

SCard Reader Series

Technical Manual



S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1000S
SP1100A / SP1100B

Version: V1.10

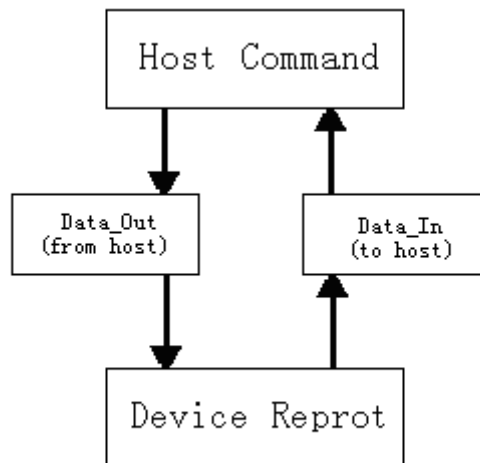
1 Protocol

1.1 USB VCOM

It's convenient and compatible to use VCOM as the communication interface. The default communication parameter was set 9600, N, 8, 1 (9600 bps, No parity bit, 8 data bits, 1 stop bit). If any application needs a different baud rate, just send a command to change baud rate from 9600 bps to 115200 bps.

1.2 USB HID

As the communication interface between device and PC, HID send and receive data package in a cascading fashion, with 64 byte data in each package. The package number depends on application data in the first package. As host, PC sends command package to device and receives response package from device.



- Data_Out package, from host to device, in the method of SetReport.
- Data_In package, from device to host, in the method of GetReport.

1.3 USB CCID

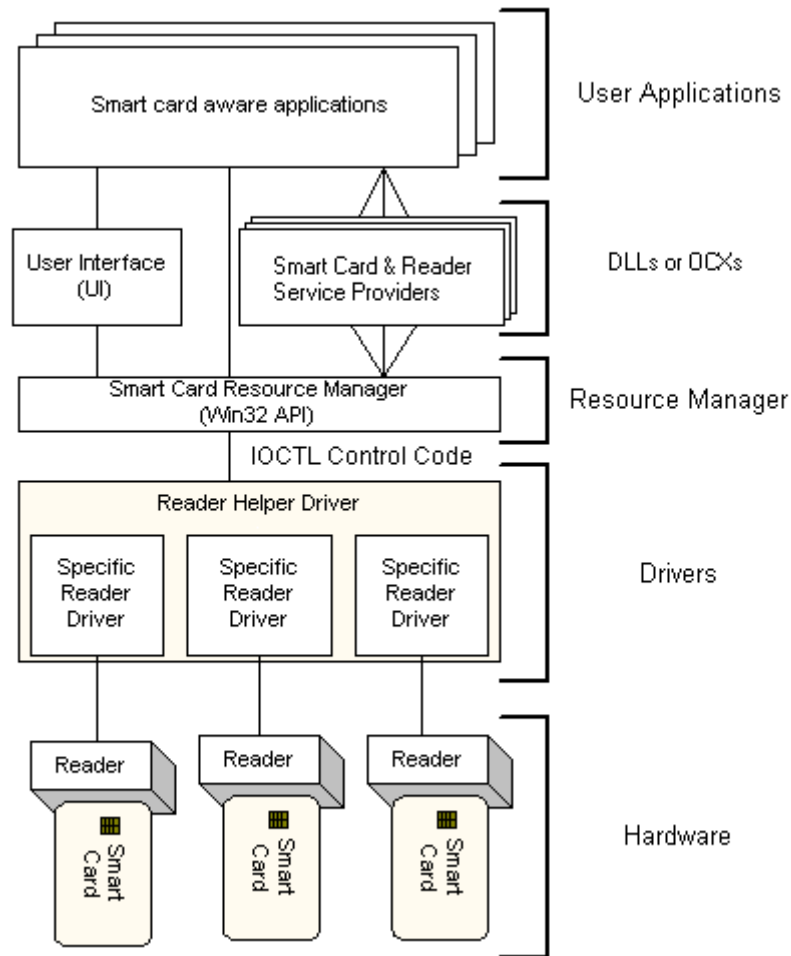
USB CCID (Integrated Circuit Cards Interface) combines USB 2.0, ISO 7816-1~4, EMV '96 standards and support PC/SC, and Microsoft Smart Card Base Components software. You can call Microsoft Smart Card SDK API to control a reader to access smart card inserted but not by

manufacturer command set. It only supports to access smart cards but not all reader functions like magnetic stripe reading and other I/O controls.

http://www.usb.org/developers/docs/devclass_docs/DWG_Smart-Card_CCID_Rev110.pdf

<http://www.pcscworkgroup.com/>

[http://msdn.microsoft.com/en-us/library/windows/desktop/aa374731\(v=vs.85\).aspx#smart_card_functions](http://msdn.microsoft.com/en-us/library/windows/desktop/aa374731(v=vs.85).aspx#smart_card_functions)



