Spectrum Pro Reader
Low Level API Manual

80140505-001

Rev. E

September 20, 2017

ID TECH
10721 Walker St.
Cypress, CA 90630

support@idtechproducts.com **Visit: http://www.idtechproducts.com**

Contents

1 Introduction

1.1 Purpose

The purpose of this document is to provide an overview of the communications protocols used to control the Spectrum Pro Insert Reader, and low-level (firmware) commands that can be used to control the device when communicating (for example) via USB.

Note: ID TECH makes available a Universal SDK for the Spectrum Pro (and other ID TECH products), which hides most of the complexity of dealing with low-level calls, allowing you to create apps in a high-level language, using your favorite Integrated Development Environment. Using the Universal SDK will eliminate the need to send low-level commands and will greatly facilitate debugging. We recommend that you use the Universal SDK when developing applications that talk to the Spectrum Pro. Contact your ID TECH representative for more information.

1.2 Scope

This document describes the serial communication protocol between the HOST (Customer System Control Unit), the CR (the card reader: Spectrum Pro Insert Reader), and any connected PINPAD (such as ID TECH's SmartPIN L100).

1.3 Glossary

AID	Application Identifier
BWT	Block waiting time
CBC	Cipher Block Chaining
CLRC	Card Track Data Longitudinal Redundancy Check
CR	Card Reader
CRIND	Card Reader in Dispenser
CRL	Certification Revocation List
CSR	Certificate Signing Request
DES	Data Encryption Standard
HOST	Secure System Control Unit, the controller of Card Reader
ICC	Integrated Circuit Card
ICCR	Integrated Circuit Card Reader
IV	Initialization Vector
LRC	Longitudinal Redundancy Check
LSB	Least Significant Bit(s)
MSB	Most Significant Bit(s)

PIN	Personal Identification Number
PCI	Payment Card Industry
RFU	Reserved for Future Use
RSA	An algorithm for public-key encryption
SDES	Single DES
SHA-256	Secure Hash Algorithm 256-bit digest
TDES	Triple-DES (double length = 16 bits, Key3 = Key1)
TDES3	Triple-DES (triple length = 24 bits, three independent keys)
UID	Unique Identifier

1.4 Abbreviations and Definitions for Line Level Communication

Symbol/Name	Description	Length	Value(s)
ETX	End of Text	1	0x03
LRC	Longitudinal Redundancy Check	1	0x00-0xff
ACK	Acknowledgement	1	0x06
NAK	Negative Acknowledgement	1	0x15
STX	Start of Text	1	0x02
TP_PACKET	Transport Data Packet	Variable	0x00-0xff

1.5 Notation

The following notation is used in this document.

```
()          - Encloses Variable data
<>          - Encloses symbolic reference
””          - Encloses character literal data
[]x         – Encloses data that is encrypted with key x.
[]/x        - Encloses data that is decrypted with key x.
{}          - One or more certificates
||    - Concatenation
A<B>(C)     - Computation A done using key(s)B on data C.
<Object name>:<num><type>
      - Object size is <num> of unit <type>.
              <type> not present = bytes, ‘b’ = bits
```

1.6 References and Related Documents

[1]	*EMV v4.3 Book1*	Application Independent ICC to terminal Interface Requirements
[2]	*EMVv4.3 Book3*	Application Specification
[3]	*PCI_PTS_POI_DTR*	Payment Card Industry – PIN Transaction Security – Point of Interaction – Modular Derived Test Requirements, Version 3.1
[4]	*PTS_POI_Tech_FAQ*	Payment Card Industry – PTS POS Security Requirements – Technical FAQ, Version 3
[5]	*X9 TR-31 2010*	Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms December 9, 2010
[6]	*X9 TR34-2012*	Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques: Part 1 - Using Factoring-Based Public Key Cryptography Unilateral Key Transport

2 Card Reader Communication Protocol

All transmissions are handled by the following four protocol layers:

- Physical Layer
- Data Link Layer
- Transport Layer
- Application Layer

The physical layer defines the physical connectivity between the devices: the electrical characteristics of the communication channel and the transmitted signals such as voltage levels.

The data link layer defines how data is formatted for transmission.

The transport layer defines the frame format and transferring rules: error recognition and recovery.

The application layer defines the commands, responses and the specific data contained within each packets.

2.1 Physical Layer

2.1.1 Serial Communication Parameters

2.1.1.1 UART Communication

Parameter	Specification
Transmission protocol	Asynchronous
Communication method	Full Duplex
Start bit	1 bit
Data length	8 bits (Bit7: MSB, Bit0: LSB)
Parity	None
Stop bit	1 bit
Transmission speed (Baud rate)	115200 bps (default)

The baud rate will be maintained within +2% in order to minimize data error.

2.1.1.2 USB Communication

The Product ID (PID) is 0x4010.
The Vendor ID (VID) is 0xACD.

- **Device Descriptor**

```
   0x12,          /* bLength = 18                        */
0x01,          /* bDescriptorType = Device (1)      */
0x00, 0x02,    /* bcdUSB(L/H) USB spec rev (BCD)    */
0x00,          /* bDeviceClass = Unspecified        */
0x00,          /* bDeviceSubClass                   */
0x00,          /* bDeviceProtocol                   */
0x40,          /* bMaxPacketSize0 is 64 bytes       */
0xcd, 0x0a,    /* idVendor(L/H) */
0x20, 0x31,    /* idProduct(L/H)                    */
0x00, 0x01,    /* bcdDevice -- 01.00                */
0x00,          /* iManufacturer Descriptor ID       */
0x00,          /* iProduct Descriptor ID            */
0x00,          /* iSerialNumber Descriptor ID       */
0x01           /* bNumConfigurations                */
```

- **Configuration Descriptor**

```
0x09,          /*  bLength = 9                      */
0x02,          /*  bDescriptorType = Config         */
```

```
        0x29, 0x00,     /*  wTotalLength(L/H) = 34 bytes     */
        0x01,           /*  bNumInterfaces                   */
        0x01,           /*  bConfigValue                     */
        0x00,           /*  iConfiguration                   */
        0xc0,           /*  bmAttributes (no remote wakeup) */
        0x32,           /*  MaxPower 100ma (units are 2ma/bit) */
```

First Interface Descriptor

```
        0x09,           /*  bLength = 9                      */
        0x04,           /*  bDescriptorType = Interface (4)  */
        0x00,           /*  bInterfaceNumber                 */
        0x00,           /*  bAlternateSetting                */
        0x02,           /*  bNumEndpoints (one for OUT)      */
        0x03,           /*  bInterfaceClass = HID            */
        0x00,           /*  bInterfaceSubClass
                                00: no subclass
                                01: boot interface subclass 2-255
                                reserve
                                */
        0x00,           /*  bInterfaceProtocol               */
        0x00,           /*  iInterface */
```

HID Descriptor

```
        0x09,           /*  bFunctionalLength = 5            */
        0x21,           /*  bDescriptorType = HID            */
        0x01, 0x01,     /*  bcdHID(L/H) Rev 1.1              */
        0x00,           /*  bCountryCode                     */
        0x01,           /*  bNumDescriptors                  */
        0x22,           /*  bDescriptorType = Report         */
        0x1c, 0x00,     /*  wDescriptorLength(L/H)           */
```

OUT Endpoint 2

```
        0x07,           /*  bLength                           */
        0x05,           /*  bDescriptorType (Endpoint)        */
        0x02,           /*  bEndpointAddress (EP2-OUT)        */
        0x03,           /*  bmAttributes (interrupt)          */
        0x40, 0x00,     /*  wMaxPacketSize(L/H) (64)          */
        0x04,           /*  bInterval (16 milliseconds)       */
```

IN Endpoint 1

```
        0x07,          /*  bLength                          */
        0x05,          /*  bDescriptorType (Endpoint)       */
        0x81,          /*  bEndpointAddress (EP1-IN)        */
        0x03,          /*  bmAttributes (interrupt)         */
        0x40, 0x00,    /*  wMaxPacketSize(L/H) (64)         */
        0x04,          /*  bInterval (16 milliseconds)      */
```

- **HID Descriptor**

```
   0x09, //LENGTH OF THIS DESC.
   0x21, //HID DESCRIPTOR TYPE
   0x11, //
   0x01, //HID CLASS SPECIFICATION
   0x00, //HARDWARE TARGET COUNTRY
   0x01, //NUMBER OF HID CLASS DESCRIPTORS TO FOLLOW
   0x22, //REPORT DESCRIPTOR TYPE
   0x44,    //20110609
0x1F , //20110609---
   0x00, //TOTAL LENGTH OF REPORT DESCRIPTOR
```

- **HID Report**

```
   0x05, 0x02,              // USAGE_PAGE (Simulation Controls)
   0x09, 0x26,              // USAGE (Driving Control)
   0xa1, 0x01,              // COLLECTION (Application)
   0x05, 0x0c,              //   USAGE_PAGE (Consumer Devices)
   0x15, 0x00,              //   LOGICAL_MINIMUM (0)
   0x26, 0xff, 0x00,        //   LOGICAL_MAXIMUM (255)
   0x75, 0x08,              //   REPORT_SIZE (8)
   0x95, 0x40,              //   REPORT_COUNT (64)
   0x81, 0x03,              //   INPUT (Cnst,Var,Abs)
   0x09, 0x00,              //   USAGE (Undefined)
   0x75, 0x08,              //   REPORT_SIZE (8)
   0x95, 0x40,              //   REPORT_COUNT (64)
   0x91,0x03, 0xc0
```

2.2 Data Link Layer

2.2.1 Control Word

The data link layer defines the protocol used between the HOST and the Card Reader. All data link control is accomplished by a "select" sequence. The HOST acts as the master and issues the "select sequence" to send/receive data.

Two methods of error detection are employed by this protocol to attempt to insure data integrity. An even parity check and sum check are performed on each character, and a longitudinal redundancy check (LRC) and CHECKSUM are performed to total data bits within the message block.

The LRC/CHECKSUM characters are accumulated at both the sending and receiving stations during transmission of a data block. The accumulated value is transmitted before the ETX character. The received LRC/CHECKSUM characters are compared to the locally calculated LRC/CHECKSUM characters; the two LRCs/CHECKSUMs will match exactly on a 'good' transmission. They will be different if a longitudinal error occurred. The LRC/CHECKSUM values are calculated by XORing (LRC) or adding (CHECKSUM) all data bytes that will be included in the <TP_PACKET>. Simply XOR all bytes together, or ADD all bytes together and discard overflow (keeping just the lowest 8 bits).

The parity check, LRC, and CHECKSUM should be used in combination to insure data integrity.

The protocol allows the transmission of any data character in the range 0x00 to 0xff.

2.2.2 Wake Up from Low Power Mode

Spectrum Pro has various sleep and low-power modes, described hereunder.

Note that when RS-232 communication is used, the serial bus can be monitored to determine when the reader is "waking up." (It will wake up whenever a card is inserted in the slot. Hence, this wakeup can be used to help determine whether a card is being presented. You can put the unit to sleep programmatically, then listen for the wakeup.)

When Spectrum Pro wakes up, the following bytes are sent (by Spectrum Pro) over the serial bus:

```
02 05 00 67 46 51 00 00 70 fe 03
```

STX is 0x02. Payload length is 05 00. Task ID is 67. Function ID is 51. Data is 00 00. LRC is 70, checksum is FE. ETX is 0x03.

The Wakeup function is described immediately below. Run modes are described below that. (LLS = Low Leakage Stop. LLWU = Low Leakage Wake Up.)

Function 51 – Wakeup Signal

Output:

Result byte	If the packet is correctly formed, the following status byte is possible: • Complete
Task ID	'67' or '27'
Function ID	'51'
Length	0
Data	None

Run Mode: Target current: 120mA
If card is in the slot, no low power mode is allowed.

Sleep Mode: Target current: 15uA on K21 (LLS) + 30uA on NFC chip (100ms wake up mode) + 120uA on MSR Head + 6uA on UART chip at 25C. Device can be awakened by either communication or Magnetic/Contactless Card or Switches or press button.

For Magnetic and Smart Card, Front Switch and Seated Switch will wake up the device.

For Contactless, the NFC chip will enter wake-up mode, with 200ms timeout and 20us wake-up period. When the chip detects amplitude change, it will send IRQ to wake up K21 from LLS mode. From the LLWU event to power on it takes 0.3ms (K21 LLS->RUN requires 5us max., LLWU ISR requires 270us).

Low Power Sleep Mode: Target current: 15uA on K21 (LLS) + 30uA on NFC chip (100ms wake up mode) + 6uA on UART chip at 25C. Device can be awakened by either communication or Contactless Card or Switches or press button.

For Serial Communication, ten extra bytes (ten 0xff values) should be send out to wake up Card Reader from LLS mode (K21 LLS->RUN requires 5us max, LLWU ISR requires 270us and PLL initialization requires 270us). By sending out 0xffs on Serial port, the start bit appears as a pulse to trigger the LLWU pin interrupt, then all the other bits appears as 1 which can generate the IDLE status for Serial port. All the bytes follows 0xffs can be received by Card Reader, which is Control Package described below.

For USB Communication, device can only enter VLPS mode instead of LLS mode, this will add an extra 20uA on the K21. When there is activities on USB, it will wake up K21 from VLPS mode and K21 issues a USB rest event on the bus then starts USB enumeration. The USB enumeration takes about 5 seconds depends on the HOST.

Front Switch and Seated Switch will wake up the device.

For Contactless, the NFC chip will enter wake-up mode, with 200ms timeout and 20us wake-up period. When the chip detects amplitude change, it will send IRQ to wake up K21 from LLS mode. From the LLWU event to power on it takes 0.3ms (K21 LLS->RUN requires 5us max., LLWU ISR requires 270us).

When device is awakened by communication, K21 will enter Sleep Mode which enables card reading function. Device goes back to Stop Mode if it keeps in IDLE mode for 2 minutes. IDLE means there is no any communication and no card reading action.

Stop Mode: Target current: 15uA on K21 (LLS) + 5uA on NFC chip (Power-down mode) + 6uA on UART chip at 25C. Device can be awakened by either communication or Switches or press button.
For Serial Communication, ten extra bytes 0xffs should be send out to wake up Card Reader from LLS mode (K21 LLS->RUN requires 5us max., LLWU ISR requires 270us and PLL initialization requires 270us). By sending out 0xffs on Serial port, the start bit appears as a pulse to trigger the LLWU pin interrupt, then all the other bits appears as 1 which can generate the IDLE status for Serial port.

For USB Communication, device can only enter VLPS mode instead of LLS mode; this will add an extra 20uA on the K21. When there are activities on USB, it will wake up K21 from VLPS mode and K21 issues a USB rest event on the bus, then starts USB enumeration. The USB enumeration takes about 5 seconds and depends on the HOST.

Front Switch and Seated Switch will wake up the device.
.
For Contactless, the NFC chip will enter Power-down mode.

From the LLWU event to power on it takes 0.3ms (K21 LLS->RUN requires 5us max., LLWU ISR requires 270us).

When device is awakened by communication, K21 will enter Sleep Mode which enables card reading function. Device goes back to Stop Mode if it keeps in IDLE mode for 2 minutes. IDLE means there is no any communication and no card reading action.

Low Power Stop Mode: Target current: 10uA on K21 (VLLS0) + 5uA on NFC chip (Power-down mode) + 6uA on UART chip at 25C. Device can only be awakened by Switches or press button or conditional communication.

For Serial Communication, 0xff should be send out to wake up Card Reader from VLLS0 mode. By sending out 0xff on Serial port, the start bit appears as a pulse to trigger the LLWU pin interrupt, then K21 starts reset.

Front Switch and Seated Switch will wake up the device.

From the VLLS0 event to power on it takes 100ms, including reset.

Very Low Power Stop Mode: Target current: 10uA on K21 (VLLS0) at 25C. Device can only be awakened by Switches or press button.

Front Switch and Seated Switch will wake up the device.

From the VLLS0 event to power on it takes 100ms, including reset.

2.2.3 Control Package

Command and response Format:
<STX><LenL><LenH><TP_PACKET><LRC><CHECKSUM><ETX>

Note:
<LenL><LenH> is a two byte length of <TP_PACKET>
<LRC> and <CHECKSUM> are calculated for <TP_PACKET>

2.2.4 Select Sequence

Selection is used by the HOST to transmit data to the Card Reader.

The following is an example of how the select sequence is formatted:
<STX><LenL><LenH><TP_PACKET><LRC><CHECKSUM><ETX>

The Card Reader will send one of the following responses to a select sequence:

Example 1.1: Select sequence and received ok, Reader response received ok

HOST / READER
<STX><LenL><LenH><TP_PACKET><LRC><CHECKSUM><ETX> —>

<—<STX><LenL><LenH><TP_PACKET><LRC><CHECKSUM><ETX>

Example 1.2: Select sequence and received ok, Reader response received in error

HOST / READER
<STX><LenL><LenH><TP_PACKET><LRC><CHECKSUM><ETX> —>
<—<STX><LenL><LenH><TP_PACKET><LRC><CHECKSUM><ETX>
<STX><LenL><LenH><NAK><Result Byte><LRC><CHECKSUM><ETX> —>
<—<STX><LenL><LenH><TP_PACKET><LRC><CHECKSUM><ETX>

Example 2: Select sequence, received <STX> in error

HOST / READER
<STX><LenL><LenH><TP_PACKET><LRC><CHECKSUM><ETX> —>

Example 3: Select sequence, received in error and retransmitted

HOST / READER
<STX><LenL><LenH><TP_PACKET><LRC><CHECKSUM><ETX> —>
<— <STX><LenL><LenH><NAK><Result Byte><LRC><CHECKSUM><ETX>
<STX><LenL><LenH><TP_PACKET><LRC><CHECKSUM><ETX> —>
<—<STX><LenL><LenH><TP_PACKET><LRC><CHECKSUM><ETX>

Example 4: Select sequence, received in error, retransmitted with "n" retries

HOST / READER
<STX><LenL><LenH><TP_PACKET><LRC><CHECKSUM><ETX> —>
<— <STX><LenL><LenH><NAK><Result Byte><LRC><CHECKSUM><ETX>
<STX><LenL><LenH><TP_PACKET><LRC><CHECKSUM><ETX> —>
<—<STX><LenL><LenH><NAK><Result Byte><LRC><CHECKSUM><ETX>

<<Sent "n" retries, see Errors and Handling>>, n is 5

Note: NAK must be sent in BWT (see Errors and Handling) when it is needed, otherwise the sender will not be able to resend the message because any data in a raw communication buffer is kept no longer than BWT.

