CONTENT

1. Communication Data Format

Baud Rate(BPS): 9600/19200/38400/57600(Auto Detection and Self-Adaptive)

Communication Type: Asynchronous Communication
Communication Mode: Half-Duplex, Daisy Chain Supported for multiple Connection of up to 16 machines.
Data Frame Structure:

Start bit	D0	D1	D2	D3	D4	D5	D6	D7	Stop sbit

Start Bit:1 bit
Data Bit: 8 bits
Parity Bit: None;
Stop Bit: 1 Bit
Encode Mode: 8-bit ASCII

2. Communication Method and Control Bytes

Dispenser Machine is the slave part and can be operated only by receiving effective commands from host machines.

Related Control Bytes:

ACK (06H)	Acknowledgement
NAK (15H)	No Acknowledgement
EOT (04H)	End of Text

3. Communication Packet Format and Related bytes

Command Format (From Host)

STX (0xF2)	**ADDR** 1byte	**LENH** 1byte	**LENL** 1 byte	**CMT** 1 byte	**CM** 1byte	**PM** 1byte	**DATA** N bytes	**ETX** 1 byte	**BCC** 1 byte

(Text Package)

(Range of BCC Calculation)

(Maximum Package Length: 1024 Bytes)

STX(F2H)	Start Byte
ADDR	Machine Address
LENH(1 byte)	High Byte for Length of Text Packet
LENL(1 byte)	Low Byte for Length of Text Packet
CMT	Command Header (‘C’,0x43H)
CM	Command Byte
PM	Command Parameters
DATA	Command Data (N byte,N=0~512)
ETX (03H)	End Byte
BCC(1 bytes)	XOR Parity Check Byte

Normal Response Format (From Dispenser)

STX	ADDR	LENH	LENL	PMT	CM	PM	st0	st1	st2	DATA	ETX	BCC
(0xF2)	1byte	1byte	1 byte	1 byte	1byte	1byte	1byte	1byte	1byte	N bytes	1 byte	1 byte

(Text Package)

(Range of BCC Calculation)

(Maximum Package Length: 1024 Bytes)

STX (F2H)	Start Byte
ADDR	Machine Address Byte
LENH (1 byte)	High Byte for Length of Text Packet
LENL (1 byte)	Low Byte for Length of Text Packet
PMT	Header Byte of Response Data (‘P’,0x50H)
CM	Returned Command Byte
PM	Returned Command Parameter
st1, st0, st2	Returned Machine Status Code
DATA	Returned Data (N bytes, N=0~512)
ETX (03H)	Stop Byte
BCC (1 byte)	XOR Parity Check Byte

Error Response Format (From Dispenser)

STX	ADDR	LENH	LENL	PMT	CM	PM	e1	e0	DATA	ETX	BCC
(0xF2)	1byte	1byte	1 byte	1 byte	1byte	1byte	1byte	1byte	N bytes	1 byte	1 byte

(Text Package)

(Range of BCC Calculation)

(Maximum Package Length: 1024 Bytes)

STX (F2H)	Start Byte
ADDR	Machine Address
LENH (1 byte)	High Byte for Length of Text Packet
LENL (1 byte)	Low Byte for Length of Text Packet
EMT	Returned Header for Error Data (‘N’,0x4EH)
CM	Returned Command Byte
PM	Returned Command Parameter
e1, e0	Returned Error Codes
DATA	Returned Data (N bytes, N=0~512)
ETX (03H)	Stop Byte
BCC (1 byte)	XOR Parity Check Byte

4. Machine Address Setting

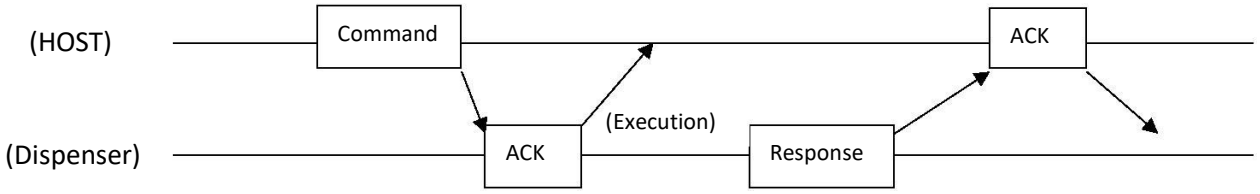
Multiple Machines can be controlled via one COM port by Daisy Chain connection of multiple machines with different addresses. Address Definition is as following:

Machine Address	ADDR
#0	00H
#1	01H
#2	02H
#3	03H
#4	04H
#5	05H
#6	06H
#7	07H
#8	08H
#9	09H
#10	0AH
#11	0BH
#12	0CH
#13	0DH
#14	0EH
#15	0FH

Notes: Ex-work machine has default address of #0(0FH). If control of multiple machines is needed, a unique address should be set for each machine.