2 Command Set

2.1 Command List

| Description | | Command Code | Response Code |
|-------------|-----------------------------|--|---|
| 1 | Give Up Action | 1B 25 20 4D | OK: 1B 00 00 Edc(1B) Fail: 1B 01 00 Edc(1A) |
| 2 | Reset Reader | 1B 25 21 4D | Version String |
| 3 | Get Ack | 1B 25 22 4D | 1B 00 00 Edc(1B) |
| 4 | Get Track123 Data | 1B 25 66 4D | 1B 73 "T2 Data" 41 "T3 Data" 7E "T1 Data" 3F 1C |
| 5 | Check ICC1 Slot | 1B 25 2B 4D | Insert: 1B 00 00 Edc(1B) Noninset: 1B 01 00 Edc(1A) |
| 6 | Select ICC1 | 1B 25 30 4D | |
| 7 | Select SAM1 | 1B 25 32 4D | |
| 8 | Select SAM2 | 1B 25 33 4D | |
| 9 | CPU Card Power On and Reset | 1B 25 36 4D | OK: 1B 00 HLen LLen "ATR" Edc Fail: 1B 01 00 Edc(1A) |
| 10 | CPU Card Power Off | 1B 25 37 4D | OK: 1B 00 00 Edc(1B) Fail: 1B 01 00 Edc(1A) |
| 11 | Read /Write CPU Card | 1B 25 38 4D HLen LLen "C-APDU" Edc | OK: 1B 00 HLen LLen "R-APDU" Edc Fail: 1B 01 00 Edc(1A) |
| 12 | Get CPU Card Status | 1B 25 39 4D "ICC Slot" | OK: 1B 00 "Status" Edc SlotError: 1B 01 00 Edc(1A) |
| 13 | Select Memory Card Type | 1B 25 40 00 00 01 Type Code Edc | OK: 1B 00 00 Edc(1B) Fail: 1B 01 00 Edc(1A) |
| 14 | Memory Card Power On | 1B 25 40 01 | OK: 1B 00 HLen LLen "ATR" Edc Fail: 1B 01 00 Edc(1A) |
| 15 | Memory Card Get Type | 1B 25 40 02 | OK: 1B 00 00 01 Type Code Edc Fail: 1B 01 00 Edc(1A) |
| 16 | Memory Card Read Data | 1B 25 40 03 HLen LLen AdrH AdrL Le Edc | OK: 1B 00 HLen LLen "R-APDU" Edc Fail: 1B 01 00 Edc(1A) |
| 17 | Memory Card Write Data | 1B 25 40 04 HLen LLen AdrH AdrL Ln "C-APDU" Edc | OK: 1B 00 00 Edc(1B) Fail: 1B 01 00 Edc(1A) |
| 18 | Memory Card Power Off | 1B 25 40 05 | OK: 1B 00 00 Edc(1B) |
| 19 | Read Error Counter | 1B 25 40 07 HLen LLen 00 00 01 Edc | OK: 1B 00 00 01 Error Counter Edc Fail: 1B 01 00 Edc(1A) |
| 20 | Verify PSC | 1B 25 40 08 HLen LLen 00 00 Ln "PSC" Edc | OK: 1B 00 00 Edc(1B) Fail: 1B 01 00 Edc(1A) |

| | | | |
|----|--------------------------------------|---|---|
| 21 | Get PSC | 1B 25 40 09 HLen LLen 00 00 Le Edc | OK: 1B 00 HLen LLen "PSC" Edc Fail: 1B 01 00 Edc(1A) |
| 22 | Modify PSC | 1B 25 40 0A HLen LLen 00 00 Ln "PSC" Edc | OK: 1B 00 00 Edc(1B) Fail: 1B 01 00 Edc(1A) |
| 23 | Read Data With Protect Bit | 1B 25 41 00 HLen LLen AdrH AdrL Le Edc | OK: 1B 00 HLen LLen "D0 PB0...Dn PBn" Edc Fail: 1B 01 00 Edc(1A) |
| 24 | Write Data With Protect Bit | 1B 25 41 01 HLen LLen AdrH AdrL Ln D0...Dn Edc | OK: 1B 00 00 Edc(1B) Fail: 1B 01 00 Edc(1A) |
| 25 | Read Protection Data | 1B 25 42 00 | OK: 1B 00 HLen LLen "D0...Dn" Edc Fail: 1B 01 00 Edc(1A) |
| 26 | Write Protection Data | 1B 25 42 01 HLen LLen AdrH AdrL Ln D0...Dn Edc | OK: 1B 00 00 Edc(1B) Fail: 1B 01 00 Edc(1A) |
| 27 | Reset Main Key & Working Key | 1B 25 72 4D | OK: 1B 00 00 Edc(1B) |
| 28 | Update MainKey Use Cleartext | 1B 25 73 4D HLen LLen Msn "Md0...Mdn" Edc | OK: 1B 00 00 Edc (1B) Fail: 1B 01 00 Edc(1A) |
| 29 | Update Working Key Use Cleartext | 1B 25 74 4D HLen LLen Msn Wsn "Md0...Mdn" "Wd0...Wdn" Edc | OK: 1B 00 00 Edc (1B) Fail: 1B 01 00 Edc(1A) |
| 30 | Update Working Key Use Ciphertext | 1B 25 75 4D HLen LLen Msn Wsn "Wd0...Wdn" Edc | OK: 1B 00 00 Edc (1B) Fail: 1B 01 00 Edc(1A) |
| 31 | Select the WorkingKey | 1B 25 76 4D HLen LLen Msn Wsn Edc | OK: 1B 00 00 Edc (1B) Fail: 1B 01 00 Edc(1A) |
| 32 | Picc Config | 1B 25 80 00 00 01 Type Edc | OK: 1B 00 00 Edc (1B) Fail: 1B 01 00 Edc(1A) |
| 33 | Antenna On/Off | 1B 25 80 01 00 01 Status Edc | OK: 1B 00 00 Edc (1B) Fail: 1B 01 00 Edc(1A) |
| 34 | Activate Card | 1B 25 80 02 | OK: 1B 00 HLen LLen "UID" Edc Fail: 1B 01 00 Edc(1A) |
| 35 | Deactivate Card | 1B 25 80 03 | OK: 1B 00 00 Edc (1B) Fail: 1B 01 00 Edc(1A) |
| 36 | Picc Rats | 1B 25 80 04 | OK: 1B 00 HLen LLen "ATS" Edc Fail: 1B 01 00 Edc(1A) |
| 37 | Picc Apdu | 1B 25 80 05 HLen LLen "C-APDU" Edc | OK: 1B 00 HLen LLen "R-APDU" Edc Fail: 1B 01 00 Edc(1A) |
| 38 | Mifare Auth Key | 1B 25 81 00 HLen LLen Mode Sector Key[6] Edc | OK: 1B 00 00 Edc (1B) Fail: 1B 01 00 Edc(1A) |
| 39 | Mifare Read | 1B 25 81 02 HLen LLen Block Edc | OK: 1B 00 HLen LLen "D0...Dn" Edc Fail: 1B 01 00 Edc(1A) |

| | | | |
|----|---------------------------|--|---|
| 40 | Mifare Write | 1B 25 81 03 HLen LLen Block "D0...Dn" Edc | OK: 1B 00 00 Edc (1B) Fail: 1B 01 00 Edc(1A) |
| 41 | Mifare Increment | 1B 25 81 04 HLen LLen Block Value[4] Edc | OK: 1B 00 00 Edc (1B) Fail: 1B 01 00 Edc(1A) |
| 42 | Mifare Decrement | 1B 25 81 05 HLen LLen Block Value[4] Edc | OK: 1B 00 00 Edc (1B) Fail: 1B 01 00 Edc(1A) |
| 43 | Write Series Number | 1B 25 9A 4D HLen LLen "Series Number" Edc | OK: 1B 00 00 Edc (1B) Fail: 1B 01 00 Edc(1A) |
| 44 | Read Series Number | 1B 25 9B 4D | OK: 1B 00 HLen LLen "Series Number" Edc Fail: 1B 01 00 Edc(1A) |
| 45 | Keypad Enable | 1B 25 90 4D | |
| 46 | Keypad Disable | 1B 25 91 4D | |
| 47 | Keypad Enable Encryption | 1B 25 92 4D | |
| 48 | Keypad Disable Encryption | 1B 25 93 4D | |
| | | | |