2.3 Transport Layer

2.3.1 Format

A transport packet (TP_PACKET) consists of a variable length data packet. The transport packet has the following format:

Command Packet:

Data Field

Task ID	0x46 ('F')	Function ID	[Length]	[DATA]
1 byte	1 byte	1 or 2 bytes	2byte	0 to 4096 bytes

Response Packet:

- **If command protocol is wrong**

Data Field				
NAK	Result byte	Task ID	0x46 ('F')	Function ID
1 byte	2 byte	1 byte	1 byte	1 byte or 2 bytes

NOTE: Some commands have two bytes for the Function. The response packet will also return two bytes for Function if the original command used two bytes.

- **If command protocol is correct**

Data Field					
ACK	Task ID	0x46 ('F')	Function ID	[Length]	[DATA]
1 byte	1 byte	1 byte	1 byte or 2 bytes	2 byte	0 to 4096 bytes

For each message received from the HOST, the Card Reader must only validate the LRC before processing the message.

2.3.2 Data Packet

The TP_PACKET is either directed to the transport layer or the application layer for processing. All TP_PACKETs that begin with 0x00 thru 0xFF are to be processed by the application layer.

2.3.3 Length of Data

The length field in transport layer is by default formatted as: 2 byte, unsigned, little-endian: <LenL><LenH>

2.4 Errors and Error Handling

2.4.1 Link layer errors and handling

The data link layer must handle errors in such a manner that the system can recover without loss of data from errors and unexpected conditions encountered during message communication.

The following errors will be detected by the link layer:

1. BWT time-out

   The maximum interval between the leading edge of the start bit of the last character that gave the right to send to the Card Reader and the leading edge of the start bit of the first character sent by the Card Reader. It is recommended that the time-out period for BWT is 500 milliseconds.

2. Wrong control symbols in some positions of STX, ETX, NAK.
3. Transmission error, including parity, LRC and CHECKSUM error
4. Message buffer overflow: Receipt of message, which is greater than the buffering capabilities of the Card Reader, will cause the Card Reader to transmit a NAK response to the message.

If any of the above errors occur, the Card Reader should not process the message and should wait for the Controller to retry the select sequence.

If any of the above errors occur in the message from a card reader, the HOST should have three times transport layer tries. If the error still happens after the tries, the transport layer should report to application layer.

2.4.2 Transport layer errors and handling

After three tries, the transport layer should report an error to the application layer.

2.5 Application Layer

2.5.1 Task ID

To / From	K21 HUB	MSR Header	Contactless	PINPAD	CHIPCARD Reader	Host
K21 HUB	N/A	'23'	'24'	'25'	'26'	'27'
MSR Header	'32'	N/A	'34'	'35'	'36'	'37'
Contactless	'42'	'43'	N/A	'45'	'46'	'47'
PINPAD	'52'	'53'	'54'	N/A	'56'	'57'
CHIPCARD Reader	'62'	'63'	'64'	'65'	N/A	'67'
Host	'72'	'73'	'74'	'75'	'76'	N/A

2.5.2 Result Codes (Error Codes)

Type	Result byte	Meaning
General	'90','31'	Unknown command
	'90',‘32’	Wrong parameter (such as the length of the command is incorrect)
	'90',‘3A	Number of retries over limit
State error	'90',‘40’	Invalid Manufacturing system data
	'90',‘41’	Not authenticated
	'90',‘42’	Invalid Master DUKPT Key
	'90',‘43’	Invalid MAC Key
	'90',‘44’	Reserved for future use
	'90',‘45’	Reserved for future use
	'90',‘46’	Invalid DATA DUKPT Key
	'90',‘47’	Invalid PIN Pairing DUKPT Key
	'90',‘48’	Invalid DATA Pairing DUKPT Key
	'90',‘49’	No nonce generated
	'90',‘4A	Not ready
	'90',‘4B’	Not Mag data
Data error	'90',‘50’	Invalid Certificate
	'90',‘51’	Duplicate detected
	'90',‘52’	AT checks failed
	‘90’,‘53	TR34 checks failed
	‘90’,‘54	TR31 checks failed
	‘90’,‘55	MAC checks failed
	‘90’,‘56	Firmware download failed

Resource	‘90’,‘60	Log is full
	‘90’,‘61	Removal sensor unengaged
	‘90’,‘62	Any hardware problems
Third party	‘90’,‘70	ICC communication timeout
	‘90’,‘71	ICC data error (such check sum error)
	‘90’,‘72	Smart Card not powered up
ICC EMV	‘F2’,‘00	No AID or No Application Data
	‘F2’,‘01	No Terminal Data
	‘F2’,‘02	Wrong TLV format
	‘F2’,‘03	AID list is full, maxim is 16
	‘F2’,‘04	No any CA Key
	‘F2’,‘05	No CA Key RID
	‘F2’,‘06	No CA Key Index
	‘F2’,‘07	CA Key list is full, maxim is 16
	‘F2’,‘08	Wrong CA Key hash
	‘F2’,‘09	Wrong Transaction Command Format
	‘F2’,‘0	Unexpected Command
	‘F2’,‘0	No CRL
	‘F2’,‘0	CRL list is full, maxim is 90
	‘F2’,‘0	No amount , other amount and transaction type in Transaction Command
	‘F2’,‘0E	Wrong CA Hash and Encryption algorithm
	‘F2’,‘0F	No Financial Card
	‘F2’,‘10	Invalid CRL length
	‘F2’,‘11	ICC L2 is not in idle state
	‘F2’,‘12	Transaction Type Error
	‘F2’,‘13	Can’t modify major bits in terminal setting
	‘6C’,’00’	Unknown parameter in command – Protocol task ID and command are right, but length is out of the requirement.
	‘6A’,’0	Unsupported Command – Protocol and task ID are right, but command is
	‘60’,’00	Save or Config Failed / Or Read Config Error, Flash Error
	‘62’,’02	No TransArmor TID

2.6 Commands Reference

Consolidated Command Listing (Alphabetical by Command Name)
Note that some commands are one byte; some are two bytes.

Command	Name
45	Activate and Deactivate Removal Sensor
05 02	Authenticate Card and Process Transaction
05 03	Authenticate Issuer and Process Transaction
06	Cancel Transaction
91	Clear Log, Manufacture
0A 02	Clear Transaction Log
42	Configure Card Reader
B0	Display and Get Key
81	Download Firmware (for K21 HUB or Maxq1050)
22	Enter Low Power Mode
30	Get Card Data
3E	Get DUKPT KSN
61	Get ICC Status
27	Get Nonce
43	Get Parameters
21	Host gets CR Version, UID and Session Control
60	Manually Lock Card and Power On Card
25	Poll Card Reader
67	Power Down and Remove ICC Card
82	Program Chip (for K21 HUB or Maxq1050)
31	Purge Card Data
90	Read Log
01 04	Remove All Application Data
04 04	Remove All CA Public Key
85 04	Remove All CRLs
01 02	Remove Application Data
04 02	Remove CA Public Key
85 02	Remove CRLs
02 02	Remove Terminal Data
03 01	Retrieve AID List
01 01	Retrieve Application Data
04 01	Retrieve CA Public Key
04 05	Retrieve CA Public Key List
85 01	Retrieve CRLs
08 01	Retrieve EMV L2 Version
09 01	Retrieve Kernel Check Value
08 02	Retrieve Kernel Version
02 01	Retrieve Terminal Data
87 01	Retrieve Terminal ID
88 01	Retrieve Terminal Major Configuration

07 01	Scripting and Retrieve Transaction Result
94	Self Test
01 03	Set Application Data
04 03	Set CA Public Key
85 03	Set CRLs
02 03	Set Terminal Data
87 03	Set Terminal ID
88 03	Set Terminal Major Configuration
80	Start Firmware Upgrade (for K21 HUB or Maxq1050)
05 01	Start Transaction
2E	Warm Reset

Consolidated Command Listing (Sorted by Command Number)

Command	Name
01 01	Retrieve Application Data
01 02	Remove Application Data
01 03	Set Application Data
01 04	Remove All Application Data
02 01	Retrieve Terminal Data
02 02	Remove Terminal Data
02 03	Set Terminal Data
03 01	Retrieve AID List
04 01	Retrieve CA Public Key
04 02	Remove CA Public Key
04 03	Set CA Public Key
04 04	Remove All CA Public Key
04 05	Retrieve CA Public Key List
05 01	Start Transaction
05 02	Authenticate Card and Process Transaction
05 03	Authenticate Issuer and Process Transaction
06	Cancel Transaction
07 01	Scripting and Retrieve Transaction Result
08 01	Retrieve EMV L2 Version
08 02	Retrieve Kernel Version
09 01	Retrieve Kernel Check Value
0A 02	Clear Transaction Log
21	Host gets CR Version, UID and Session Control
22	Enter Low Power Mode
25	Poll Card Reader
27	Get Nonce
2E	Warm Reset
30	Get Card Data
31	Purge Card Data
3E	Get DUKPT KSN
42	Configure Card Reader

43	Get Parameters
45	Activate and Deactivate Removal Sensor
60	Manually Lock Card and Power On Card
61	Get ICC Status
67	Power Down and Remove ICC Card
80	Start Firmware Upgrade (for K21 HUB or Maxq1050)
81	Download Firmware (for K21 HUB or Maxq1050)
82	Program Chip (for K21 HUB or Maxq1050)
85 01	Retrieve CRLs
85 02	Remove CRLs
85 03	Set CRLs
85 04	Remove All CRLs
87 01	Retrieve Terminal ID
87 03	Set Terminal ID
88 01	Retrieve Terminal Major Configuration
88 03	Set Terminal Major Configuration
90	Read Log
91	Clear Log, Manufacture
94	Self Test
B0	Display and Get Key

2.6.1 20 – Pass-Through Mode Control

Description:

Puts unit in pass-through mode. This command can be issued any time.

For Pass-Through mode, SP passes all the commands to PinPad.

For non-Pass-Through mode, SP doesn't pass commands to PinPad until this command is run.

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	06	00	72 46 20 <LengthL><LengthH> <Data>	14	DA	03

Output Hex String: 02060072462001000114DA03

In this example:
Length of data is 01 00 and data is 01, where data can be one of:
00 – Pass-through mode OFF (default)
01 – Pass-through mode ON

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Any hardware problems • Wrong parameter
Task ID	'27'
Function ID	'20'
Length	0
Data	None

2.6.2 21 – Get CR Version, UID, and Session Control

Description:

This command may be issued when Card Reader/PINPAD is in any state.

The Card Reader will respond with the version of the firmware and the 8-byte Unique ID (UID) installed in the device.

After Card Reader/PINPAD processes the command, it starts/ends the session for this specific HOST.

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	13	00	76 46 21 <OverallLenL><OverallLenH> <HOSTIDLenL><HOSTIDLenH> <HOST ID> <TIMEOUTLenL><TIMEOUTLenH> <TIMEOUT>	71	75	03

Output Hex String: 0213007646210e000800000102030405060702006400717503

In this example:
Timeout is 64 00 (little-endian; 100 seconds), length of Timeout data is 02 00.
HOST ID is 0001020304050607, length of HOST ID is 08 00.
Overall data length is thus 0E 00 (2 bytes timeout data, 8 bytes HOST ID, 2 bytes each for lengths).

Data must include:
• Overall length (little-endian) means total length of data
• Length of HOST ID portion of data in 2 bytes (little endian)
• HOST ID (range 0x01~0xFF)
• Length of Session Timeout for this HOST ID, in 2 bytes (little endian)
• Session Timeout (in Seconds) for this HOST ID: Little endian. Zero means the immediate end of Session. All 0xff means never timeout.

For each HOST ID, CR/PINPAD assigns a 100kbyte (25 pages) sector in the external flash memory for key and configuration storage.

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02		00	06 <DATA>			03

Response Hex String:
02d30006674621cd00080068005000191b03652700494420544543482053706563747
2756d2050726f204669726d776172652056312e30302e3039312a0049442054454348
20537065637472756d2050726f204170706c69636174696f6e2056312e30302e303937
2e00494420544543482053706563747 2756d50726f204861726477617265205665727
3696f6e2056312e30362e3030312d00494420544543482054 4d332053656375726548
656164205253323332205350205265616465722056 20352e33330a000000000000000
0000000010002fb4303

Where DATA is:
• Length of Unique identification number (UID).
• Unique identification number (UID), 8 bytes.
• Length of firmware version.
• ANSI string "ID TECH Spectrum Pro Firmware x.yy.zzz": x-major release; yy-release version; zzz-debug version.
• Length of application version.
• ANSI string "ID TECH Spectrum Pro Application Vx.yy.zzz": x-major release; yy-release version; zzz-debug version.
• Length of MSR Header version, (Optional for Manufacture test).
• ANSI string MSR Header “ID TECH TM3 SecureHead RS232 SP Reader V x.yy”: x-major release; yy-minor firmware version.
• Length of hardware version.
• Hardware version ANSI string "ID TECH SpectrumPro Hardware Version x.yy.zzz": x-major release; yy-main board version; zzz-SecureHead version.
• Length of ID TECH S/N.
• ID TECH S/N derived from UID; 10 bytes.
• Length of Symmetric or Asymmetric flag.
• Symmetric or Asymmetric flag
    0 - Symmetric only
    1- Asymmetric only
    2- Both Symmetric and Asymmetric

Note: Check value is using 2-byte CRC.

2.6.3 22 – Enter Low Power Mode (Applies to UART interface ONLY)

Description:

This command may be issued when CR is in any state, but requires UART interface. (For USB interface, USB Bus will control the low power mode.)

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	06	00	76 46 22 <LenL><LenH><Data>			03

Where:
LenL is the low byte of the length of overall data.
LenH is the high byte of the length of overall data.
Data is:
• Length of Timeout, 2 bytes
• Time out for automatically entering Low Power mode, in seconds, 1 byte.
Note: 0 for disabling automatically enter timeout.
• Length of Low power mode, 2 bytes
• Low power mode type, 1 byte:
0- Normal run mode
1- Low Power Sleep mode: MSR off, Contactless on, UART on, Switch on
2- Stop mode: MSR off, Contactless off, UART on, Switch on
3- Low Power Stop mode: MSR off, Contactless off, UART on, Switch on
4- Very Low Power Stop mode: MSR off, Contactless off, UART off, Switch on

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02	06	00	06 67 46 22 00 00	05	D5	03

Response Hex String: 02060006674622000005d503

Success: 06 (ACK) or else Not Ready or Wrong Parameter.

2.6.4 23 – Host Get CR/PINPAD Version (Verbose)

Description:

This command gets the detailed firmware version info for the unit. The command may be issued when Card Reader/PINPAD are in any state.

The Card Reader will respond with the UID (8 bytes) and version of the firmware, hardware, etc., as below.

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	05	00	76 46 23 00 00	13	DF	03
Command Hex String: 020500764623000013DF03						

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02	06	00	06 67 46 23 <LenL><LenH><Data>	05	D5	03

Response Hex String (example): 02 27 01 06 67 46 23 21 01 08 00 39 00 50 00 2a 5c e3 65 27 00 49 44 20 54 45 43 48 20 53 70 65 63 74 72 75 6d 20 50 72 6f 20 46 69 72 6d 77 61 72 65 20 56 31 2e 30 30 2e 31 31 35 2a 00 49 44 20 54 45 43 48 20 53 70 65 63 74 72 75 6d 20 50 72 6f 20 41 70 70 6c 69 63 61 74 69 6f 6e 20 56 31 2e 30 30 2e 31 33 37 27 00 49 44 20 54 45 43 48 20 53 70 65 63 74 72 75 6d 20 50 72 6f 20 48 61 72 64 77 61 72 65 20 56 31 2e 30 36 2e 30 30 30 2d 00 49 44 20 54 45 43 48 20 54 4d 33 20 53 65 63 75 72 65 48 65 61 64 20 52 53 32 33 32 20 53 50 20 52 65 61 64 65 72 20 56 20 35 2e 33 34 35 00 49 44 20 54 45 43 48 20 53 70 65 63 74 72 75 6d 20 50 72 6f 20 41 70 70 6c 69 63 61 74 69 6f 6e 20 42 6f 6f 74 6c 6f 61 64 65 72 20 56 31 2e 30 30 2e 30 30 31 31 00 49 44 20 54 45 43 48 20 53 70 65 63 74 72 75 6d 20 50 72 6f 20 46 69 72 6d 77 61 72 65 20 42 6f 6f 74 6c 61 64 65 72 20 56 31 2e 30 30 2e 30 30 30 8a ea 03

ASCII:
ID.TECH.Spectrum.Pro.Firmware.V1.00.115*.ID.TECH.Spectrum.Pro.Application.V1.00.137'.ID.TECH.Spectrum.Pro.Hardware.V1.06.000-.ID.TECH.TM3.SecureHead.RS232.SP.Reader.V.5.345.ID.TECH.Spectrum.Pro.Application.Bootloader.V1.00.0011.ID.TECH.Spectrum.Pro.Firmware.Bootlader.V1.00.000

Success: 06 (ACK)
Error: Any hardware problems.

Length (little-endian): 21 01

Data:
• Length of Unique identification number (UID) – 8 bytes
• Unique identification number (UID), 8 bytes.
• Length of firmware version
• ANSI string "ID TECH Spectrum Pro Firmware x.yy.zzz": x-major release; yy-release version; zzz-debug version
• Length of application version
• ANSI string "ID TECH Spectrum Pro Application Vx.yy.zzz": x-major release; yy-release version; zzz-debug version
• Length of hardware version
• Hardware version ANSI string "ID TECH SpectrumPro Hardware Version x.yy.zzz": x-major release; yy-main board version; zzz-SecureHead version
• Length of MSR Header version (Optional for Manufacture test)
• ANSI string MSR Header “ID TECH TM3 SecureHead RS232 SP Reader V x.yy”: x-major release; yy-minor firmware version
• Length of application bootloader version
• ANSI string "ID TECH Spectrum Pro Application Bootloader Vx.yy.zzz": x-major release; yy-release version; zzz-debug version
• Length of firmware bootloader version
• ANSI string "ID TECH Spectrum Pro Firmware Bootloader x.yy.zzz": x-major release; yy-release version; zzz-debug version

2.6.5 25 – Poll Card Reader

Description:

This command can be issued when Card Reader is in any state.

The Card Reader responds to this command with six status bytes.

After Card Reader processes the command, the state does not change.

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	05	00	76 46 25 00 00	15	E1	03
Output Hex String: 020500764625000015e103 Command is 76 46 25 and zero length of data: 00 00						

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02	0C	00	06 67 46 25 <DataLenL><DataLenH><Data>	57	89	03
Response Hex String: 020c000667462506000000 4034082f578903 Where Length will generally be 06 00. Data will be the 6 data bytes (bytes 0 thru 5) discussed in the tables further below.						

