequence number of selected line, hex format

Note:

1. This command should be issued after CR and PINPAD have established MAC Key .

2. In response to this command, PINPAD will control its LCD display.

3. When display message has more characters than the LCD screen can support, use F1 key as page up and F2 key as page down.

4. Function Key Value, ASCII of the 1st character:

Cancel:	0x43
Backspace:	0x42
Enter:	0x45
#:	0x23

*:	0x2A
F1 (pg up):	0x46
F2 (pg dn):	0x47
F3:	0x48

Get PIN (command only between CR-PINPAD)

Command:

Task ID	'65'
	'46'
Function ID	'AE'
Length	Length of data
Data	Mode byte: - 0x00 – Cancel (cancel through command) - 0x01 - Online PIN DUKPT - 0x02 - Online PIN MKSK - 0x03 - Offline PIN If Mode byte is "Cancel", don't need to send below field. If Online PIN, Length of DATA_PAIRING_DUKPT KSN If Online PIN, DATA_PAIRING_DUKPT KSN If Online PIN, Length of encrypted Truncated PAN If Online PIN, Encrypted Truncated PAN If Online PIN, Length of Host ID If Online PIN, Host ID Length start PIN input timeout Start PIN input time out in seconds Length PIN entry interval PIN entry interval in seconds Length Display Message Language Display Message Language, 2 byte EN - English (default) ES - Spanish ZH - Chinese FR - French note: the Display Message as follows: English – "ENTER PIN:" French – "ENTRER PIN:" Spanish – "ENTRAR NPI:" Chinese – "请输入密码" Length MAC-CR MAC-CR Length of KSN KSN

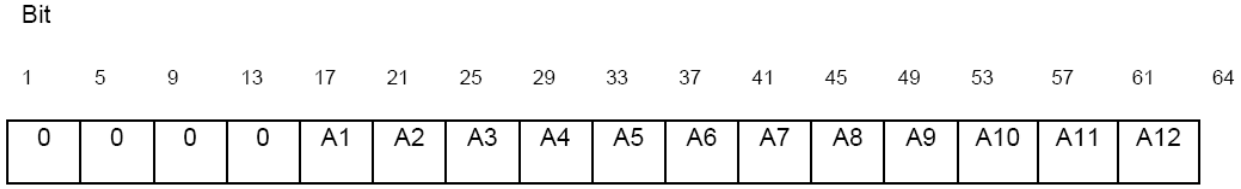
Response:

Result byte	If success, return ACK. If failed , return NAK <Error Code>
Task ID	'56'
Function ID	'AE'
Length	Length of data
Data	If Mode byte is "Cancel", don't need to send below field. If Mode byte is "Online PIN", PIN_KEY is PIN_DUKPT_KEY. If Mode byte is "Offline PIN", PIN_KEY is PIN_PAIRING_DUKPT_KEY. Mode byte: - 0x00 – Cancel (Can be cancel through command or user presses cancel key on the key pad) - 0x01 - Online PIN DUKPT - 0x02 - Online PIN MKSK - 0x03 - Offline PIN If Online PIN DUKPT, Length of PIN_DUKPT_KEY KSN; if Offline PIN, Length of PIN_PAIRING_DUKPT_KEY. If Online PIN DUKPT, PIN_DUKPT_KEY KSN; if Offline PIN, PIN_PAIRING_DUKPT_KEY KSN. Length Enciphered PIN Enciphered PIN Length MAC-PINPAD MAC- PINPAD

180 seconds as suggested timeout for starting PIN input. Once PIN input starts, 20 seconds as suggested timeout for finishing PIN input.

Note:

1. Plain text of Truncated Primary Account Number (PAN) pack



A1 ... A12 = Account number - Content is the 12 right-most digits of the primary account number (PAN) excluding the check digit. A12 is the digit immediately preceding the PAN's check digit. If the PAN excluding the check digit is less than 12 digits, the digits are right justified and padded to the left with zeros. Permissible values are 0000 (zero) to 1001 (9).