- * HLen: the high byte of the data length.
- * LLen: the low byte of the data length.
- * Edc: Error Detection Code, checksum with LRC algorithm (xor all bytes)

2.2 Command Explanation

2.2.1 Give Up Action

- **Function:** Request the reader to give up any card operation function.
- **Related Command:** Any card operation function
- **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1000S / SP1100A / SP1100B

Command:

| | |
|-----|-------------|
| HEX | 1B 25 20 4D |
|-----|-------------|

Response:

Correct:

| | |
|-----|--------------|
| HEX | 1B 00 00 Edc |
|-----|--------------|

Error:

| | |
|-----|--------------|
| HEX | 1B 01 00 Edc |
|-----|--------------|

2.2.2 Reset Reader

- **Function:** Request the reader to reset itself.
- **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1000S / SP1100A / SP1100B

Command:

| | |
|-----|-------------|
| HEX | 1B 25 21 4D |
|-----|-------------|

Response:

| | |
|-----|--------------------|
| HEX | [Verson String...] |
|-----|--------------------|

2.2.3 Get ACK

- **Function:** Request the reader response.
- **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1000S / SP1100A / SP1100B

Command:

| | |
|-----|-------------|
| HEX | 1B 25 22 4D |
|-----|-------------|

Response:

| | |
|-----|--------------|
| HEX | 1B 00 00 EDC |
|-----|--------------|

2.2.4 Get Track123 Data

- **Function:** Request the reader to wait for a swipe and LED is turned on until a magnetic card to be swiped. If its reading is successful, it will respond track data; or it will respond "0x7F".
- **Applicability:** S512 / SCR35 / SP1000EP / SP1000S / SP1100B

Command:

| | | | | |
|-----|----|----|----|----|
| HEX | 1B | 25 | 66 | 4D |
|-----|----|----|----|----|

Response:

Correct:

| | | | | | | | | | |
|-----|----|----|---------|----|---------|----|---------|----|----|
| HEX | 1B | 73 | T2 Data | 41 | T3 Data | 7E | T1 Data | 3F | 1C |
|-----|----|----|---------|----|---------|----|---------|----|----|

Error:

| | | | | | | | | | |
|-----|----|----|----|----|----|----|----|----|----|
| HEX | 1B | 73 | 7F | 41 | 7F | 7E | 7F | 3F | 1C |
|-----|----|----|----|----|----|----|----|----|----|

2.2.5 Check ICC1 Slot

- **Function:** Request the reader respond if a card is inserted in IC card socket1.
- **Related Command:** Any IC card operation function
- **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1000S / SP1100A / SP1100B

Command:

| | |
|-----|-------------|
| HEX | 1B 25 2B 4D |
|-----|-------------|

Response:

| State | A card Inserted | No Card Inserted |
|-------|-----------------|------------------|
| HEX | 1B 00 00 Edc | 1B 01 00 Edc |

2.2.6 Select ICC1

- **Function:** Request the reader to operate IC Card1 in the Socket1. Afterwards, all the IC Card operating command is to IC Card1 until a command to select another IC or SAM card.
- **Related Command:** Any IC card operating function
- **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1000S / SP1100A / SP1100B

Command:

| | |
|-----|-------------|
| Hex | 1B 25 30 4D |
|-----|-------------|

Response:

| | |
|-----|--------|
| HEX | (None) |
|-----|--------|

2.2.7 Select SAM1

- **Function:** Request the reader to operate SAM1. Afterwards, all the IC Card operating command is to SAM1 until a command to select another IC or SAM card.
- **Related Command:** Any IC card operating function
- **Applicability:** S512 / Q512 / SCR100 / SP1000EP / SP1000S / SP1100A / SP1100B

Command:

| | |
|-----|-------------|
| HEX | 1B 25 32 4D |
|-----|-------------|

Response:

| | |
|-----|--------|
| HEX | (None) |
|-----|--------|

2.2.8 Select SAM2

- **Function:** Request the reader to operate SAM2. Afterwards, all the IC Card operating command is to SAM2 until a command to select another IC or SAM card.
- **Related Command:** Any IC card operating function
- **Applicability:** S512 / Q512 / SCR100 / SP1000EP

Command:

| | | | | |
|-----|----|----|----|----|
| HEX | 1B | 25 | 33 | 4D |
|-----|----|----|----|----|

Response:

| | |
|-----|--------|
| HEX | (None) |
|-----|--------|

2.2.9 CPU Card Power On And Reset

- **Function:** Request the reader to power on (reset) the CPU card selected. If successful, return the ATR values of this card.
- **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1000S / SP1100A / SP1100B /

Command:

| | | | | |
|-----|----|----|----|----|
| HEX | 1B | 25 | 36 | 4D |
|-----|----|----|----|----|

Response:

Correct:

| | | | | | | |
|-----|----|----|------|------|-----|-----|
| HEX | 1B | 00 | HLen | LLen | ATR | Edc |
|-----|----|----|------|------|-----|-----|

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.10 CPU Card Power Off

- **Function:** Request the reader to power off the CPU card selected.
- **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1000S / SP1100A / SP1100B

Command:

| | | | | |
|-----|----|----|----|----|
| HEX | 1B | 25 | 37 | 4D |
|-----|----|----|----|----|

Response:

Correct:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 00 | 00 | Edc |
|-----|----|----|----|-----|

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.11 Read/Write CPU card (APDU response/command)

➤ **Function:** Request the reader to read/write the CPU card selected and then send back the response from the CPU card (read APDU response/write APDU command).