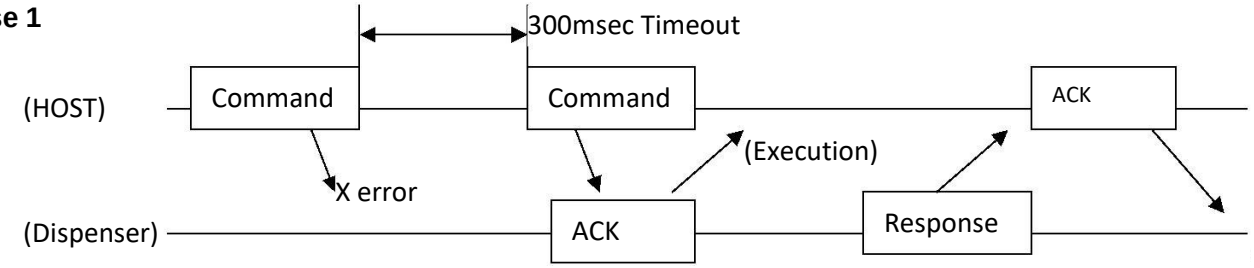
5. Communication Procedures/Steps

5.1 Normal Communication (Command and Response)

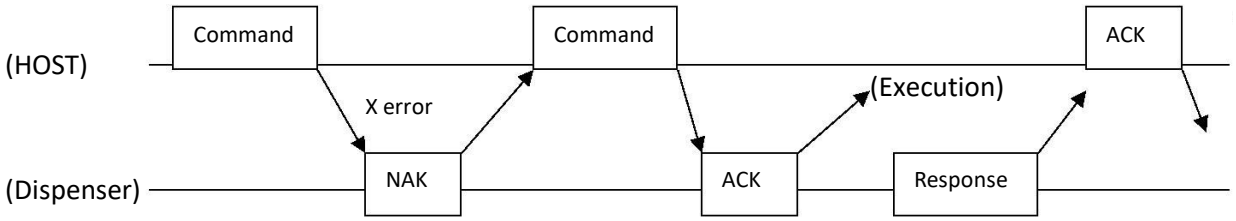


5.2 Abnormal Communication (Command and Response)

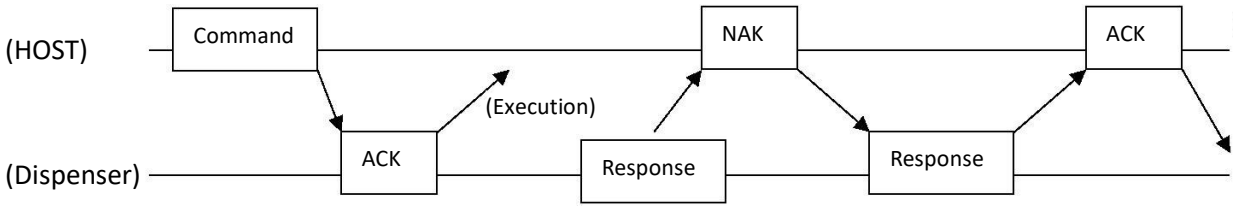
Case 1



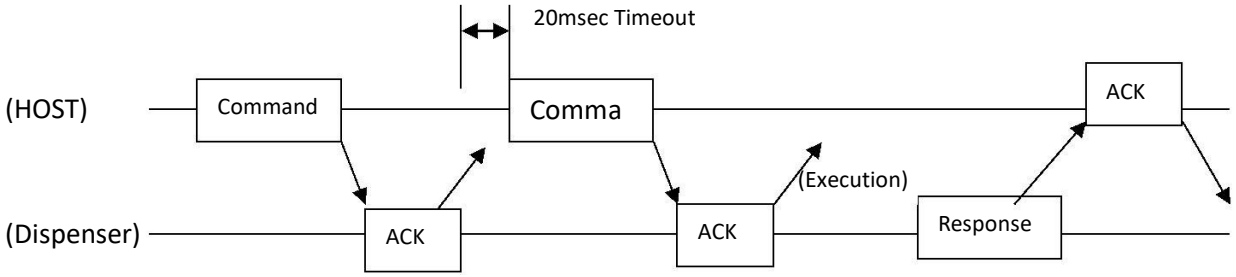
Case 2



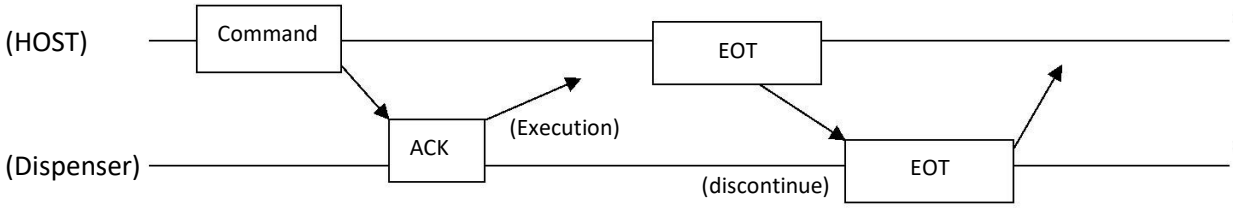
Case 3



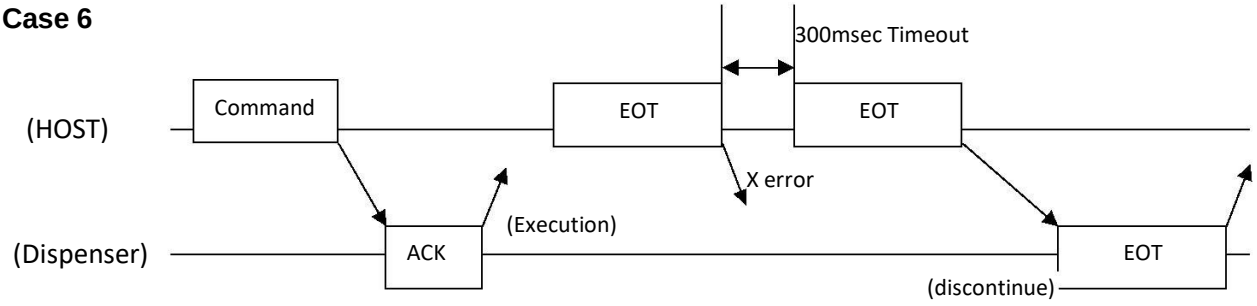
Case 4



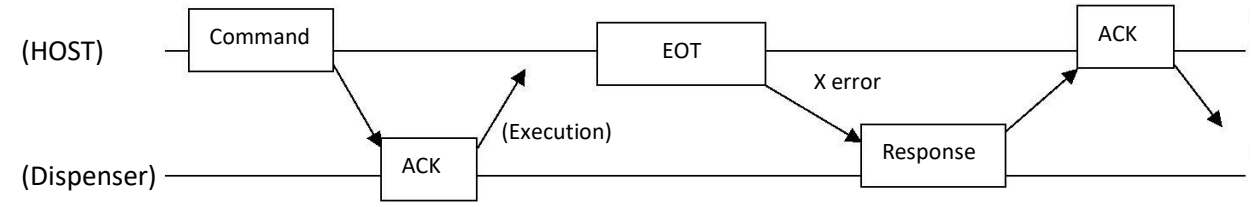
Case 5



Case 6


300msec Timeout
(HOST)
Command
EOT
EOT
X error
(Dispenser)
ACK
(Execution)
EOT
(discontinue)

Case 7


(HOST)
Command
EOT
ACK
X error
(Execution)
(Dispenser)
ACK
Response

6. Card machine operation command list

Chapter	Command	Function Description	Command (CM)	Parameter (PM)	Command Parameter Descritpion
Ch9.1	Reset/Initialization	If Card is inside machine, move to target position. If no card, rotate motor and return firmware version.	30H	30H	Reset &Hold card at bezel
				31H	Reset &Capture card into capture box
				33H	Reset &No Movement
				34H	As 30H &Enable Capture Counter
				35H	As 31H &Enable Capture Counter
				37H	As 33H and Enable Capture Counter
Ch9.2	Inquire Status	Get Machine Status	31H	30H	Inquire current status of machine
				31H	Inquire basic machine status(Se Status)
Ch9.3	Card Movement	Move Card inside machine between different positions	32H	30H	Move &Hold card at bezel
				31H	Move card to Contact IC position
				32H	Move card to RF position
				33H	Capture Card
				39H	Move Card out of Bezel(Eject Card)
Ch9.4	Front Insertion Setting		33H	30H	Allow front card insertion
				31H	Forbid front card Insertion
Ch9.5	IC/RF Card Detection		50H	30H	Auto detect contact IC type
				31H	Auto detect RF card type
Ch9.6	CPU Card Operation		51H	30H	CPU Card Cold Reset
				31H	CPU Card Power Down
				32H	CPU Card Status
				33H	T=0 CPU card APDU Data Transmission
				34H	T=1 CPU card APDU Data Transmission
				38H	CPU Card Warm Reset
				39H	Auto detect T=0/T=1 CPU APDU data Transmission
Ch9.7	SAM Card Operation		52H	30H	SAM Card Cold Reset
				31H	SAM Card Power Down
				32H	SAM Card Status
				33H	T=0 SAM card APDU Data Transmission
				34H	T=1 SAM card APDU Data Transmission
				38H	SAM Card Warm Reset
				39H	Auto detect T=0/T=1 SAM APDU data Transmission
				40H	Select SAM Slot
Ch9.8	SLE4442/4428 memory card Operation		53H	30H	SLE4442/4428 Reset(Activation)
				31H	SLE4442/4428 Power Down(Release)
				32H	Check status of SLE4442/4428 card
				33H	Operate SLE4442 Card
				34H	Operate SLE4428 Card
Ch9.9	I2C Memory Card Operation	24C01—24C256 Card Operations	54H	30H	I2C Reset(Activation)
				31H	I2C Power Down(Release)
				32H	Check status of I2C Card
				33H	Read I2C Card
				34H	Write I2C Card
Ch9.10	RF Card Operation (13.56 MHZ)	Mafare standard card Type A & B T=CL cards operations	60H	30H	RF Card Activation
				31H	RF Card Power Down
				32H	RF Status Inquiry
				33H	Read/Write Mifare standard Card
				34H	Type A T=CL card APDU data transmission
				35H	Type B T=CL card APDU data transmission
				39H	RF Awake/Sleep
Ch9.11	Serial Number	Read Serial Number of machine	A2H	30H	Read Machine Serial NO.
Ch9.12	Machine Configuration	Get Dispenser Configuration	A3H	30H	Read Machine Configuration
Ch9.13	Firmware Version	Get Firmware Version	A4H	30H	Firmware Version
Ch9.14	Capture Counter	Read/Reset Capture Counter	A5H	30H	Read Captue Counter.
				31H	Reset Capture Counter

7. Card Status Code (st0, st1, st2)

st0	Description
“0”	No Card in Card Channel
“1”	Card Held at Gate
“2”	Card on RF/IC Position

st1	Description
“0”	No Card in Hopper
“1”	Not Enough Card in Hopper
“2”	Enough Cards in Hopper

st2	Description
“0”	Error card bin not full
“1”	Error card bin full

The Card Status Code will be returned on running Reset/Initialization (30H) or Status Inquiry (31H) Command

8. e1, e0 Error Code List

e1, e0	Content
“00”	Undefined Command
“01”	Command Parameter Error
“02”	Command Sequence Error
“03”	Unsupported Command
“04”	Command Data Error
“05”	ICC Card Contact Not Released
“06” --”09”	
“10”	Card Jam
“11”	
“12”	Sensor Error
“13”	Too Long Card
“14”	Too Short Card
“15” --”39”	
“40”	Card Removed accidentally when recycling
“41”	Electro-Magnet Error of ICC Module
“42”	
“43”	Unable to Move Card to IC Card Position
“44”	
“45”	Card Moved Manually (to a non-standard position)
“46”	
“47”	
“48”	
“49”	
“50”	Overflow of Error Card Counter
“51”	Motor error
“52” --”59”	
“60”	Short Circuit of IC Card Supply Power
“61”	Fail to Activate IC Card
“62”	Command Not Supported by the IC Card
“63”	
“64”	
“65”	IC Card not activated
“66”	IC Card don’t support command
“67”	IC Card Data transmission Error
“68”	IC Card Data transmission Overtime
“69”	CPU/SAM APDU not complying to EMV
“A0”	No Card Inside hopper
“A1”	Error Card Bin is full
“A2” – “A9”	
“B0”	Fail to Reset/Initialize

9. Command Description

9.1 Reset/Initialization

HOST Command:

"C"	30H	Pm

Positive Return:

"P"	30H	Pm	st0	st1	st2	Firmware Version

Negative Return:

"N"	30H	Pm	e1	e0

This is the first necessary command after powering on and can be executed anytime during operation.

On first run, dispenser will check and adapt to host baud rate.

After this command, error code will be cleared, and machine will be reset to default status (e.g. Insertion Card from front will be disabled).

