	SPECIFICATION	Model No.	CRT-310-NU01
		Date	2017/04/06
	PROTOCOL	Ver.	
		Page	1/90

CRT-310-NU01 MOTORIZED CARD READER

PROTOCOL

V1.0

SHEN ZHEN CREATOR CHINA TECH
CO.,LTD

VERSION	DATE	ILLUSTRATION
1.0	2014-11-05	FIRST RELEASE

CONTANT

1	Communication description.....	5
1.1	USB interface.....	5
1.2	Communication controlling procedure	5
1.3	USB offline dealing	5
1.4	Transmission Control Characters.....	6
1.5	Transmission Format	6
2	Transmission / Control protocol	7
2.1	Timing chart.....	7
2.2	Cancel of command	8
2.3	Protocol.....	8
2.3.1	Ordinary operation	8
2.3.2	Irregular operation and back-up	8
2.3.3	State transition matrix	10
3	Command/Response	11
3.1	TEXT format.....	11
4	User program code area	12
4.1	Command list.....	12
4.2	Status code	15
4.3	Error code	16
5	Command explanation of user program code area	18
5.1	Initialize command	18
5.2	Status request command	20
5.3	Entry command.....	22
5.4	Card carry command.....	23
5.5	Retrieve command	23
5.6	LED command.....	24
5.7	Mag-track read command	25
5.8	Intake/withdraw command	26
5.9	Enable / Disable command	28
5.10	Sensor Level transmit command.....	30
5.11	Control command for contact IC card moving	31
5.12	Revision command	32
5.13	Counter common	33
5.14	IC Card control command.....	34
5.14.1	Activate ICC command	34
5.14.2	Deactivate ICC command.....	36
5.14.3	Inquire ICC status command	36
5.14.4	ICC communication T=0	37
5.14.5	ICC communication T=1	38
5.14.6	ICC extended communication 1	39
5.14.7	ICC extended communication 2	40
5.14.8	ICC extended communication 3	40
5.14.9	ICC warm reset.....	41
5.14.10	ICC automatic communication	42
5.15	SAM (Secure Application Module) control command	43

INTERFACE SPECIFICATION		CRT-310-NU01	4/90
5.15.1	Activate SAM command	43	
5.15.2	Deactivate SAM command.....	44	
5.15.3	Inquire SAM status command	45	
5.15.4	SAM Communication T=0	46	
5.15.5	SAM communication T=1	47	
5.15.6	SAM extended communication 1	48	
5.15.7	SAM extended communication 2	49	
5.15.8	SAM extended communication 3	49	
5.15.9	SAM warm reset	50	
5.15.10	SAM automatic communication	50	
5.15.11	Select SAM.....	51	
5.16	Switch command	52	
5.17	Simons memory card control command	53	
5.17.1	Simens memory card power on and activate	53	
5.17.2	Simens meomory card power off.....	53	
5.17.3	Inquire status of Simens memory card.....	54	
5.17.4	Communicate with SLE4442.....	54	
5.17.5	Communicate with SLE4428.....	59	
5.18	I2C memory card control command	64	
5.18.1	I2C Power on	64	
5.18.2	I2C Power off.....	64	
5.18.3	Inquire Status of I2C.....	65	
5.18.4	I2C Communication.....	65	
5.19	command for Contactless card.....	68	
5.19.1	Reset activated	68	
5.19.2	Contactless card deactive / release.....	69	
5.19.3	Inquiry status of contactless card.....	69	
5.19.4	Mifare one card operation.....	错误！未定义书签。	
5.19.5	APDU communication for contactless Type A CPU card.....	错误！未定义书签。	
5.19.6	APDU communication for contactless Type B CPU card.....	错误！未定义书签。	
5.20	Automatically test the type of IC card / contactless card.....	78	
5.21	Command for the counting of Shutter, Contact, Magnetic Head working.....	79	
5.22	Read S/N of ICRW	80	
6	Explanation of error code	82	
6.1	Error in communication	82	
6.2	Error at card feeding	82	
6.3	Error in reading card	83	
6.4	Other error codes	83	
7	ANNEX	84	
7.1	ANNEX 1 Calculation method of CRCC	84	
7.2	Annex2 : Supportable TA1 & TA2 values	85	
7.3	ANNEX3 Values of ATR parameter	89	
7.4	ANNEX 4 C-APDU Format	90	

1 Communication description

The protocol transmitted from HOST is automatically recognized by ICRW after a power-on.

After the recognition, communication is executed according to each protocol.

Protocol type is recognized only after power-on.

And the protocol cannot be switched to another protocol during communication.

1.1 USB interface

- 1) USB version 2.0
- 2) Full speed 12Mbps
- 3) terminal EP0: transporting controlling 64 bytes
 EP1: interrupt input/output input 64 bytes; output 64 bytes
- 4) Vendor ID 23D8
- 5) Product ID 0350
- 6) Producer identification "CREATOR TECH CO.,LTD"
- 7) Production identification "CRT310-NU01"
- 8) USB type HID(Human Interface Device) 1.11
- 9) Repoprt size 64 bytes
- 10) Report format

Report ID	Report data (64 bytes)
-----------	------------------------

1.2 Communication controlling procedure

ICRW receives specified operation 'command packet' from Host, send the result by 'ATR packet' to Host after executing.

1.3 USB offline dealing

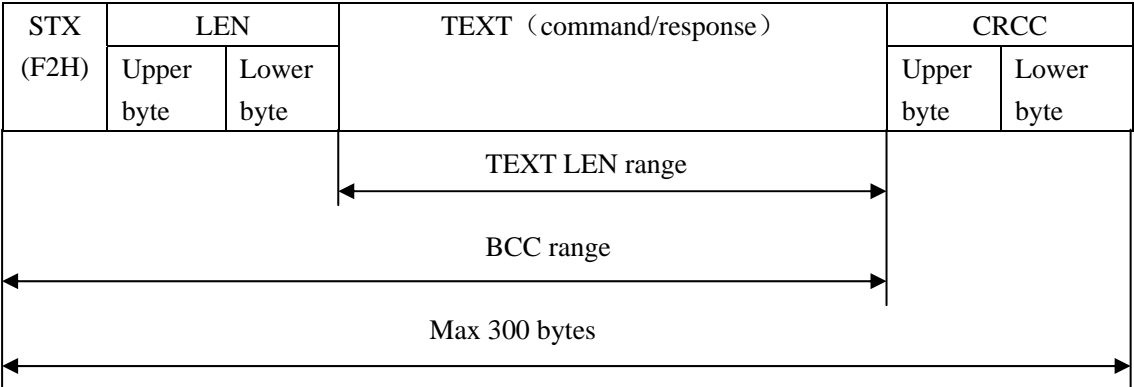
When VBUS deactivation is checked, ICRW executes automatically reset activity.

Disconnect USB between ICRW and Host before resetting. Then ICRW executes related activities (EX:ejecting card) according to reset parameter Pd. If VBUS recovers when ICRW is executing reset activities, then ICRW does not respond immediately. Icrw will return to initial state and reset software after executing related activities. After that, ICRW again restart the fuction of plug and play self-recognition.

1.4 Transmission Control Characters

STX (F2H)	Indicate start of text. STX code is F2h
ACK (06H)	Acknowledge
NAK (15H)	Negative acknowledge.
DLE,EOT (10H 04H)	Clear the line
LEN(2 bytes)	Text length
TEXT	Command or response
CRCC(2 bytes)	Cyclic redundancy code。 Polynomial $X^{16}+X^{12}+X^5+1$ ， Initial value is 0000h。

1.5 Transmission Format



Notes 1.Gap between characters STX to CRCC is less than 250 msec

If the total length is exceed 64 bytes, it will be separated to 2 or more many of packets

2 Transmission / Control protocol

2.1 Timing chart

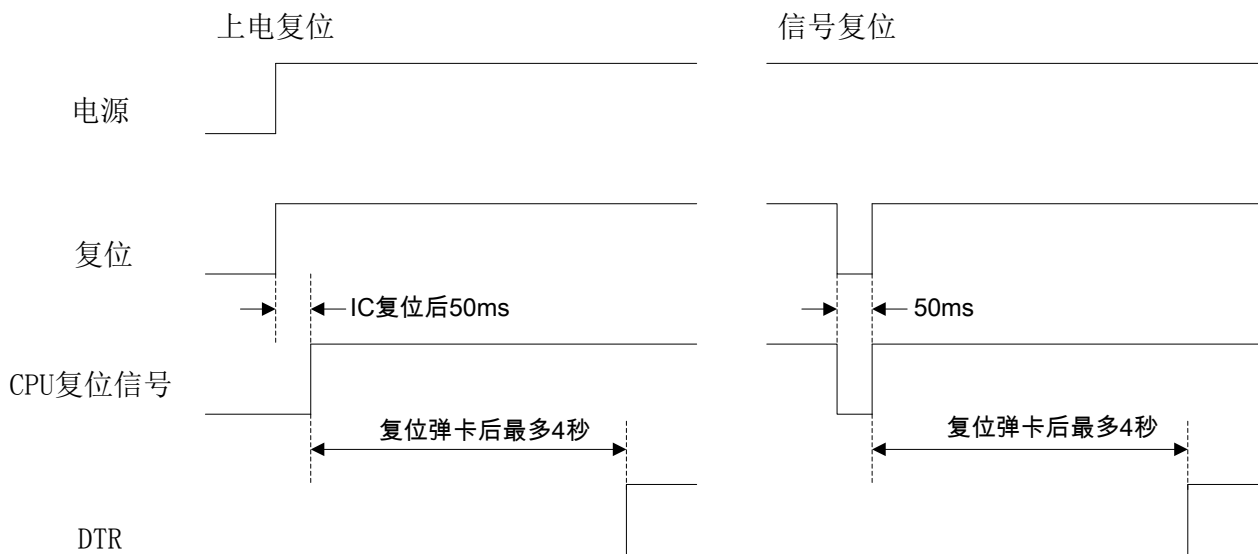
1) Power-on-reset and Signal-reset (User program code area only)

After the reset operation, ICRW ejects the card in ICRW. "DTR" is turned on after the card was ejected.