➤ **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1000S / SP1100A / SP1100B

Command:

| | | | | | | | | |
|-----|----|----|----|----|------|------|--------|-----|
| HEX | 1B | 25 | 38 | 4D | HLen | LLen | C-APDU | Edc |
|-----|----|----|----|----|------|------|--------|-----|

- C-APDU = INS CLS P1 P2 lc D0...Dn le

Response:

Correct:

| | | | | | | |
|-----|----|----|------|------|--------|-----|
| HEX | 1B | 00 | HLen | LLen | R-APDU | Edc |
|-----|----|----|------|------|--------|-----|

- R-APDU = D0...Dn SW1 SW2

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.12 Get CPU Card Status

➤ **Function:** Request the reader respond that the previous state of CPU card.

➤ **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1000S / SP1100A / SP1100B

Command:

| | | | | | |
|-----|----|----|----|----|----------|
| HEX | 1B | 25 | 39 | 4D | ICC Slot |
|-----|----|----|----|----|----------|

- Slot 0x00 is CPU card.
- Slot 0x01 is SAM1.
- Slot 0x02 is SAM2.

Response:

Correct:

| | | | | |
|-----|----|----|--------|-----|
| HEX | 1B | 00 | Status | Edc |
|-----|----|----|--------|-----|

Error: Slot selection error

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

Status:

| Status | Description |
|-----------|------------------------------|
| 0x00,0x01 | Card activated (CPU card) |
| 0x00,0x02 | Card no activated (CPU card) |
| 0x00,0x03 | No supported card (CPU card) |
| 0x00,0x04 | No card Inserted (CPU card) |
| 0x01,0x01 | Card activated (SAM card) |
| 0x01,0x02 | Card no activated (SAM card) |
| 0x01,0x03 | No supported card (SAM card) |

2.2.13 Select Memory Card Type

- **Function:** Request the reader to operate the specified IC Card in the Socket1. Afterwards, all the IC Card operating command is to the specified IC Card until a command to select another type of IC card.
- **Related Command:** Any IC card operating function
- **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1100A / SP1100B

Command:

| | | | |
|-----|-------------------|-----------|-----|
| Hex | 1B 25 40 00 00 01 | Type Code | Edc |
|-----|-------------------|-----------|-----|

Memory Card Type:

| Model | Type Code | Model | Type Code |
|---------|-----------|----------|-----------|
| SLE4442 | 0x02 | AT24C08 | 0x0D |
| SLE4428 | 0x04 | AT24C16 | 0x0E |
| AT24C01 | 0x0A | AT24C32 | 0x13 |
| AT24C02 | 0x0B | AT24C64 | 0x14 |
| AT24C04 | 0x0C | CPU CARD | 0x55 |

Response:

Correct:

| | | |
|-----|----------|-----|
| HEX | 1B 00 00 | Edc |
|-----|----------|-----|

Error: Not Support

| | | |
|-----|----------|-----|
| HEX | 1B 01 00 | Edc |
|-----|----------|-----|

2.2.14 Memory Card Power On

- **Function:** Request the reader to power on (reset) the memory card selected. If successful, return the ATR values of this card.
- **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1100A / SP1100B

Command:

| | |
|-----|-------------|
| HEX | 1B 25 40 01 |
|-----|-------------|

Response:

Correct:

| | | | |
|-----|-----------------|-----|-----|
| HEX | 1B 00 HLen LLen | ATR | Edc |
|-----|-----------------|-----|-----|

- SLE4442/SLE4428 ATR have 4 bytes. The rest memory cards are "1B 00 00 Edc".

Error:

| | | |
|-----|----------|-----|
| HEX | 1B 01 00 | Edc |
|-----|----------|-----|

2.2.15 Memory Card Get Type

- **Function:** Request the reader to respond the memory Card type in the Socket1.
- **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1100A / SP1100B

Command:

| | |
|-----|-------------|
| Hex | 1B 25 40 02 |
|-----|-------------|

Response:

Correct:

| | | | |
|-----|-------------|-----------|-----|
| HEX | 1B 00 00 01 | Type Code | Edc |
|-----|-------------|-----------|-----|

Memory Card Type:

| Model | Type Code | Model | Type Code |
|---------|-----------|----------|-----------|
| SLE4442 | 0x02 | AT24C08 | 0x0D |
| SLE4428 | 0x04 | AT24C16 | 0x0E |
| AT24C01 | 0x0A | AT24C32 | 0x13 |
| AT24C02 | 0x0B | AT24C64 | 0x14 |
| AT24C04 | 0x0C | CPU CARD | 0x55 |

Error: Not Support

| | | |
|-----|----------|-----|
| HEX | 1B 01 00 | Edc |
|-----|----------|-----|

2.2.16 Memory Card Read Data

- **Function:** Request the reader to read the memory card selected and then send back the response from the card (read APDU response).
- **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1100A / SP1100B

Command:

| | | | | | | | |
|-----|-------------|------|------|------|------|----|-----|
| HEX | 1B 25 40 03 | HLen | LLen | AdrH | AdrL | Le | Edc |
|-----|-------------|------|------|------|------|----|-----|

- AdrH is the high byte of the start address of the card.
- AdrL is the low byte of the start address of the card.
- Le is the Read data length.

Response:

Correct:

| | | | | | |
|-----|-------|------|------|--------|-----|
| HEX | 1B 00 | HLen | LLen | R-APDU | Edc |
|-----|-------|------|------|--------|-----|

Error:

| | | |
|-----|----------|-----|
| HEX | 1B 01 00 | Edc |
|-----|----------|-----|

2.2.17 Memory Card Write Data

➤ **Function:** Request the reader to write the memory card selected (write APDU command).

➤ **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1100A / SP1100B

Command:

| | | | | | | | | | | | |
|-----|----|----|----|----|------|------|------|------|----|--------|-----|
| HEX | 1B | 25 | 40 | 04 | HLen | LLen | AdrH | AdrL | Ln | C-APDU | Edc |
|-----|----|----|----|----|------|------|------|------|----|--------|-----|

- AdrH is the high byte of the start address of the card.
- AdrL is the low byte of the start address of the card.
- Ln is the Write data length.