Pm: Command parameter

If there is no card in card channel, motor rotates slightly for self-test

If there is a card inside channel, the following parameters may be applied:

30H: Move and Hold the card at gate;

31H: Capture Card to Error Card Bin;

33H: No Movement, Retain the Card Inside;

34H: As 30H, and Error Card Counter increment;

35H: As 31H, and Error Card Counter increment;

37H: As 33H, and Error Card Counter increment;

Firmware Version: E.g. "QU-TK-F31-V1.10"

9.2 Inquire Status

HOST Command

“C”	31H	Pm

Positive response

“P”	31H	Pm	st0	st1	st2	Sensor (10 bytes)

Negative response

“N”	31H	Pm	e1	e0

Pm=30H: Report current card status with st0, st1, st2.

Pm=31H: Report Sensor Status with 10 bytes of data. (Usually used for Debugging and Maintenance)

Refer to Sensor Layout Drawing For locations of different sensors. (Sensor location may vary for different QU-TK-F3 machines)

Sensor	Status
S1	30H Not Blocked
	31H Blocked
S2	30H Not Blocked
	31H Blocked
S3	30H Not Blocked
	31H Blocked
S4	30H Not Blocked
	31H Blocked
S5 (reserved)	
S6	30H Not Blocked
	31H Blocked
S7	30H Not Blocked
	31H Blocked
S8	30H Not Blocked
	31H Blocked
S9	30H Not Blocked
	31H Blocked
S10	30H Not Blocked
	31H Blocked
KS1	30H Not Blocked
	31H Blocked
KS2	30H Not Blocked
	31H Blocked

9.3 Card Movement

HOST Command

"C"	32H	Pm

Positive response

"P"	32H	Pm	st0	st1	st2

Negative response

"N"	32H	Pm	e1	e0

Pm=30H Move and hold card at gate position;

Pm=31H Move card to contact IC position;

Pm=32H Move card to RF Antenna Position;

Pm=33H Capture Card to Error Card Bin (Recycle Box)

Pm=39H Eject Card out of Machine

Notes:

1. If card cannot be moved to target position, dispenser will return Card Jam Error;
2. If error card bin is full, error card bin error will be returned when recycling card.

9.4 Front Insertion Setting

HOST Command

"C"	33H	Pm

Positive response

"P"	33H	Pm	st0	st1	st2

Negative response

"N"	33H	Pm	e1	e0

After card insertion allowed, dispenser will withdraw and move card to RF operation position when a card is detected at the gate. Card Insertion operation can be confirmed by "Inquiring Status" Command.

Pm=30H Allow Card Insertion

Pm=31H Forbid Card Insertion

Note: Machine will reset to default forbidden mode after reset/initialization.

9.5 IC/RF Card Detection

9.5.1 Auto-Check IC Card Type:

HOST Command

"C"	50H	30H

Positive response

"P"	50H	30H	st0	st1	st2	**Card Type**

Negative response

"N"	50H	30H	e1	e0

Detect contact IC Card Type. Move to Contact IC Card position and card type information may be one of the following:

Cart Type (2 bytes)		Specification
'0'	'0'	Unknown
'1'	'0'	T=0 CPU Card
	'1'	T=1 CPU Card
'2'	'0'	SLE4442 Card
	'1'	SLE4428 Card
'3'	'0'	AT24C01 Card
	'1'	AT24C02 Card
	'2'	AT24C04 Card
	'3'	AT24C08 Card
	'4'	AT24C16 Card
	'5'	AT24C32 Card
	'6'	AT24C64 Card
	'7'	AT24C128 Card
	'8'	AT24C256 Card

9.5.2 Auto-Check RF Card Type:

HOST Command

"C"	50H	31H

Positive response

"P"	50H	31H	st0	st1	st2	**Card Type**

Negative response

"N"	50H	31H	e1	e0

Detect RF Card Type. Move to RF Card position and card type information may be one of the following

Card Type (2 bytes)		Specification
'0'	'0'	Unknow RF Type
'1'	'0'	Mifare one S50 Card
	'1'	Mifare one S70 Card
	'2'	Mifare one UL Card
'2'	'0'	Type A CPU Card
'3'	'0'	Type B CPU Card
'5'	'0'	ISO15693 Card

9.6 CPU Card Operation

9.6.1 CPU Card Reset

HOST Command

"C"	51H	30H	Vcc

Positive response

"P"	51H	30H	st0	st1	st2	Type	ATR

Negative response

"N"	51H	30H	e1	e0	ATR

Cold Reset: machine provides power (Vcc), clock (CLK), and reset (RST) signals to card and card responds with ATR. Vcc options:

30H: Vcc=+5V and mode EMV2000 ver4.0.

33H: Vcc=+5V and mode ISO/IEC7816-3.

35H: Vcc=+3.3V and mode EMV2000 ver4.0 ISO/IEC7816-3.

If Vcc value is not provided, Vcc=30H will be used by default.

Notes:

1. If ATR can't comply with EMV, error code return: e1,e0="69"
2. On IC Power Error during reset, error code return: e1, e0="60"

CPU Card Protocols:

30H T=0 protocol CPU Card

31H T=1 protocol CPU Card

ATR format:

TS	TO	TA1	TB1	…	TCK

9.6.2 CPU Card Power Down

HOST Command

"C"	51H	31H

Positive response

"P"	51H	31H	st0	st1	st2

Negative response

"N"	51H	31H	e1	e0

This commands powers down the activated CPU card.

9.6.3 CPU Card Status

HOST Command

"C"	51H	32H

Positive response

"P"	51H	32H	st0	st1	st2	Sti

Negative response

"N"	51H	32H	e1	e0

Machine tells the status of IC card with sti status:

sti =**30H** Card is not activated

=**31H** Card is activated, current CPU Card working frequency is 3.57 MHZ

=**32H** Card is activated, current CPU Card working frequency is 7.16 MHZ

If IC Card power error, Error Code: **e1, e0= "60"**

9.6.4 T=0 CPU Card APDU Transmission

HOST Command

"C"	51H	33H	C-APDU

Positive response

"P"	51H	33H	st0	st1	st2	R-APDU

Negative response

"N"	51H	33H	e1	e0

This exchanges data between T=0 card and machine

C-APDU from HOST ranges from 4 bytes to 261 bytes

CLA	INS	P1	P2	LC	Data1	……	Le

R-APDU to HOST ranges from 2 bytes to 258 bytes

Data1	…..	Data(n)	Sw1	Sw0

Error code "60" is returned on power failure.

If protocol type of IC card is not T=0, error code "62" returns.

If ICC won't respond within valid Wait Time, machine deactivates the card and returns error code "63".

If protocol error occurs, machine deactivate IC card firstly and returns error code "64".

If HOST communicates before IC card activation, error code "65" returns.

Note: Refer to ISO/IEC7816-3 for more details of T=0 APDU and get C-APDU information from the Card COS manual.

9.6.5 T=0 CPU Card APDU Transmission

HOST Command

"C"	51H	34H	C-APDU

Positive response

"P"	51H	34H	st0	st1	st2	R-APDU

Negative response

"N"	51H	34H	e1	e0

This exchanges data between CPU card by protocol T=1

Dispenser should follow T=1 protocol to combine C-APDU as I-block and send to CPU card. CPU card should return R-APDU to HOST

C-APDU

CLA	INS	P1	P2	Lc	Data1	···	Data (Lc)	Le

I-block

NAD	PCB	LEN	CLA	INS	P1	P2	Lc	Data1	…	Data (Lc)	Le	EDC
Head block			Information block									End block

QU-TK-F31 returns "R-APDU" data to HOST

I-block

Head block			Information block									End block
NAD	PCB	LEN	CLA	INS	P1	P2	Lc	Data1	…	Data (Lc)	Le	EDC

R-APDU

CLA	INS	P1	P2	Lc	Data1	…	Data (Lc)	Le

Error code "60" is returned on power failure.

If protocol type of IC card is not T=0, error code "62" returns.

If ICC won't respond within valid Wait Time, machine deactivates card and returns error code "63".

If protocol error occurs, machine deactivate IC card and returns error code "64".

If HOST communicates before IC card activation, error code "65" returns.

Note: Refer to ISO/IEC7816-3 for more details of T=1 APDU and get C-APDU information from the Card COS manual.

9.6.6 CPU Card Warm Reset

HOST Command

"C"	51H	38H

Positive response

"P"	51H	38H	st0	st1	st2	Type	ATR

Negative response

"N"	51H	38H	e1	e0

Warm Reset keeps the card activated and get the ATR again.

Type: CPU Card communication protocol

=**30H** T=0 Protocol

=**31H** T=1 Protocol

9.6.7 Automatic APDU Transmission for either T=0 or 1

HOST Command

"C"	51H	39H	C-APDU

Positive response

"P"	51H	39H	st0	st1	st2	R-APDU

Negative response

"N"	51H	39H	e1	e0

Card Protocol is detected automatically (T=0 or 1) and target C-APDU is sendt Set data to "C-APDU". QU-TK-F31 returns "R-APDU" data to HOST.