Command:

Task ID	'76'
Function ID	'25'
Length	0
Data	None

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter
Task ID	'67'
Function ID	‘25’

Length	Length of data
Data	• Byte 0: Key Status 0 • Byte 1: Key Status 1 • Byte 2: Tamper Status • Byte 3: Voltage of Backup Battery(V) • Byte 4: Card Status • Byte 5: Peripheral Status

Key Status 0 (Byte 0) is coded as shown in the following table.

b7	b6	b5	b4	b3	b2	b1	b0	Meaning
x								MFK and RSA Key pairs are valid if set to 1
	x							Data Key valid if set to 1
		x						RKI Key valid if set to 1
			x					Device Manufacturing CA data valid if set to 1
				x				MAC Key valid if 1
					x			RFU
						x		Authenticated with Host if set to 1
							x	Device Manufacturing Secure data valid if set to 1

Note: The 'Reader Manufacturing system data valid' means

- All HOST static certificates have passed signature check
- ALL CR certificates including CERT_CEK and CERT_CSK have passed signature check
- The private keys CEKs and CSKs have passed integrity check.

Key Status 1 (Byte 1) is coded as shown in the following table.

b7	b6	b5	b4	b3	b2	b1	b0	Meaning
x								LCL-KEK valid if set to 1
	x							PCI Pairing valid if set to 1
		x						PIN Pairing Key valid if set to 1
			x					Data Pairing Key valid if set to 1
				x				Pinpad MAC Key valid if 1
					x			RFU
						x		Authenticated with Pinpad if set to 1
							x	RFU

Tamper Status (Byte 2) is coded as shown in the following table:

b7	b6	b5	b4	b3	b2	b1	b0	Meaning
x								Removal Tamper Error if set to 1
	x							Tamper Switch#2 Error if set to 1
		x						Maxq Firmware Auth Error if set to 1

							x	Voltage Sensor Error if set to 1
						x		Temperature Error if set to 1
					x			Battery Backup Error if set to 1
				x				Tamper Switch#1 Error if set to 1
			x					K21 Firmware Auth Error if set to 1

Note:

- The Firmware Auth error is described in the section of Security Handling.
- The 'Other Tamper Error' can be used to indicate an unknown tamper, but it needs to be addressed in the log file.

Backup Battery Status (Byte 3) is coded as shown as follows.

```
0x32 : > 3.2V
0x31 : > 3.1V
   …
0x24 : > 2.4V
0x23 : > 2.3V
```

Card Status (Byte 4) is coded as shown in the following table:

b7	b6	b5	b4	b3	b2	b1	b0	Meaning
x								Tamper detector active if set to 1
	x							Removal sensor active if set to 1
		x						Latch Mechanism Active if set to 1
			x					Card Present (Seated Switch) if set
				x				Removal sensor disconnected if set
					x			Card Insert (Front Switch) if set to
						x		Mag Data Present if set to 1
							x	Log is full if set to 1

Note:

- The 'Latch Mechanism Active' means an IC card seating, latched and powered.
- The 'Card Present' is set when card seated sensor is pressed.
- The 'ICC Present' bit indicates a card is seating and it is an IC card.
- The 'Card Insert' bit is set when card front sensor is pressed.
- The 'Mag Data Present' flag is set when card data (most likely magnetic stripe card data) is ready. When the card data has been sent to the HOST, this flag is reset.

Peripheral Status (Byte 5) is coded as shown in the following table:

b7	b6	b5	b4	b3	b2	b1	b0	Meaning
x								0-Maxq Manufacture FW; 1-Maxq Production
	x							0-K21 Manufacture FW; 1-K21 Production FW
		x						MSR Header connected if set to 1

			x	PINPAD connected if set to 1
			x	0-Test Certificates; 1-Production Certificates
			x	Host connected if set to 1
			x	Chip card reader available if set
			x	SAM available if set to 1

Note:

- Reader can't detect Contactless antenna, so the Contactless available bit only indicates firmware has Contactless function or not.

2.6.6 27 – Get Nonce

Description:

This command may be issued when Card Reader/PINPAD is in any state.

This command must be used just before a command (that requires NONCE values) is issued.

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 okay to use the same NONCE value again, as this would defeat the purpose of the NONCE. So after one side completes a command that uses a NONCE, it will reset the NONCE value to indicate there is no active NONCE value.

After this command, the state does not change.

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	17	00	76 46 27 <DataLenL><DataLenH><NonceLenL><NonceLenH> <Nonce>	15	7D	03
Output Hex String: 021700764627120010000001020304050607080 90A0B0C0D0E0F157D03 Where DataLenL, DataLenH is the little-endian overall data payload length, typically 0x12. NonceLenL, NonceLenH is the nonce length, little-endian: 10 00 (16 bytes) Nonce is 16 bytes.						

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02	18	00	06 <Data>	46	36	03
Response Hex String: 0218000667462712001000 3d03d0f9870dd38da8fc0719346324be463603						

Command:

Task ID	‘76’ or '65' or '75'
Function ID	'27'
Length	Length of data

Data	• Length of NONCE • NONCE, HOST or CR, 16 bytes

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter
Task ID	‘67’ or '56' or '57'
Function ID	‘27’
Length	Length of data
Data	• Length of NONCE • NONCE, CR or PINPAD, 16 bytes

2.6.7 30 – Get Card Data

Description:

When card data are available or a card read error has occurred, the Get Card Data response is returned as described below. It requires the ready state.

For each Bank Card Data session that returns available data or card read error, the data is encrypted using `DATA_DUKPT_FUTURE_KEY_TABLE`. CR MUST advance `DATA_DUKPT_KEY`_KSN and update `DATA_DUKPT_FUTURE_KEY_TABLE` before encrypting new card data.

NOTE: The card reader will limit the number of transactions to 120 transactions per hour.

The card reader (CR) has a combined ICC and MSR; when the MSR of the card is read and the service code begins with a '2' or '6' indicating that an ICC is present, CR will process the transaction using the ICC. When CR attempts and fails to read the ICC but the MSR is successfully read, the terminal will set the POS Entry Mode Code in the transaction message(s) to 'Magnetic stripe read, last transaction was an unsuccessful IC read' if the service code on the magnetic stripe indicates that an ICC is present. Payment system rules determine whether fallback to MSR is allowed after the failure of an IC-read transaction.

Here is the flow for a card read process:

- MSR read on insertion
- If no MSR data on insertion, or MSR data exists but Service Code begins with a '2' or '6', read ICC; else wait for MSR read on card withdrawn
- For read ICC, send out ICC data if success, fallback to MSR read on withdrawn if ICC failed and fallback is enabled.
- MSR read on card withdrawn

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	05	00	76 46 30 00 00 00	00	EC	03
Output Hex String: 02060076463000000000EC03						

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02	87	00	See below	BD	F3	03
Response Hex String: 028700805700240082923b353435372a2a2a2a2a2a2a2a303031323d2a2a2a2a2a2a2a2a2a2a2a2a2a2a2a2a2a2a2a3f2a8734cd14763ba466c4f1cff08e533a6f8cd6058da4c1642f89a						

4657b297e5063ca2310ba9dc42718e6ebb4e93f9ff9658d72b51b21502197549c9b06e4
72cecf2467aeaa4190fbaf53505450524f30303031ec9d18bbc6738c4000eebdf303

Command:

Task ID	'76'
Function ID	'30'
Length	0
Data	None

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • No mag data
Data	Card Data

The Card Data is structured according to the specification below.

- Card encoding type (80: ISO/ABA 81: AAMVA, 83: Others)
- Track status (bit 0,1,2:T1,2,3 decode, bit 3,4,5:T1,2,3 sampling, bit 6: 1-SHA256, 0-SHA1, bit7: Extend field)
- Track 1 unencrypted length (1 byte, 0 for no track1 data)
- Track 2 unencrypted length (1 byte, 0 for no track2 data)
- Track 3 unencrypted length (1 byte, 0 for no track3 data)
- Clear/masked data sent status (bit 0,1,2:T1,2,3 clear/mask data present, bit 3:0-DUKPT, bit 4:0-TDES/1-AES, bit5:0-No ICC/1-use ICC, bit 6:0-Data variant, bit 7: Maghead SN)
- Encrypted/Hash data sent status (bit 0,1,2:T1,2,3 encrypted, bit 3,4,5:T1,2,3 hash, bit6:0-no session ID, bit 7: KSN)
- Extend field-1 (bit 0:Hash-SHA256)
- Track 1 masked
- Track 2 masked
- Track 3 masked
- Track 1 encrypted (TDES2/AES-128 encrypted data)
- Track 2 encrypted (TDES2/AES-128 encrypted data)
- Track 3 encrypted (TDES2/AES-128 encrypted data)
- Track 1 hashed (32 bytes Prepending Salted-SHA256-Xor)
- Track 2 hashed (32 bytes Prepending Salted-SHA256-Xor)
- Track 3 hashed (32 bytes Prepending Salted-SHA256-Xor)
- DATA DUKPT Key KSN (10 bytes)

For further details on the MSR data output format, see ID TECH 80000502-001, *Encrypted Data Output*.

Notes:

Track 1, Track 2 and Track 3 Unencrypted Length

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

Track 1, Track 2 and Track 3 Masked

Track data masked with '*'. The first and last four characters in PAN can be in the clear. Account name is in clear also.

Track 1, Track 2 and Track 3 Encrypted

This field is the encrypted Track data, using either TDES2-CBC with initial vector of zero. If the original data is not a multiple of 8 bytes for TDES2, the reader right pads the data with zero.

The key management scheme is DUKPT. The key used for encrypting data is the DUKPT variant Key, or Data Key. Data Key is generated by first taking the DUKPT Derived Key exclusive or'ed with 0000000000FF00000000000000FF0000 to get the resulting intermediate variant key. The left side of the intermediate variant key is then TDES2 encrypted with the entire 16-byte variant as the key. After the same steps are performed on the right side of the key, combine the two key parts to create the Data Key.

Encrypted Data Length

Track 1, Track 2 and Track 3 data are encrypted as separate fields. In order to get the number of bytes for encrypted data field, we need to get Track unencrypted length first. The field length is always a multiple of 8 bytes for TDES2. This value will be zero if there was no data on both tracks or if there was an error decoding both tracks. Once the encrypted data is decrypted, all padding zeros need to be removed.

Track 1, Track 2 and Track 3 Hashed

Salted-SHA-256 is used to generate hashed data for Track 1, Track 2, and Track 3 unencrypted data. It is 32 bytes long for each track.

2.6.8 31 – Clear Card Data

Description:

This command may be issued when Card Reader/PINPAD is in any state.

This command can be used to clear previous MSR Card Data from the buffer.

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	05	00	76 46 31 00 00	01	ED	03
Output Hex String: 020500764631000001ed03						

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02	06	00	06 67 46 31 00 00	16	E4	03
Response Hex String: 0206000667463100016e403						

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Complete • Wrong parameter

2.6.9 38 – PIN Pad Pairing

The Spectrum Pro is capable of pairing with ID TECH's SmartPIN L100 encrypting PIN pad, for a full chip-and-PIN solution.

Before running this command, ensure that the Spectrum Pro as well as the L100 PIN pad has been injected with a Pairing Key. For a detailed description of the pairing process, see document P/N 80141505-001, *ID TECH Spectrum Pro and SmartPIN L100 Pairing*.

The pairing command is 76 38 00 00.

Command:

Task ID	'76'
Function ID	'38'
Length	0
Data	None

Note: The full command string (with protocol wrapper) is:
02050076463800000 8F403.

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Duplicate detected; must do command sequence again. • TR31 checks failed • Invalid Master DUKPT key • Any hardware problems • Number of retries over limit
Task ID	'67'
Function ID	'38'
Length	0
Data	None

2.6.10 2E – Warm Reset

Description:

This command can be issued when the Card Reader is in any state.

After a card reader processes the command, the card reader will do following:

1. Card data is cleared, resetting card status bits.
2. Response data of the previous command is cleared.
3. Restart reader.

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	05	00	76 46 2E 00 00	1E	EA	03
Output Hex String: 02050076462E00001EEA03						

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02	06	00	06 67 46 2e 00 00	09	E1	03
Response Hex String: 0206000667462e000009e103						

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Complete • Wrong parameter
Length	0
Data	None

2.6.11 3E – Get DUKPT KSN

This command retrieves the current Key Serial Number for the type of key queried. If the key does not exist, the command gives an error code of 0x9042.

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	06	00	76 46 3E 01 00 02	0D	FD	03
Output Hex String: 02060076463e0100020dfd03						

Command:

Task ID	'76'
'Function ID	'3E'
Length	Length of data
Data	• Key Index, 1 byte 0x2 – Data Encryption Key (DEK) 0x5 – MAC Key (MAC) 0xA – PCI Pairing Key (PCK), BDK for PINPAD and IPEK for Reader 0xC – RKI Key Encryption Key (RKI-KEK 0x14 – LCL-KEK

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Invalid Master DUKPT key • Any hardware problems
Task ID	'67'
Function ID	'3E'
Length	Length of DUKPT KSN (0x0A – ten bytes)
Data	• DUKPT KSN

2.6.12 40 01 – Get TransArmor TID

Description:

Host gets TransArmor 8 byte TransArmor TID.

Command:

Task ID	'72'
Function ID	'40',’01’
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • No TransArmor TID
Task ID	'27'
Function ID	‘40’, ‘01’
Length	0
Data	None

2.6.13 40 02 – Set TransArmor TID

Description:

Host sets 8 bytes TransArmor TID.

Command:

Task ID	'72'
Function ID	'40',’02’
Length	Length of data
Data	• TID

Note:

- TID must be 8 bytes ASCII (0x20 – 0x7F).

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter
Task ID	'27'
Function ID	‘40’,’02’
Length	0
Data	None

2.6.14 40 03 – Load Certificate for TransArmor Encryption

Description:

Load, Root CA, Intermediate CA, or TA Key Certificates.

Command:

Task ID	'72'
Function ID	'40','03'
Length	Length of data
Data	• Certificate in X.509 PEM format

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Number of retries over limit • Invalid Certificate
Task ID	'27'
Function ID	'40','03'
Length	0
Data	None

- The Certification Chain includes the following:
  - Root CA Certification
  - Intermediate CA Certification
  - TA Key Certification
- The detailed:
  - Root CA Certification is hardcoded in firmware. The **Certificate** needs to be loaded is **Intermediate CA Certificate** or **TA Key Certificate**.
  - POS software sends Key Update message requesting for Intermediate CA Certificate and it receives the Intermediate CA Certificate in the Key Update response from First Data Server. POS software passes the Intermediate CA Certificate to Card Reader. The Card Reader uses the Root CA Key to validate the Intermediate CA Certificate. After the Intermediate CA Certificate is validated, the Root CA Key extracts the Intermediate CA Key from the Intermediate CA Certificate.
  - POS software sends Key Update message requesting for TA Key Certificate and it receives the TA Key Certificate in the Key Update response from First Data Server. POS software passes the TA Key Certificate to Card Reader. The Card Reader uses the Intermediate CA Key to validate the TA Key Certificate. After the TA Key Certificate is validated, the Intermediate CA Key extracts the TA Key. The TA Key is used to encrypt the sensitive cardholder data in the TA authorization request. TA Key Certificate uses TA Key ID as Common Name.

- The more detailed:
  - If Intermediate CA Certification is loaded successfully, TA Key Certification should be erased immediately.

2.6.15 40 04 – Erase TransArmor Certificates

Description:

Erase TransArmor Certificates.

Command:

Task ID	'72'
Function ID	'40',’04’
Length	6
Data	• “IDTECH” string

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter
Task ID	'27'
Function ID	‘40’, ‘04’
Length	0
Data	None

2.6.16 40 05 – Get TransArmor Certificates Status

Description:

Get status of TransArmor Certificates.

Command:

Task ID	'72'
Function ID	'40',’05’
Length	0
Data	• None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter
Task ID	'27'
Function ID	‘40’, ‘05’
Length	1
Data	• TransArmor Certificates Status

TransArmor Certificates Status is shown in the following table:

b7	b6	b5	b4	b3	b2	b1	b0	Meaning
X								RFU
	X							RFU
		X						RFU
			X					RFU
				X				RFU
					0			1- TA Key Certificate loaded
						0		1- Intermediate CA Certificate
							1	1- Root CA Certificate loaded

Note: Root CA Certificate is always loaded.

2.6.17 40 08 – Get TransArmor KeyID

Description:

Host gets TransArmor 11-byte KeyID.

Command:

Task ID	'72'
Function ID	'40',’08’

Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • No TransArmor TID
Task ID	'27'
Function ID	‘40’, ‘08’
Length	0
Data	None

2.6.18 42 - Configure Card Reader

Description:

After Card Reader processes the command, the state doesn't change.

Command:

Task ID	'76' or '62'
Function ID	'42'
Length	Length of data
Data	• Length of CFG (configuration) bytes • Byte 0: CR Comm. CFG - baud rate • Byte 1: CR Op. CFG - Reader operation configuration • Byte 2: CR ICC CFG - Reader ICC configuration • Byte 3: RFU • Byte 4: RFU

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter
Task ID	'67'
Function ID	‘42’
Length	0
Data	None

CR Comm. CFG (Byte 0) is shown in the following table:

b7	b6	b5	b4	b3	b2	b1	b0	Meaning
X								RFU
	X							RFU
		X						RFU
			X					RFU
				X				RFU
					X			RFU
						0	0	19200 bps
						0	1	38400 bps
						1	0	57600 bps
						1	1	115200 bps(default setting)

CR Op. CFG (Byte 1) is shown in the following table:

B7	b6	b5	b4	b3	b2	b1	b0	Meaning
X								RFU
	0	1						ICC SAM1 Enable if set to 0 1
	1	0						ICC SAM2 Enable if set to 1 0
			0					CPU card: 0 (0: default) ;
				0				EMV card: 0 (0: default) ; ISO
					1	1	1	SLE4406 SLE4436 SLE5536
					1	1	0	SLE4404 and AT88SC101
					1	0	1	GPM271 card
					1	0	0	GPM276 card
					0	1	1	SLE4442 and SLE4432 cards
					0	1	0	SLE4428 and SLE4418 cards
					0	0	1	4-byte I^2C memory card
					0	0	0	3-byte I^2C memory card

CR ICC CFG (Byte 2) is shown in the following table:

b7	b6	b5	b4	b3	b2	b1	b0	Meaning
X								RFU
	X							RFU
		0						ICC Main 5V card: 0; 3V card: 1
			0					ICC SAM1 5V card: 0; 3V card:
				0				ICC SAM2 5V card: 0; 3V card:
					X			RFU
						X		RFU
							X	RFU

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Number of retries over limit
Task ID	'67' or ‘26’
Function ID	‘42’
Length	Length of Data
Data	If Card Reader command checks pass, else data not present.