Response:

Correct:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 00 | 00 | Edc |
|-----|----|----|----|-----|

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.18 Memory Card Power Off

➤ **Function:** Request the reader to power off the memory card selected.

➤ **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1100A / SP1100B

Command:

| | | | | |
|-----|----|----|----|----|
| HEX | 1B | 25 | 40 | 05 |
|-----|----|----|----|----|

Response:

Correct:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 00 | 00 | Edc |
|-----|----|----|----|-----|

2.2.19 Memory Card Read Error Counter

➤ **Function:** Request the reader to read the Error Counter of memory card selected. If successful, return the Error Counter of this card. It's for SLE4442 /SLE4428 card only.

➤ **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1100A / SP1100B

Command:

| | | | | | | | | | | |
|-----|----|----|----|----|------|------|----|----|----|-----|
| HEX | 1B | 25 | 40 | 07 | HLen | LLen | 00 | 00 | 01 | Edc |
|-----|----|----|----|----|------|------|----|----|----|-----|

Response:

Correct:

| | | | | | | |
|-----|----|----|----|----|---------------|-----|
| HEX | 1B | 00 | 00 | 01 | Error Counter | Edc |
|-----|----|----|----|----|---------------|-----|

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.20 Memory Card Verify PSC

➤ **Function:** Request the reader to verify PSC of memory card selected. It's for SLE4442 /SLE4428 card only.

➤ **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1100A / SP1100B

Command:

| | | | | | | | | | | | |
|-----|----|----|----|----|------|------|----|----|----|-----|-----|
| HEX | 1B | 25 | 40 | 08 | HLen | LLen | 00 | 00 | Ln | PSC | Edc |
|-----|----|----|----|----|------|------|----|----|----|-----|-----|

- Ln is the PSC length.

Response:

Correct:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 00 | 00 | Edc |
|-----|----|----|----|-----|

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.21 Memory Card Get PSC

➤ **Function:** Request the reader to get PSC of memory card selected. If successful, return the PSC of this card. It's for SLE4442 /SLE4428 card only.

➤ **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1100A / SP1100B

Command:

| | | | | | | | | | | |
|-----|----|----|----|----|------|------|----|----|----|-----|
| HEX | 1B | 25 | 40 | 09 | HLen | LLen | 00 | 00 | Le | Edc |
|-----|----|----|----|----|------|------|----|----|----|-----|

- Le is the PSC length.

Response:

Correct:

| | | | | | | |
|-----|----|----|------|------|-----|-----|
| HEX | 1B | 00 | HLen | LLen | PSC | Edc |
|-----|----|----|------|------|-----|-----|

- There is 3-byte PSC for SLE4442.
- There is 2-byte PSC for SLE4428.

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.22 Memory Card Modify PSC

➤ **Function:** Request the reader to modify PSC of memory card selected. It's for SLE4428 card only.

➤ **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1100A / SP1100B

Command:

| | |
|-----|--|
| HEX | 1B 25 40 0A HLen LLen 00 00 Ln PSC Edc |
|-----|--|

- Ln is the PSC length.

Response:

Correct:

| | |
|-----|--------------|
| HEX | 1B 00 00 Edc |
|-----|--------------|

Error:

| | |
|-----|--------------|
| HEX | 1B 01 00 Edc |
|-----|--------------|

2.2.23 Memory Card Read Data With Protect Bit

➤ **Function:** Request the reader to read data with protect bit of memory card selected. It's for SLE4428 card only.

➤ **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1100A / SP1100B

Command:

| | |
|-----|--|
| HEX | 1B 25 41 00 HLen LLen AdrH AdrL Le Edc |
|-----|--|

- AdrH is the high byte of the start address of the card.
- AdrL is the low byte of the start address of the card.
- Le is the Read data length.

Response:

Correct:

| | |
|-----|-------------------------------------|
| HEX | 1B 00 HLen LLen D0 PB0...Dn PBn Edc |
|-----|-------------------------------------|

- D0 PB0...Dn PBn is the Read Data with Protect bit.

Error:

| | |
|-----|--------------|
| HEX | 1B 01 00 Edc |
|-----|--------------|

2.2.24 Memory Card Write Data With Protect Bit

➤ **Function:** Request the reader to write data with protect bit of memory card selected. It's for SLE4428 card only.

➤ **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1100A / SP1100B

Command:

| | | | | | | | | | | | |
|-----|----|----|----|----|------|------|------|------|----|---------|-----|
| HEX | 1B | 25 | 41 | 01 | HLen | LLen | AdrH | AdrL | Ln | D0...Dn | Edc |
|-----|----|----|----|----|------|------|------|------|----|---------|-----|

- AdrH is the high byte of the start address of the card.
- AdrL is the low byte of the start address of the card.
- Ln is the Write data length.
- D0...Dn is the Write data.

Response:

Correct:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 00 | 00 | Edc |
|-----|----|----|----|-----|

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.25 Memory Card Read Data With Protect Bit

➤ **Function:** Request the reader to read data with protect bit of memory card selected. It's for SLE4442 card only.

➤ **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1100A / SP1100B

Command:

| | | | | |
|-----|----|----|----|----|
| HEX | 1B | 25 | 42 | 00 |
|-----|----|----|----|----|

Response:

Correct:

| | | | | | | |
|-----|----|----|------|------|---------|-----|
| HEX | 1B | 00 | HLen | LLen | D0...Dn | Edc |
|-----|----|----|------|------|---------|-----|

- D0...Dn is the Read Data with Protect bit. Only 4 byte for SLE4442.

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.26 Memory Card Write Data With Protect Bit

➤ **Function:** Request the reader to write data with protect bit of memory card selected. It's for SLE4442 card only.

➤ **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1100A / SP1100B

Command:

| | | | | | | | | | | | |
|-----|----|----|----|----|------|------|------|------|----|---------|-----|
| HEX | 1B | 25 | 42 | 01 | HLen | LLen | AdrH | AdrL | Ln | D0...Dn | Edc |
|-----|----|----|----|----|------|------|------|------|----|---------|-----|

- AdrH is the high byte of the start address of the card.
- AdrL is the low byte of the start address of the card.
(SLE4442 Protection Memory Address: 0~31(decimal))
- Ln is the Write data length.
- D0...Dn is the Write data.