The HOST should monitor if the ICRW turn on "DTR" after power-on-reset or signal-reset..

For the signal reset, the reset line should be activating more than 50msec.

The time concerning ICRW initializing and card discharging is a maximum of 4sec at the time of card jam was occurring.



2) LED blinking after reset

On normal reset operation, ICRW blinks green LED. The blinking interval is 2 sec.。

If the user area program is illegal condition, card is not ejected and the blinking interval is 1 sec.。

After receiving the initial command correctly, ICRW turns off LED。

3) Data gap

During receiving mode, if 250ms Time-out occurs, ICRW assumes receiving the Text character data is completed.

4) Eject Operations

All of eject operations caused by reset, power down, DSR off, initial command and eject command moves card to a gate and a card stops in the state where it was held at the roller.

5) Transmit cancel / recover

If CTS signal off in ICRW data transmitting, ICRW will stop transfer. Max is 2 sec stop time. When CTS recover, data transmitting recover in 1 ms too.

6) Eject card operation

Reset executed, deactivate, DSR off; initialize, eject card command causes all eject operation to move the card to the front card holding position. (the card is under the rollers)。

2.2 Cancel of command

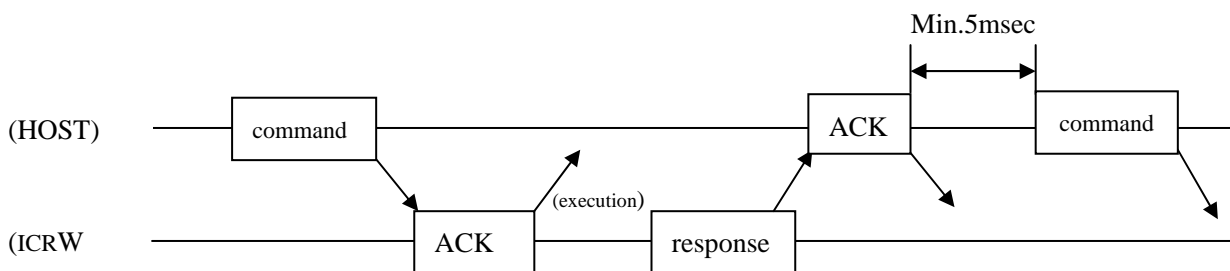
When ICRW receives "DLE,EOT", ICRW will interrupt execution of a command immediately. And then ICRW transmits "DLE,EOT" and waits for the following command.

If "DLE,EOT" is received during response transmission, ICRW will be in the state waiting for a command, after it completes response transmission.

If "DLE,EOT" is received for the entry, retrieve, and eject commands at the time of execution, each operation will be interrupted and a card will be ejected.

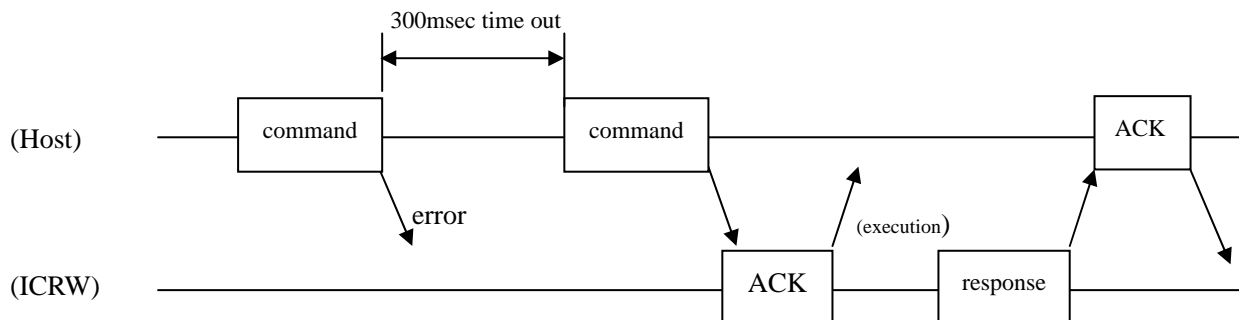
2.3 Protocol

2.3.1 Ordinary operation

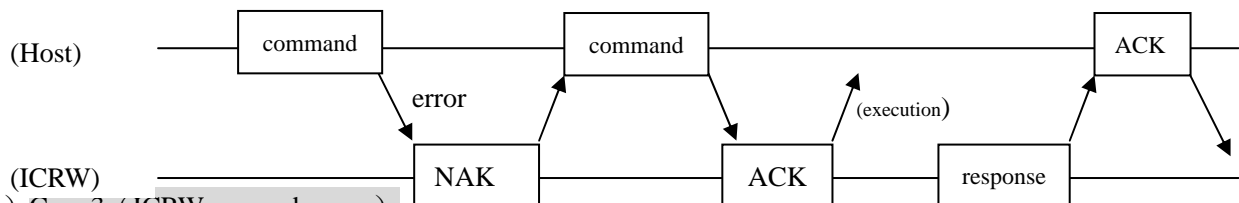


2.3.2 Irregular operation and back-up

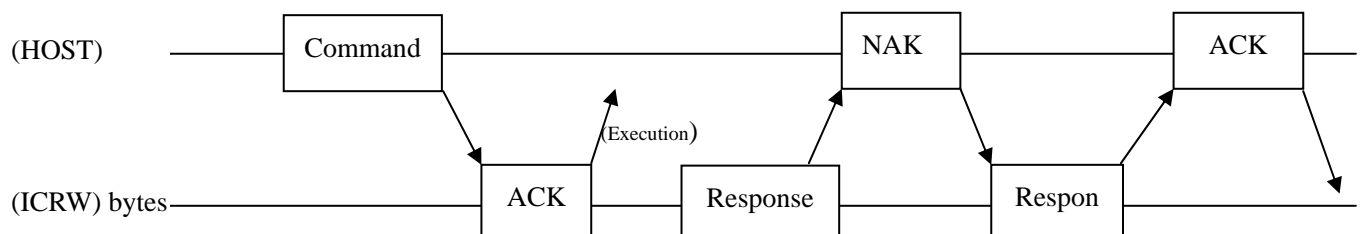
1) Case 1 (ICRW doesn't receive any command)



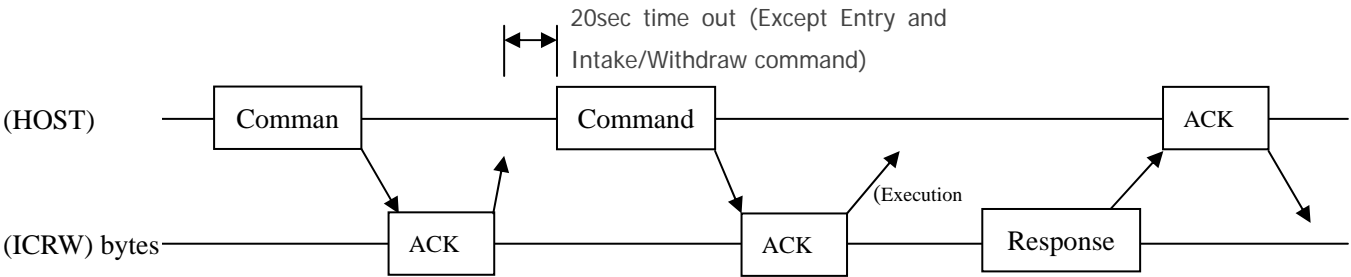
2) Case 2 (ICRW receives error command)



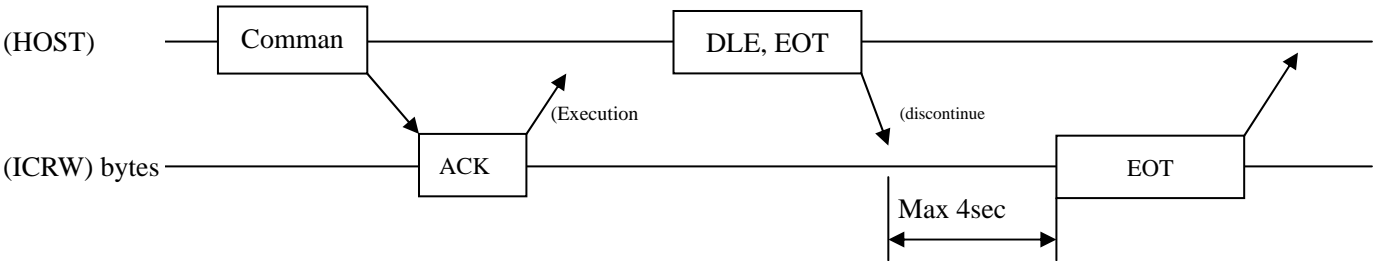
3) Case 3 (ICRW responds error)



4) Case 4 (waiting time out for ATR)



5) Case 5 (command end execution)



2.3.3 State transition matrix

1) HOST

Character Mode	ACK	NAK	STX(F2H)	Others	Time out	Timer
(1) Wait for ACK after command	Go to(2)	Re-send command Go to(1)*	Ignore	Ignore	Re-send command Go to(1)*	300msec
(2) Wait for response after ACK	Ignore	Ignore	Go to(3)	Ignore	Re-send command Go to(1)*	20sec**
(3) Wait for LEN	Receive 2 bytes as length, Receive 2 bytes then go to(4)				Send NAK, Go to(2)	250msec
(4) Wait for TEXT	Receive Text, the length is LEN, Go to(5)				Send NAK, Go to(2)	250 msec
(5) Wait for CRCC	Receive 2 bytes as CRCC OK then Normal receipt: Send ACK & go to(1) NG then Irregular receipt: Re-send NAK & go to(2)				Send NAK, Go to(2)	250 msec

*: If it is over the re-try count, it will be judged an error.