2.6.19 43 - Get Parameters

Description:

This command can be issued at any time.
After Card Reader processes the command, the state doesn't change.
For processing details, refer to: Process Details – Get Parameters

Command:

Task ID	'76'
Function ID	'43'
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems
Task ID	'67'
Function ID	'43'
Length	Length of data
Data	If Card Reader command checks pass, else data not present. • Length of CFG bytes • Byte 0: CR Comm. CFG - baud rate • Byte 1: CR Op. CFG - reader operation configuration • Byte 2: CR Enc CFG - Reader encryption configuration • Byte 3: RFU • Byte 4: RFU • Length of Manufacture CFG bytes • Byte 0: Manufacture CFG • Length RTC • RTC, 6 bytes

CR Comm. CFG (Byte 0) is shown in the following table:

b7	b6	b5	b4	b3	b2	b1	b0	Meaning
X								RFU
	X							RFU
		X						RFU
			X					RFU
				X				RFU
					X			RFU
						0	0	19200 bps
						0	1	38400 bps
						1	0	57600 bps
						1	1	115200 bps(default setting)

CR Op. CFG (Byte 1) is shown in the following table:

b7	b6	b5	b4	b3	b2	b1	b0	Meaning
1								ICC Main Enabled if set to 1
	0	1						ICC SAM1 Enable if set to 01
	1	0						ICC SAM2 Enable if set to 10
			0					CPU card: 0 (0: default) ;
				0				EMV card: 0 (0: default) ; ISO
					1	1	1	SLE4406 SLE4436 SLE5536 and
					1	1	0	SLE4404 and AT88SC101 cards
					1	0	1	GPM271 card
					1	0	0	GPM276 card
					0	1	1	SLE4442 and SLE4432 cards
					0	1	0	SLE4428 and SLE4418 cards
					0	0	1	4-byte I^2C memory card, page size
					0	0	0	3-byte I^2C memory card (default),

CR Enc. CFG (Byte 2) is shown in the following table:

b7	b6	b5	b4	b3	b2	b1	b0	Meaning
X								RFU
	X							RFU
		X						ICC Main 5V card: 0; 3V card: 1
			X					ICC SAM1 5V card: 0; 3V card: 1
				X				ICC SAM2 5V card: 0; 3V card: 1
					X			RFU
						X		RFU
							X	RFU

Manufacture CFG (Byte 0) is shown in the following table:

b7	b6	b5	b4	b3	b2	b1	b0	Meaning
X								RFU
	X							RFU
		X						RFU
			X					RFU
				X				RFU

		0	0-DUKPT(default); 1-TransAmor
	X		RFU
		0	0-Data variant (default); 1-PIN

Time data – 6 bytes RTC value:
-Year, one byte in BCD, 00~99
-Month, one byte in BCD, 01~12
-Day, one byte in BCD, 01~31
-Hour, one byte in BCD, 00~23
-Minute, one byte in BCD, 00~59
-Second, one byte in BCD, 00~59

2.6.20 44 – Read/Set MSR Settings

Description:

This command can be issued at any time.
After Card Reader processes the command, the state doesn't change.

Command:

Task ID	'73
Function ID	'44'
Length	Length of data
Data	• MSR command

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems
Task ID	'37'
Function ID	'44'
Length	Length of data
Data	• MSR response

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

Function ID	Hex	Len	Description	Default Setting	Description	Opt	Comments
FmVerID	22	1	Firmware Version		Get firmware version string	nr	

PrePANID	49	1	PAN to not mask	4 (0-6)	# leading PAN digits to display	e	
PostPANID	4A	1	PAN to not mask	4 (0-4)	# of trailing PAN digits to display	e	
MaskCharID	4B	1	mask the PAN with this character	'*' (0x20-0x7E)	any printable character	e	
DispExpDateID,	50	1	mask or display expiration date	'0''0'-'1'	'1' don't mask expiration date	e	
SecureLrcID	6F	1	Secured output format Lrc option	'1' ('0'-'1')	'1' to send LRC in secured output data	e	
SecurityLevelID	7E	1	Security level	'1' ('1'-'3')	'1' no load Data encryption Key '3' has loaded Data encryption Key	nr	

Note:

- e: can be written (0x53) and read (0x52);
- nr: only can be read (0x52);
- r : can be set only one time, then always can be read (0x52);
- SecureLrcID can't be read or set when reader is configured for TransArmor.

Example: 02 09 00 73 46 44 04 00 53 49 01 06 68 A4 03
02 06 00 06 37 46 44 00 00 33 C7 03
Set PrePAN length to 6.

02 07 00 73 46 44 02 00 52 49 68 9A 03
02 09 00 06 37 46 44 03 00 49 01 06 7E 1A 03
Read PrePAN length.

2.6.21 45 – Activate and Deactivate Removal Sensor, ATed or MACed

Note: The HOST or PINPAD must use a dual authorized process prior to issuing this command.

Description:

This command should be issued after the Card Reader has passed mutual authentication with PIN pad (L100 or equivalent).

There MUST be room in the log to log this event, else this command will fail.

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.
For processing details, refer to: Processing Details – Activate and Deactivate Removal Sensor.

For command between PINPAD-CR and HOST-CR:
Command:

Task ID	'76' or '56'
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 For Symmetric only PINPAD • MAC-PINPAD (Optional for manufacture mode version) For Asymmetric only or both PINPAD and host • Length AT-Manufacture or AT-PINPAD (Optional for manufacture mode version) • AT-Manufacture or AT-PINPAD (Optional for manufacture mode

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Log is full • No nonce generated • Invalid MAC Key • MAC checks failed • Number of retries over limit • AT checks failed • Duplicate detected
Task ID	'67' or '65'
Function ID	‘45’
Length	0
Data	None

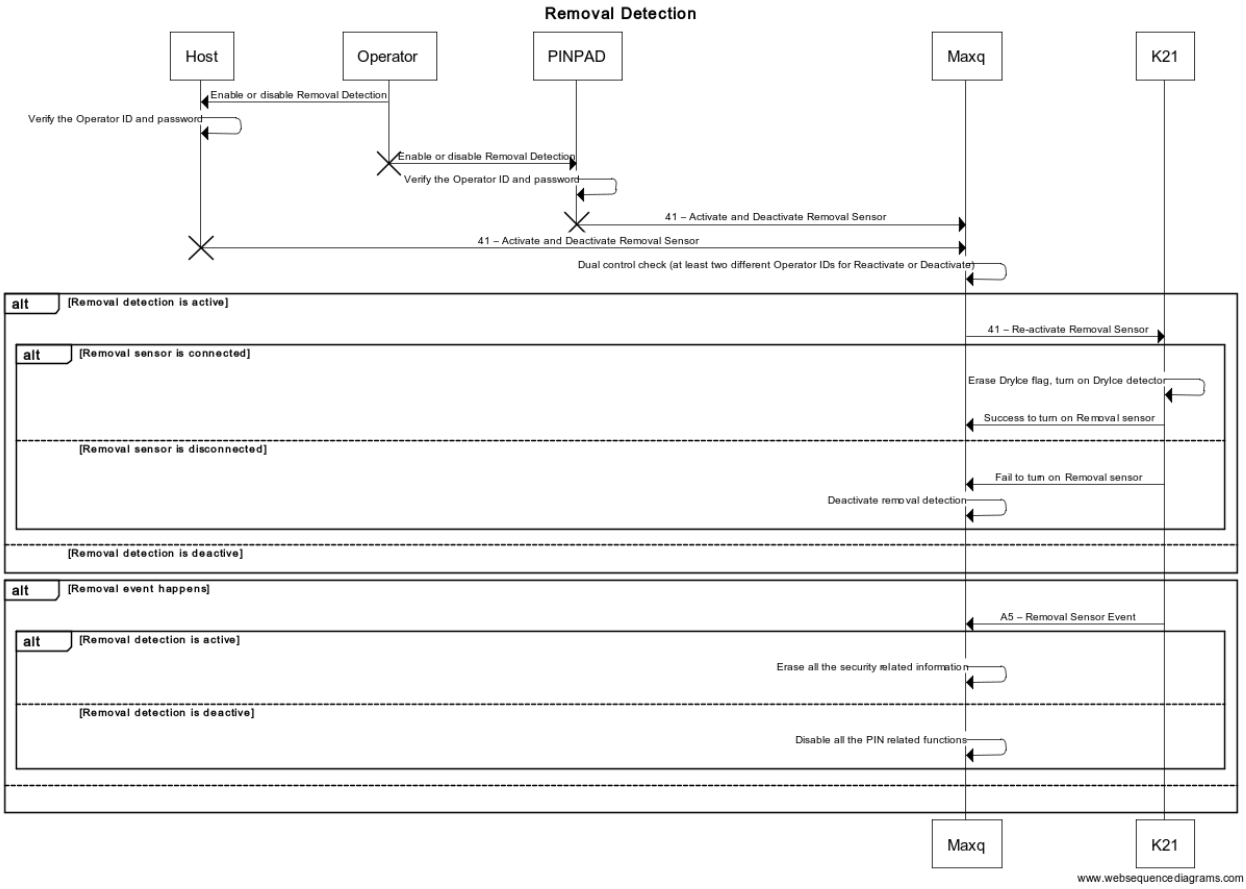
Note:

Operator ID is an 8-byte hexadecimal byte array. If PinPad or Host doesn’t support account management (no Operator ID supported), it can send all 0 as Operator ID1 to indicate this case and UID as the Operator ID2.

Card Reader should receive at least two different Operator IDs for Reactivate or Deactivate, from dual control’s concern.

Sensor control timeout: A timeout within which the dual control need to be finished. The timeout field in the 1st input of dual control is the timeout, ignore the field in the 2nd input.

Flow Chart


Removal Detection
Host
Operator
PINPAD
Maxq
K21
Enable or disable Removal Detection
Verify the Operator ID and password
Enable or disable Removal Detection
Verify the Operator ID and password
41 – Activate and Deactivate Removal Sensor
41 – Activate and Deactivate Removal Sensor
Dual control check (at least two different Operator IDs for Reactivate or Deactivate)
alt
[Removal detection is active]
41 – Re-activate Removal Sensor
alt
[Removal sensor is connected]
Erase Drylce flag, turn on Drylce detector
Success to turn on Removal sensor
[Removal sensor is disconnected]
Fail to turn on Removal sensor
Deactivate removal detection
[Removal detection is deactive]
alt
[Removal event happens]
A5 – Removal Sensor Event
alt
[Removal detection is active]
Erase all the security related information
[Removal detection is deactive]
Disable all the PIN related functions
Maxq
K21
www.websequencediagrams.com

2.6.22 46 – Activate and Deactivate Removal Sensor, ATed or MACed

Note: The HOST must require a dual authorized process prior to issuing this command.

Description:

This command is similar to 45 (above) but uses an ICC and PIN, rather than using the SmartPIN L100 itself.

This command should be issued after the Card Reader has passed mutual authentication.

There MUST be room in the log to log this event, else this command will fail.

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.
For processing details, refer to: Processing Details – Activate and Deactivate Removal Sensor

For command between HOST-CR:
Command:

Task ID	'76'
Function ID	'46'
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 Operator PIN • Operator PIN, 8 bytes For Asymmetric only • Length AT-Manufacture or MAC (Optional for manufacture mode version) • AT-Manufacture or MAC (Optional for manufacture mode version)

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Log is full • No nonce generated • Number of retries over limit • AT checks failed • Duplicate detected
Task ID	'67'
Function ID	‘46’
Length	0
Data	None

Note:

Operator ID is an 8-byte hexadecimal byte array.

The procedure for using smart card to authenticate removal control:

- The certificate chain of Smart Card (PIVKEY C910) is loaded into SCR during manufacture.

Note:

1. Smart Card uses Taglio RootCA and pivkey DeviceCA.
2. Smart Card requires PIN to enable security related command-signing mechanism.
3. Each Smart Card has a unique serial number. Smart Card's certificate has the information of this unique serial number.
4. Customer has a secure database which associates each Smart Card's unique serial number with its unique PIN.

Overall Procedure:

1. The operator who is going to "turn on/off removal detector" inserts his Smart Card in the field, then sends message to customer's remote server.

2. Remote server searches its database to find the unique PIN of that smart card.

3. The 2nd operator needs to login to remote server (use his own log in credential) and verify this request. Only after the 2nd operator approves this request, remote server sends SCR secure command to enable the Smart Card validating process for "turn

on/off removal detector". This command has nonce and device ID as part of the message and signature for authentication. The Smart Card's unique PIN is also part of the message.

4. SCR receives the command, validates the signature then saves the PIN and starts verifying Smart Card.

5. SCR reads certificate of card and verifies signature against pivkey DeviceCA and taglio RootCA.

6. SCR uses the unique PIN to activate signing mechanism in Smart Card. (This is how smart card authenticates SCR)

7. SCR sends clear PKCS1.5 signature to Smart Card.

8. Smart Card uses private key to sign signature and sends back to SCR.

9. SCR uses public key from card to verify signature (This is how SCR authenticates smart card).

10. If everything passes, SCR activates or deactivates removal sensor according to command parameter. To successfully do this, the operator needs the correct card and the unique PIN.

2.6.23 47 – Set Force Encryption Option

Description: This command sets the parameter that determines encrypted output from MSR sessions. Use it to force encryption of non-financial data.

Command:

Task ID	'76'
Function ID	'47'
Length	1
Data	• Force encryption option byte

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter
Task ID	'67'
Function ID	'47'
Length	0
Data	None

Bit 0 : T1 force encrypt
Bit 1 : T2 force encrypt
Bit 2 : T3 force encrypt
Bit 3 : T3 force encrypt when card type is 0
Bit 4: RFU
Bit 5 : RFU
Bit 6 : RFU
Bit 7 : RFU

2.6.24 48 – Get Force Encryption Option

Description: This command allows to get the force encryption option status.

Command:

Task ID	'76'
Function ID	'48'
Length	None
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter
Task ID	'67'
Function ID	'47'
Length	1
Data	• Force encryption option byte

Bit 0 : T1 force encrypt
Bit 1 : T2 force encrypt
Bit 2 : T3 force encrypt
Bit 3 : T3 force encrypt when card type is 80
Bit 4: RFU
Bit 5 : RFU
Bit 6 : RFU
Bit 7 : RFU

2.6.25 60 – Manually Lock Card and Power On Card

Description:

This command should be issued when Card Reader in any state.

The Card Reader will send “Latch Control” command to K21-HUB which controls the latch, then Card Reader powers up the ICC. If it is successful, Card Reader should set Latch Mechanism Active flag and have no state change after processing this command.

Command:

Task ID	‘76’ or '72' (SAM)
Function ID	'60'
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Smart Card not powered up
Task ID	‘67’ or '27' (SAM)
Function ID	‘60’
Length	0
Data	None

Note: If Card Reader has latch and it couldn’t successfully lock an ICC card, Card Reader should respond with ‘Any hardware problems’ in BWT. If Card Reader doesn’t have latch, ignore the result of lock ICC card.

2.6.26 61 - Get ICC Status

Description:

This command can be issued when the Card Reader is in any state.

The Card Reader gets ICC ATR Data and the status of the Smart Card interface: Smart Card voltage, protocols parameters (T = 0, T = 1).

HOST uses this command to retrieve ICC response data based on Card Status bits returned in the Poll Card Reader response.

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	05	00	72 46 61 00 00	55	19	03
Output Hex String: 0205007246610000551903						

Response Example:

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02	14	00		05	F3	03
Response Hex String: 021400062746610e000a000403000000000000000000005f303						

Command:

Task ID	‘76’, '26' or '72' (SAM)
Function ID	'61'
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter
Task ID	‘67’, '62' or '27' (SAM)
Function ID	‘61’
Length	Length of data

Data	• Length of info bytes (from byte0 to last byte before ATR Data Length). • Byte 0: Card status • Byte 1: Current voltage of ICC • Byte 2: Current protocol use T=0 ('00') or T=1 ('01') • Byte 3-5: Current parameter for protocol T=0; 3 bytes (If Byte2 is T=l, all Byte3-5 is set in "0".) Byte 3 = TA1 (FI/DI) Byte 4 = TC1 (Guard Time) Byte 5 = WI • Byte 6 - 9: Current parameter for protocol T= 1; 4 bytes (If Byte2 is T=0, all Byte6-9 is set in "0".) Byte 6 = TA1 (FI/DI) Byte 7 = TC1 (EGT) Byte 8 = TB3 (BWI/CWI) Byte 9 = IFSC • Length of ATR Data • ATR Data is included when card is inserted and no other errors returned.

The Card Presence (Byte 0) is coded as shown in the following table:

b7	b6	b5	b4	b3	b2	b1	Meaning
0	0						RFU
		x					Latch Mechanism Active if set to 1.
			0	0			RFU
				x			Error activating/resetting ICC
					x		Error communicating with ICC
						x	Card inserted if bit is set to 1

The Current setting and Voltage of ICC (Byte 1) is coded as shown in the following table:

b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0 0 0		0			RFU
					0	0	The card is not powered up.
					0	1	The card is powered with 1.8 V (Not
					1	0	The card is powered with 3 V
					1	1	The card is powered with 5 V

Note: If Card Reader has latch and it couldn't successfully lock an ICC card, Card Reader will respond with 'Any hardware problems.'