Response:

Correct:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 00 | 00 | Edc |
|-----|----|----|----|-----|

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.30 Update WorkingKey Use Ciphertext

- **Function:** Request the reader to modify a working key in ciphertext format. Decrypt an string S with the selected main key and then save the result as a new working key.
- **Applicability:** SP1000EP / SP1000S / SP1100A / SP1100B

Command:

| | | | | | | | | | | |
|-----|----|----|----|----|------|------|-----|-----|-----------|-----|
| HEX | 1B | 25 | 75 | 4D | HLen | LLen | Msn | Wsn | Wd0...Wdn | Edc |
|-----|----|----|----|----|------|------|-----|-----|-----------|-----|

- Msn is the Main Key Number (0x00~0x1E).
- Wsn is the Working Key Number (0x00~0x02).
- Wd0...Wdn: 16 byte, ASCII code

Response:

Correct:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 00 | 00 | Edc |
|-----|----|----|----|-----|

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

Ex:

Main Key No.: 0x00

Working Key No.: 0x01

Main Key:

0x38 0x38 0x38 0x38 0x38 0x38 0x38 0x38 0x38 0x38 0x38 0x38 0x38 0x38 0x38 0x38

An string:

0x3B 0x2C 0x7C 0x7E 0x68 0x29 0xAE 0xDA 0xA8 0x66 0xD0 0xC8 0xEA 0x43 0x06 0xEE

New Working Key is the decryption result of the above string decrypted by 3DES with main key:

0x31 0x32 0x33 0x34 0x35 0x36 0x37 0x38 0x31 0x32 0x33 0x34 0x35 0x36 0x37 0x38

Command(HEX):

| | HLen | LLen | Msn | Wsn | Wd0...Wdn | Edc |
|----------|------|------|-----|-----|----------------------------------|-----|
| 1B25754D | 00 | 12 | 00 | 01 | 3B2C7C7E6829AEDAA866D0C8EA4306EE | A2 |

2.2.31 Select the WorkingKey

➤ **Function:** Request the reader to select a working key N under a main key M. Default settings: Master Key No.0, Session Key No.0.

➤ **Applicability:** SP1000EP / SP1000S / SP1100A / SP1100B

Command:

| | | | | | | | | | |
|-----|----|----|----|----|------|------|-----|-----|-----|
| HEX | 1B | 25 | 76 | 4D | HLen | LLen | Msn | Wsn | Edc |
|-----|----|----|----|----|------|------|-----|-----|-----|

- Msn is the Main Key Number (0x00~0x1E).
- Wsn is the Working Key Number (0x00~0x02).

Response:

Correct:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 00 | 00 | Edc |
|-----|----|----|----|-----|

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.32 RF Card Picc Config

➤ **Function:** Request the reader to set RF card configuration.

➤ **Applicability:** SCR100

Command:

| | | | |
|-----|-------------------|------|-----|
| HEX | 1B 25 80 00 00 01 | Type | Edc |
|-----|-------------------|------|-----|

- Type:
0x41: Type A.
0x42: Type B.

Response:

Correct:

| | | |
|-----|----------|-----|
| HEX | 1B 00 00 | Edc |
|-----|----------|-----|

Error:

| | | |
|-----|----------|-----|
| HEX | 1B 01 00 | Edc |
|-----|----------|-----|

2.2.33 RF Card Antenna on/off

➤ **Function:** Request the reader to turn the RF antenna on/off.

➤ **Applicability:** SCR100

Command:

| | | | |
|-----|-------------------|--------|-----|
| HEX | 1B 25 80 01 00 01 | Status | Edc |
|-----|-------------------|--------|-----|

- Status:
0x00: antenna off.
0x01: antenna on.

Response:

Correct:

| | | |
|-----|----------|-----|
| HEX | 1B 00 00 | Edc |
|-----|----------|-----|

Error:

| | | |
|-----|----------|-----|
| HEX | 1B 01 00 | Edc |
|-----|----------|-----|

2.2.34 RF Card Activate Card

➤ **Function:** Request the reader to active RF card.

➤ **Applicability:** SCR100

Command:

| | |
|-----|-------------|
| HEX | 1B 25 80 02 |
|-----|-------------|

Response:

Correct:

| | | | |
|-----|-----------------|-----|-----|
| HEX | 1B 00 HLen LLen | UID | Edc |
|-----|-----------------|-----|-----|

Error:

| | | |
|-----|----------|-----|
| HEX | 1B 01 00 | Edc |
|-----|----------|-----|

2.2.35 RF Card Deactivate Card

- **Function:** Request the reader to stop RF card operation.
- **Applicability:** SCR100

Command:

| | |
|-----|-------------|
| HEX | 1B 25 80 03 |
|-----|-------------|

Response:

Correct:

| | |
|-----|--------------|
| HEX | 1B 00 00 Edc |
|-----|--------------|

Error:

| | |
|-----|--------------|
| HEX | 1B 01 00 Edc |
|-----|--------------|

2.2.36 RF Card Picc Rats

- **Function:** Request the reader to select RF card activated.
- **Applicability:** SCR100

Command:

| | |
|-----|-------------|
| HEX | 1B 25 80 04 |
|-----|-------------|

Response:

Correct:

| | |
|-----|-------------------------|
| HEX | 1B 00 HLen LLen ATS Edc |
|-----|-------------------------|

Error:

| | |
|-----|--------------|
| HEX | 1B 01 00 Edc |
|-----|--------------|

2.2.37 RF Card Picc Apdu

- **Function:** Request the reader to read/write the RF card activated and then send back the response from the RF card (read APDU response/write APDU command).
- **Applicability:** SCR100

Command:

| | |
|-----|----------------------------------|
| HEX | 1B 25 80 05 HLen LLen C-APDU Edc |
|-----|----------------------------------|

Response:

Correct:

| | |
|-----|----------------------------|
| HEX | 1B 00 HLen LLen R-APDU Edc |
|-----|----------------------------|

Error:

| | |
|-----|--------------|
| HEX | 1B 01 00 Edc |
|-----|--------------|

2.2.38 RF Card Mifare auth

➤ **Function:** Request the reader to specify the memory location of the Mifare card activated and uses the corresponding key for the authentication. After a successful authentication all memory operations are encrypted.