**: Except Entry and Intake/Withdraw command.

2) ICRW

Character Mode	ACK	NAK	STX (F2H)	DLE,EOT	Others	Time out	Timer
(1) Neutral	Ignore	Ignore	Go to(2)	Go to (1) after sent DLE,EOT	Ignore	None	
(2) Wait for LEN	Receive 2 bytes as Length.Receive 2 bytes then go to(3)					Send NAK & go to(1)	250msec
(3) Wait for TEXT	Receive Text in the Length bytes. Receive the Length bytes then go to(4)					Send NAK & go to(1)	250msec
(4) Wait for CRCC	Receive 2 bytes as CRCC OK then send ACK,execute command and go to(5) NG then send NAK and go to(1)					Send NAK & go to(1)	250msec
(5) Wait for ACK after sending Resp	Go to(1)	Resend Resp. Go to(5)	Go to (2)	Go to (1) after sent DLE,EOT	Ignore	Go to(1)	300msec

During command execution, all characters except "DLE, EOT" are ignored.

3 Command/Response

1. Host sends commands to ICRW for controlling purpose (the command followed operated data)
2. ICRW checks parity packet successfully after receiving commands, responds ACK to Host to confirm.
3. ICRW executes current command, responds results to Host by ATR.
4. Host receives ATR, respond ACK to ICRW after parity checking success.
5. ICRW continue to operate next command, 5ms delaying is necessary.

3.1 TEXT format

An ASCII character is expressed as shown in "C"(=43h), and a binary code is shown like 30h(="0") by hexadecimal. Command and response format is as follow:

"C" (43h)	"0" (30h)	"0" (30h)	Data (Binary 2bytes)
--------------	--------------	--------------	-------------------------

Especially when not written clearly, it becomes 1 byte of one division. The division surrounded by the dotted line shows the data which may not be considered as the case where it exists.

1) Command format(HOST->ICRW)

"C" (43h)	cm	pm	Data
--------------	----	----	------

cm: Command code

pm: Parameters

This is the format of the command transmit to ICRW from HOST.

The first character should be "C"(43h). there are some of commands with data part and some without data part.

The data what indicated in dashed line frame depends on the different command

Another is 'parameter default', reader executes according to the default parameter

2) Positive response format (ICRW->HOST)

"P" (50h)	cm	pm	st1	st0	Data
--------------	----	----	-----	-----	------

st1,st0: Status code

This is the format of response when command was executed normally.

The first character should be "P"(50h). There are positive responses with data part and without data part.

In this format cm and pm returns the same valued which were received with command transmission except for IC card control

3) Negative response format(ICRW->HOST)

"N" (4Eh)	cm	pm	e1	e0	Data
--------------	----	----	----	----	------

e1, e0: Error code

This is the format of response when command was executed abnormally.

The first character should be "P" (50h) {"N" (4Eh)}. Some of ATR with data there is, some there isn't.

In this format cm and pm returns the same values which were received with command transmission except for IC card control

4 User program code area

4.1 Command list

List 1

cm: Command code

pm: Parameters

Command	cm	Function	pm	Details of operation
INITIALIZE	"0" (30h)	Initialize ICRW	"0"(30h)	Initialize, set up and eject a card
			"1"(31h)	Initialize, set up and capture a card
			"2"(32h)	Initialize, set up and re-positioning a card
			"3"(33h)	Initialize, set up without card operation
			"8"(38h)	Initialize parameter report
STATUS REQUEST	"1" (31h)	Inquire status	"0"(30h)	Report presence of card and its position
			"1"(31h)	Report presence of sensor status in detail
ENTRY	"2" (32h)	Card Entry	"0"(30h)	Card Entry(Mag-Track read)
		Backside card entry	"2"(32h)	Wait synchronic card insertion at backside
CARD CARRY	"3" (33h)	Eject	"0"(30h)	Move card to Gate from inside of ICRW
		Capture	"1"(31h)	Capture card to rear side of ICRW
RETRIEVE	"4"(34h)	Retrieve	"0"(30h)	Retrieve card from eject position
LED	"5" (35h)	LED off	"0"(30h)	All color LED off
		LED Green On	"1"(31h)	LED Green On
		LED Red On	"2"(32h)	LED Red On
		LED Orange On	"3"(33h)	LED Orange On
Mag-Track READ	"6" (36h)	ISO #1 read	"1"(31h)	ISO Track#1 reads Transmit read data
		ISO #2 read	"2"(32h)	ISO Track#2 reads Transmit read data
		ISO #3 read	"3"(33h)	ISO Track#3 reads Transmit read data
		All tracks read	"5"(35h)	Transmit all channel data
		Read Status	"7"(37h)	Data buffer status read
		ISO #1 error read	"9"(39h)	ISO Track#1 reads Transmit read data
		ISO #2 error read	":"(3Ah)	ISO Track#2 reads Transmit read data
		ISO #3 error read	";"(3Bh)	ISO Track#3 reads Transmit read data
INTAKE/WITHDRAW	"9" (39h)	Withdraw	"0"(30h)	Withdraw the card
		Intake	"1"(31h)	Card Intake
		Intake with Mag.Chk	"2"(32h)	Card intake with the magnetic recording detection
Asynchronously cardinsertion controlling	":" (3Ah)	Enable	"0"(30h)	Enable card entry
		Disable	"1"(31h)	Disable card entry
		Jitter card controlling set	"X" (58h)	Jitter card controlling set
		Unable to insert card at backside asynchronously	"@"(40h)	Unable to insert card at backside asynchronously
		enable to insert card at backside asynchronously	"A"(41h)	enable to insert card at backside asynchronously

INTERFACE SPECIFICATION	CRT-310-NU01	13/90
--------------------------------	--------------	-------

List 2

cm: Command code

pm: Parameters

Command	cm	Function	pm	Details of operation
SENSOR LEVEL TRANSMIT	“>” (3Eh)	NORMAL check	“0”(30h)	Transmit sensor A/D level with normal condition
IC card moving	“@” (40h)	Contact to IC card	“0”(30h)	Moving to the position, contacting to the IC card
		Release IC card	“2”(32h)	Deactive and release
REVISION	“A” (41h)	Revision	“1”(31h)	Revision of User program code area
			“2”(32h)	Revision of EMV2000 code area
			“3”(33h)	Transmit the EMV approval number
			“4”(34h)	Reserve
			“5”(35h)	Transmit the IFM number of the EMV approval
COUNTER	“C” (43h)	Pass Counter Read	“2”(32h)	Inquire of card pass count
		Capture Counter Read	“3”(33h)	Inquire of card capture count
		Capture Alert Count Set and Clear Counter	“4”(34h)	Set capture alert count and clear counter
		Capture Alert Count Set	“5”(35h)	Set capture alert count
		Capture Counter Clear	“6”(36h)	Clear capture counter
IC CARD CONTROL	“I” (49h)	Activate	“0”(30h)	Activate IC
		Deactivate	“1”(31h)	Deactivate IC
		Inquire Status	“2”(32h)	Inquire of IC status
		Communication T=0	“3”(33h)	IC Communication T=0
		Communication T=1	“4”(34h)	IC Communication T=1
		Communication 1	“5”(35h)	IC extended Communication 1
		Communication 2	“6”(36h)	IC extended Communication 2
		Communication 3	“7”(37h)	IC extended Communication 3
		Warm Reset	“8”(38h)	IC Warm reset
		Automatic Communication	“9”(39h)	IC automatic communication

List 3

cm: Command

pm: Patameters

Command	cm	Function	pm	Details of operation
SAM CONTROL	"T" (49h)	Activate	"@"(40h)	Activate SAM
		Deactivate	"A"(41h)	Deactivate SAM
		Inquire Status	"B"(42h)	Inquire of SAM status
		Communication T=0	"C"(43h)	SAM Communication T=0
		Communication T=1	"D"(44h)	SAM Communication T=1
		Communication 1	"E"(45h)	SAM extended Communication 1
		Communication 2	"F"(46h)	SAM extended Communication 2
		Communication 3	"G"(47h)	SAM extended Communication 3
		Warm Reset	"H"(48h)	SAM Warm reset
		Automatic Communication	"I"(49h)	SAM Automatic Communication
		Select SAM	"P"(50h)	Select SAM
SWITCH	"K"(4B)	Area switch	"0"(30h)	Switch to Supervisor program code area
Siemens Memory Card Control	"R" (52h)	Power on	"0"(30h)	Power Supply and Activate to Siemens card
		Power off	"1"(31h)	Deactivate to Siemnts card
		Status request	"2"(32h)	Inquire status of Siemens card
		Communication	"3"(33h)	Exchange data for 4442 card
		Communication	"4"(34h)	Exchange data for 4428 card
I2C MEMORY CONTROL	"S" (53h)	Activate	"0"(30h)	To activate I2C and To close the shutter
		Deactivate	"1"(31h)	To deactivate I2C
		Inquire Status	"2"(32h)	To inquire status of I2C
		Communication	"3"(33h)	To exchange data between I2C
Auto-test card type	(90h)	Test contact IC type	"0"(30h)	Auto-test type of IC card in ICRW
		Test contactless IC type	"2"(32h)	Auto-test type of contactless in ICRW
Contactless IC card reading & writing	"Z" (5Ah)	Activate contactless IC	"0"(30h)	Activate contactless IC
		Deactivate contactless IC card	"1"(31h)	Deactivate contactless IC card
		Mifare one read&write	"3"(33h)	Mifare standard card communication
		Type A,B communication	"4"(34h)	Type A,B communication
		Type A,B extend communication 1	"5"(35h)	Type A,B extend communication
		Type A,B extend communication 2	"6"(36h)	Type A,B extend communication
		Type A,B extend communication 3	"7"(37h)	Type A,B extend communication
		Contactless IC card reset	"8"(38h)	Contactless IC card interface reset
Counter operated for moving parts	(A1h)	Read count of used part	"0"(30h)	Read count of used part
		Count of initialization	"1"(31h)	Count of initialization
ICRW S/N operation	(A2h)	Read S/N of ICRW	"0"(30h)	Read S/N of ICRW
Get the type of ICRW	(AAh)	Get the type of ICRW	"0"(30h)	Return the type of ICRW

Notes: Do not use any other codes than those shown by this table.