An error "60" is returned when a power failure is detected.

If protocol type of IC card is not T=0, error code "62"is sent.

If IC Card does not respond within Working Wait Time, QU-TK-F31 deactivates an IC card and error code "63" is sent.

If any other protocol error occurs, machine deactivates an IC card and error code "64" is sent.

If HOST tries to communicate before IC card activation, error code "65" is sent.

9.7 SAM Card Operation

9.7.1 Active SAM Command

HOST Command

"C"	52H	30H	Vcc

Positive response

"P"	52H	30H	st0	st1	st2	Type	ATR

Negative response

"N"	52H	30H	e1	e0	ATR

The QU-TK-F31 supplies power (VCC) and clock (CLK), then reset (RST) release.

Type: SAM protocol type

=30H T=0 protocol

=31H T=1 protocol

ATR (Answer to Reset) format:

TS	TO	TA1	TB1	…	TCK

See details from ISO7816 standard

Vcc=30H: ICRW supplies with +5V to VCC and activates in line with the EMV2000 ver4.0.

Vcc=33H: ICRW supplies with +5V to VCC and activates in line with the ISO/IEC7816-3.

Vcc=35H: ICRW supplies with +3V to VCC and activates in line with the ISO/IEC7816-3.

In case there is no Vcc provided, it will have 30H as default value

If ATR is not compliance to EMV, return e1,e0="69"

Notes: There will be error and return ATR & Type when reset in line with EMV return

When a power failure is recognized while a power supply is supplied to the card, error code "60" is returned.

9.7.2 Deactivate SAM Command

HOST Command

"C"	52H	31H

Positive response

"P"	52H	31H	st0	st1	st2

Negative response

"N"	52H	31H	e1	e0

This deactivates SAM

9.7.3 Inquire SAM Status Command

HOST Command

"C"	52H	32H

Positive response

"P"	52H	32H	st0	st1	st2	Sti	Stj

Negative response

"N"	52H	32H	e1	e0

QU-TK-F31 returns the status of SAM with sti. stj

Sti =30H SAM is deactivated

Sti =31H SAM is activated, working frequency is 3.57 MHZ

Sti =32H SAM is activated, working frequency is 7.16 MHZ

Stj =30H First SAM card connector

Stj =31H Second SAM card connector (Optional)

Stj =32H Third SAM card connector (Optional)

Stj =33H Fourth SAM card connector (Optional)

Stj =34H Fifth SAM card connector (Optional)

An error e1,e0="60" is returned when a power failure is detected.

9.7.4 T=0 SAM Card APDU Communication

HOST Command

"C"	52H	33H	C-APDU

Positive response

"P"	52H	33H	st0	st1	st2	R-APDU

Negative response

"N"	52H	33H	e1	e0

This exchanges data between SAM by protocol T=0

If IC Card power error, return e1, e0= "60"

If protocol type of IC card is not T=0, error code "62"is sent.

If ICC does not respond within Working Wait Time, QU-TK-F31 deactivates an IC card and error code "63" is sent.

If any other protocol error occurs, QU-TK-F31 deactivates an IC card and error code "64" is sent.

If HOST tries to communicate before IC card activation, error code "65" is sent.

Note: If you want to more about T=0 APDU format. Please refer to ISO/IEC7816-3 and COS command

9.7.5 T=1 SAM Card APDU Communication

HOST Command

"C"	52H	34H	C-APDU

Positive response

"P"	52H	34H	st0	st1	st2	R-APDU

Negative response

"N"	52H	44H	e1	e0

This exchange data between SAM by protocol T=1

If IC Card power error, return e1, e0 = "60"

If protocol type of IC card is not T=0, error code "62"is sent.

If ICC does not respond within Working Wait Time, QU-TK-F31 deactivates an IC card and error code

“63” is sent.

If any other protocol error occurs, QU-TK-F31 deactivates an IC card and error code “64” is sent.

If HOST tries to communicate before IC card activation, error code “65” is sent.

Note: Refer to ISO/IEC7816-3 and COS command for more about T=1 APDU

9.7.6 SAM Warm Reset

HOST Command

“C”	52H	38H

Positive response

“P”	52H	38H	st0	st1	st2	Type	ATR

Negative response

“N”	52H	38H	e1	e0

Keeping the status of the SAM activated, then returns response upon receiving.

Type: SAM protocol type

=30H T=0 Protocol

=31H T=1 Protocol

9.7.7Auto-Check SAM Card T=0/T=1 Protocol

HOST Command

“C”	52H	39H	C-APDU

Positive response

“P”	52H	39H	st0	st1	st2	R-APDU

Negative response

“N”	52H	39H	e1	e0

If IC Card power error, return e1,e0=“60”

If protocol type of IC card is not T=0, error code e1,e0= “62”is sent.

If ICC does not respond within Working Wait Time, QU-TK-F31 deactivates an IC card and returns error code e1,e0=“63”.

If any other protocol error occurs, QU-TK-F31 deactivates the IC card and returns error code e1,e0=“64”.

If HOST tries to communicate before IC card activation, error code e1,e0=“65” is sent.

9.7.8 Select SAM

HOST Command

"C"	52H	40H	SAMn

Positive response

"P"	52H	40H	st0	st1	st2

Negative response

"N"	52H	40H	e1	e0

HOST can select SAM 1,2,3,4 or 5.

Sel = 30H: SAM 1.

Sel = 31H: SAM 2. (option)

Sel = 32H: SAM 3. (option)

Sel = 33H: SAM 4. (option)

Sel = 34H: SAM 5. (option)

SAM command is effective only in the module selection.

When Initialize command is executed, SAM 1 will be selected.

9.8 SLE4442/4428 Control

9.8.1 SLE4442/4428 Reset

HOST Command

"C"	53H	30H

Positive response

"P"	53H	30H	st0	st1	st2	ATR(4 byte)

Negative response

"N"	54H	30H	e1	e0

The QU-TK-F31 supplies power (VCC) and clock (CLK), then reset (RST) release. After reset, return ATR.

ATR: SLE4442 Card ATR="A2H, 13H, 10H, 91H"

SLE4442 Card ATR="92H, 23H, 10H, 91H"

9.8.2 Deactivate SLE4442/4428

Command

"C"	53H	31H

Positive response

"P"	53H	31H	st0	st1	st2

Negative response

"N"	53H	31H	e1	e0

9.8 SLE4442/4428 Control

9.8.1 SLE4442/4428 Reset

HOST Command

"C"	53H	30H

Positive response

"P"	53H	30H	st0	st1	st2	ATR(4 byte)

Negative response

"N"	54H	30H	e1	e0

The QU-TK-F31 supplies power (VCC) and clock (CLK), then reset (RST) release. After reset, return ATR.

ATR: SLE4442 Card ATR="A2H, 13H, 10H, 91H"

SLE4442 Card ATR="92H, 23H, 10H, 91H"

9.8.2 Deactivate SLE4442/4428

Command

"C"	53H	31H

Positive response

"P"	53H	31H	st0	st1	st2

Negative response

"N"	53H	31H	e1	e0

The QU-TK-F31 stop supplying power (VCC) and clock (CLK), then reset (RST) release.

9.8.3 Inquire status of SLE4442/4428:

HOST Command

"C"	53H	32H

Positive response

"P"	53H	32H	st0	st1	st2	Sti

Negative response

"N"	54H	32H	e1	e0

QU-TK-F31 tells the status of SLE4442/4428 with Sti after the command successfully execute.

Sti= 30H SLE4442/4428 Deactivated

Sti= 31H SLE4442 Activated

Sti= 32H SLE4428 Activated

9.8.4 SLE4442 Control

These functions are specified by a command data form like C-APDU which format is based on T=0 standard.

In this case, QU-TK-F31 recognizes the meaning of the command data, and executes the treatment related to the card by controlling hardware.

After the command was executed properly, QU-TK-F31 returns a positive response with response data 9000H like from the IC card. When an error occurs during the communication with SLE4442, QU-TK-F31 returns a positive response with status information in response data "sw1+sw2" which is based on ISO/IEC 7816-3

Sw1	Sw2	Specification
90H	00H	Success
6FH	00H	Fail
6FH	01H	Key Validation error
6FH	02H	Key Validation error and Lock
67H	00H	Address overflow
6BH	00H	Operation length overflow

9.8.4.1. Data read from main memory on SLE4442

HOST Command

"C"	53H	33H	00H	B0H	00H	abH	cdH

Positive response

"P"	53H	33H	st0	st1	st2	data

Negative response

"N"	53H	33H	e1	e0

Notes: ab H: the start address to read data in the main memory

cd H: the length of bytes of data to read

QU-TK-F31 reads data from the main memory of SLE4442, and transmits data on cdH bytes from the address abH.

The capacity of the main memory is 256 bytes.