➤ **Applicability:** SCR100

Command:

| | | | | | | | | | | |
|-----|----|----|----|----|------|------|------|--------|---------|-----|
| HEX | 1B | 25 | 81 | 00 | HLen | LLen | Mode | Sector | K0...Kn | Edc |
|-----|----|----|----|----|------|------|------|--------|---------|-----|

- Mode:
 - TypeA: 0x41(for Mifare only)
 - TypeB: 0x42
- Sector is the memory location of the Mifare card.
- K0...Kn: 6 byte(HEX), the corresponding key for the authentication.

Response:

Correct:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 00 | 00 | Edc |
|-----|----|----|----|-----|

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.39 RF Card Mifare read

➤ **Function:** Request the reader to read block of Mifare card activated after a successful authentication.

➤ **Applicability:** SCR100

Command:

| | | | | | | | | |
|-----|----|----|----|----|------|------|-------|-----|
| HEX | 1B | 25 | 81 | 02 | HLen | LLen | Block | Edc |
|-----|----|----|----|----|------|------|-------|-----|

- Block is the memory location of the Mifare card.

Response:

Correct:

| | | | | | | |
|-----|----|----|------|------|---------|-----|
| HEX | 1B | 00 | HLen | LLen | D0...Dn | Edc |
|-----|----|----|------|------|---------|-----|

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.40 RF Card Mifare write

➤ **Function:** Request the reader to write the contents of a block of Mifare card activated after a successful authentication.

➤ **Applicability:** SCR100

Command:

| | | | | | | | | | |
|-----|----|----|----|----|------|------|-------|---------|-----|
| HEX | 1B | 25 | 81 | 03 | HLen | LLen | Block | D0...Dn | Edc |
|-----|----|----|----|----|------|------|-------|---------|-----|

- Block is the memory location of the Mifare card.
- D0...Dn: 16 byte(HEX), the contents of a block of Mifare card.

Response:

Correct:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 00 | 00 | Edc |
|-----|----|----|----|-----|

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.41 RF Card Mifare Increment

➤ **Function:** Request the reader to increment the contents of a block of Mifare card activated after a successful authentication.

➤ **Applicability:** SCR100

Command:

| | | | | | | | | | |
|-----|----|----|----|----|------|------|-------|----------|-----|
| HEX | 1B | 25 | 81 | 04 | HLen | LLen | Block | Value[4] | Edc |
|-----|----|----|----|----|------|------|-------|----------|-----|

- Block is the memory location of the Mifare card.
- Value[4]: 4 byte(HEX), the maximum size of a value is 4 byte including sign bit.

Response:

Correct:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 00 | 00 | Edc |
|-----|----|----|----|-----|

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.42 RF Card Mifare Decrement

➤ **Function:** Request the reader to decrement the contents of a block of Mifare card activated after a successful authentication.

➤ **Applicability:** SCR100

Command:

| | | | | | | | | | |
|-----|----|----|----|----|------|------|-------|----------|-----|
| HEX | 1B | 25 | 81 | 05 | HLen | LLen | Block | Value[4] | Edc |
|-----|----|----|----|----|------|------|-------|----------|-----|

- Block is the memory location of the Mifare card.
- Value[4]: 4 byte(HEX), the maximum size of a value is 4 byte including sign bit.

Response:

Correct:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 00 | 00 | Edc |
|-----|----|----|----|-----|

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.43 Write Series Number

- **Function:** Request the reader to write the unique series number.
- **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1000S / SP1100A / SP1100B

Command:

| | | | | | | | | |
|-----|----|----|----|----|------|------|---------------|-----|
| HEX | 1B | 25 | 9A | 4D | HLen | LLen | Series Number | Edc |
|-----|----|----|----|----|------|------|---------------|-----|

- Series Number: 1~16Byte

Response:

Correct:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 00 | 00 | Edc |
|-----|----|----|----|-----|

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.44 Read Series Number

- **Function:** Request the reader to read the unique series number.
- **Applicability:** S512 / Q512 / SCR35 / SCR100 / SP1000EP / SP1000S / SP1100A / SP1100B

Command:

| | | | | |
|-----|----|----|----|----|
| HEX | 1B | 25 | 9B | 4D |
|-----|----|----|----|----|

Response:

Correct:

| | | | | | | |
|-----|----|----|------|------|---------------|-----|
| HEX | 1B | 00 | HLen | LLen | Series Number | Edc |
|-----|----|----|------|------|---------------|-----|

Error:

| | | | | |
|-----|----|----|----|-----|
| HEX | 1B | 01 | 00 | Edc |
|-----|----|----|----|-----|

2.2.45 Keypad Enable

- **Function:** Request the reader to enable keypad input.
- **Applicability:** SP1000EP / SP1000S / SP1100A / SP1100B

Command:

| | |
|-----|-------------|
| HEX | 1B 25 90 4D |
|-----|-------------|

Response:

| | |
|-----|--------|
| HEX | (None) |
|-----|--------|

2.2.46 Keypad Disable

- **Function:** Request the reader to disable keypad input.
- **Applicability:** SP1000EP / SP1000S / SP1100A / SP1100B

Command:

| | |
|-----|-------------|
| HEX | 1B 25 91 4D |
|-----|-------------|

Response:

| | |
|-----|--------|
| HEX | (None) |
|-----|--------|

2.2.47 Keypad Enable Encryption

- **Function:** Request the reader to enable 3DES algorithm of keypad input.
- **Applicability:** SP1000EP / SP1000S / SP1100A / SP1100B

Command:

| | |
|-----|-------------|
| HEX | 1B 25 92 4D |
|-----|-------------|

Response:

| | |
|-----|--------|
| HEX | (None) |
|-----|--------|

2.2.48 Keypad Disable Encryption

- **Function:** Request the reader to disable 3DES algorithm of keypad input.
- **Applicability:** SP1000EP / SP1000S / SP1100A / SP1100B