4.2 Status code

st1, st0: ICRW status code

Status code	Meaning
“00” (30h,30h)	No card detected within ICRW
“01” (30h,31h)	Card locates at card Gate
“02” (30h,32h)	Card locates inside ICRW

4.3 Error code

List 1

e1,e0: error code

Error code	Meaning
"00" (30h,30h)	A giveb command code is unidentified
"01" (30h,31h)	Parameter is not correct
"02" (30h,32h)	Command execution is impossoble
"03" (30h,33h)	Function is not implemented
"04" (30h,34h)	Command data error
"05" (30h,35h)	
"06" (30h,36h)	Key for decrypting is not received
"07" (30h,37h)	
"08" (30h,38h)	
"09" (30h,39h)	Intake withdraw timeout
"10" (31h,30h)	Card jam
"11" (31h,31h)	Shutter error
"12" (31h,32h)	
"13" (31h,33h)	Irrdgular card length(long)
"14" (31h,34h)	Irrdgular card length(short)
"15" (31h,35h)	FLASH Memory Parameter Area CRC error
"16" (31h,36h)	Card position Move(and pull out error)
"17" (31h,37h)	Jam error at retrieve
"18" (31h,38h)	Two card error
"19" (31h,39h)	
"20" (32h,30h)	Read mag-card error (verifying faulty (VRC error))
"21" (32h,31h)	Read mag-card error (start character error, end character error or LRC error)
"22" (32h,32h)	
"23" (32h,33h)	Read mag-card error (no data, start character , end character and LRC only)
"24" (32h,34h)	Read mag-card error (no mag-stripe or code)
"25" (32h,35h)	
"26" (30h,36h)	
"27" (32h,37h)	
"28" (32h,38h)	
"29" (32h,39h)	
"30" (33h,30h)	Power down
"31" (33h,31h)	DSR signal is OFF
"32" (33h,32h)	Voltage is higher than 13V
"33" (33h,33h)	Voltage is lower than 10V
"34" (33h,34h)	
"35" (33h,35h)	
"36" (33h,36h)	
"37" (33h,37h)	
"38" (33h,38h)	
"39" (33h,39h)	

List 2

e1,e0: error code

Error code	Meaning
“40” (34h,30h)	Pull Out Error
“41” (34h,31h)	
“42” (34h,32h)	
“43” (34h,33h)	IC Positioning Error
“44” (34h,34h)	
“45” (34h,35h)	
“46” (34h,36h)	
“47” (34h,37h)	
“48” (34h,38h)	
“49” (34h,39h)	
“50” (35h,30h)	Capture Counter Overflow Error
“51” (35h,31h)	
“52” (35h,32h)	
“53” (35h,33h)	
“54” (35h,34h)	
“55” (35h,35h)	
“56” (35h,36h)	
“57” (35h,37h)	
“58” (35h,38h)	
“59” (35h,39h)	
“60” (36h,30h)	Abnormal Vcc condition error of IC card or SAM
“61” (36h,31h)	ATR communication error of IC card or SAM
“62” (36h,32h)	Invalid ATR error to the selected activation for IC card or SAM
“63” (36h,33h)	No response error on communication from IC card or SAM
“64” (36h,34h)	Communication error to IC card or SAM(except for no response)
“65” (36h,35h)	Not activated error of IC card or SAM
“66” (36h,36h)	Not supported IC card or SAM error by ICRM(only for EMV activation)
“67” (36h,37h)	
“68” (36h,38h)	
“69” (36h,39h)	Not supported IC card or SAM error by EMV2000(only for EMV activation)
“73” (37h,33h)	EEPROM error
“B0” (42h,30h)	Not received Initialize command

5 Command explanation of user program code area

5.1 Initialize command

* * * * * => see note1

Command	"C" (43h)	"0" (30h)	pm	"3" (33h)	"2" (32h)	"4" (34h)	"1" (31h)	fm	Pd	Ty	Ds	Cc	30H	30H	30H
----------------	--------------	--------------	----	--------------	--------------	--------------	--------------	----	----	----	----	----	-----	-----	-----

Positive response	"P" (50h)	"0" (30h)	pm	st1	st0	Type recognizing code (ASCII 16 bytes)									
--------------------------	--------------	--------------	----	-----	-----	---	--	--	--	--	--	--	--	--	--

Negative response	"N" (4Eh)	"0" (30h)	pm	e1	e0
--------------------------	--------------	--------------	----	----	----

This command set the operation conditions for ICRW and initializes ICRW.

This command set the operation conditions for ICRW and initializes ICRW

If this command is executed when the card is in the ICRW, the ICRW moves the card according to the parameter of the command.

When the enable condition of the card insertion, this command disables the card insertion condition

This Command returns the ICRW from various error conditions to normal condition

And this command clears the mag stripe data buffer.

Note1: * These parameters have no meaning, but remained for the command format compatibility to the command format of the other models. The parameter codes "0"(30h) to "4"(34h) are admitted as the correct parameter to get positive response with the type recognizing code under the condition that the model type is unknown.

pm: This parameter sets the card move mode

- "0"(30h) Eject the card to the gate portion and finish the command even if the card is not taken out
- "1"(31h) Capture the card to the rear side
- "2"(32h) Re-position the card to the home position in the ICRW
- "3"(33h) Don't move card
- "4"(34h) eject the card to the front side and respond, function is same as "0"(30h)。
- "5"(35h) capture the card from rear side。 Function is same as "1"(31h)。
- "6"(36h) retrieve the card to the reader inside。 The function is same as "2"(32h)。
- "8"(38h) To report the initialization parameter

fm: Not used .Always "0"(30h).

Pd: Power down card control

- "0"(30h) The ICRW ejects the card in the ICRW.(Default value at omit this code)
- "1"(31h) The ICRW does not move the card in the ICRW
- "2"(32h) The ICRW captures the card to the inside of the ICRW
- "3"(33h) The ICRW retrieves the card to the inside of the ICRW

➤ The setting is held in the non volatile memory even after the power on/reset

Ty: Reader type recognition code control

“0”(30h) No data is contained in the response.(Default value at omit this code)

“1”(31h) Response includes type recognition code

Type recognition code (16 bytes)

ISO #1	ISO #2	ISO #3	“0” (30h)	IC contact	RF interface	“0” (30h)	Recovery function	“0” (30h)	shutter	“0” (30h)	SAM1	SAM2	SAM3	SAM4	“0” (30h)
Magnetic head: “0”(30h”) = Not available “1” (31h) =Available				Function: “0”(30h”) = Not available “1” (31h) = Availabel						SAM information: “0”(30h) = Socket is not mounted “1”(31h) = Socket is empty “2”(32h) = SAM is inserted “3”(33h) = SAM is inserted but VCC error					

➤ Ds: no meaning

Cc: Capture counter control

“0”(30h) Turn off the capture counter(default value at omit this code)

“1”(31h) Turn on the capture counter

➤ The setting is held in the non volatile memory even after the power on/reset

Re: reset eject control

Set power on reset with card eject or not。 This set will be saved in nonvolatile memory of the machine。

“0”(30h) open reset function for the card ejecting, ICRW will eject the card to the front in reset.

“1”(31h) close reset function, ICRW doesn't eject the card in reset (default).

“2”(32h) ICRW will capture the card from rear end in reset after power on.

“3”(33h) ICRW will retrieve the card in reset after power on.

➤ This set will be save into non volatile memory

Notes Pd,Ty,Ds,Cc,are omissible。 When Pd,Ty,Ds orCc are not reset,these are set “0”(30h)。

When Pd,Cc are not set,the ICRW control the card according to the previous value

When power failure occurs at the same timing of DSR off,power failure handling routine has priority.

5.2 Status request command

Command	“C” (43h)	“1” (31h)	pm			
Positive response	“P” (50h)	“1” (31h)	pm	st1	st0	Se
Negative response	“N” (4Eh)	“1” (4Bh)	pm	e1	e0	

Negative response is send against status request command if mechanical failure remains from the prior operation.

pm = “0”(30h)

Report current status of after execution of previous command ICRW 。

pm = “1”(31h)

The response is include “Se” (sensor status information,with the staus information obtained.

The locations of sensor are referred to appearance drawing:

	b7							b0	
Se=	0	CAP	PI2	PI1	PD4	PD3	PD2	Card Width Sensor	(binary)

Card Width Sensor	1: card exists 0: card does not exist
PD2	1: card exists 0: card does not exist
PD3	1: card exists 0: card does not exist
PD4	1: card exists 0: card does not exist
PI1	1: shutter open 0: shutter close
PI2	1: IC contact is set 0: IC contact is not set
CAP	1: Capture Sensor connector high level 0: Capture Sensorconnector low level (This connector terminal is pulled up,therefore this bit is 1 when the connector is open or not mount)

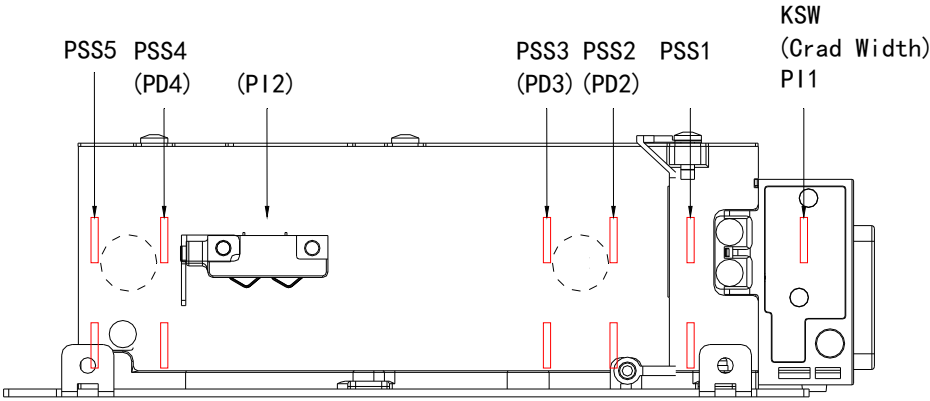
5.3 Sensor status inquiry command

Command	“C” (43h)	“1” (31h)	pm								
Positive response	“P” (50h)	“1” (31h)	pm	st1	st0	PSS1	PSS2	PSS3	PSS4	PSS5	KSW
Negative response	“N” (4Eh)	“1” (4Bh)	pm	e1	e0						

pm = “@”(40h) report current sensors status of ICRW after excuting previous command (6 byte), including present sensors status PSS1..KSW in negative reponse. Specified as following:

Sensor(6 byte)	“1”(31h): card in	“0”(30h): no card
PSS1	“1”(31h): card in	“0”(30h): no card
PSS2	“1”(31h): card in	“0”(30h): no card
PSS3	“1”(31h): card in	“0”(30h): no card
PSS4	“1”(31h): card in	“0”(30h): no card
PSS5	“1”(31h): card in	“0”(30h): no card
KSW	“1”(31h): card in	“0”(30h): no card

Figure: CRT-310 sensors deployment



5.4 Entry command

Command	“C” (43h)	“2” (32h)	pm	mg
---------	--------------	--------------	----	----

Positive response	“P” (50h)	“2” (32h)	pm	st1	st0
-------------------	--------------	--------------	----	-----	-----

Negative response	“N” (4Eh)	“2” (32h)	pm	e1	e0
-------------------	--------------	--------------	----	----	----

This is the acct ot carry the card inside ICRW.This command does not allow ICRW to send response to HOST until ICRW completes to carry the card inside ICRW.

If ICRW can not move the card on the way of carrying it, ICRW sends jam error “10”(31h,30h) to HOST.If another card already stays inside ICRW,ICRW sends error “02”(30h,32h) to HOST.

Send DLE, EOT from HOST in order to cancel this command.

While the card is carried inside ICRW, data on the mag stripe is read to data buffer by ICRW.(Even if read error occurs,ICRWsends positive response to HOST upon completion of carrying the card inside ICRW).

If ICRW is in the ENABLE mode, ICRW sends execution impossible error to HOST.

pm = “0”(30h) To accept the card from front

When receiving the command with this parameter, ICRW becomes card insertion waiting mode.

After detection a card insertion ,ICRW rotate the motor forward and carry the card into inside of ICRW。

When ICRW completes to carry the card to the rear end of ICRW, ICRW closes the shutter,ICRW stops the motor and sends positive response

If the card is pulled out before roller catch the card, ICRW becomes card insertion waiting mode again without error response. Then, if a card is not inserted for 5sec, card ejecting error “40”(34h,30h) will be transmitted to HOST.

pm = “2” (32h) To accept the card from rear

When receiving the command with this parameter, ICRW becomes card insertion waiting mode.

After detection a card insertion ,ICRW rotate the motor forward and carry the card into inside of ICRW。

When ICRW completes to carry the card to the rear end of ICRW, ICRW closes the shutter, ICRW stops the motor and sends positive response.

If the card is pulled out before roller catch the card, ICRW becomes card insertion waiting mode again without error response. Then,if a card is not inserted for 5sec ,card ejecting error “40”(34h,30h) will be transmitted to HOST.

mg = “0”(30h) Mag data detect off

ICRW executes card accept operation without mag data detection.”mg”is omissible and this value is default.

Only use for pm = “0”(30h).

mg = “1”(31h) Mag data detect on

ICRW executes card accept operation with mag data detection.If mag data is not detect,ICRW stops the card 卡 accept operation and eject the card with negative response “24”(32h,34h)(Now mag error)

Only use for pm = “0”(30h).

5.5 Card carry command

Command	“C” (43h)	“3” (33h)	pm		
Positive response	“P” (50h)	“3” (33h)	pm	st1	st0
Negative response	“N” (4Eh)	“3” (33h)	pm	e1	e0

pm = “0” (30h) eject

ICRW moves the card from inside of ICRW to gate with roller on position.

After card was ejected, ICRW executes a status request command ,when it is shown that the card was completely pull out from the gate

It takes a maximum of 10sec after ICRW received a command until it returns a response

If a card is not in ICRW, ICRW will return the positive response directly

pm = “1”(31h) Capture

ICRW moves the card from inside of ICRW rear side

After card was ejected, ICRW executes a status request command ,when it is shown that the card was completely pull out from the gate

It takes 2 maximum of 7sec after ICRW receives a command until it returns a response

If a card is not in ICRW, ICRW sends error “02”(30h,32h) to HOST against receipt of this command

5.6 Retrieve command

Command	“C” (43h)	“4” (34h)	“0” (30h)		
Positive response	“P” (50h)	“4” (34h)	“0” (30h)	st1	st0
Negative response	“N” (4Eh)	“4” (34h)	“0” (30h)	e1	e0

ICRW moves card from gate with roller on position to inside of ICRW

This command is available after eject command

This command does not ensure mag stripe read operation for read command after this command

5.7 LED command

command	“C” (43h)	“5” (35h)	pm	<div> <div>Turn on timer (ASCII 2byte)</div> <div>Turn off timer (ASCII 2byte)</div> </div>	
Positive response	“P” (50h)	“5” (35h)	pm	st1	st0
Negative response	“N” (4Eh)	“5” (35h)	pm	e1	e0

This function controls the LED on front bezel of ICRW.LED on commands for every color is able to changedirectly from the condition of after color on.

pm = “0”(30h) LED off
pm = “1”(31h) LED green on
pm = “2”(32h) LED red on
pm = “3”(33h) LED orange on

The turn ON/OFF time is available for the LED blinking .The turn on time and turn off time are able to be set 点 independently .Each timer values are set by the 0.1second unit which is given as 2 bytes ASCII code therefore, the minimum value 0.1 second and the maximum value is 9.9 second. If these values are omitted, the LED is only turned on. This blinking function does not affect to the other functions

Ex: Green LED blinking turn on time=1.0 sec. turn off time=0.5sec.=> “C511005”。

5.8 Mag-track read command

Command	“C” (43h)	“6” (36h)	pm			
Positive response	“P” (50h)	“6” (36h)	pm	st1	st0	Read data (ASCII max 219byte (pm= “5”(35h)))
Negative response	“N” (4Eh)	“6” (36h)	pm	e1	e0	Read data (ASCII max 104byte (pm= “;”(3Bh)))

pm = “1”(31h) read data on track#1
pm = “2”(32h) read data on track #2
pm = “3”(33h) read data on track#3

When ICRW takes in a card ,the magnetic data read into the buffer is edited and is converted into an ASCII 当卡 code.If this data is normal ,it will transmit to HOST as read data

The data transmitted to HOST excepting the start code, end code, and LRC on mag stripes

The command with the above parameters allows ICRW not to read the card, but only to transmit the data of buffer, which have been normally read during the card acceptance.

When read error occurs, ICRW sends negative response

In case of card jamming, ICRW sends negative response too.

When the card has no magnetic track, ICRW makes no retrying and sends negative response(error code “24”(32h,34h) is not magnetic track).

When the card has a track with the sentinels but no data,ICRW sends negative response(error code “23(32h,33h))。

Ex:

<p>Track# 1 (max 76 bytes)</p> <p style="padding-left: 40px;">bit 5 4 3 2 1 0</p> <p>data=0 0 1 0 0 0 0 -> 30h</p> <p>data=A 1 0 0 0 0 1 -> 41h</p> <p>track #3 (max 104bytes)</p> <p style="padding-left: 40px;">bit 3 2 1 0</p> <p>data=0 0 0 0 0 -> 30h</p> <p>data=9 1 0 0 1 -> 39h</p>	<p>track #2 (max 37bytes)</p> <p style="padding-left: 40px;">bit 3 2 1 0</p> <p>data=0 0 0 0 0 -> 30h</p> <p>data=9 1 0 0 1 -> 39h</p>
--	---

pm = “5”(35h) all tracks simultaneous read and transmit

The contents of read data are the order of track 1 data, track 2 data and track 3 data.

Among those, a maximum of three tracks to which ICRW corresponds are transmitted by HOST on both sides of separator “~”(7EH).

When one of the tracks is not read, its data area becomes blank

Either of the tracks are not read ,error “20”(32h,30h), “21”(32h,32h), “23”(32h,33h)or “24”(32h,34h)is send to HOST

EX:

Track 1data	“~”(7Eh)	Track 2 data	“~”(7Eh)	Track 3 data	(max 219bytes)
-------------	----------	--------------	----------	--------------	----------------

pm = “7”(37h) Indicateds in response if track is eccod/not encoded

ICRW does not carry the card.

ISO#1: “0”(30h): ISO # 1is not eccoded . “1”(31h): ISO #1 is encoded.

ISO#2: “0”(30h): ISO # 2is not eccoded . 1”(31h): ISO #2 is encoded.

ISO#3: “0”(30h): ISO # 3is not eccoded . “1”(31h): ISO #3 is encoded.

ISO#1	ISO#2	ISO#3	“0”(30h)
-------	-------	-------	----------

pm = “9”(39h) read data on ISO track #1 by another way

pm = “:”(3Ah) read data on ISO track #2 by another way

pm = “;”(3Bh) read data on ISO track #3 by another way

The above parameters differ from pm= “1”(31h), “2”(32h), “3”(33h) in the following contents:

If the parity error occurs, the ICRW tries to send the data row before the error portion.

This partial readied data is concatenated the negative response

If start sentinel is not detected, ICRW does not data.

5.9 Intake/withdraw command

Command	“C” (43h)	“9” (39h)	pm	Timer value (ASCII 2bytes)		
Positive response	“P” (50h)	“9” (39h)	pm	st1	st0	Se (1bytes)
Negative response	“N” (4Eh)	“9” (39h)	pm	e1	e0	Se (1bytes)

This command executes the wait of the card insertion and the intake, or the card eject and the wait of the pull out.