All the contents of the main memory can be read with the following command.

ex). "CR3"+00B0000000

9.8.4.2. Data read from protection memory on SLE4442

HOST Command

"C"	53H	33H	00H	B0H	01H	abH	cdH

Positive response

"P"	53H	33H	st0	st1	st2	data

Negative response

"N"	53H	33H	e1	e0

Notes: ab H: the start address to read data in the main memory

cd H: the length of bytes of data to read

QU-TK-F31 handles the data of all 32bits in the protection memory as the data on 4bytes.

The contents (32bit) of the protection memory can be read with the following command.

Ex) "CR3"+00B0010004

9.8.4.3 Data read from security memory on SLE4442

HOST Command

"C"	53H	33H	00H	B0H	02H	abH	cdH	efH…

Positive response

"P"	53H	33H	st0	st1	st2	data

Negative response

"N"	53H	33H	e1	e0

Notes: ab H: the start address to read data in the main memory

cd H: the length of bytes of data to read

QU-TK-F31 handles the data of all 32bits in the security memory as the data on 4bytes.

The contents (32bit) of the security memory can be read with the following command.

Ex) "CR3"+00B002000

9.8.4.4 Data write to main memory on SLE4442

HOST Command

"C"	53H	33H	00H	D0H	00H	abH	cdH	efH…

Positive response

“P”	53H	33H	st0	st1	st2	data

Negative response

“N”	53H	33H	e1	e0

Notes: ab H: the start address to write data in the main memory

cd H: the length of bytes of data to write

ef H: the data to write first (cd H bytes)

Before write to main memory, the validation of key is must.

The capacity of the main memory is 256 bytes. The byte number "00" of data to write means 256bytes.

The example that data are written in the whole area of the main memory is shown in the following.

ex). "CR3"+ 00D0000000 + Write Data (256byte)

After command execution, QU-TK-F31 returns response with 9000H or sw1+sw2 as the result.

If the addressed data on main memory is protected by the protect status, Data is not allowed.

9.8.4.5 Data write to protection memory on SLE4442

HOST Command

“C”	53H	33H	00H	D0H	01H	abH	cdH	efH…

Positive response

“P”	53H	33H	st0	st1	st2	data

Negative response

“N”	53H	33H	e1	e0

Notes: ab H: the start address to write data in the main memory

cd H: the length of bytes of data to write

ef H: the data to write first (cd H bytes)

Before write to the memory, the validation of key is must.

The address of the main memory that the protection is possible is 1Fh from 00h. Each protection condition of the protectable main memory can be controlled with 4byte (32bits) in the protection memory. For example, if bit0 of the protection memory byte0 is '1', data on the address 00H of the main memory are protected.

The content of protect status cannot be change once setting protection.

For example: write 20H data to 10H address and set up protection

Ex) “CR3” +00D001100120

After command execution, QU-TK-F31 returns with 9000H or sw1+sw2 as the result.

ICRW reads data first from the main memory, and it is compared with the value that it was received.

When this is wrong, writing isn't begun.

Protection condition can be set up at one time in the data which continued in the main memory.

9.8.4.6 Data write to security memory on SLE4442

HOST Command

"C"	53H	33H	00H	D0H	02H	abH	cdH	efH…

Positive response

"P"	53H	33H	st0	st1	st2	data

Negative response

"N"	53H	33H	e1	e0

Notes: ab H: the start address to write data in the main memory

cd H: the length of bytes of data to write

ef H: the data to write first (cd H bytes)

After a password check is finished normally, the Reference-Data area of 3byte can be changed.

All 32bits are handled as 4bytes. How to change the Reference-Data is as the following.

ex). "CR3"+ 00D0020103123456

After command execution, ICRW returns response with 9000H or sw1+sw2 as the result.

Notes: Better not ot writ, because the Error-counter is always allowed to write and easily make a failure. Error-Counter is controlled when password is checked.

9.8.4.7 Verification data present to SLE4428

HOST Command

"C"	53H	33H	00H	20H	03H	01H	03H	efH…

Positive response

"P"	53H	33H	st0	st1	st2	data

Negative response

"N"	53H	33H	e1	e0

Notes: ef H: the data to compare (3bytes)

Before changing data, password must be check

Because this function should be made effective, the issue of the next command is necessary.

Ex) "CR3" +0020030103xxxxxx (xxxxxx: security code 3bytes)

Card will verify password between card and command.

A user must know password at least when a user wants to rewrite the data on SLE4442 card.

Error-Counter can be reset in the zero if password is given to SLE4442 card properly if the value of Error-Counter is 2 or less.

9.8.5 SLE4428 Control

These functions are specified by a command data form like C-APDU which format is based on T=0 standard.

In this case, QU-TK-F31 recognizes the meaning of the command data, and executes the treatment related to the card by controlling hardware.

After the command was executed properly, QU-TK-F31 returns a positive response with response data 9000H like from the IC card. When an error occurs during the communication with SLE4442, QU-TK-F31 returns a positive response with status information in response data "sw1+sw2" which is base on ISO/IEC 7816-3

Sw1	Sw2	Specification
90H	00H	Success
6FH	00H	Fail
6FH	01H	Key Validation error
6FH	02H	Key Validation error and Lock
6BH	00H	Address overflow
67H	00H	Operation length overflow

9.8.5.1 Data Reading of main-memory of SLE4428

HOST Command

“C”	53H	34H	00H	B0H	0aH	bcH	deH

Positive response

“P”	53H	34H	st0	st1	st2	data

Negative response

“N”	53H	34H	e1	e0

Notes: abc H: the start address to read data in the main memory

de H: the number of bytes of data to read

QU-TK-F31 read data from main memory of SLE4428 through abcH and deH

The capacity of the main memory is 1024bytes.

De="00"

Data to read means 256bytes.

The head part of the main memory can be read with the following command.

Ex) "CR4"+00B0000000

9.8.5.2. Reading of protection-bit of SLE4428

HOST Command

“C”	53H	34H	00H	B0H	10H	abH	cdH

Positive response

“P”	53H	34H	st0	st1	st2	data

Negative response

“N”	53H	34H	e1	e0

Notes: ab H: the start address to read the image of protection data of the main memory

cd H: the number of bytes of data to read

The protection conditions of 1024bytes of main-memory are changed into the data on 1024bits, and it is read.

1024bits is equivalent to 128bytes. (1024 = 128 x 8)

Data to read first become protection information to address (000H-007H) of main-memory in the case of abH=00H.

The contents of the whole protection image can be read with the following command.

ex). "CR4"+00B0100080

QU-TK-F31 read protection-bit of SLE4428 according to abH

9.8.5.3 Data writing to main-memory of SLE4428

HOST Command

“C”	53H	34H	00H	D0H	0aH	bcH	deH	fgH…

Positive response

“P”	53H	34H	st0	st1	st2	data

Negative response

“N”	53H	34H	e1	e0

Notes: abcH: the start address to write data in the main memory

deH: the number of bytes of data to write

fgH: the data to write first (de H bytes)

QU-TK-F31 writes data in the main memory. QU-TK-F31 returns a result after written data are checked.

Before doing this operation, password check must be done
The capacity of the main memory is 1024 bytes.

The example that data are written in from the address 100H is shown in the following.

ex). "CR4"+ 00D0010000 + Write Data (256byte)

After command execution, ICRW returns response with 9000H or sw1+sw2 as the result.

If the addressed data on main memory is protected, the write operation is not available.

9.8.5.4 Data writing to main-memory of SLE4428 with protecting

HOST Command

“C”	53H	34H	00H	D0H	1aH	bcH	deH	fgH…

Positive response

“P”	53H	34H	st0	st1	st2	data

Negative response

"N"	53H	34H	e1	e0

Notes: abcH: the start address to write data in the main memory

de H: the number of bytes of data to write

fg H: the data to write first (de H bytes)

QU-TK-F31 writes data in the main memory. QU-TK-F31 returns a result after written data are checked.

Before doing this operation, password check must be done.

9.8.5.5 Written with protection-bit

HOST Command

"C"	53H	34H	00H	D0H	2aH	bcH	deH	fgH…

Positive response

"P"	53H	34H	st0	st1	st2	data

Negative response

"N"	53H	34H	e1	e0

Notes: abcH: the start address to write data in the main memory

de H: the number of bytes of data to write

fgH: the data to write first (de H bytes)

Before doing this operation that writing data with protection-bit, password check must be done

After command execution, ICRW returns response with 9000H or sw1+sw2 as the result.

QU-TK-F31 reads data first from the main memory, and it is compared with the value that it was received.

When this is wrong, writing isn't begun. Protection condition can be set up at a time in the data which continued in the main memory.

9.8.5.6 Verification of password present to SLE4428

HOST Command

"C"	53H	34H	00H	20H	00H	00H	02H	efH…

Positive response

"P"	53H	34H	st0	st1	st2	data

Negative response

"N"	53H	34H	e1	e0

Notes: efH: the data to compare (2bytes)

Before changing data, Password must be checked properly with SLE4428.