Command:

| | |
|-----|-------------|
| HEX | 1B 25 93 4D |
|-----|-------------|

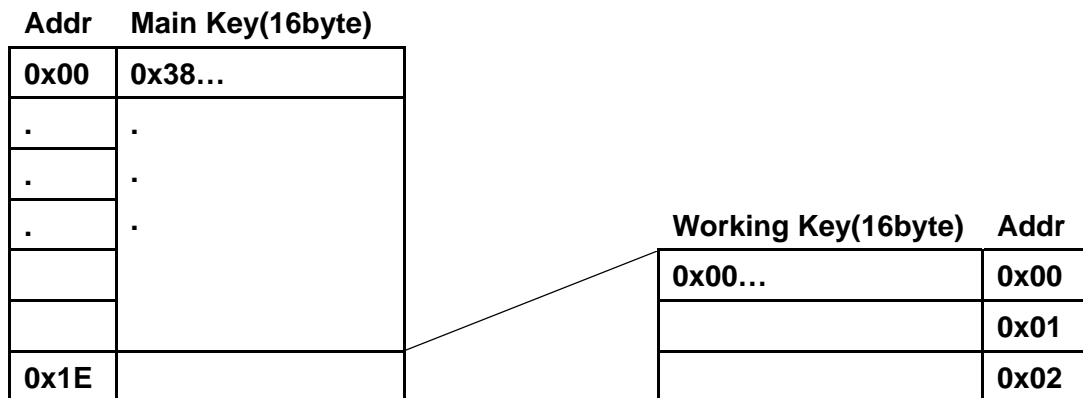
Response:

| | |
|-----|--------|
| HEX | (None) |
|-----|--------|

3 Encryption Key Memory

- **Default Main Key (hex):** 38383838383838383838383838383838(=0x38*16).
- **Default Working Key (hex):** 00000000000000000000000000000000(=0x00*16).
- **Key Map:**

As following, there are 31 sets of Main Key (0x00~0x1E), and each including 3 sets of Working Key(0x00~0x02).



4 Keypad Operation Procedure

4.1 Get Normal Keypad Data

1. Send "Keypad Enable" command (1B 25 90 4D) to reader from host.
2. To start input, press "Password" key on keypad then the reader response "1B 00 00 01 F1 Edc".
3. After each key pressed, the reader will response to the host :

| Key | Response | | | | | |
|-----|----------|------|-----|-----|----|----|
| | HLen | LLen | Ack | Edc | | |
| 0~9 | 1B | 00 | 00 | 01 | F9 | E3 |
| F | 1B | 00 | 00 | 01 | F2 | E8 |

4. To cancel input, press "Cancel" key on keypad then the reader response "1B 00 00 01 F3 Edc".
5. To response the input key, press "Enter" key on keypad.

Ex. If key "1234567890" pressed, the reader will response:

| HLen | LLen | key | Edc |
|------|------|-----|----------------------------------|
| 1B00 | 00 | 0A | 31 32 33 34 35 36 37 38 39 30 10 |

6. Send "Keypad Disable" command (1B 25 91 4D) to reader from host.

4.2 Get Encryption Keypad Data

1. Send "Keypad Enable Encryption" command (1B 25 92 4D) to reader from host.
2. To start input, press "Password" key on keypad then the reader response "1B 00 00 01 F1 Edc".
3. After each key pressed, the reader will response to the host :

| Key | Response | | | | |
|-----|----------|------|-----|-----|-------|
| | HLen | LLen | Ack | Edc | |
| 0~9 | 1B | 00 | 00 | 01 | F9 E3 |
| F | 1B | 00 | 00 | 01 | F2 E8 |

4. To cancel input, press "Cancel" key on keypad then the reader response "1B 00 00 01 F3 Edc".
5. To response the input key with 3DES encryption, press "Enter" key on keypad.

Ex. If key "1234567890" pressed, and working key(HEX) "

0x31,0x32,0x33,0x34,0x35,0x36,0x37,0x38,0x39,0x30,0x31,0x32,0x33,0x34,0x35,0x36", the reader will response:

| HLen | LLen | Encrypted key | | | | Edc |
|------|------|---------------|--|--|--|-----|
| 1B00 | 00 | 20 | BC5708BC02FEBF2F05EF2AE0446F8E90191D0C32D48779FB191D0C32D48779FB | | | 1D |

6. Send "Keypad Disable Encryption" command (1B 25 93 4D) to reader from host.

Note:

1. When keypad enable encryption, nomatter how many keys pressed, the reader will always response 32-byte encrypted data to host because of 3DES algorithm.

2. 3Des reference data:

| | | |
|------------------|---------|---------------|
| Working key | 16 Byte | Wd0...Wd15 |
| Unencrypted Data | 8 Byte | D0...D7 |
| Cache Data | 8 Byte | B0...B7 |
| Encrypted Data | 8 Byte | 3Des0...3Des7 |

- if unencrypted data is less than 8 byte, add 0x00 to 8 byte.

3. 3DES algorithm

Step1. Encrypt D0...D7 by Wd0...Wd7, result: B0...B7

Step2. Decrypt B0...B7 by Wd8...Wd15, result: B0...B7

Step3. Encrypt B0...B7 by Wd0...Wd7, result: 3Des0...3Des7

Revision History:

| Revision | Date | Description | By |
|----------|------------|---|----------|
| V1.0 | 2011/11/04 | Created | Alan |
| V1.1 | 2012/03/05 | Add Keypad command | Alan |
| V1.2 | 2012/07/23 | Add RF card command | Alan |
| V1.3 | 2012/08/22 | Modify Memory card command | Alan |
| V1.4 | 2012/11/27 | 1. Add 3DES encryption of Keypad 2. Modify Memory card command | Yurry |
| V1.5 | 2013/05/13 | 1. Modify Select SAM2 command 2. Modify Memory Card command 3. Add protocol instruction | Alan |
| V1.6 | 2013/05/14 | Modify RF card command | Stephany |
| V1.7 | 2013/6/7 | Add Get CPU Card Status command | Edison |
| V1.8 | 2013/7/11 | Add more explanation of Mifare card command | Edison |
| V1.9 | 2014/1/3 | 1. Modify RF card command 2. Modify "Get Ack" response | Edison |
| V1.10 | 2014/3/6 | Add 1.3 USB CCID | Pauline |