2.6.27 ICC EMV Level II

2.6.27.1 CRL (Certificate Revocation List)

2.6.27.1.1 **85 01 – Retrieve CRLs**

Command: 72 46 85 01

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	06	00	72 46 85 01 00 00	B0	3E	03
Output Hex String: 020600724685010000b03e03 Data: None						

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02			27 46 85 01 <Length> <Data>			03
Response Hex String: 02070015f20b27468501090503 (In this example, no CRL was returned, hence the error code 0xF20B: No CRL.) If the packet and command are correctly formed, the following status is possible: • Wrong parameter • Unknown parameter in command • Unsupported Command • Invalid CRL length • No CRL Length bytes: Length of data Data: • Length RevokedCertificateNDate, 2 bytes • RevokedCertificateNDate 1…RevokedCertificateNDate N Note: RevokedCertificateNDate format: • RID, 5 Bytes (Support at least 30 CRLs for each RID) • CA Index, 1 Byte • Certificate Serial Number of Issuer Public Key Certificate, 3 Bytes						

2.6.27.1.2 **85 02 – Remove CRLs**

Command:

Task ID	'72'
Function ID	'85', '02'

Length	Length of data
Data	• Length RevokedCertificate, 2 bytes • RevokedCertificate1…RevokedCertificateN Note: RevokedCertificate format: • RID, 5 Bytes (Support at least 30 CRLs for each RID) • CA Index, 1 Byte • Certificate Serial Number of Issuer Public Key Certificate, 3 Bytes

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • Invalid CRL length • CRL list is full • Save or Config Failed / Or Read Config Error, Flash Error • Number of retries over limit
Task ID	'27'
Function ID	'85', '02'
Length	0
Data	None

2.6.27.1.3 **85 03 – Set CRLs**

Command:

Task ID	'72'
Function ID	'85', '03'
Length	Length of data
Data	• Length RevokedCertificate, 2 bytes • RevokedCertificate1…RevokedCertificateN Note: RevokedCertificate format: • RID, 5 Bytes (Support at least 30 CRLs for each RID) • CA Index, 1 Byte • Certificate Serial Number of Issuer Public Key Certificate, 3 Bytes

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • Invalid CRL length • CRL list is full • Save or Config Failed / Or Read Config Error, Flash Error • Number of retries over limit
Task ID	'27'
Function ID	'85', '03'
Length	0
Data	None

2.6.27.1.4 **85 04 – Remove All CRLs**

Command:

Task ID	'72'
Function ID	'85', '04'
Length	Length of data
Data	

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • Save or Config Failed / Or Read Config Error, Flash Error • Number of retries over limit
Task ID	'27'
Function ID	'85', '04'
Length	0
Data	None

2.6.27.2 Application Data

Each host has its specific application data. The application data needs to be loaded the first time the terminal connects to a host.

2.6.27.2.1 01 01 – Retrieve Application Data (Retrieve AID)

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	0F	00	72 46 01 01 <Length> <Data>			03
Output Hex String: 020f00724601010900070 0a0000000310109 98d03 Length: 2 bytes, little-endian, value 5 to 16 Data: AID identifier						

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02	63	00	27 46 01 01 <Length> <Data>			03
Response Hex String: 02630006274601015c005a009f010656495341303 05f5701005f2a0208409f09020096 5f3601029f1b0400003a98df25039f3704df28039f0802dfee150101df1305000000000 0df14050000000000df15050000000000df180100df170400002710df190100aad803 If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Unknown parameter in command • Unsupported Command • No AID or No Application Data • No Terminal Data Data: TLVs						

2.6.27.2.2 01 02 – Remove Application Data

Command:

Task ID	'72'
Function ID	'01', '02'
Length	Length of data
Data	• Length AID • AID, 5~16 bytes

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • No AID or No Application Data • No Terminal Data• Save or Config Failed / Or Read Config Error, Flash Error • Number of retries over limit
Task ID	'27'
Function ID	'01', '02'
Length	0
Data	None

2.6.27.2.3 01 03-Set Application Data

Command:

Task ID	'72'
Function ID	'01', '03'
Length	Length of data
Data	• Length AID • AID, 5~16 bytes • Number of TLV • TLV1…TLVn

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • Wrong TLV format • Can't modify major bits in terminal setting • AID list is full, maxim is 16 • Save or Config Failed / Or Read Config Error, Flash Error • Number of retries over limit
Task ID	'27'
Function ID	'01', '03'
Length	0
Data	None

2.6.27.2.4 **01 04 -Remove All Application Data**

Command:

Task ID	'72'
Function ID	'01', '04'
Length	Length of data
Data	

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • Save or Config Failed / Or Read Config Error, Flash Error • Number of retries over limit
Task ID	'27'
Function ID	'01', '04'
Length	0
Data	None

2.6.27.2.5 03 01-Retrieve AID List

Command:

Task ID	'72'
Function ID	'03', '01'
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Unknown parameter in command • Unsupported Command • No AID or No Application Data
Task ID	'27'
Function ID	'03', '01'
Length	Length of data
Data	• Length AID Block • AID Block 1…AID Block N Note: AID Block format: • Length AID • AID, 5~16 bytes

2.6.27.3 Terminal Data

2.6.27.3.1 02 01-Retrieve Terminal Data

Command Example

STX	Len Low	Len High	Command Body	LRC	CHK SUM	ETX
02	06	00	72 46 02 01 00 00	37	BB	03
Output Hex String: 02060072460201000037bb03						

Response Example

STX	Len Low	Len High	Response Body	LRC	CHK SUM	ETX
02	63	00	27 46 02 01 <Length> <Data>			03

Response Hex String:
02cf000627460201c800c6005f3601029f1a0208409f3501259f33036008c89f40056000f050019f1e085465726d696e616c9f150212349f160f303030303030303030303030303030309f1c0838373635343332319f4e22313037323120576 16c6b65722053742e20437970726573732c204341202c5553412edf260101df1008656e667265737a68df110101df270100dfee150101dfee160100dfee170107dfee180180dfee1e08d09c20f0c20e1400dfee1f0180dfee1b0830303031353130 30dfee20013cdfee21010adfee2203323c3cfa6803

If the packet and command are correctly formed, the following status byte is possible:
- Complete
- Wrong parameter
- Any hardware problems
- No nonce generated
- Wait [Note]
- Number of retries over limit
- ICC communication timeout
- ICC data error
- ICC EMV Lv2 Error-No Terminal Data

Data: TLVs

2.6.27.3.2 02 02-Remove Terminal Data

Command:

Task ID	'72'
Function ID	'02', '02'
Length	Length of data
Data	

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • No AID or No Application Data • No Terminal Data • Save or Config Failed / Or Read Config Error, Flash Error • Number of retries over limit
Task ID	'27'
Function ID	'02', '02'
Length	0
Data	None

2.6.27.3.3 02 03-Set Terminal Data

Command:

Task ID	'72'
Function ID	'02', '03'
Length	Length of data
Data	• Number of TLV • TLV1…TLVn

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • Wrong TLV format • Can't modify major bits in terminal setting • AID list is full, maxim is 16 • Save or Config Failed / Or Read Config Error, Flash Error • Number of retries over limit
Task ID	'27'
Function ID	'02', '03'
Length	0
Data	None

2.6.27.4 Public Key

2.6.27.4.1 04 01-Retrieve CA Public Key

Command:

Task ID	'72'
Function ID	'04', '01'
Length	Length of data
Data	• RID (Registered Application Provider Identifier), 5 bytes (= first 5 bytes of AID) • CA Index, 1 byte

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Unknown parameter in command • Unsupported Command • No CA Key RID • No CA Key Index
Task ID	'27'
Function ID	'04', '01'
Length	Length of data
Data	• RID, 5 bytes • CA Index, 1 byte • Hash Algorithm, 1-SHA1 • Encryption Algorithm, 1-RSA • Hash, 20 bytes • CA Key Exponent, 4 bytes, left pad with 0 • Length CA Key Modulus • CA Key Modulus, m bytes Where: <Hash> is signature of <RID> <CA Index> <CA Key Modulus> <CA Key Exponent>

2.6.27.4.2 04 02-Remove CA Public Key

Command:

Task ID	'72'
Function ID	'04', '02'
Length	Length of data
Data	• RID, 5 bytes • CA Index, 1 byte

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • No CA Key RID • No CA Key Index • Save or Config Failed / Or Read Config Error, Flash Error • Number of retries over limit
Task ID	'27'
Function ID	'04', '02'
Length	0
Data	None

2.6.27.4.3 04 03-Set CA Public Key

Command:

Task ID	'72'
Function ID	'04', '03'
Length	Length of data
Data	• RID, 5 bytes • CA Index, 1 byte • Hash Algorithm, 1-SHA1 • Encryption Algorithm, 1-RSA • Hash, 20 bytes • CA Key Exponent, 4 bytes, left pad with 0 • Length CA Key Modulus • CA Key Modulus, m bytes Where: <Hash> is signature of <RID> <CA Index> <CA Key Modulus> <CA Key Exponent> Note: Device supports up to 16 RID. Each RID has up to 6 CA Index.

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • No CA Key RID • No CA Key Index • Wrong CA Hash and Encryption algorithm • CA Key list is full, maxim is 16 • Wrong CA Key hash • Wrong Transaction Command Format • Save or Config Failed / Or Read Config Error, Flash Error • Number of retries over limit
Task ID	'27'
Function ID	'04', '03'
Length	0
Data	None

2.6.27.4.4 **04 04-Remove All CA Public Key**

Command:

Task ID	'72'
Function ID	'04', '04'
Length	Length of data
Data	

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • Save or Config Failed / Or Read Config Error, Flash Error • Number of retries over limit
Task ID	'27'
Function ID	'04', '04'
Length	0
Data	None

2.6.27.4.5 04 05-Retrieve CA Public Key List

Command:

Task ID	'72'
Function ID	'04', '05'
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Unknown parameter in command • Unsupported Command • No any CA Key
Task ID	'27'
Function ID	'04', '05'
Length	Length of data
Data	• Length RID-Index • RID-Index1… RID-IndexN The format of RID-Index: • RID, 5 bytes • CA Index, 1 byte

2.6.27.5 General

2.6.27.5.1 08 01-Retrieve EMV L2 Version

Command:

Task ID	'72'
Function ID	'08', '01'
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Unknown parameter in command • Unsupported Command
Task ID	'27'
Function ID	'08', '01'
Length	Length of data
Data	• Length Kernel Version • Kernel Version, in the format of "EMVL2 X.YY"

2.6.27.5.2 08 02-Retrieve Kernel Version

Command:

Task ID	'72'
Function ID	'08', '02'
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Unknown parameter in command • Unsupported Command
Task ID	'27'
Function ID	'08', '02'
Length	Length of data
Data	• Length Kernel Version • Kernel Version, in the format of "EMVL2 X.YY.ZZZ"

2.6.27.5.3 09 01-Retrieve Kernel Check Value

Command:

Task ID	'72'
Function ID	'09', '01'
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Unknown parameter in command • Unsupported Command
Task ID	'27'
Function ID	'09', '01'
Length	Length of data
Data	• Length Check Value • 20 bytes SHA-1

2.6.27.5.5 09 02-Retrieve EMV L2 Configuration Check Value

Command:

Task ID	'72'
Function ID	'09', '02
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Unknown parameter in command • Unsupported Command
Task ID	'27'
Function ID	'09', '02'
Length	Length of data
Data	• Length Check Value • 20 bytes SHA-1

2.6.27.5.6 **87 01-Retrieve Terminal ID**

Command:

Task ID	'72'
Function ID	'87', '01'
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Unknown parameter in command • Unsupported Command • No Terminal Data
Task ID	'27'
Function ID	'87', '01'
Length	Length of data
Data	• Length Terminal ID • Terminal ID, 8 bytes printable characters.

2.6.27.5.7 **87 03-Set Terminal ID**

Command:

Task ID	'72'
Function ID	'87', '03'
Length	Length of data
Data	• Length Terminal ID • Terminal ID, 8 bytes printable characters.

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • Save or Config Failed / Or Read Config Error, Flash Error • Number of retries over limit
Task ID	'27'
Function ID	'87', '03'
Length	0
Data	None

2.6.27.5.8 88 01-Retrieve Terminal Major Configuration

Command:

Task ID	'72'
Function ID	'88', '01'
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Unknown parameter in command • Unsupported Command
Task ID	'27'
Function ID	'88', '01'
Length	Length of data
Data	• Length Major Configuration • Terminal Major Configuration, 1 byte.

Terminal Major Configuration in ICS	Values
1C	0x31
2C	0x32
3C	0x33
4C	0x34

2.6.27.5.9 88 03-Set Terminal Major Configuration

Command:

Task ID	'72'
Function ID	'88', '03'
Length	Length of data
Data	• Length Major Configuration • Terminal Major Configuration, 1 byte.

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • Save or Config Failed / Or Read Config Error, Flash Error • Number of retries over limit
Task ID	'27'
Function ID	'88', '03'
Length	0
Data	None

Terminal Major Configuration in ICS	Values
1C	0x31
2C	0x32
3C	0x33
4C	0x34

2.6.27.6 Transaction

Precondition of transaction:

- Set CRL
- Set Application Data
- Set Terminal Data
- Set CA Public Key

2.6.27.6.1 05 01-Start Transaction (optionally MACed)

Command:

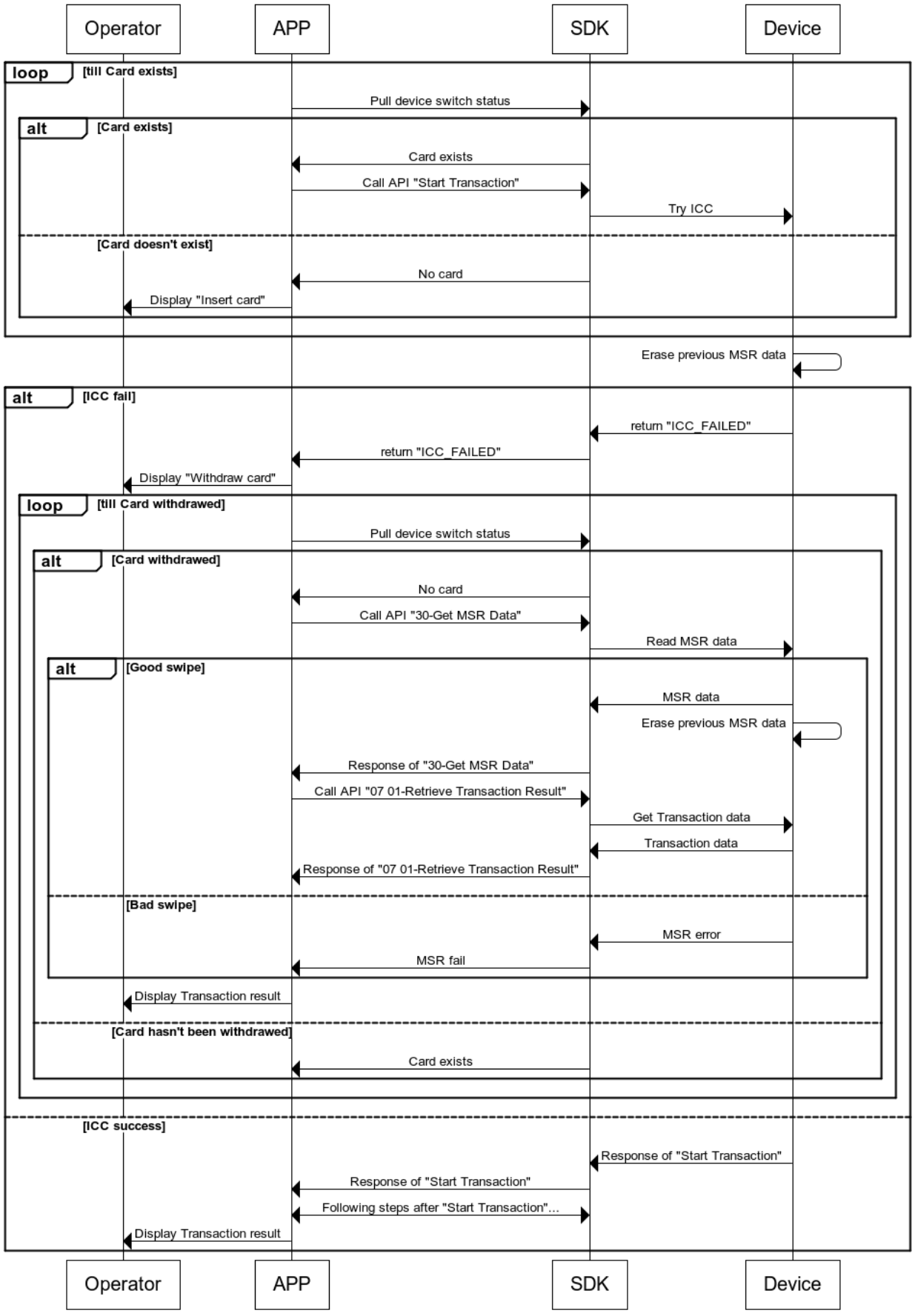
Task ID	'72'
Function ID	'05', '01'
Length	Length of data
Data	• Fallback to MSR: 1Byte 1-In the case smart card transaction fails, application can fallback to MSR 0-Never fallback to MSR • Card Seat Time Out: 2 bytes, in seconds • Wait till "Authenticate Card and Process Transaction" command Time Out: 2 bytes, in seconds • Length Transaction Data • Transaction Data, TLV1…TLVn

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • ICC L2 is not in idle state • Invalid DATA DUKPT Key • No AID or No Application Data • No Terminal Data • Wrong Transaction Command Format • No amount, other amount and transaction type in Transaction Command • Can't modify major bits in terminal setting • Transaction Type Error
Task ID	'27'
Function ID	'05', '01'
Length	Length of data
Data	• Length Output Data • Length Output Data, TLV1…TLVn • MAC-CR(Optional)

Note:
Tag ‘DF EE 25’ is Response Code, 2 Bytes
Note:
1).First response code format
Bit 0 --- if transaction have advice, this bit is 1.
Bit 1 --- if transaction have reversal, this bit is 1.
Tag ‘DF EE 26’ is Attribution: 2 Bytes:
Byte 1:
Bit 4/3/0: Captured Data Type
0 0 0 = Contact Card
0 0 1 = Contactless Card / EMV
1 0 1 = Contactless Card / MSD
0 1 x = MSR Card
Bit 2/1: Encryption Mode
0 0 = TDES
0 1 = AES
1 x = Encryption Mode Extension(Refer "Byte 2: Encryption Mode Extension”)
Bit 5: Reserved for Attribution Byte Extension.
Bit 6/7: Encryption Status (For ViVOpay IDG)
0 0 = MSR/MSD off, EMV off
0 1 = MSR/MSD off, EMV on
1 0 = MSR/MSD on, EMV off
1 1 = MSR/MSD on, EMV on
Byte 2: (Optional)
Bit 3/2/1/0: Encryption Mode Extension
0 0 0 0 = TDES
0 0 0 1 = AES
0 0 1 0 = TransArmor Algorithm
0 0 1 1 = Voltage Algorithm
0 1 0 0 = Visa FPE
0 1 0 1 = Verifone FPE
0 1 1 0 = Desjardins
0 1 1 1 = RFU
1 x x x = RFU
Bit 6/5/4: Reserved
Bit 7:
0 = Without MAC Verification Data
1 = With MAC Verification DataTag ‘DF EF 1F’ is auto authenticate, 2 bytes
Byte 1:1-Auto authenticate, 0-No auto authenticate
Byte 2:1-Force online if auto authenticate, 0-Don’t care
Tag ‘DF EF 20’ is MAC in response, 1 byte
1-MAC in response for all the Transaction commands, 0-No MAC

Start Transaction



2.6.27.6.2 05 02-Authenticate Card and Process Transaction (optionally MACed)

For issuer to process online transactions, there must be verification of the data and cryptogram from the card together with data from the terminal, plus generation of a cryptogram allowing the card to authenticate the issuer. There will also be verification of online cardholder PINs as part of standard authorization processing. Issuer approves or declines a transaction in response to an online authorization request from a merchant via an acquirer.