The setting unit of the card waiting time is second.The meaning of the setting values are following

Watching time	Watching function	Response at time out
Omit	Infinite time	Not time out
00 second	Waiting 0.1sec	Positive response(The card condition can be recognized by the st1,st0 bytes of the positive response)
01 second	Waiting 1sec	Negative response
99second	Waiting 99sec	Negative response

The positive response is send when the ICRW detects the card pull out or the finishing of the card intake

Each command is able to be executed and check the status even after the time out

The negative response is send immediately, when the card jamming occur.

The positive response and negative response is sent with the card sensor status byte Se.

The setment of Se bytes and meaning as follow:

	b7							b0	
Se=	0	CAP	PI2	PI1	PD4	PD3	PD2	Card Width Sensor	(binary)

Card Width Sensor	1: card exists 0: card does not exist
PD2	1: card exists 0: card does not exist
PD3	1: card exists 0: card does not exist
PD4	1: card exists 0: card does not exist
PI1	1: shutter open 0: shutter close
PI2	1: ICcontact is set 0: IC contact is not set
CAP	1: Capture Sensor connector high level 0: Capture Sensor connector low level (This connector terminal is pulled up,therefore this bit is 1 when the connector is open or not mount)

pm="0" Withdraw command (card eject and waiting pull out)

(30h) This command disables the card intake, ejects the card and watch the ejected card pull out.

The positive response is sent immediately, if the ICRW receive this command after the card pull out.

pm="1" Intake command (waiting card insertion and take in the card)

(31h) This command enables the card intake and watch the finishing of the card intake.

The positive response is sent immediately, if the ICRW receive this command after the card intake.

The intake enable state is kept after the time out. Therefore, the card can be take in the interval of the sequential intake command. If the time out is occur while the card intake, the card intake is continued and negative response is sent.

pm="2" Intake command with magnetic records detection (waiting card insertion and take in the card with magnetic records check).

This command check the magnetic record while the intake.

The no magnetic records error "24"(32h,34h) is sent, if the magnetic records are not detected.

The decode error of the magnetic records are not checked in this command.

Note 1) Intake mode disabled automatically in case of the following conditions.

*Receipt of Initialize command.

*When power failure occurred.

*ICRW detects DSR signal off.

5.10 Enable / Disable command

Command	“C” (43h)	“.” (39h)	pm	mg or set_time (1byte)	
Positive response	“P” (50h)	“.” (39h)	pm	st1	st0
Negative response	“N” (4Eh)	“.” (39h)	pm	e1	e0

Control command to accept/inhibit card entry. ICRW sends response upon receipt of this command .

ICRW status should be recognized by Status request command from HOST.

Choose Enable/Disable command or Entry command according to customer's control system.

Although a card will be taken in if the enable command is executed when the discharged card is in a gate position , the reading result of magnetic data is not guaranteed.

Since execution of the enable command and the entry command cannot be performed.

pm="0" Enable to accept card. (Enable mode)

(30h) ICRW is changed into a card entry state, and positive response is immediately transmitted to HOST.

And ICRW detected insertion of a card at a gate, it will rotate a motor in the right direction and will take in a card to inside. If a card is drawn out before being taken in by the roller, ICRW will suspend a motor and will be again set to card entry state.

If a card is conveyed to an internal rear side, motor will stop its rotation and a shutter will be closed automatically. In this operation, a response is not transmitted to HOST.

Mg="0" mag data detect off

(31h) ICRW executes card accept operation with mag data detection. If mag data is not detect, ICRW stops the card accept operation and eject the card with negative response "24"(32h,34h).(No mag error)

The point of mag data detection is approx. 15mm from card front edge.

Pm="1" Disable to accept card. (Disable mode)

(31h) It changes into a prohibition state from the permission state of accepting a card.

Pm="X" (58h) Command to accept card with shake from front edge.

The mode of Set-time control to accept card with shake

set_time = "0"(30h) Disable to accept card with shake

set_time = "1"(31h) Accept card with shake for a single

pm = "A"(41h) Enable to accept card from back (Enable mode)

It changes into a card entry state and positive response is immediately transmitted to HOST.

And ICRW detected insertion of a card at a gate, it will rotate a motor in the right direction and will take in a card to inside. If a card is drawn out before being taken in by the roller, ICRW will suspend a motor and will be again set to card entry state.

If a card is conveyed to an internal rear side, motor will stop its rotation and a shutter will be closed automatically. In this operation, a response is not transmitted to HOST

pm = "@"(40h) Disable to accept card. (Disable mode)

It changes into a prohibition state from the permission state of accepting a card.

Notes: 1) Enable mode change automatically to disable mode in case of the following conditions.

- *Receipt of Initialize command.
- *When power failure occurred.
- *ICRW detects VBUS signal off.

5.11 Sensor Level transmit command

Command	“C” (43h)	“>” (3Eh)	“0” (30h)										
Positive response	“P” (50h)	“>” (3Eh)	“0” (30h)	st1	st0	v1h	v1l	v2h	v2l	v3h	v3l	v4h	v4l
Negative response	“N” (4Eh)	“>” (3Eh)	“0” (30h)	e1	e0								

This command converts voltage level of photo sensor from Analog to Digital and reports the value.

“vih”, “vil” are upper nibble and lower nibble divided from 1 byte of A/D conversion value and ‘0’(30h) added respectively.

Ex): A/D data=E5h

Convert to the Voltage data.

E5h=229(decimal)=>5[V] (229/255)=4.5[V]=>”4”(34h),vil=”5”(35h)

Comparison of vi and each sensor is as follows;

V1:PD1, v2:PD2 v3: PD3 v4: PD4

5.12 Control command for contact IC card moving

Command	“C” (43h)	“@” (40h)	pm		
Positive response	“P” (50h)	“@” (40h)	pm	st1	st0
Nagtive response	“N” (4Eh)	“@” (40h)	pm	e1	e0

Control contacting or releasing for IC contact.

If there's no card, ICRW sends an error code “02”(30h,32h)。

pm = “0”(30h) Moving card and touching with IC contact .

If it's error, operation tolerance is two times, if it's still error, sends nagtive information to HOST.

If it's ok, moving again.

When ICRW receives initial command, it automatically releases contact and moves card according to requirement.

pm = “1”(31h) again move to the IC card position

if the card is not in the IC card position, move the card to the IC card position and contacting.

If the card is in the IC card position, release the contacts first, separate the contact from the IC card position, after that again move to the IC card position and contact it.

pm = “2”(32h) Releasing contact and moving to rear position of the Mag-head.

If there is no card at the position of IC card, directly move to rear position of the Mag-head and send positive information to HOST.

5.13 Revision command

Command	“C” (43h)	“A” (41h)	pm
----------------	--------------	--------------	----

Positive response	“P” (50h)	“A” (41h)	pm	st1	st0	Revision data (ASCII 8bytes) Approval Number (ASCII max 22bytes)
--------------------------	--------------	--------------	----	-----	-----	---

Negative response	“N” (4Eh)	“A” (41h)	pm	e1	e0
--------------------------	--------------	--------------	----	----	----

- pm = “1”(31h) Indicates User program code area revision in positive response. (Data length=8)
Ex: “A-1308 8”。
- pm = “2”(33h) Indicates EMV controller’s firmware revision in positive response. (Data length=8)
Ex: “E-081215”。
- pm = “3”(33h) Sends the EMV approval number to HOST (Data length=21). Before EMV approved, 21 bytes space characters return. EMV approval number is checked by specification.
Ex: “11993 1106 400 20 BCT”。
- pm = “4”(34h) (Reserve)
Note: This parameter is left for compatibility with an old ICRW. 22 bytes space charactes return.
- pm = “5”(35h) Sends the IFM Identification of the EMV approval to HOST (Data length=11). IFM Identification is checked by specification. Ex: “IFM310N0100”。

5.14 Counter common

Command	“C” (43h)	“C” (43h)	pm	Counter value (ASCII Max 3bytes)	
Positive response	“P” (50h)	“C” (43h)	pm	st1	st0
Negative response	“N” (4Eh)	“C” (43h)	pm	e1	e0

pm = “2”(32h) This command reports cards pass count of the card transport in the ICRW.
One pass is one round trip of the card in the transport.
The pass count number is reported as the seven digit of ASCII decimal number.

pm = “3” This command is for the capture counter function.
(33h) This command reports the cards capture count from the card transport to the back end of the ICRW.
The count up function operates by the Cc parameter setup of the initialize command.
The capture count number is reported as the three digit of ASCII decimal number from “000” to “999”.
The capture command is executed when the capture count number is over the alert count set by below function, the capture operation performs to usual and transmits the capture counter overflow bellow function, the capture operation performs to usual and transmits the capture counter overflow error “50”(35h,30h) to the HOST.

pm = “4”(34h) This command is for the capture counter function.
This command sets the capture alert count number and clear the capture counter in the ICRW.
The set capture alert count should be the three digit of ASCII decimal number from “000” to “999”

pm = “5”(35h) This command is for the capture counter function.
The command only sets the capture alert count number in the ICRW.
The set capture alert count should be the three digit of ASCII decimal number from “000” to “999”The capture counter is not cleared by this command.

pm = “6”(36h) This command is for the capture counter function.
This command only clear the capture counter in the ICRW.
The capture alert count is not changed by this command and kept the previous setting value.
The counter value should not be added for this command.

5.15 IC Card control command

5.15.1 Activate ICC command

Command	“C” (43h)	“I” (49h)	“0” (30h)	Vcc (1byte)	
Positive response	“P” (50h)	“I” (49h)	“0” (30h)	st1	st0 ATR (Binary max 65 bytes)
Negative response	“N” (4Eh)	“I” (49h)	“0” (30h)	e1	e0 ATR (Binary max 65bytes)

This command activates an IC card. The ICRW supplies power (VCC) and clock (CLK), and releases reset(RST).

Vcc = “0”(30h)

The ICRW supplies +5V to the VCC and activates according to the EMV version 4.2.