2. Plain text of PIN Block

The plaintext PIN block which will be enciphered shall be formatted as follows 8 bytes:

C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

Note:

	Name	Value
C	Control field	4 bit binary number with value of 0010 (Hex '2')
N	PIN length	4 bit binary number with permissible values of 0100 to 1100 (Hex '4' to 'C')
P	PIN digit	4 bit binary number with permissible values of 0000 to 1001 (Hex '0' to '9')
P/F	PIN/filler	Determined by PIN length
F	Filler	4 bit binary number with a value of 1111 (Hex 'F')

Symmetric Key loading

3B – Set Key: Master and Working Key
Description:
Working key includes PIN/PIN Master /PIN Pairing/ Data Pairing/ MAC Key.
This command should be issued after the Card Reader and PINPAD have established the RKL_DUKPT_KEY.
Note:
Yellow: Optional block-KeyIndex
Green: Optional block-KeySlot
Red: Optional block-KSN/KeyID

KBH for Master DUKPT Key:
B0136B1TX00E0300010800000208000OKS18FFFF9876543210E00000

KBH for PIN DUKPT Key:
B0136B1TX00E0300010800010208000OKS18FFFF0000000000000000

MK/SK PIN Master Key:
B0112K0TB00E02000108000802080000

DATA Pairing DUKPT Key:
B0136B1TX00E0300010800040208000OKS18FFFF0000000000000000

PIN Pairing DUKPT Key:
B0136B1TX00E0300010800030208000OKS18FFFF0000000000000000

Command:

Task ID	'65’ or '75’
Function ID	'3B’

	‘46’
Length	Length of data
Data	• Length of Encrypted key ASN.1BLK • Encrypted key ASN.1 BLK, using TR31_B • Length RKL_DUKPT_KEY_KSN • RKL_DUKPT_KEY_KSN

Encrypted key ASN.1 structure::= Sequence
{
    Encrypted key ASN.1 structure version = 1 (INTEGER)
    Keys ::= Set
    {
        keyinfo ::= Sequence
        {
            TR31Key = (PRINTABLESTRING)
            keyType = (INTEGER)
            ksn = (OCTET STRING) -- If keyType is not DUKPT, 00000000000000000000
            keySlot = (INTEGER)
            keyName = (PRINTABLESTRING)
            KCV = (OCTET STRING) -- 2 bytes
        }
    }
}

Response 1:

Result byte	If success, return ACK. If failed , return NAK <Error Code>
Task ID	'56' or '57'
	‘46’
Function ID	‘3B’
Length	Length of data
Data	KCV ASN.1 structure

KCV ASN.1 structure::= Sequence
{
    KCV ASN.1 structure version = 1 (INTEGER)
    Keys ::= Set
    {
        keyinfo ::= Sequence
        {
            keyName = (PRINTABLESTRING)
            errorCode = (INTEGER) --‘0’ signifies a successful load
            errorMessage = (PRINTABLESTRING)
            KCV = (OCTET STRING) -- 3 bytes, algorithm refer to x9.24
        }

```
    }
}
```

3C – Set Working Key

Description:

Working key includes PIN/PIN Master /PIN Pairing/ Data Pairing/ MAC Key.

This command should be issued after the Card Reader and PINPAD have established the CR_PINPAD_MASTER_DUKPT_KEY.

Note:

Yellow: Optional block-KeyIndex

Green: Optional block-KeySlot

Red: Optional block-KSN/KeyID

KBH for PIN DUKPT Key:

B0136B1TX00E03000108000102080000KS18FFFF0000000000000000

MK/SK PIN Master Key:

B0112K0TB00E02000108000802080000

DATA Pairing DUKPT Key:

B0136B1TX00E03000108000402080000KS18FFFF0000000000000000

PIN Pairing DUKPT Key:

B0136B1TX00E03000108000302080000KS18FFFF0000000000000000

MAC Key:

B0136B1TX00E03000108000502080000KS18FFFF0000000000000000

Command:

Task ID	'65' or '75'
Function ID	'3C'
	'46'
Length	Length of data
Data	• Length of Encrypted key ASN.1BLK • Encrypted key ASN.1 BLK, using TR31_B • Length MASTER_DUKPT_KEY_KSN • MASTER_DUKPT_KEY_KSN

```
Encrypted key ASN.1 structure::= Sequence
{
    Encrypted key ASN.1 structure version = 1 (INTEGER)
    Keys ::= Set
    {
        keyinfo ::= Sequence
```

```
        {
            TR31Key = (PRINTABLESTRING)
            keyType = (INTEGER)
            ksn = (OCTET STRING) -- If keyType is not DUKPT, 00000000000000000000
            keySlot = (INTEGER)
            keyName = (PRINTABLESTRING)
            KCV = (OCTET STRING) -- 2 bytes
        }
    }
}
```

Response 1:

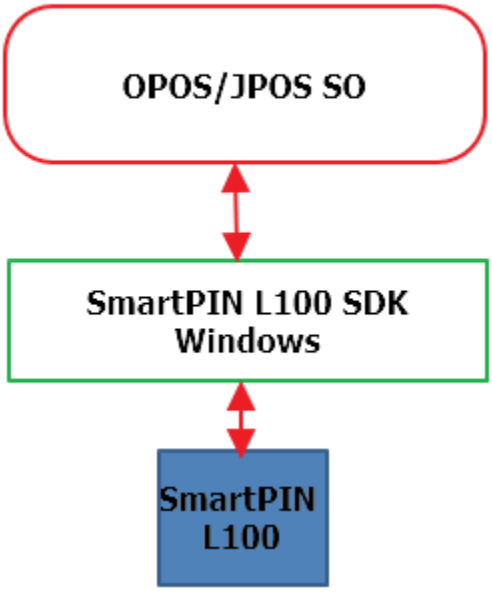
Result byte	If success, return ACK. If failed , return NAK <Error Code>
Task ID	'67' or '56' or '57'
	'46'
Function ID	'3C'
Length	Length of data
Data	KCV ASN.1 structure

```
KCV ASN.1 structure::= Sequence
{
    KCV ASN.1 structure version = 1 (INTEGER)
    Keys ::= Set
    {
        keyinfo ::= Sequence
        {
            keyName = (PRINTABLESTRING)
            errorCode = (INTEGER) --'0' signifies a successful load
            errorMessage = (PRINTABLESTRING)
            KCV = (OCTET STRING) -- 3 bytes, algorithm refer to x9.24
        }
    }
}
```

Appendix B: OPOS/JPOS

OS: Windows 7 or later, 32 bit and 64 bit
UPOS version: 1.14
JRE : Java 8 or later

Both OPOS and JPOS are supported.



Methods, Properties and Events:

AutoDisable	Unsupported
CapCompareFirmwareVersion	Unsupported
CapPowerReporting	Unsupported
CapStatisticsReporting	Unsupported
CapUpdateFirmware	Unsupported
CapUpdateStatistics	Unsupported
CheckHealthText	Full
Claimed	Full
DataCount	Full
DataEventEnabled	Full
DeviceEnabled	Full
FreezeEvents	Full
OutputID	Unsupported

PowerNotify	Unsupported
PowerState	Unsupported
State	Full
DeviceControlDescription	Full
DeviceControlVersion	Full
DeviceServiceDescription	Full
DeviceServiceVersion	Full
PhysicalDeviceDescription	Full
PhysicalDeviceName	Full
CapDisplay	Full
CapKeyboard	Unsupported
CapLanguage	Full
CapMACCalculation	Unsupported
CapTone*	Unsupported
AccountNumber	Full
AdditionalSecurityInformation	Full
Amount	Full
Currency	Full
AvailableLanguagesList	Full
AvailablePromptsList	Full
EncryptedPIN	Full
MaximumPINLength	Full
MerchantID	Full
MinimumPINLength	Full
PINEntryEnabled	Full
Prompt	Full
PromptLanguage	Full
TerminalID	Full
Track1Data	Full
Track2Data	Full
Track3Data	Full
Track4Data	Full
TransactionType	Full
Methods (UML operations)	
open (logicalDeviceName)	Full
close ( )	Full
claim (timeout)	Full
release ( )	Full
checkHealth (level)	Full

clearInput ( )	Full
clearInputProperties ( )	Full
clearOutput ( )	Full
directIO (command , inout data , inout obj object)	Full
compareFirmwareVersion	Unsupported
resetStatistics (statisticsBuffer)	Unsupported
retrieveStatistics (inout statisticsBuffer)	Unsupported
updateFirmware (firmwareFileName)	Unsupported
updateStatistics (statisticsBuffer)	Unsupported
Specific	
beginEFTTransaction (PINPadSystem , transactionHost)	Full
computeMAC (inMsg , outMsg object)	Unsupported
enablePINEntry( )	Full
endEFTTransaction (completionCode)	Full
updateKey (keyNum , key)	Unsupported
verifyMAC (message)	Unsupported
Events (UML interfaces)	
uposeventsDataEvent	Full
uposeventsDirectIOEvent	Unsupported
uposeventsErrorEvent	Full
uposeventsStatusUpdateEvent	Unsupported

*Full -- this item is full supported and functional.
*Unsupported -- this item is not supported or disabled.