Because this function should be made effective, the issue of the next command is necessary.

Ex) "CR4"+ 0020000002xxxx (xxxx: security code 2bytes)

The presented data are compared with internal data in SLE4428 card itself.

User should know the password of card if they want to change the data in SLE4442, Error-Counter can be reset in the zero from 7 or less than 7. When error-counter is reset as zero, lock the card.

9.9 I2C Memory Card Control Command

9.9.1 Activate I2C memory card

HOST Command

“C”	54H	30H	Wrd	Vcc

Positive response

“P”	54H	30H	st0	st1	st2

Negative response

“N”	54H	30H	e1	e0

To activate (24C01, 24C02, 24C04, 24C08, 24C16, 24C32, 24C64, 24C128, 24C256) card QU-TK-F31 supplies a power supply (Vcc), clock (CLK), reset (RST).

Including:

Wrd set I2C type

Wrd =30H To activate(24C01,24C02,24C04,24C08,24C16,24C32,24C64,24C128,24C256) card

Wrd =31H activate 24C01card

Wrd =32H activate 24C02 card

Wrd =33H activate 24C04 card

Wrd =34H activate 24C08 card

Wrd =35H activate 24C16 card

Wrd =36H activate 24C32 card

Wrd =37H activate 24C64 card

Wrd =38H activate 24C128 card

Wrd =39H activate 24C256 card

Vcc choose voltage to card

Vcc=30H 5V

Vcc=31H 3V

Vcc is optional parameter, no Set parameter in command is equal to Set=30H

9.9.2 Deactivate I2C memory card

HOST Command

“C”	54H	31H

Positive response

“P”	54H	31H	st0	st1	st2

Negative response

“N”	54H	31H	e1	e0

QU-TK-F31 stop supplying a power supply (Vcc), Clock(CLK), Reset(RST).

9.9.3 Inquire Status of I2C memory card

HOST Command

“C”	54H	32H

Positive response

“P”	54H	32H	st0	st1	st2	Sti

Negative response

“N”	54H	32H	e1	e0

This command is used to inquire status of I2C card and return status by Sti.

Sti meanings:

Sti=30 H No I2C be activated

Sti=31 H Activated 24C02

Sti=32 H Activated 24C02

Sti=33 H Activated 24C04

Sti=34 H Activated 24C08

Sti=35 H Activated 24C16

Sti=36H Activated 24C32

Sti=37H Activated 24C64

Sti=38H Activated 24C128

Sti=39H Activated 24C256

9.9.4 I2C Control

These functions are specified by a command data form like C-APDU which format is based on T=0 standard.

In this case, QU-TK-F31 recognizes the meaning of the command data, and execute the treatment related to the card by controlling hardware.

After the command was executed properly, QU-TK-F31 returns a positive response with response data 9000H like from the IC card. When an error occurs during the communication with I2C, QU-TK-F31 returns a positive response with status information in response data "sw1+sw2” which is based on ISO/IEC 7816-3

Sw1	Sw2	Specification
90H	00H	Success

6FH	00H	Fail
6BH	00H	Address overflow
67H	00H	Operation length overflow

Write/Read I2C and Address scope is showed below:

Card_type	ab, cd
24C01	0000H ~ 007FH
24C02	0000H ~ 00FFH
24C04	0000H ~ 01FFH
24C08	0000H ~ 03FFH
24C16	0000H ~ 07FFH
24C32	0000H ~ 0FFFH
24C64	0000H ~ 1FFFH
24C128	0000H ~ 3FFFH
24C256	0000H ~ 7FFFH

9.9.4.1 Read data from I2C

HOST Command

“C”	54H	33H	00H	B0H	abH	cdH	efH

Positive response

“P”	54H	33H	st0	st1	st2	Data

Negative response

“N”	54H	33H	e1	e0

Value:

abH: The upper address of head address which begins to read data

cdH: The lower address of head address which begins to read data

efH: The number of bytes of data to read

QU-TK-F31 read efH length and return to HOST according to address specified by abH, cdH.The length of efH cannot be surpass the length of I2C address up limit.

When the following command is transmitted, data can be read from the I2C memory card.

Ex) "CU3"+00B000000

9.9.4.2 Write data to I2C

HOST Command

“C”	54H	34H	00H	D0H	abH	cdH	efH	ghH…

Positive response

“P”	54H	34H	st0	st1	st2	Data

Negative response

“N”	54H	34H	e1	e0

This command is recognized as follows.

abH: The upper address of head address which begins to write data

cdH: The lower address of head address which begins to write data

efH: The number of bytes of data to write

ghH: the data to write first (the head data of the data on ef H bytes)

QU-TK-F31 read efH length and return to HOST according to address specified by abH, cdH.The length of efH cannot be surpass the length of I2C address up limit.

The example which data on 8bytes are written into I2C

Ex) "CU3"+ 00D0000008 + Write Data (8bytes)

After command execution, ICRW returns response with 9000H or sw1+sw2 as the result.

9.10 Contactless IC card Operation

9.10.1 Activated contactless IC card

HOST Command

“C”	60H	30H	Set1	Set2

(1) Mifare One Card Positive Response

“P”	60H	30H	st0	st1	st2	Rtype	ATQA	UID_len	UID_data	SAK

Mifare One Dard Negative Response

“N”	60H	30H	e1	e0	Rtype	ATQA	UID_len	UID_data	SAK

(2) 14443 Type A Card Positive Response

“P”	60H	30H	st0	st1	st2	Rtype	ATQA	UID_len	UID_data	SAK	ATS

14443 Type A Card Negative Response

“N”	60H	30H	e1	e0	Rtype	ATQA	UID_len	UID_data	SAK	ATS

(3) 14443 Type B Card Positive Response

“P”	60H	30H	st0	st1	st2	Rtype	ATQB

14443 Type b Card Negative Response

“N”	60H	30H	e1	e0	Rtype	ATQB

Activate RFID card

QU-TK-F31 support activated IEC/ISO14443 Type A and IEC/ISO 14443 Type B

The process is show as below:

1).Mifare one card: 1.Request A (REQ A)/ Answer Request A (ATQ A).

2.Anticollision

3.Select (SEL) / Unique Identifier (UID) & Select Acknowledge (SAK)

When Mifare card successfully activate, QU-TK-F31return:

ATQA(2 byte), UID_data (4—10 byte) and SAK(1 byte).

2).ISO/IEC 14443 Type A: 1.Request A (REQ A)/ Answer Request A (ATQ A).

2.Anticollision

3.Select (SEL) / Unique Identifier (UID) & Select Acknowledge (SAK)

4.Request for answer to select (RATS) / Answer to Select (ATS)

5.Protocol and parameter selection request (PPSR)/PPS start (PPSS)

When ISO/IEC 14443 Type A card successfully activated, QU-TK-F31 return:

Mifare card return value increase (ATS (1-254 byte) and protocol parameter (1 byte))

3).ISO/IEC 14443 Type B: 1.Request B (REQ B)/ Answer Request B (ATQ B).

2.Attribute (A TTRIB)/ Answer to ATTRIB

When ISO/IEC 14443 Type B card successfully activated, QU-TK-F31 return ATQB 12 byte (including following information):

50H, PUPI (4 byte), App.data(4 byte), Protoclol info (3 byte)

Notes:

Set1, Set2 set sequence of operation for different type of protocol

Valid value: 41H (‘A’= Type A), 42H(‘B’= Type B), 30H(‘0’= Do not use)

Ex1:Set1= ‘A’, Set2 = ‘B’ (default)

Activate sequence: Type A protocol (first sequence), Type B protocol (second sequence)

Ex2:Set1= ‘B’, Set2 = ‘A’

Activate sequence: Type B protocol (first sequence), Type A protocol (second sequence)

Ex3:Set1= ‘A’, Set2 = ‘0’

Activate sequence: Type A protocol (first sequence), Type B protocol (Deactivated)

Ex4:Set1= ‘B’, Set2 = ‘0’,

Activate sequence: Type B protocol (first sequence), Type A protocol (Deactivated)

Rtype: Protocol

= 41H (‘A’) In line with ISO/IEC 14443 Type A protocol

= 42H (‘B’) In line with ISO/IEC 14443 Type B protocol

= 4DH (‘M’) In line with Philips Mifare one card protocol

When Rtype= 4DH (‘M’)

ATQA= 0044H Mifare Ultralight Card

ATQA= 0004H Mifare S50 1K Card

ATQA= 0002H Mifare S70 4K Card

Mifare one, ISO/IEC 14443 Type A return UID (The length of UID_data)

UID_len=4 The length of UID_data is 4 byte.

UID_len=7 The length of UID_data is 7 byte.

UID_len=10 The length of UID_data is10 byte.

9.10.2 Deactivate RFID card

HOST Command

"C"	60H	31H

Positive response

"P"	60H	31H	st0	st1	st2

Negative response

"N"	60H	31H	e1	e0

Deactivate RFIN card and Output signal to antanna is closed.