Vcc = “3”(33h)

The ICRW supplies +5V to the VCC and activates according to the ISO/IEC7816-3:2006.

Vcc = “5”(35h)

The ICRW supplies +3V to the VCC and activates according to the ISO/IEC7816-3:2006.

After receiving the ATR, the ICRW changes the voltage of the VCC in accordance with the T=15 value of the ATR.

Vcc = “6”(36h)

The ICRW supplies with +5V to the VCC and activates according to the ISO/IEC7816-3:2006. After receiving the ATR, the ICRW changes the voltage to the VCC in accordance with the T=15 value of the ATR.

Vcc = “8”(38h)

The ICRW activates ICC according to ISO/IEC7816-3:2006. VCC is supplied in order of 5V, 3V, and 1.8V.

Vcc = “@”(40h)

The ICRW supplies +5V to the VCC and activates according to the MONEO card specification.

The Vcc parameter can be omitted, and the default value is “0”(30h).

Note:

Vcc=30H is used on EMV comply card.

Vcc=33H is used on old ISO/IEC7816-3 card. (Only 5V card)。

Vcc=35H(VCC=3V then 5V), Vcc=36H(VCC=5V then 3V) and Vcc=38H(5V,3V then 1.8V) are used on ISO/IEC7816-3:2006 card.

Also, Answer to reset (ATR) from the IC card is received and transmitted to the HOST.

ATR	TS	T0	TA1	TB1	...	TCK
-----	----	----	-----	-----	-----	-----

INTERFACE SPECIFICATION	CRT-310-NU01	35/90
-------------------------	--------------	-------

When a power failure is detected while a power supply is supplied to the IC card, the error code “60”(36,30) is returned.

If the activation error is occurred, the ICRW initiate the deactivation sequence, and sends the error code “61”(36h,31h), “63”(36h,33h) or “64”(36h,34h).

When the Vcc parameter “0”(30h) is selected and ATR value is not based on the EMV, the ICRW initiate the deactivation sequence, and sends the error code “69”(36h,39h).

When the VCC parameter “3”(33h), “5”(35h), “6”(36h) or “8”(38h), are selected and the ATR value is not supported by the ICRW, the ICRW initiates the deactivation sequence, and sends the error code “66”(36h,36h)。

The Vcc parameter is not related to the IC card communication. The IC card communication complies with the EMV version 4.2.

The activation command “CI@”(Vcc= “@”(40h)) is only for the MONEO application with the MONEO card. For the other application (CB, EMV and the others) with the MONEO card , the activation commands “C100”, “C103”, “C105”, “C108” are available.

The IC card automatic communication command “C19” must be used after the ICC activation by “C10” (ISO7816 or EMV)。

5.15.2 Deactivate ICC command

Command	“C” (43h)	“I” (49h)	“1” (31h)		
Positive response	“P” (50h)	“I” (49h)	“1” (31h)	st1	st0
Negative response	“N” (4Eh)	“I” (49h)	“1” (31h)	e1	e0

The Command deactivates the IC card.

The timing chart of close IC card refer to relevant standard ISO7816 or EMV

5.15.3 Inquire ICC status command

Command	“C” (43h)	“I” (49h)	“2” (32h)			
Positive response	“P” (50h)	“I” (49h)	“2” (32h)	st1	st0	sti (1byte)
Negative response	“N” (4Eh)	“I” (49h)	“2” (32h)	e1	e0	

The ICRW reports the state of the IC card in the sti of a positive response

The definition of every bit of sti is presented as following:

	b7	b6	b5	b4	b3	b2	b1	b0
sti=	0	1	0	V18	CLK1	CLK0	V5V3	Active

sti

b7	b6	b5	b4	b3	b2	b1	b0	content
0	1	0	X	-	-	-	-	V18
0	1	0	0	-	-	-	-	-VCC is defined by V5V3
0	1	0	1	-	-	-	-	-VCC=1.8V

0	1	0	-	X	X	-	-	CLK frequency
0	1	0	-	0	0	-	-	-No clock
0	1	0	-	0	1	-	-	-CLK=3.58MHz
0	1	0	-	1	0	-	-	-CLK=7.16MHz
0	1	0	-	1	1	-	-	-Reserve
0	1	0	-	-	-	X	-	V5V3
0	1	0	-	-	-	0	-	-VCC=5V if V18=0
0	1	0	-	-	-	1	-	-VCC=3V if V18=0
0	1	0	-	-	-	-	X	Active
0	1	0	-	-	-	-	0	-Inactive
0	1	0	-	-	-	-	1	-Active

While a power supply is supplied to the IC card, the ICRW monitors the VCC (the power supply line of the 当卡 IC card). The error “60”(36h,30h) is returned when a power failure is detected.

5.15.4 ICC communication T=0

Command	“C” (43h)	“I” (49h)	“3” (33h)	C-APDU (Binary max. 261 bytes)
----------------	--------------	--------------	--------------	-----------------------------------

Positive response	“P” (50h)	“I” (49h)	px	st1	st0	R-APDU (Binary max. 258 bytes)
--------------------------	--------------	--------------	----	-----	-----	-----------------------------------

Negative response	“N” (4Eh)	“I” (49h)	“3” (33h)	e1	e0
--------------------------	--------------	--------------	--------------	----	----

This command exchanges data with the IC card using protocol T=0.

In this command, the HOST has to set the “C-APDU” data.

C-APDU	CLA	INS	P1	P2	Lc	Data1	...	Data(Lc)	Le
--------	-----	-----	----	----	----	-------	-----	----------	----

THE ICRW returns the “R-APUD” data to the HOST.

R-APDU	Data1	Data(Licc)	SW1	SW2
--------	-------	------------	-----	-----

px = “3”(33h) The received data from the IC card is 258 bytes or less.

px = “5”(35h) The received data from the IC card is 259 bytes or more.

The ICRW requires the following R-APDU data receiving.

The HOST has to receive the remaining R-APDU data using the “CI7” comand

The maximum data size which can be handled with the ICRW is 261 bytes. If the ICRW receives 262 bytes data from the HOST, the ICRW sends the error code "04"(30h,34h) to the HOST. The maximum

length of the R-APDU in the positive response is 258 bytes. If the R-APDU length from the IC card is 259 bytes or more, the ICRW returns the response with the parameter px="5"(35h) and first 258 bytes data. The remaining R-APDU data are sent as the positive response data of the command "CI7".

While a power supply is supplied to the IC card, the ICRW monitors the VCC (the power supply line of the IC card). The ICRW is returned the error code "60"(36h,30h) when a power failure is detected.

If the protocol type of the IC card is not T=0, error code "62"(36h,32h) is sent.

If IC card does not respond within WWT(Working Wait Time), the ICRW deactivates the IC card and the error code "63"(36h,33h) is sent.

If any other protocol error occurs, the ICRW deactivates the IC card and the error code "64"(36h,34h) is sent.

If HOST tries to communicate before the IC card activation, the error code "65"(36h,35h) is sent.

Note) Licc is the data length which the IC card returns. Please refer to the specifications of the IC card about Licc.

5.15.5 ICC communication T=1

Command	"C" (43h)	"T" (49h)	"4" (34h)	C-APDU (Binary max 261bytes)	
Positive response	"P" (50h)	"T" (49h)	px	st1	st0
Negative response	"N" (4Eh)	"T" (49h)	"4" (34h)	e1	e0

R-APDU
(Binary max 258bytes)

This command exchanges data with the IC card using the protocol T=1.

In this command, the HOST has to set the "C-APDU" data. The ICRW adds the Prologue field and the Epilogue field to the "C-APDU", and sends to the IC card.

If the C-APDU length is greater than the information field size for the IC card (IFSC), the ICRW divides the C-APDU into several consecutive blocks.

C-APDU				CLA	INS	P1	P2	Lc	Data1	..	Data(Lc)	Le	
				↓	↓	↓	↓	↓	↓	↓	↓	↓	
chip data	NAD	PCB	LEN	CLA	INS	P1	P2	Lc	Data1	..	Data(Lc)	Le	EDC
	Prologue field			Information field									Epilogue field

The ICRW sets the R-APDU data which received from the IC card into the positive response, and transmits to the HOST.

chip data	Prologue fiel			Information field					Epilogue field
	NAD	PCB	LEN	Data1	...	Data(Licc)	SW1	SW2	EDC
				↓	↓	↓	↓	↓	
R-APDU				Data1	...	Data(Licc)	SW1	SW2	

px = "4"(34h) The received R-APDU from the IC card is 258 bytes or less.

px = "5"(35h) The received R-APDU from IC card is 259 bytes or more.
The ICRW requires the following R-APDU receiving to the HOST.
The HOST has to receive the remaining R-APDU data using "CI7" command.

px = "?"(3Fh) The ICRW received the S(ABORTrequest) block from the IC card, suspended the data transmission to the IC card, and deactivated the IC card. The HOST has to stop the following data transmitting.

The maximum data size which can be handled by the ICRW is 261 bytes. If the ICRW receives more than 262 bytes data from the HOST, the ICRW sends the error code "04"(30h,34h) to the HOST.

When the C-APDU data size is 262 bytes or more, the HOST has to transmit the C-APDU exceeding 261 bytes using the command "CI5" or "CI6".

The maximum length of the R-APDU in the positive response is 258 bytes. If the R-APDU length from the IC card is 259 bytes or more, ICRW returns the response with the parameter px="5"(35h) and first 258 bytes data. The remaining R-APDU data are sent as the positive response data of the command "CI7".

While a power supply is supplied to the IC card, the ICRW monitors the VCC (the power supply line of the IC card). The error "60"(36h,30h) is returned when a power failure is detected.

If the protocol type of IC card is not T=1, the error code "62"(36h,32h) is sent.

If the IC card does not respond within BWT(Block Waiting Time) or CWT(Character Waiting Time), the ICRW deactivates the IC card and the error code "63"(36h,33h) is sent.

If any other protocol error occurs, the ICRW deactivates the IC card and the error code "64"(36h,34h) is sent.