Online authentication methods are used to validate the card to the issuer (or a representative of the issuer) and the issuer to the card as well as to prove the authenticity of received data.

With Online Card Authentication (CAM) the issuer online system validates a cryptogram (an Application Cryptogram called an ARQC) generated by the card from important transaction data using its unique secret key, to show that the card is not counterfeit and that the data has not been altered. The online request also includes card and terminal indicators of the results of offline processing.

In response to the ARQC, there is Online Issuer Authentication. The issuer optionally creates an authorization response cryptogram (ARPC). The card validates the ARPC to assure that the authorization response came unaltered from the issuer.

In addition to the ARPC described above, issuers can perform post-issuance updates of cards using issuer script commands for internal card management, such as the reset of offline counters. For example the issuer can change the Offline PIN or update a card's risk parameters. The issuer protects these script commands from undetected alteration by generating a cryptogram (MAC) from the command data. The card validates the MAC before applying the changes. Confidential data is enciphered, such as a replacement PIN value during transport between the issuer and the card.

For approved transactions the terminal sends a cryptogram (an Application Cryptogram called a TC) generated by the card with the clearing information for verification by the issuer as evidence of the validity of the completed transaction.

Command:

Task ID	'72'
Function ID	'05', '02'
Length	Length of data
Data	• ForceOnline: 1 byte 1-Force to online authorization of the transaction 0-not force to online authorization of the transaction • Wait for host's response Time Out, if Online: 2 bytes, in second • Length Transaction Data • Transaction Data, TLV1…TLVn

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • Unexpected Command • Invalid DATA DUKPT Key • Wrong Transaction Command Format • Can’t modify major bits in terminal setting
Task ID	'27'
Function ID	'05', '02'
Length	Length of data
Data	• Length Output Data • Length Output Data, TLV1…TLVn • MAC-CR(Optional)• MAC-CR(Optional)

2.6.27.6.3 05 03-Authenticate Issuer and Process Transaction (optionally MACed)

Command:

Task ID	'72'
Function ID	'05', '03'
Length	Length of data
Data	• OnlineProcessingAbility, 1 byte 1-able to go online 0-unable to go online • Authorization Response Code, Tag 8A (Optional for online) • Issuer Authentication Data, Tag 91 (Optional for online) • Issuer Scripting (generate update scripts to the card application), Tag 71/72 (Optional for online) • Transaction Data, TLV1…TLVn

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • Unexpected Command • Invalid DATA DUKPT Key • Wrong Transaction Command Format • Can't modify major bits in terminal setting
Task ID	'27'
Function ID	'05', '03'
Length	Length of data
Data	• Length Output Data • Length Output Data, TLV1…TLVn • MAC-CR(Optional)

2.6.27.6.4 06-Cancel Transaction

Command:

Task ID	'72'
Function ID	'06'
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Unknown parameter in command • Unsupported Command
Task ID	'27'
Function ID	'06'
Length	0
Data	None

2.6.27.6.5 07 01 -- Scripting and Retrieve Transaction Result

Command:

Task ID	'72'
Function ID	'07', '01'
Length	Length of data
Data	• Length Tag • Tag1…Tagn

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Unknown parameter in command • Unsupported Command • Invalid DATA DUKPT Key • Wrong Transaction Command Format
Task ID	'27'
Function ID	'07', '01'
Length	Length of data
Data	• Length Output Data • Length Output Data, TLV1…TLVn, See P127, EMV4.3 book3 • MAC-CR(Optional)

2.6.27.6.6 **0A 02 -- Clear Transaction Log**

Command:

Task ID	'72'
Function ID	'0A', '02'
Length	Length of data
Data	

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • Save or Config Failed / Or Read Config Error, Flash Error • Number of retries over limit
Task ID	'27'
Function ID	'0A', '02'
Length	0
Data	None

2.6.28 67 - Power Down and Remove ICC Card

Description:

This command can be issued when the Card Reader is in any state, and there is no state change after processing this command.

This command powers down the Smart Card, as defined in ISO/IEC 7816-3 and allows the card to be removed by releasing the lock mechanism, and then resets Latch Mechanism Active flag.

Command:

Task ID	‘76’, ‘26’ or '72' (SAM)
Function ID	'67'
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems
Task ID	‘67’, ‘62’ or '27' (SAM)
Function ID	‘67’
Length	0
Data	None

2.6.29 80 – Start Firmware Upgrade (for K21 HUB or Maxq1050)

Description:

This command can be issued when the Card Reader is in any state and there is no state change after processing this command.

The HOST uses this command to tell the reader that a firmware download for K21 HUB or Maxq1050 is about to begin.

The Card Reader sets a 15 minute timer and is then ready to accept the first data block. If all blocks are not fully received (Download and Write commands complete) within 15 minutes, the Card Reader will reject the firmware download.

For additional details, please refer to: Download Firmware for K21 HUB

Command:

Task ID	'72' or '76'
Function ID	'80'
Length	Length of data
Data	• Firmware header

Note:
Firmware header:

- Length firmware information
- Firmware information: string “SP K21 APP Vx.xx.xxx” or “SP MAX APP Vx.xx.xxx”, this is the name of BIN file
- Length encryption type
- Encryption type, 1byte: 0-plaintext, 1-TDES ECB, PKCS#5 padding, 2-TDES CBC, PKCS#5, IV is all 0.
- Length encrypted firmware session key blob
- Encrypted firmware session key blob, TR-31 Rev B, wrapped by FW Key (Optional, none if firmware is plaintext)
- Length size of signed encrypted firmware in bytes
- Size of signed encrypted firmware in bytes (Block# 0 signature block is included), 4 bytes

Encrypt only the file to sign and have the signature outside of the encrypted file.

The Length of the encrypted firmware is an unsigned 4-byte little-endian parameter indicating the length of the firmware including the 256 bytes signature field which locates at the beginning.

All the firmware files are signed by CA Server, using RSASSA_PSS_SHA256, salt setting is random. The generated 256 bytes binary file will be used as block#0.

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems
Task ID	'27' or '67'
Function ID	‘80’
Length	0
Data	None

2.6.30 81 – Download Firmware (for K21 HUB or Maxq1050)

Description:

This command can be issued when the Card Reader has successfully sent ‘Start Download for K21 HUB or Maxq1050’ command and there is no state change after processing this command.

The HOST uses this command to download firmware data to the Card Reader.

For additional details, please refer to: Download Firmware for K21 HUB

Command:

Task ID	'72' or '76'
Function ID	'81'
Length	Length of data
Data	• Download block sequence number, unsigned 2-byte little-endian, start at zero • Length of the download block [Note]

Note:

- Firmware file is enciphered BIN file. The maximum size of BIN file is 1M bytes for K21 HUB and 128K bytes for Maxq. K21 HUB and Maxq firmware is saved in the external flash memory. There is a 1M bytes (256 pages) sector in the external flash memory for new firmware BIN file storage.
- Block# 0 has 256 bytes firmware signature. Signature algorithm is RSASSA_PSS_SHA256. Signed by manufacture public key.
- Firmware data starts from Block# 1. Length of the download block is 4k bytes if not reach the final block of firmware file. The final Block# n may not have 4k bytes data. The size of the final block is the actual bytes left, zero padding before encryption.

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Firmware download failed [Note]
Task ID	'27' or '67'
Function ID	‘81’
Length	0
Data	None

Note: sending ‘Firmware download failed’ if the ‘Start download for K21 HUB or Maxq1050’ command has not successfully been received.

2.6.31 82 – Program Chip (for K21 HUB or Maxq1050)

Description:

This command can be issued when the Card Reader is in any state.

This command becomes possible to use only after the firmware download is completed.

After CR processes this command, the Reader checks the integrity and authenticity of the downloaded firmware. If the checks pass then the reader accepts the new firmware, resets and starts executing the downloaded firmware.

Command:

Task ID	‘72’ or '76'
Function ID	'82'
Length	0
Data	None

Note:

- For K21 HUB firmware upgrading, after receiving this command, K21-HUB will apply SHA-256 on Block# 1~n data, send those 32 bytes Hash result and Block# 0 firmware signature to Maxq in command “Validate Signature”. If the signature is valid CR replace the old K21 HUB firmware with the new one then sends back the response for “Program Chip for K21 HUB” and start using the new firmware. If the signature is invalid, K21 HUB needs to fully erase the loaded firmware file and keeps using the old firmware.
- For Maxq firmware upgrading, after receiving this command, Maxq will apply SHA-256 on Block# 1~n data, then validate those 32 bytes Hash result against Block# 0 firmware signature. If the signature is validated, the firmware data can be used to replace the existing firmware. If the signature is invalid, Maxq needs to fully erase the loaded firmware file and keeps using the old firmware.

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Firmware download failed • Number of retries over limit • Any hardware problems • AT checks failed
Task ID	‘27’ or '67'
Function ID	‘82’
Length	0
Data	None

Note: If the response can't be sent to HOST in BWT, Card Reader responds 'Wait', and then HOST keeps sending Poll command to wait for the response. The total waiting time for HOST should not be longer than 60 seconds.

2.6.32 84 – Retrieve Whitelist

This command retrieves any existing white list. See also functions FA and FB (elsewhere in this manual) for setting and removing whitelisted cards.

Command:

Task ID	'76'
Function ID	'84'
Length	0
Data	none

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Invalid Certificate
Task ID	'67'
Function ID	'84'
Length	Length Whitelist
Data	• Whitelist (No signature needed)

2.6.33 89 01-Retrieve ICC Mask Options

Command:

Task ID	'72'
Function ID	'89', '01'
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Unknown parameter in command • Unsupported Command
Task ID	'27'
Function ID	'89', '01'
Length	Length of data
Data	• Length of mask option • Mask options, 5 bytes.

Byte 1: PrePAN, value scope is [0, 6],
Byte 2: PosPAN, value scope is [0, 4],
Byte 3: MaskAscii, value scope is [20h, 7Eh],
Byte 4: MaskHex, value scope is [0Ah, 0Fh]
Byte 5: Expire date output option,
0x30=Mask, 0x31=NotMask, default 0x31

2.6.34 89 03-Set ICC Mask Options

Command:

Task ID	'72'
Function ID	'89', '03'
Length	Length of data
Data	• Length of mask options • Mask Options, 5 bytes

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Unknown parameter in command • Unsupported Command • Save or Config Failed / Or Read Config Error, Flash Error
Task ID	'27'
Function ID	'89', '03'
Length	0
Data	None

Byte 1: PrePAN, value scope is [0, 6],
Byte 2: PosPAN, value scope is [0, 4],
Byte 3: MaskAscii, value scope is [20h, 7Eh],
Byte 4: MaskHex, value scope is [0Ah, 0Fh]
Byte 5: Expire date output option,
0x30=Mask, 0x31=NotMask, default 0x31

2.6.35 90 – Read Log

Description:

This command can be issued any time and there is no state change after processing this command.

In response to this command, CR will return all log entries

Command:

Task ID	'76’
Function ID	'90’
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter
Task ID	'67’
Function ID	‘90’
Length	Length of data
Data	If Card Reader command checks pass, else data not present. • Length of binary block. • Zero or more card reader log entries (binary block). See Log Mechanism section for format of log entry.

2.6.36 91 – Clear Log, Manufacture (MACed)

Description:

This command should be issued after HOST and CR have established Maintenance Certificate and have nonce exchanged. There is no state change after processing this command.

In response to this command, CR will clear all log entries.

After all log entries are cleared, a new Log Cleared entry will be added to the log.

Command:

Task ID	'76'
Function ID	'91'
Length	Length of data
Data	• Length Operator Id • Operator Id • Length AT-Manufacture (Optional for manufacture test version) • AT-Manufacture (Optional for manufacture test version)

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • No nonce generated • Number of retries over limit • Invalid Certificate • AT checks failed
Task ID	'67'
Function ID	'91'
Length	0
Data	None

Note: Operator ID is an 8-byte hexadecimal byte array.

2.6.37 94 – Self Test

Description:

This command is for K21-HUB or HOST to send out self-test command to CR. CR will check the firmware, certificate and whitelist.

Command:

Task ID	'76', '72' or '26'
Function ID	'94'
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Invalid Manufacturing system data
Task ID	'67' or '62'
Function ID	'94'
Length	0
Data	None

Note: Event to trigger the self-test

1. Set RTC value (A2 – CR reads/writes K21 HUB RTC or RTC Event Trigger)
2. Every 23 hours (PCI requires no more than 24 hours, so we use 23 hours)

2.6.38 AE – Get PIN

Description:

For each Bank Card Data session that returns available data or card read error, the data is encrypted using `DATA_PAIRING_DUKPT_FUTURE_KEY_TABLE`. CR will advance `DATA_PAIRING_DUKPT_KEY_KSN` and update `DATA_PAIRING_DUKPT_FUTURE_KEY_TABLE` before encrypting new card data. Same as `PIN_DUKPT_KEY and PIN_PAIRING_DUKPT_KEY`, PINPAD must advance `PIN_DUKPT_KEY_KSN` or `PIN_PAIRING_DUKPT_KEY_KSN` and update `PIN_DUKPT_FUTURE_KEY_TABLE` or `PIN_PAIRING_DUKPT_FUTURE_KEY_TABLE` before encrypting new PIN data.

Cancel command stops any ongoing “Get PIN” waiting. Timeouts also apply (see further below).

For Online PIN command, K21 HUB sends this command to Maxq then Maxq sends encrypted PAN to PINPAD. As a response, PINPAD encrypts PIN block (twisted with PAN) using PIN_DUKPT_KEY. This enciphered PIN block will be passed through Maxq and stores in K21 HUB EMV Lv2 kernel.

Command:

Task ID	'76'
Function ID	'AE'
Example	0213007646ae0e00010102001e0002003c000200454ebb6d03
Length	Length of data
Data	• Mode byte: - 0x00 - Cancel(cancel through command) - 0x01 - Online PIN DUKPT - 0x02 - Online PIN MKSK • MSR PAN, 1 byte 0 – ICC PAN 1 – MSR PAN • If ICC PAN: Length plain text ICC PAN • If ICC PAN: Plain text ICC PAN • Length start PIN input timeout • Start PIN input timeout in seconds • Length of PIN entry interval • PIN entry interval in seconds • Length of Display Message Language (2 bytes) • Display Message Language, 2 byte EN - English (default) ES - Spanish ZH - Chinese FR - French

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems

Task ID	'67', '62'
Function ID	'AE'
Length	Length of data
Data	If Mode byte is "Cancel" or "Offline PIN", below info not applicable. If Mode byte is "Online PIN", below fields appear: ▪ 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 Online PIN DUKPT, PIN_DUKPT_KEY KSN ▪ Length Enciphered PIN ▪ Enciphered PIN

All the timeout values are little-endian.
180 seconds is timeout for starting PIN input. Once PIN input starts, 20 seconds is timeout for finishing PIN input.

2.6.39 B0 – Display and Get Key

Description:

This command should be issued after CR and PINPAD/HOST have established MAC Key and there is no state change after processing this command.

In response to this command, PINPAD/HOST will control its display.

Command:

Task ID	'25' or '27'
Function ID	'B0'
Length	Length of data

Data	• Display mode 1- Menu Display 2- Normal Display get function key 3- Display without key input 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: For "Language Menu Display", external display should extend the Message String to full string. For example: EN – English ES – Espanol ZH – 中文 FR - Francis Message ID: 1 byte, check 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 the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems
Task ID	'52' or '72'
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 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:
When display message has more characters than the screen can support, use F1 key as page up and F2 key as page down.

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

2.6.40 D1 – Set Session Key

Description:
Load Session Keys into device.

Command:

Task ID	'78'
Function ID	'D1'
Length	Length of data
Data	• Length of Session Key type • Session Key type • Length of Session Key • Session Key • Length of check digits • Check digits

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Any hardware problems • Invalid Master DUKPT Key • Invalid Data DUKPT Key • Invalid MAC DUKPT Key
Task ID	'67'
Function ID	'D1'
Length	0
Data	• None

Key Type
0 – Data
1 – MAC
Session Key (16 bytes) and check digits (2 bytes) are in hexadecimal. Session Key is encrypted with Master Key. The check digits are from the clear Session Key.

2.6.41 D3 – Generate MAC for Host

Description:

Generate TDES CBC MAC for host with MAC session key.

Command:

Task ID	'78'
Function ID	'D3'
Length	Length of input stream
Data	• Input stream

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Invalid MAC DUKPT Key
Task ID	'67'
Function ID	'D3'
Length	Length of data
Data	• MAC data

Input stream is in ASCII. Use symbol 0xC0, 0xD0 for clear track 2 data in input stream.
Example:
Input Stream: 31311C393138C0D04511
Track 2:
3B3531353037313032303031303739363 03D303930393130313430303030333535 3F
Input Stream to be MAC-hashed:
31311C3931383B3531353037313032303031303739363 03D303930393130313430303 0303335353F4511
MAC data is 8 bytes.
The algorithm is defined in ISO 16609 as TDES CBC MAC.

2.6.42 D4 – Get Key ID

Description:

Get Key ID associated with a Master Key set.

Command:

Task ID	‘78’
Function ID	'D4’
Length	0
Data	None

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • Duplicate detected
Task ID	‘78’
Function ID	‘D4’
Length	Length of Key ID
Data	• Key ID

Key ID is 8 bytes alphanumeric.

2.6.43 FA – Load Secure Data (Whitelist), ATed or MACed

Description:

This command normally requires Card Reader be under “Manufacture” status, and “Load Certificate from CA Server” is already done. Because the command is secure, it must use a MAC hash conforming to the HMAC standard. Use the Universal SDK or UDemo app, as applicable, to issue this command.