9.10.3 Inquire status of RFID card

HOST Command

"C"	60H	32H

Positive response

"P"	60H	32H	st0	st1	st2	sti	stj

Negative response

"N"	60H	32H	e1	e0

Inquire status of RFID sti,stj:

sti	stj	Specification
'0'	'0'	Deactivated RF
'1'	'0'	Mifare one S50 card
	'1'	Mifare one S70 card
	'2'	Mifare one UL card
'2'	'0'	Type A CPU card
'3'	'0'	Type B CPU card

9.10.4 Mifare 1 card control

These functions are specified by a command data form like C-APDU which format is based on T=0 standard.

In this case, QU-TK-F31 recognizes the meaning of the command data, and executes the treatment related to the card by controlling hardware.

After the command was executed properly, QU-TK-F31 returns a positive response with response data 9000H like from the IC card. When an error occurs during the communication with Mifare 1 card QU-TK-F31 returns a positive response with status information in response data "sw1+sw2"

which is based on ISO/IEC 7816-3.

Sw1	Sw2	Specification
90H	00H	Success
6FH	00H	Fail
6BH	00H	Address overflow
67H	00H	Operation length overflow

9.10.4.1 Key verification

HOST Command

"C"	60H	33H	00H	20H	ks	sn	lc	p-data

Positive response

"P"	60H	33H	st0	st1	st2	r-data

Negative response

"N"	60H	33H	e1	e0

Download key to QU-TK-F31 and verify the key directly

ks(1byte): key select(Key A=00H, Key B=01H)

sn(1byte): sector number (S50 card sn=00H-0FH, S70 card sn=00H-27H)

lc(1byte): password length lc=06H

p-data(6 byte): password data

r-data(2 byte): return data(positive response with data 9000H, and negtive response with " sw1+sw2")

9.10.4.2 Verify key from EEPROM

HOST Command

"C"	60H	33H	00H	21H	ks	sn

Positive response

"P"	60H	33H	st0	st1	st2	r-data

Negative response

"N"	60H	33H	e1	e0

Read key from EEPROM of RF module and verify the sector key

Download key via command mentioned in 9.10.4.4

EEPROM can preserve 32 groups of key data

ks (1byte): key select (Key A=00H, Key B=01H)

sn (1byte): sector number (sn=00H-0FH)

rdata (2 byte): return data (positive response with 9000H)

9.10.4.3 Modify sector key (KEY A)

HOST Command

"C"	60H	33H	00H	D5H	00H	sn	lc	p-data

Positive response

"P"	60H	33H	st0	st1	st2	r-data

Negative response

"N"	60H	33H	e1	e0

Modify sector key (key A)

This command only can modify KEY A, an d modify KEY B as "0xFF, 0xFF, 0xFF,0xFF,0xFF,0xFF" in the meantime modify control words as "0xFF, 0x07, 0x80, 0x69" (ex-work default)

Use block command to modify Key A, Key B control word

sn (1byte): sector number (S50 card sn=00H-0FH, S70 card sn=00H-27H)

lc (1byte): password length lc=06H

p-data: password data 6 bytes.

r-data (2 byte): return data

(positive response with data 9000H, and negtive response with " sw1+sw2")

9.10.4.4 Download password to EEPROM

HOST Command

"C"	60H	33H	00H	D0H	ks	sn	lc	p-data

Positive response

"P"	60H	33H	st0	st1	st2	r-data

Negative response

"N"	60H	33H	e1	e0

Read key from EEPROM of RF module and verify the sector key

EEPROM can preserve 32 groups of key data

ks(1byte): key select (Key A=00H, Key B=01H)

sn (1byte): sector number (sn=00H-0FH)

lc(1byte): password length lc=06H

p-data (6 byte): password data

r-data (2 byte): return data .

positive response sw1+sw2=9000H.

negative response sw1+sw2=6F00H

9.10.4.5 Read sector data

HOST Command

"C"	60H	33H	00H	B0H	sn	bn	le

Positive response

"P"	60H	33H	st0	st1	st2	rdata

Negative response

"N"	60H	33H	e1	e0

Read block and sequence blocks from RF card

sn (1 byte): sector number

bn (1 byte): block number

le (1 byte): block number (le=01H read one block, le=03H read three blocks)

rdata (2 byte): return data

(Positive response with data 9000H, and negative response with " sw1+sw2")

Notes:

1.Ultralight Card only have one block in one sector, every block have 4-byte data. S50, S70 have16-byte data in one block.

2. Ultralight Card, Mifare 1k (S50), Mifare 1k (S70) card range of capacity is shown as below:

Ultralight Card: sn =00H-0FH, bn=00H, le=01H-0FH

Mifare 1k (S50): sn =00H-0FH,bn=00H-03H, le=01H-04H

Mifare 1k (S70): sn =00H-20H,bn=00H-03H, le=01H-04H

sn =21H-27H, bn=00H-0FH, le=01H-10H (S70 card last 8 sectors have 16 blocks)

9.10.4.6 Write sector data

HOST Command

"C"	60H	33H	00H	D1H	sn	bn	lc	w-data

Positive response

"P"	60H	33H	st0	st1	st2	r-data

Negative response

"N"	60H	33H	e1	e0

Read block and sequence blocks from RF card

sn (1 byte): sector number

bn (1 byte): block number

le (1 byte): block number

wdata: block to write (n byte)

rdata (2 byte): return data

(Positive response with data 9000H and negtive response with "sw1+sw2")

Notes:

1. Ultralight Card only have one block in one sector, every block have 4 byte data. S50,S70 have16 byte data in one block
2. Ultralight Card, Mifare 1k(S50), Mifare 1k (S70) card card range of capacity is shown as below:

Ultralight Card: sn=00H-0FH, bn=00H-03H, lc=01H-03H

Mifare 1k(S50): sn=00H-0FH, bn=00H-03H, lc=01H-03H

Mifare 1k(S70): sn=00H-20H, bn=00H-03H, lc=01H-03H

sn=21H-27H, bn=00H-0FH, lc=01H-0FH

(last 8 sectors of S70 card have 16 blocks)

3. S50,S70 card last block of each sector is control sector to preserve Key A, read/write control words, Key B.

Cautions: Do note write last block and QU-TK-F31 also will prohibit to write last block.

9.10.4.7 Initialization

HOST Command

"C"	60H	33H	00H	D2H	sn	bn	lc	w-data

Positive response

"P"	60H	33H	st0	st1	st2	r-data

Negative response

"N"	60H	33H	e1	e0

Initialization operation to RF card

sn(1 byte): sector number

bn(1 byte): block number

lc(1byte): length lc=04H

w-data: data (4 byte)

r-data (2 byte): return data

(Positive response with data 9000H and negative response with "sw1+sw2")

Notes: Mifare 1k(S50), Mifare 1k (S70) card operation sector
(Sector cannot be out of range and last block cannot be operated)

Mifare 1k (S50): sn=00H-0FH, bn=00H-03H,

Mifare 1k (S70): sn=00H-20H, bn=00H-03H,

sn=20H-27H, bn=00H-0EH,

(S70 card last 8 sectors have 16 blocks)

9.10.4.8 Read value

HOST Command

"C"	60H	33H	00H	B1H	sn	bn

Positive response

“P”	60H	33H	st0	st1	st2	r-data

Negative response

“N”	60H	33H	e1	e0

Read value operations to RF card

sn (1 byte): sector number

bn (1 byte): block number

r-data (2 byte): return data

(Positive response with data 9000H and negative response with “sw1+sw2”)

Notes:Mifare 1k (S50), Mifare 1k (S70) card operation sector

(Sector can not be out of range and last block cannot be operated)

Mifare 1k (S50): sn=00H-0FH, bn=00H-03H,

Mifare 1k (S70): sn=00H-20H, bn=00H-03H,

sn=20H-27H,bn=00H-0EH,

(S70 card last 8 sectors have 16 blocks)

9.10.4.9 Increment

HOST Command

“C”	60H	33H	00H	D3H	sn	bn	lc	w-data

Positive response

“P”	60H	33H	st0	st1	st2	r-data

Negative response

“N”	60H	33H	e1	e0

Increment operation to RF card

sn (1 byte): sector number

bn (1 byte): block number

lc (1byte): increment length lc=04H

w-data: increment data (4 byte)

r-data (2 byte): return data

(Positive response with data 9000H, and negative response with “sw1+sw2”)

Notes:Mifare 1k (S50), Mifare 1k (S70) card operation sector

(Sector cannot be out of range and last block cannot be operated)

Mifare 1k (S50): sn=00H-0FH, bn=00H-03H,

Mifare 1k (S70): sn=00H-20H, bn=00H-03H,

sn=20H-27H,bn=00H-0EH,

(S70 card last 8 sectors have 16 blocks)

9.10.4.10 Decrement

HOST Command

“C”	60H	33H	00H	D4H	sn	bn	lc	w-data

Positive response

“P”	60H	33H	st0	st1	st2	r-data

Negative response

“N”	60H	33H	e1	e0

Decrement operation to RF sector

sn (1 byte): sector number

bn (1 byte): block number

lc (1byte): Decrement length lc=04H

w-data: Decrement data (4 byte)

r-data (2 byte): return data

(Positive response with data 9000H, and negtive response with “sw1+sw2”)

Notes: Mifare 1k(S50), Mifare 1k (S70) card operation sector

(Sector cannot be out of range and last block cannot be operated)

Mifare 1k (S50): sn=00H-0FH, bn=00H-03H,

Mifare 1k (S70): sn=00H-20H, bn=00H-03H,

sn=20H-27H,bn=00H-0EH,

(S70 card last 8 sectors have 16 blocks)

9.10.5 Type A RF card communication

HOST Command

“C”	60H	34H	C-APDU

Positive response

“P”	60H	34H	st0	st1	st2	R-APDU

Negative response

“N”	60H	34H	e1	e0

This exchanges data between RF card by protocol RF Type A T=CL according to ISO/IEC 14443-4

Notes: The max. length of C-APDU is 261 byte, the max. length of R-APDU is 258 byte.