Command:

Task ID	‘76’
Function ID	'FA’
Length	Length of data
Data	• Length Whitelist ASN.1 BLK • Whitelist ASN.1 BLK (Optional) • MAC-Host or AT-Host

```
Whitelist ASN.1 structure::= Sequence
{
        Whitelist ASN.1 structure version = 1 (INTEGER)
        BIN Exclusion::= Set
        {
                bininfo::= Sequence
                {
                        binSetName = (PRINTABLESTRING) -- 0 if no name
                        binLow = (INTEGER) -- bin >= binLow
                        binHigh = (INTEGER) -- bin <= binHigh
                }
        }
}
```

Example:
3072020101316D300C1300020304B499020304B499300C13000203092A490203092A
49300C13000203092BE00203092BE0300C13000203097DCA0203097DCB300C1300
0203099C630203099C63300C130002030BDDE402030BDE473017130B436F6D6F74
61204361726402030ACC1002030ACC73

Example for Implementation in firmware/software:

```
static const unsigned int  whitelist_Table[][2] = { // "g*","T7*" for JIS II
      // binLow                binHigh                Range
      {707600,          707699},     // [707600, 707699] or 7076, Comota card
      {777700,          777799},     // [777700, 777799] or 7077, Jack in the box
      {622026,                622027},     // [622026, 622027], Metropolitan card
      {308377,                308377},     // 308377 only, Metropolitan card
      {600649,                600649},     // 600649 only, ValueLink gift card
      {601056,                601056},     // 601056 only, SVS Gift Card, new
ValueLink card
      {629859,                629859},     // 629859 only, Transaction Resources Inc
Gift Card
      {0,               0}          // end
};
```

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • No nonce generated • Number of retries over limit • Invalid MAC Key
Task ID	'67'
Function ID	'FA'
Length	0
Data	None

2.6.44 FB – Remove White List, ATed or MACed

Description:

This command removes this White List.

Command:

Task ID	‘76’
Function ID	'FB’
Length	Length of data
Data	• MAC-Host or AT-Host

Response:

Result byte	If the packet and command are correctly formed, the following status byte is possible: • Wrong parameter • No nonce generated • Number of retries over limit • Invalid MAC Key
Task ID	‘67’
Function ID	‘FB’
Length	0
Data	None

Data	• Display mode 1- Menu Display 2- Normal Display get function key 3- Display without key input 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: For "Language Menu Display", external display should extend the Message String to full string. For example: EN – English ES – Espanol ZH – 中文 FR - Francis Message ID: 1 byte, check 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

3 Application Notes

3.1 Algorithms

3.1.1 Nonce

The nonce is a one-time/single-use token that helps to secure the command and message. Based on PCI spec of HSM, the nonce should be ensured to be 'sufficiently unpredictable' to against the test of NIST SP 800-22. The purpose of the nonce is to prevent replay attacks.

3.1.2 Padding

Padding format is defined in TR-31, but no specification exists to define how to generate it. Therefore we use here the padding format defined in TR-31 and the generation mechanism of OAEP introduced in ANS X9F1.

PKCS#5 Padding: PKCS5Padding follows the following rules:

- The number of bytes to be padded must equal "8 - numberOfBytes(clearText) mod 8". So 1 to 8 bytes will be added to the clear text data depending on the length of the clear text data.
- All padded bytes have the same value: the number of bytes padded.

Thus, for example, if M is the original clear text and PM is the padded clear text:

If numberOfBytes(clearText) mod 8 == 7, PM = M + 0x01
If numberOfBytes(clearText) mod 8 == 6, PM = M + 0x0202
If numberOfBytes(clearText) mod 8 == 5, PM = M + 0x030303
...
If numberOfBytes(clearText) mod 8 == 0, PM = M + 0x0808080808080808

3.1.3 SHA256

Use SHA-256 to calculate any hash result.

3.1.4 HMAC

Use HMAC-SHA256 (Refer to RFC2104), retaining only the left-most (high order) **16 bytes** of the calculation for MAC Authentication.

$$HMAC(K,m) = H\left((K \oplus opad) | H((K \oplus ipad)|m)\right)$$

Where

H is a cryptographic hash function (SHA256),
K is a secret key, padded to the right with extra zeros to the input block size of the hash function, or the hash of the original key if it's longer than that block size,
Secret key is the MAC key both-way variant, derived from MAC_DUKPT_BDK
m is the message to be authenticated,
| denotes concatenation,
⊕ denotes XOR,
opad is the outer padding (0x5c5c5c…5c5c, one-block-long hexadecimal constant),
ipad is the inner padding (0x363636…3636, one-block-long hexadecimal constant).

The final HMAC value consists of the first 16 bytes of the overall hash.

3.1.5 SIGN

Use 2048-bits RSASSA_PSS_SHA256 for signature calculation.

3.1.6 RSA ENCRYPT

Use 2048-bits RSA_OAEP for asymmetric key encryption.

3.2 Computations

3.2.1 AT-Manufacture

The token used to authenticate messages sent from Vendor.

This computation is used when vendor wants to load secure information to device.

AT-Manufacture = RSASSA_PSS_SHA256<DMKs>(CR_NONCE || CR_UID || msgX)

The AT-Manufacture will be the last field in a message and msgX will be 1st byte of message being built (TPPACKET.InstructionCode) up to (but not including) the AT-Manufacture 1st byte.
Note: There is no CR_NONCE || CR_UCI required because this message is generated for all the devices.

3.2.2 AT-HOST

The token used to authenticate messages sent from HOST to CR.

This computation is slower than MAC-HOST and will be used until MAC-HOST is established.

AT-HOST = RSASSA_PSS_SHA256<HSKs>(CR_NONCE || CR_UID || msgX)

The AT-HOST will be the last field in a message and msgX will be 1st byte of message being built (TPPACKET.InstructionCode) up to (but not including) the AT-HOST 1st byte.

3.2.3 AT-CR

The token used to authenticate messages sent from CR to HOST or from CR to PINPAD.

This computation is slower than MAC-CR and will be used until MAC-CR is established.

AT-CR = RSASSA_PSS_SHA256<CSKs>(HOST_NONCE || HOST_ID || msgX)
or
AT-CR = RSASSA_PSS_SHA256<CSKs>(PINPAD_NONCE || PINPAD_UID || msgX)

The AT-CR will be the last field in a message and msgX will be 1st byte of message being built (TPPACKET. InstructionCode) up to (but not including) the AT-CR 1st byte.

3.2.4 MAC-HOST

The HMAC result used to authenticate messages sent from HOST to CR.

MAC-HOST = 2bytes length_MAC + HMAC<MAC_DUKPT_KEY>(CR_NONCE || CR_UID || msgX) + 2bytes length_KSN + MAC_DUKPT_KEY_KSN

The MAC-HOST will be the last field in a message and msgX will be 1st byte of message being built (TPPACKET. InstructionCode) up to (but not including) the MAC-HOST 1st byte.

Advancing KSN is controlled by Host.

3.2.5 MAC-CR

The HMAC result used to authenticate messages sent from CR to HOST:

MAC-CR = 2bytes length_MAC + HMAC<MAC_DUKPT_KEY1>(HOST_NONCE || HOST_ID || msgX) + 2bytes length_KSN + MAC_DUKPT_KEY1_KSN

Or from CR to PINPAD:
MAC-CR = 2bytes length_MAC + HMAC<MAC_DUKPT_KEY2>(PINPAD_NONCE || PINPAD_UID || msgX) + 2bytes length_KSN + MAC_DUKPT_KEY2_KSN

The MAC-CR will be the last field in a message and msgX will be 1st byte of message being built (TPPACKET. InstructionCode) up to (but not including) the MAC-CR 1st byte.

In the CR-PINPAD communication, advancing KSN is controlled by CR.

3.3 Log Mechanism

A log mechanism will enable the recording of certain card reader events which are required by the latest release of PCI. The log creation, storing, clearing and reading follow the lastest PCI requirements.

The events include security events, such as

- Removal sensor flag just on
- Removal sensor flag just cleared
- Log records just cleared
- Manufacture system data just loaded
- Firmware downloading
- Root CA erased
- Root CA loaded

And tamper events, such as

- Tamper events just occurred
- Tamper events just disappeared.

Log mechanism properties:

1. Log entries stored in reader non-volatile memory.
2. Log entry contents (size 16 bytes):
    a. DateTime – Date and time of event.

        Format: 6-byte
        -Year, one byte in BCD, 00~99
        -Month, one byte in BCD, 01~12
        -Day, one byte in BCD, 01~31
        -Hour, one byte in BCD, 00~23
        -Minute, one byte in BCD, 00~59
        -Second, one byte in BCD, 00~59s

    b. OperatorID – Operator ID/Host ID of entity that caused the logged event.

        Format: 8 bytes
        All 0x00 – Card reader caused event:
        Can only be used by card reader caused events
        Ex: Removal flag change: cleared -> set
        Else – ID of operator that caused event (passed in HOST command).

    c. EventType – Event type.
        Format: 2 bytes, as [Byte 0], [Byte 1]
        Byte 0: Event Class:
        0x01 – Security event
        0x02 – Tamper event
        Byte 1: Event Type:
        1) Security Events:
        a. 0x01 – Log cleared.

b. 0x02 – Removal sensor flag changed: set to cleared
c. 0x03 – Removal sensor flag changed: cleared to set
d. 0x04 – Manufacturer system data just loaded
e. 0x05 – New Maxq firmware being written
f. 0x06 – New K21 firmware being written
g. 0x07– Root CA reload with signed root

2) Tamper event
   a. Mirrors Tamper Status Byte in the response to Poll Card Reader command.
   b. If the 'other tamper flag' is on, short information can be stored in the OperatorID field.

3. Must be readable (requires authentication).
4. Must be resettable (requires authentication).

Operational notes:

1. If the log is full, then certain card reader operations will be disabled (ex: Clear Removal Sensor).
2. The reader can keep at least 290 log records.

3.4 Download Firmware

3.4.1 Start Download

After receiving this command, timing should begin a download session for a maximum 15 minutes of download time. A flag is set to indicate firmware is ready for download.

3.4.2 Download Firmware

- Download ready flag should be checked at the beginning to make sure the previous step is finished, if flag is not set, return error message.
- If flag is set, copy firmware to the external flash memory.
- Firmware is copied to external flash memory by blocks. The first block is consist of 256 bytes firmware signature and starting from second block, firmware is divided into many 4k blocks, remainder bytes left are copied in the last block. 4k flash storage is assigned for each block (including the first and last), and each of them are erased before copying.
- A flag should set after saving/copying the new firmware to indicate firmware is ready for write.

3.4.3 Write Firmware

- "Download complete" flag from previous step should be checked; if flag is not set, return error message.
- If flag is set, 32 bytes of HASH is calculated from the downloaded firmware using SHA256 algorithm. Calculated Hash and firmware signature are put together (for K21 it needs to be sent to CR through AA command) to validate the firmware.
- If firmware is valid (for K21, an ACK response should be received from CR), system starts the preparation sequence for getting into bootloader to write the firmware.
    - Two 4 byte values, total of 8 bytes, of firmware upgrade flag is stored in the designated memory address.
    - Following the last byte of firmware upgrade flag, firmware size is stored into the next 2 bytes of memory address.
    - Firmware Hash is stored to designated memory address for future validation.
    - System reset is generated and system goes into bootloader.
- Bootloader will check the firmware upgrade flag; if correct flag is placed in the designated memory, new firmware stored in the external flash memory will be copied to microcontroller memory where main application is stored and replaces the original firmware.(This step is preceded by sending 4k blocks as download step.)

- After copying is completed, HASH is calculated from the updated firmware and compared to the HASH value stored in the memory in the previous steps. If Hash matches, firmware upgrade flag is cleared from the memory and the image of external flash can be cleared, then system exit bootloader starts for main application.

4 ICC EMV Level II Reference Data List

4.1 Terminal Data List

Data ID	Tag	Value name	Length (Byte)	Default Value
1	9F1A	Terminal Country Code	2	08 40
2	9F35	Terminal Type	1	25
3	9F33	Terminal Capability	3	E0 F8 C8
4	9F40	Additional Terminal Capability	5	F0 00 F0 A0 01
5	9F1E	IFD Serial Number (write only one time)	8	01 02 03 04 05 06 07 08
6	9F15	Merchant Category Code	2	
7	9F16	Merchant Identifier	15	
8	9F1C	Terminal Identification	8	
9	9F4E	Merchant Name and Location	var.	

Note: IFD Serial Number will be changed from Device Serial Number.

4.2 Application Data List

Data ID	Tag	Value name	Length (Byte)	Default Value
1	5F57	Account Type	1	
2	9F01	Acquirer Identifier	6	
	9F06	Application Identifier (AID) – terminal	5-16	
3	9F09	Terminal application version number	2	00 02
4	5F36	Transaction Currency Exponent	1	
5	9F1B	Terminal Floor Limit	4	
6	9F49	Dynamic Data Authentication Data Object List(DDOL)	var. up to 252	
7	97	Transaction Certificate Data Object List(TDOL)	var. up to 252	
8	9F39	POS Entry Mode	1	07
9	9F3C	Transaction Reference Currency Code	2	
10	9F3D	Transaction Reference Currency Exponent	1	
11	99	PIN Block	8	
12	DF10	Terminal Language Preference	8	45 4E (“EN”)
	DF11	Trans Log Support	1	1: enable
13	DF13	TAC-Default	5	
14	DF14	TAC-Denial	5	

15	DF15	TAC-Online	5	
16	DF17	Threshold Value for Biased Random Selection	var	
17	DF18	Target Percentage For Random Transaction Selection	var	
18	DF19	Maximum Target Percentage For Random Transaction Selection	var	
	DF20	Trace	1	
19	DF22	Merchant Forced Transaction Online	1	
20	DF25	Default DDOL	var	
21	DF26	Revocation list Support	1	1: enable
	DF27	Exception list Support	1	0: disable
22	DF28	TDOL	var	
23	DF30	Online DOL	var	
24	DF62	Application Selection Flag	1	
	DF63	Transaction Reference Currency Conversion	4	
25	DF34	Authorization Response Code 1-2 bytes: approved code 3-4 bytes: referral code 5-6 bytes: declined code	6	

4.3 Transaction Data List (start command parameters)

Data ID	Tag	Value name	Length (Byte)	Default Value
1	9F02	Amount, Authorised (Numeric)	6	
2	9C	Transaction Type	1	
3	5F2A	Transaction Currency Code	2	08 40
4	9A	Transaction Date	3	
5	9F21	Transaction Time	3	
6	9F03	Amount, Other(Numeric)	6	
	9F04	Amount, Other(Binary)	6	
	9F3A	Amount, Reference Currenty	4	
	9F41	Transaction Sequence Counter	1	

4.4 Output Data List

Data ID	Tag	Value name	Length (Byte)	Default Value
1	57	Track2 Equivalent Data	<=19	
2	5A	PAN	<=10	

3	5F34	PAN Sequence Number	1	
4	5F20	Cardholder Name	2~26	
5	5F24	Application Expire Date	3	
6	9F20	Track2 Discretionary Data	var.	
7	5F25	Application Effective Date	3	
8	5F2D	Language Preference	2~8	
9	50	Application Label	1~16	
10	84/4F	DF Name or ADF Name	5~16	
11	DF21	Issuer Script Results		

4.5 Option Data List

Data ID	Tag	Value name	Length (Byte)	Default Value
1	9F36	Application Transaction Counter(ATC)	2	
2	9F37	Unpredictable Number	4	
3	9F02	Amount, Authorised(Numeric)	6	
4	9F4D	Log Entry	2	
5	9F4F	Log Format	var.	
6	9F13	Last Online Application Transaction Counter(ATC) Register	2	
7	95	Terminal Verification Results	5	
8	9B	Transaction Status Information	2	
9	9F03	Amount, Other(Numeric)	6	
10	9F34	Cardholder Verification Method(CVM) Results	3	
11	99	PIN Block	8	
12	DFEE1A	Output Tag List	var.	
13	9F1D	Terminal Risk Management Data	1-8	
14	9F22	Certification Authority Public Key Index	1	

4.6 ID TECH Internal Data List

Tag	Value name	Length (Byte)	Default Value
DFEE12	KSN (send only when KSN advances)	10	
DFEE13	Track 1 Data (contactless) 1. DiscoverZip Need Use it.	var.	

<table>
<tr><td></td><td>2. Visa MSD Need Use it.
3. Amex Need Use it.
4. PBOC Need Use it.
Need masked field and encrypted field.</td><td></td><td></td></tr>
<tr><td>DFEE14</td><td>Track 2 Data (contactless)
1. DiscoverZip Need Use it.
2. Visa MSD Need Use it.
3. Amex Need Use it.
4. PBOC Need Use it.
Need masked field and encrypted field.</td><td>var.</td><td></td></tr>
<tr><td>DFEE15</td><td>Application Selection Indicator</td><td>b</td><td>1</td></tr>
<tr><td>DFEE16</td><td>DUKPT or MK/SK Select for online PIN encrypted</td><td>b</td><td>1</td></tr>
<tr><td>DFEE17</td><td>ICC Terminal Entry Mode</td><td>b</td><td>1</td></tr>
<tr><td>DFEE18</td><td>MSR Terminal Entry Mode</td><td>b</td><td>1</td></tr>
<tr><td>DFEE19</td><td>Online DOL</td><td>b</td><td>1-256</td></tr>
<tr><td>DFEE1A</td><td>Output Tag List</td><td>var</td><td></td></tr>
<tr><td>DFEE1B</td><td>Authorization Response Code</td><td>b</td><td>8</td></tr>
<tr><td>DFEE1E</td><td>Contact Terminal Configuration
(Default: F0 DC 3C F0 C2 9E 94 00)

Byte 1
<table>
<tr><th>b 8</th><th>b 7</th><th>b 6</th><th>b 5</th><th>b 4</th><th>b 3</th><th>b 2</th><th>b 1</th><th>Meaning</th></tr>
<tr><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Key Pad support</td></tr>
<tr><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>LCD support</td></tr>
<tr><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>PIN Pad support</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Print Support</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>0</td><td>x</td><td>x</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>0</td><td>x</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>0</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>X</td><td>0</td><td>RFU</td></tr>
</table>
Byte 2
<table>
<tr><th>b 8</th><th>b 7</th><th>b 6</th><th>b 5</th><th>b 4</th><th>b 3</th><th>b 2</th><th>b 1</th><th>Meaning</th></tr>
<tr><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>PSE support</td></tr>
<tr><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Cardholder confirmation</td></tr>
<tr><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Preferred display order</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Multi language</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>EMV language selection method</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>Default DDOL</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>0</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>0</td><td>RFU</td></tr>
</table>
</td><td>b</td><td>8</td></tr>
</table>

Byte 3

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	x	x	x	x	x	x	x	RFU (Revocation of Issuer Public Key Certificate (DF26))
x	1	x	x	x	x	x	x	Manual action when CA PK loading fails
x	x	1	x	x	x	x	x	CA PK verified with check sum
x	x	x	1	x	x	x	x	Bypass PIN Entry
x	x	x	x	1	x	x	x	Subsequent bypass PIN Entry
x	x	x	x	x	1	x	x	Get data for pin try counter
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Byte 4

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Amount before CVM processing
x	1	x	x	x	x	x	x	Floor limit checking
x	x	1	x	x	x	x	x	Random transaction selection
x	x	x	1	x	x	x	x	Velocity checking
x	x	x	x	0	x	x	x	RFU (Transaction Log (DF11))
x	x	x	x	x	0	x	x	RFU (Exception File (DF27))
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Byte 5

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	X	Terminal action code support

x	1	x	x	x	x	x	x	Terminal action code can be change
x	x	1	x	x	x	x	x	Terminal action code can be deleted or disable
x	x	x	1	x	x	x	x	Default Action code processing before 1st GAC
x	x	x	x	1	x	x	x	Default Action code processing after 1st GAC
x	x	x	x	x	1	x	x	TAC/IAC default process when unable to go online (Skipped)
x	x	x	x	x	x	1	x	TAC/IAC default process when unable to go online (Normal)
x	x	x	x	x	x	x	0	RFU

Byte 6

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Forced Online suppo
x	1	x	x	x	x	x	x	Forced acceptance support
x	x	1	x	x	x	x	x	Advices support
x	x	x	1	x	x	x	x	Issuer referrals suppo
X	x	x	x	1	x	x	x	Batch data capture
x	x	x	x	x	1	x	x	Online data capture
X	x	x	x	x	x	1	x	Default TDOL
X	x	x	x	x	x	x	0	RFU

Byte 7

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	amount and pin entered on the same keypad
x	1	x	x	x	x	x	x	ICC/Magstripe reader combined

	<table><tr><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Magstripe read first</td></tr><tr><td>x</td><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Support account type selection</td></tr><tr><td>x</td><td>x</td><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>On fly script processing</td></tr><tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>Internal date management</td></tr><tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>1</td><td>x</td><td>Reversal Mode (1)Unable go online (2) ARC Error 0: (3) Online Approved but reader not approved. 1: (3) Online Approved but card response AAC.</td></tr><tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>0</td><td>RFU</td></tr></table> Byte 8 <table><tr><td>b 8</td><td>b 7</td><td>b 6</td><td>b 5</td><td>b 4</td><td>b 3</td><td>b 2</td><td>b 1</td><td>Meaning</td></tr><tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>RFU</td></tr></table>		
DFEE1F	Issuer script device limit Range: 0~255 (Default: 128)	b	1
DFEE20	ICC Power on detect waiting time. (Unit: Sec) (Default: 60S)	b	1
DFEE21	ICC L1 waiting time. (Unit: Sec)(Default: 10 S)	b	1
DFEE22	Driver (Menu, Get PIN, Get MSR) Timeout. (Unit: Sec) Byte1: Timeout for Menu. (Default: 30 S) Byte2: Timeout for Get PIN. (Default: 60 S)	b	3

	Byte3: Timeout for Get MSR. (Default: 60 S)		
DFEE23	MSR Track Data	b	1~768
DFEE24	Force Acceptance (Default: 00)	b	1
DFEF1F	Auto authenticate Byte1: Auto authenticate if 1. (Default: 1) Byte2: Force online if Auto auth if 1. (Default 1)	b	2
DFEF20	Response with MAC if 1	b	1

4.7 ID TECH Enhanced TLV format (Masked and Encrypted)

The top 3 bits of the *first length byte* following a tag are used in a special way. The bits are used to indicate masked or encrypted fields (here, we use zero-based bit numbering):

Bit 7: 1 (ON) means it's necessary to check the next two bits
Bit 6: 1 (ON) if there is encrypted field
Bit 5: 1 (ON) if there is masked field

Example:

9F 20 C1 **82** 55 […]
Tag is 9F20. The length will be given by the one byte after C1, namely 0x82, which has the top two bits set; therefore encryption is used. Data starts with the byte value 0x55.

For more information on the enhanced TLV format, consult document P/N 80000502-001, *ID TECH Encrypted Data Output*.

4.8 Tags with Masked or Encrypted Field

Tag	**Data Object**	**Note**
5A	Application PAN	Need masked field and encrypted field.
9F1F	Track 1 Discretionary Data	Encrypted field only.
9F20	Track 2 Discretionary Data	Encrypted field only.
57	Track 2 Equivalent Data	PAN needs to be masked as Tag 5A. Expiry date and service code should be clear-text. Need masked field and encrypted field.
56	Track 1 Data	For MasterCard-Paypass (MagStripe) and DiscoverZip.

		Need masked field and encrypted field.
9F6B	Track 2 Data	For MasterCard-Paypass (MagStripe) only. Need masked field and encrypted field.
9F37	Unpredictable Number	Encrypted field only.
FF EE 13	Track 1 Data	1. DiscoverZip uses it. 2. Visa MSD uses it. 3. Amex uses it. 4. PBOC uses it. Need masked field and encrypted field.
FF EE 14	Track 2 Data	1. DiscoverZip uses it. 2. Visa MSD uses it. 3. Amex uses it. 4. PBOC uses it. Need masked field and encrypted field.

Note:
1. DiscoverZip uses Tag 56, FF EE 13 and FF EE 14.
2. Visa MSD, Amex and PBOC use Tag FF EE 13, FF EE 14.

4.9 Response Code and Transaction Result

No.	Error Result Code	description
1	0x00, 0x00	PROCESS_OFFLINE_APPROVED
2	0x00, 0x01	PROCESS_OFFLINE_DECLINED
3	0x00, 0x02	PROCESS_APPROVED
4	0x00, 0x03	PROCESS_DECLINED
5	0x00, 0x04	PROCESS_ONLINE
6	0x00, 0x05	PROCESS_CALL_YOUR_BANK
7	0x00, 0x06	PROCESS_NOT_ACCEPTED
8	0x00, 0x07	PROCESS_USE_MAGSTRIPE
9	0x00, 0x08	PROCESS_TIMEOUT
10	0x00, 0x10	(start transaction success)
11	0x00, 0x11	MSR_SUCCESS
Error code	0x10, 0x01	INVALID ARG
	0x10, 0x02	FILE_OPEN_FAILED
	0x10, 0x03	FILE OPERATION_FAILED
	0x20, 0x01	MEMORY_NOT_ENOUGH

	0x30, 0x01	SMARTCARD_OK
	0x30, 0x02	SMARTCARD_FAIL
	0x30, 0x03	SMARTCARD_INIT_FAILED
	0x30, 0x04	FALLBACK_SITUATION
	0x30, 0x05	SMARTCARD_ABSENT
	0x30, 0x06	SMARTCARD_TIMEOUT
	0x30, 0x07	MSR_FAILED
	0x50, 0x01	EMV_PARSING_TAGS_FAILED
	0x50, 0x02	EMV_DUPLICATE_CARD_DATA_ELEMENT
	0x50, 0x03	EMV_DATA_FORMAT_INCORRECT
	0x50, 0x04	EMV_NO_TERM_APP
	0x50, 0x05	EMV_NO_MATCHING_APP
	0x50, 0x06	EMV_MISSING_MANDATORY_OBJECT
	0x50, 0x07	EMV_APP_SELECTION_RETRY
	0x50, 0x08	EMV_GET_AMOUNT_ERROR
	0x50, 0x09	EMV_CARD_REJECTED
	0x50, 0x10	EMV_AIP_NOT_RECEIVED
	0x50, 0x11	EMV_AFL_NOT_RECEIVED
	0x50, 0x12	EMV_AFL_LEN_OUT_OF_RANGE
	0x50, 0x13	EMV_SFI_OUT_OF_RANGE
	0x50, 0x14	EMV_AFL_INCORRECT
	0x50, 0x15	EMV_EXP_DATE_INCORRECT
	0x50, 0x16	EMV_EFF_DATE_INCORRECT
	0x50, 0x17	EMV_ISS_COD_TBL_OUT_OF_RANGE
	0x50, 0x18	EMV_CRYPTOGRAM_TYPE_INCORRECT
	0x50, 0x19	EMV_PSE_NOT_SUPPORTED_BY_CARD
	0x50, 0x20	EMV_USER_SELECTED_LANGUAGE
	0x50, 0x21	EMV_SERVICE_NOT_ALLOWED
	0x50, 0x22	EMV_NO_TAG_FOUND
	0x50, 0x23	EMV_CARD_BLOCKED
	0x50, 0x24	EMV_LEN_INCORRECT
	0x50, 0x25	CARD_COM_ERROR
	0x50, 0x26	EMV_TSC_NOT_INCREASED
	0x50, 0x27	EMV_HASH_INCORRECT
	0x50, 0x28	EMV_NO_ARC
	0x50, 0x29	EMV_INVALID_ARC
	0x50, 0x30	EMV_NO_ONLINE_COMM
	0x50, 0x31	TRAN_TYPE_INCORRECT
	0x50, 0x32	EMV_APP_NO_SUPPORT

	0x50, 0x33	EMV_APP_NOT_SELECT
	0x50, 0x34	EMV_LANG_NOT_SELECT
	0x50, 0x35	EMV_NO_TERM_DATA
	0x60, 0x01	CVM_TYPE_UNKNOWN
	0x60, 0x02	CVM_AIP_NOT_SUPPORTED
	0x60, 0x03	CVM_TAG_8E_MISSING
	0x60, 0x04	CVM_TAG_8E_FORMAT_ERROR
	0x60, 0x05	CVM_CODE_IS_NOT_SUPPORTED
	0x60, 0x06	CVM_COND_CODE_IS_NOT_SUPPORTED
	0x60, 0x07	NO_MORE_CVM
	0x60, 0x08	PIN_BYPASSED_BEFORE
	0x70, 0x01	PK_BUFFER_SIZE_TOO_BIG
	0x70, 0x02	PK_FILE_WRITE_ERROR
	0x70, 0x03	PK_HASH_ERROR
	0x80, 0x01	NO_CARD_HOLDER_CONFIRMATION
	0x80, 0x02	GET_ONLINE_PIN

Appendix A: Error Codes

Type	Result byte	Meaning
General	'90','31'	Unknown command
	'90',‘32’	Wrong parameter (such as the length of the command is incorrect)
	'90',‘3A’	Number of retries over limit
State error	'90',‘40’	Invalid Manufacturing system data
	'90',‘41’	Not authenticated
	'90',‘42’	Invalid Master DUKPT Key
	'90',‘43’	Invalid MAC Key
	'90',‘44’	Reserved for future use
	'90',‘45’	Reserved for future use
	'90',‘46’	Invalid DATA DUKPT Key
	'90',‘47’	Invalid PIN Pairing DUKPT Key
	'90',‘48’	Invalid DATA Pairing DUKPT Key
	'90',‘49’	No nonce generated
	'90',‘4A’	Not ready
	'90',‘4B’	Not MagAC data
Data error	'90',‘50’	Invalid Certificate
	'90',‘51’	Duplicate detected
	'90',‘52’	AT checks failed
	‘90’,‘53’	TR34 checks failed
	‘90’,‘54’	TR31 checks failed
	‘90’,‘55’	MAC checks failed

	‘90’,‘56’	Firmware download failed
Resource error	‘90’,‘60’	Log is full
	‘90’,‘61’	Removal sensor unengaged
	‘90’,‘62’	Any hardware problems
Third party error	‘90’,‘70’	ICC communication timeout
	‘90’,‘71’	ICC data error (such check sum error)
	‘90’,‘72’	Smart Card not powered up
ICC EMV Lv2 error	‘F2’,‘00’	No AID or No Application Data
	‘F2’,‘01’	No Terminal Data
	‘F2’,‘02’	Wrong TLV format
	‘F2’,‘03’	AID list is full, maxim is 16
	‘F2’,‘04’	No any CA Key
	‘F2’,‘05’	No CA Key RID
	‘F2’,‘06’	No CA Key Index
	‘F2’,‘07’	CA Key list is full, maxim is 16
	‘F2’,‘08’	Wrong CA Key hash
	‘F2’,‘09’	Wrong Transaction Command Format
	‘F2’,‘0A’	Unexpected Command
	‘F2’,‘0B’	No CRL
	‘F2’,‘0C’	CRL list is full, maxim is 90

	‘F2’,‘0D’	No amount , other amount and transaction type in Transaction Command
	‘F2’,‘0E’	Wrong CA Hash and Encryption algorithm
	‘F2’,‘0F’	No Financial Card
	‘F2’,‘10’	Invalid CRL length
	‘F2’,‘11’	ICC L2 is not in idle state
	‘F2’,‘12’	Transaction Type Error
	‘F2’,‘13’	Can’t modify major bits in terminal setting
	‘6C’,’00’	Unknown parameter in command – Protocol task ID and command are right, but length is out of
	‘6A’,’00’	Unsupported Command – Protocol and task ID are right, but command is invalid
	‘60’,’00’	Save or Config Failed / Or Read Config Error, Flash Error

Appendix B: 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 BON?	CORRECTA CANTIDAD?	确定金额
3	MSG_APPROVED	APPROVED	APPROUVE	APROVADO	通过
4	MSG_CALL_YOUR_BANK	CALL YOUR BANK	APP VOTRE BANQUE	LLAME A SU BANCO	请联系您的银行
5	MSG_CANCEL_OR_ENTER	CANCEL OR ENTER	ANNULER OU ACCEP	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	ENTRE LE MONTANT	INGRESE LA CANTIDAD	输入金额
9	MSG_ENTER_PIN	ENTER PIN:	ENTRER PIN:	ENTRAR NPI (Numero de Identificación Personal):	请输入密码
10	MSG_INCORRECT_PIN	INCORRECT PIN	CODE INCORRECT	NIP INCORRECTO	密码错误
11	MSG_ICC_MSR1	SWIPE OR INSERT	PASSER OU INSERER	DESLIZAR O INSERTAR	请刷卡或插卡
12	MSG_ICC_MSR2	CARD	CARTE	TARJETA	卡
13	MSG_INSERT_CARD	INSERT CARD	INSERER CARTE	INSERTAR LA TARJETA	请插卡
14	MSG_USE_CHIP_READER	USE CHIP READER	UTI LECTEUR PULE	LECTOR DE USO CHIP	使用芯片卡
15	MSG_NOT_ACCEPTED	NOT ACCEPTED	PAS ACCEPTE	NO ACEPTADA	无法接受
16	MSG_PIN_OK	GET PIN OK	CODE BON	OBTENER PIN OK	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 DE PROCESAMIENTO	处理错误
19	MSG_USE_MAGSTRIPE	USE MAGSTRIPE	UTILISER CARTE MAG	USE BANDA MAGNETICA	使用磁条卡
20	MSG_TRY_AGAIN	TRY AGAIN	REESSAYEZ	INTENTAR DE NUEVO	请重试
21	MSG_ONLINE	GO ONLINE	ALLER EN LIGNE	CONECTESE A LA LINEA	在线
22	MSG_TRANSACTION_ERROR	TRANSACTION ERR	ERREUR DE TRANSAC	ERROR DE TRANSACCION	交易错误
23	MSG_TERMINATE	TERMINATE	TERMINER	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	ESSAIS CODE DEPASSE	LIMITE INTENTO DE PROBAR EL NIP	密码尝试次数过多

28	MSG_ISSUER_AUTH_FAIL	ISSUER AUTH FAIL	EMETTEUR ERREUR	EMISOR FALLA	与发卡机构认证
29	MSG_CONTINUE_PROCESS	CONTINUE PROCESS	CONTINUER	CONTINUAR EL PROCES	继续处理
30	MSG_GET_PIN_ERROR	GET PIN ERROR	ERREUR CODE	OBTENER EL ERROR DE NIP	密码错误
31	MSG_GET_PIN_FAIL	GET PIN FAIL	ERREUR CODE	OBTENER EL FALLO DE NIP	获取密码错误
32	MSG_NOKEY_GET_PIN	NO KEY GET PIN	NO KEY GET PIN	NO LLAVE OBTENER EL NIP	无法输入密码
33	MSG_CANCELLED	CANCELLED	ANNULE	CANCELADO	取消
34	MSG_LAST_PIN_TRY	LAST PIN TRY	DERNIER ESSAI CODE	INTENTO AL ULTIMO PRUEBO DEL NIP	最后一次密码尝试
35	MSG_WELCOME	WELCOME	BIENVENUE	BIENVENIDOS	欢迎使用
36	MSG_AMOUNT_OTHER	AMOUNT OTHER	MONTANT AUTRES	IMPORTE OTRAS	返现
37	MSG_ENTER_AMOUNT_OTHER	ENTER AMOUNT OTHER	ENTRER MONTANT AUTRES	ENTRAR IMPORTE OTRAS	输入返现
38	MSG_CAPK_HASH_VALUE_FAIL	CAPK HASH VALUE FAIL	CAPK HASH VALEUR FAIL	CAPK HASH VALOR FAIL	公钥哈希值错误
39	MSG_REMOVE_CARD	REMOVE CARD	RETIRER LA CARTE	RETIRE LA TARJETA	请取卡

Change History

Revision	Date	Description of Changes	Author(s)
50	8/8/2013	Draft	DD
51	2/16/2016	Remove internal information	DD
52	2/18/2016	Edit for clarity/consistency, add copyright notice, format.	KT
53	4/4/2016	Update Response code for each command	DD
54	4/6/2016	Added mention of Universal SDK; explained the length-byte top-bit scheme (re encryption/masking) and referred to new doc 80000501-001 (ID TECH Encrypted Data Output); added Error Codes as Appendix A.	KT
55	6/24/2016	Remove MAC requirement from the following commands: Remove CRLs Set CRLs Remove All CRLs Remove Application Data Set Application Data Remove All Application Data Remove Terminal Data Set Terminal Data Remove CA Public Key Set CA Public Key Remove All CA Public Key Set Terminal ID Set Terminal Major Configuration Clear Transaction Log Remove Exchange APDU with Host command.	KT
A	11/14/2016	Add Consolidated Command List Tables with hot links.	KT
B	11/22/2016 12/19/2016 2/3/2017 2/9/2017 2/13/2017	Add command examples (tabular format). Clarify HMAC description. Edits for clarity. Add Get Firmware Version (Verbose), Function 23 Expanded tables in Poll Reader command. Added explanation (in Transport Layer command structure and elsewhere) that some Functions are two bytes; others are one byte. Add description of Wakeup function (Function ID 51) and mention that a wakeup can be triggered by card insertion.	KT
C	4/5/2017	Added 40-0x commands. Update command 42 and remove MAC requirement. Added commands 44, 46. Added commands 89 01 and 89 03.	KT
D	5/16/2017 5/31/2017 6/01/2017 6/05/2017	Added functions 84, FA, FB on white list management. Added Appendix B on LCD Message Foreign Language Mappings.mma Fix command B0. Updates to commands 22, 25, 42, 43, 05 01, 05 02, 05 03. Add commands D1, D3.	KT
E	9/20/2017	Set Session Key added. Add 40-08, D4, and changes to 25 and 44.	KT