9.10.6 Type B RFcard communication

HOST Command

“C”	60H	35H	C-APDU

Positive response

“P”	60H	35H	st0	st1	st2	R-APDU

Negative response

“N”	60H	35H	e1	e0

This exchanges data between RF card by protocol RF Type B T=CL according to ISO/IEC 14443-4

Notes: The max. length of C-APDU is 261 bytes, the max. length of R-APDU is 258 byte.

9.10.7 ISO15693 RF card Communication

9.10.7.1 Read serial number

HOST Command

“C”	60H	70H	CMP

CMP	Length(Bytes)	Meaning
<1>	1	The number of blocks
<2>	1	Block address, one block 4 bytes

Positive response

“P”	60H	70H	st0	st1	st2	RDT

Negative response

“N”	60H	70H	e1	e0

RDT	Length (Bytes)	Meaning
<1>	4	Block data, one block 4 bytes

9.10.7.2 Write Serial Number of QU-TK-F31

HOST Command

“C”	60H	71H	CMP

CMP	Length (Bytes)	Meaning
<1>	1	Number of blocks
<2>	1	Block Address
<3>	4	Block data, one block 4 bytes

Positive response

“P”	60H	71H	st0	st1	st2

Negative response

“N”	60H	71H	e1	e0

9.10.7.3 Lock block command

HOST Command

“C”	60H	72H

Positive response

“P”	60H	72H	st0	st1	st2

Negative response

“N”	60H	72H	e1	e0

9.10.7.4 Write AFI

HOST Command

"C"	60H	77H	CMP

CMP	Length(Bytes)	Meaning
<1>	1	AFI

Positive response

"P"	60H	77H	st0	st1	st2

Negative response

"N"	60H	77H	e1	e0

9.10.7.5 Lock Block AFI

HOST Command

"C"	60H	78H

Positive response

"P"	60H	78H	st0	st1	st2

Negative response

"N"	60H	78H	e1	e0

9.10.7.6 Write DSFID

HOST Command

"C"	60H	79H	CMP

CMP	Length (Bytes)	Meaning
<1>	1	DIFID

Positive response

"P"	60H	79H	st0	st1	st2

Negative response

"N"	60H	79H	e1	e0

9.10.7.7 Lock Block AFI

HOST Command

"C"	60H	7AH

Positive response

"P"	60H	7AH	st0	st1	st2

Negative response

"N"	60H	7AH	e1	e0

9.10.8 SRIX 4K TRANSPARENCY

HOST Command

“C”	60H	80H	CMP

Positive response

“P”	60H	80H	st0	st1	st2	RDT

Negative response

“N”	60H	80H	e1	e0

E.g. For Reading Block #0: 43 60 02 08 00

9.11 Read Serial Number

9.11.1 Read serial number

HOST Command

“C”	A2H	30H

Positive response

“P”	A2H	30H	st0	st1	st2	len	ICRW_SN

Negative response

“N”	A2H	30H	e1	e0

Len: read length of QU-TK-F31serial number (0byte-18byte)

ICRW_SN: QU-TK-F31 serial number

9.11.2 Write Serial Number of QU-TK-F31

Omitted

9.12 Read QU-TK-F31 configuration

HOST Command

“C”	A3H	30H

Positive response

“P”	A3H	30H	st0	st1	st2	ICRW_Config

Negative response

“N”	A3H	30H	e1	e0

QU-TK-F31 configuration specification:

Name	Value	Description
S1		QU-TK Reader Identifier word
	“7”	S1 = “37”
S2/S3/S4 (3 Byte)		User Code option
	“V10”	QU-TK Firmware version
	“XXX”	Customize version
S5		Card r/w type option
	“0”	Dispensing available, Read/Write unavailable
	“I”	IC card r/w
	“C”	RF card r/w
	“E”	IC + RF card r/w
S6		Interface type option

	“R”	RS-232Interface type
S7		IC card write type
	“0”	IC card writing unavailable
	“1”	IC card connector for third-party usage
	“2”	Standard IC card read/write
S8		RF card write type
	“0”	RF card write/read unavailable
	“1”	RF card antenna for third-party usage
	“2”	Standard RF card read/write
S9		SAM option
	“0”	Not SAM
	“1”	SAM 1
	“2”	SAM 2
	“3”	SAM 3
	“4”	SAM 4
	“5”	SAM 5
S10	“0”	Components related to dispense cards
	“1”	Components related to remove cards

9.13 Read QU-TK-F31 version information

HOST Command

“C”	A4H	Pm

Positive response

“P”	A4H	30H	st0	st1	st2	Rev

Negative response

“N”	A4H	30H	e1	e0

Read QU-TK-F31 version information

Pm=30H Read machine software information

Ex:Rev =“C571_V1.00_A_090910”

Pm=31H Read IC Card software information

Ex:Rev =“ICCARD_V10_A_090910”

Pm=32H Read RF Card software information

Ex:Rev =“RFCARD_V10_A_090910”

9.14 Error-card Bin Counter Control

Error Card Bin counter function is available on certain specified models.

9.14.1 Read error-card bin counter

HOST Command

“C”	A5H	30H

Positive response

“P”	A5H	30H	st0	st1	st2	Count (3 byte)

Negative response

“N”	A5H	30H	e1	e0

After reset error-card bin counter, Capture on card, counter one plus

Count= “000” ~ “999”

Counter overflow will return machine status (e1,e0=“50”)

9.14.2 Set initial value of error-card bin

HOST Command

“C”	A5H	31H	Count (3 byte)

Positive response

“P”	A5H	31H	st0	st1	st2

Negative response

“N”	A5H	31H	e1	e0

Set initial value of error-card bin.

Count= “000” ~ “999”

Count value range (0-999)

9.15 Machine Address Setting (Soft Setting)

QU-TK-F3x series supports machines address setting for up to 15 sets, which facilitates daisy chain connection communication. Address setting may be available in 2 modes:

1. DIP Switch Setting (By switch the DIP Switch to different positions as listed below, target machine addresses are set as the following table):

4-Digit DIP Switch				Machine Address
4	3	2	1	
ON	ON	ON	ON	‘00’ (Default)
ON	ON	ON	OFF	‘01’
ON	ON	OFF	ON	‘02’
ON	ON	OFF	OFF	‘03’
ON	OFF	ON	ON	‘04’
ON	OFF	ON	OFF	‘05’
ON	OFF	OFF	ON	‘06’
ON	OFF	OFF	OFF	‘07’
OFF	ON	ON	ON	‘08’
OFF	ON	ON	OFF	‘09’
OFF	ON	OFF	ON	‘0A’
OFF	ON	OFF	OFF	‘0B’
OFF	OFF	ON	ON	‘0C’
OFF	OFF	ON	OFF	‘0D’
OFF	OFF	OFF	ON	‘0E’
OFF	OFF	OFF	OFF	‘0F’

2. Software Setting allows host machine to set address of the dispenser machine by sending commands. Software setting is available on certain specified models.
   Host Machine uses **0F** address as broadcasting address to set target machine address from 0x01 to 0x0E (1~14 in decimal)
   HOST Command

"C"	FFH	30H	Addr

   Positive response

"P"	FFH	30H	st0	st1	st2

   Negative response

"N"	FFH	30H	e1	e0

9.16 LED control

LED control command is applicable on certain models for controlling ON/OFF and flashing of the LED indicator on the bezel.

Host Command:

"C"	31H	60H	**CMP**

Positive Response:

"P"	31H	60H	st0	st1	st2	RDT

Positive Response:

"N"	31H	60H	e1	e0

CMP -> One byte, for LED1 control.
BIT7-BIT6 for LED1 work mode as defines below:
0x00：LED1 off;
0x01：LED1 on ；
0x02：LED1 flash.
BIT0-BIT5 for flash periods in 100ms. 0xff for always flashing.
0x03 to disable LED control