If the HOST tries to communicate before the IC card activation, the error code "65"(36h,35h) is sent.

In case there is any trouble in the sequence of command receiving, the error code "02"(30h,32h) is sent. If the error code "02"(30h,32h) is sent, please re-start from the activation.

Note) The Licc is data length which the IC card returns. Please refer to specifications of the IC card about length of Licc.

5.15.6 ICC extended communication 1

Command	"C" (43h)	"I" (49h)	"5" (35h)	C-APDU (Binary max 261bytes)	
Positive response	"P" (50h)	"I" (49h)	px	st1	st0
Negative response	"N" (4Eh)	"I" (49h)	"5" (35h)	e1	e0

This command transmits the C-APDU exceeding 261 bytes to the IC card. The HOST has to divide the C-APDU into 261 bytes or less and transmits using this command repeatedly.

px = "7"(37h)

The ICRW requires the following C-APDU data to the IC card. There is no data portion of the positive response.

The HOST has to transmit the remaining C-APDU data using the command "CI5" or "CI6".

px = “?”(3Fh)

The ICRW received the S(ABORTrequest) block from the IC card, suspended the data transmission to the IC card, and deactivated the IC card. The HOST has to stop the following data transmitting.

While a power supply is supplied to the IC card, the ICRW monitors the VCC (the power supply line of the IC card). The error code "60" is returned when a power failure is detected.

If the protocol type of the IC card is not T=1, the error code "62"(36h,32h) is sent.

If the IC card does not respond within BWT(Block Waiting Time) or CWT(Character Waiting Time), the ICRW deactivates the IC card and error code "63"(36h,33h) is sent.

If any other protocol error occurs, the ICRW deactivates the IC card and the error code "64"(36h,34h) is sent.

If the HOST tries to communicate before the IC card activation, the error code "65"(36h,35h) is sent.

5.15.7 ICC extended communication 2

Command	“C” (43h)	“T” (49h)	“6” (36h)	C-APDU (Binary max 261bytes)	
Positive response	“P” (50h)	“T” (49h)	px	st1	st0
Negative response	“N” (4Eh)	“T” (49h)	“6” (36h)	e1	e0

R-APDU
(Binary max 258bytes)

This command is used for transmitting the last part of the devided C-APDU. The size of the last data which can be transmitted is 261 bytes or less.

px = “4”(34h) The received R-APDU from the IC card is 258 bytes or less.

px = “5”(35h) The received R-APDU from the IC card is 259 bytes or more.
The ICRW requires the following R-APDU data receiving.
The HOST has to receive the remaining R-APDU data using the "CI7" command.

px = “?”(3Fh) The ICRW received the S(ABORTrequest) block from the IC card, suspended the data transmission to the IC card, and deactivated the IC card. The HOST has to stop the following data transmitting.

While a power supply is supplied to the card, the ICRW monitors the VCC (the power supply line of the card). The error "60"(36h,30h) is returned when a power failure is detected.

If protocol type of the IC card is not T=1, the error code "62"(36h,32h) is sent.

If the IC card does not respond within BWT(Block Waiting Time) or CWT(Character Waiting Time), the ICRW deactivates the IC card and error code "63"(36h,33h) is sent.

If any other protocol error occurs, the ICRW deactivates the IC card and the error code "64"(36h,34h) is sent.

If the HOST tries to communicate before the IC card activation, the error code "65"(36h,35h) is sent.

5.15.8 ICC extended communication 3

Command	“C” (43h)	“T” (49h)	“7” (37h)
----------------	--------------	--------------	--------------

INTERFACE SPECIFICATION	CRT-310-NU01	41/90
--------------------------------	--------------	-------

Positive response

"P" (50h)	"T" (49h)	px	st1	st0
--------------	--------------	----	-----	-----

R-APDU (Binary max 258bytes)

Negative response

"N" (4Eh)	"T" (49h)	"7" (37h)	e1	e0
--------------	--------------	--------------	----	----

This command is used for receiving the divided R-APDU exceeding 258 bytes. The HOST has to receive all of the remaining R-APDU data using this command repeatedly until the response of this command becomes px="6"(36h).

px = "5"(35h) The received R-APDU from the IC card is 259 bytes or more.
The ICRW requires the following R-APDU data receiving.
The HOST has to receive the remaining R-APDU data using "CI7" command.

px = "6"(36h) There is no remaining R-APDU data from the IC card.

px = "?"(3Fh) The ICRW received the S(ABORTrequest) block from the IC card, suspended the data transmission to the IC card, and deactivated the IC card. The HOST has to stop the following data transmitting.

While a power supply is supplied to the card, the ICRW monitors the VCC (the power supply line of the card). The error "60"(36h,30h) is returned when a power failure is detected.

If the IC card does not respond within WWT(T=0), BWT(T=1) or CWT(T=1), ICRW deactivates the IC card and the error code "63"(36h,33h) is sent.

If any other protocol error occurs, the ICRW deactivates the IC card and the error code "64"(36h,34h) is sent.

If HOST tries to communicate before an IC card activation, the error code "65"(36h,35h) is sent.

5.15.9 ICC warm reset

Command

"C" (43h)	"T" (49h)	"8" (38h)
--------------	--------------	--------------

Positive response

"P" (50h)	"T" (49h)	"8" (38h)	st1	st0	ATR (Binary max 65bytes)
--------------	--------------	--------------	-----	-----	-------------------------------

Negative response

"N" (4Eh)	"T" (49h)	"8" (38h)	e1	e0	ATR (Binary max 65bytes)
--------------	--------------	--------------	----	----	-----------------------------

The ICRW sends a reset pulse, keeping the state where the IC card is activated (VCC,CLK), and receives the ATR from the IC card again (Warm Reset).

If the ATR is not supported by the ICRW with the selected condition at the activate command, the ICRW initiate the deactivation sequence, and sends the error code "66"(36h,36h) or "69"(36h,39h) with the ATR.

If the ATR receive error is occurred, the ICRW initiate the deactivation sequence, and sends the error code " 61"(36h,31h), "63"(36h,33h) or "64"(36h,34h).

The ICRW returns error code "65"(36h,35h) if the IC card does not activated.

While a power supply is supplied to the IC card, the ICRW monitors the VCC (the power supply line of the IC card). The error code "60"(36h,30h) is returned when a power failure is detected.

5.15.10 ICC automatic communication

Command	“C” (43h)	“T” (49h)	“9” (39h)	C-APDU ((Binary max 261 bytes)	
Positive response	“P” (50h)	“T” (49h)	px	st1	st0
Negative response	“N” (4Eh)	“T” (49h)	“9” (39h)	e1	e0

R-APDU
(Binary max 258bytes)

This command exchanges data with the IC card using the protocol T=0 or T=1. These protocols are selected automatically by the ICRW. In this command, the HOST has to set "C-APDU" data. Other functions are same as "C13" or "C14".

px = “4”(34h) The received R-APDU from the IC card is 258 bytes or less.

px = “5”(35h) The received R-APDU from the IC card is 259 bytes or more.
The ICRW requires the following R-APDU data receiving.
The HOST has to receive the remaining R-APDU data using "C17" command.

px = “?”(3Fh) The ICRW received the S(ABORTrequest) block from the IC card, suspended the data transmission to the IC card, and deactivated the IC card. The HOST has to stop the following data transmitting.

While a power supply is supplied to the IC card, the ICRW monitors the VCC (the power supply line of the card). The ICRW is returned the error code "60"(36h,30h) when a power failure is detected.

If the IC card does not respond within WWT(T=0), BWT(T=1) or CWT(T=1), the ICRW deactivates the IC card and error code "63"(36h,33h) is sent.

If any other protocol error occurs, the ICRW deactivates the IC card and the error code "64"(36h,34h) is sent.

If the HOST tries to communicate with this command before the IC card activation, the error code "65"(36h,35h) is sent.

When the protocol is T=1 and C-APDU data is 262 bytes or more, the HOST has to use "C15" and "C16" to sends the following C-APDU data.

5.16 SAM (Secure Application Module) control command

5.16.1 Activate SAM command

Command	“C” (43h)	“I” (49h)	“@” (40h)	Vcc (1byte)		
Positive response	“P” (50h)	“I” (49h)	“@” (40h)	st1	st0	ATR (Binary max 65bytes)
Negative response	“N” (4Eh)	“I” (49h)	“@” (40h)	e1	e0	ATR (Binary max 65bytes)

This command activates a SAM. The ICRW supplies power (VCC) and clock (CLK), and releases reset (RST).

Vcc = “0”(30h)

The ICRW supplies +5V to the VCC and activates according to the EMV version 4.2.

Vcc = “3”(33h)

The ICRW supplies +5V to the VCC and activates according to the ISO/IEC7816-3:2006.

Vcc = “5”(35h)

The ICRW supplies +3V to the VCC and activates according to the ISO/IEC7816-3:2006.

After receiving the ATR, the ICRW changes the voltage of the VCC in accordance with the T=15 value of the ATR.

Vcc = “6”(36h)

The ICRW supplies with +5V to the VCC and activates according to the ISO/IEC7816-3:2006. After receiving the ATR, the ICRW changes the voltage to the VCC in accordance with the T=15 value of the ATR.

Vcc = “8”(38h)

The ICRW activates ICC according to ISO/IEC7816-3:2006. VCC is supplied in order of 5V, 3V, and 1.8V.

Vcc = “@”(40h)

The ICRW supplies +5V to the VCC and activates according to the MONEO card specification.

The Vcc parameter can be omitted, and the default value is "0"(30h).

Note) Vcc=30H is used on EMV comply card.

Vcc=33H is used on old ISO/IEC7816-3 card. (only 5v card)

Vcc=35H (VCC=3V then 5V), Vcc=36H(VCC=5V then 3V) and Vcc=38H(5V, 3V then 1.8V) are used on ISO/IEC7816-3:2006 card.

Also, Answer To Reset (ATR) from the SAM is received and transmitted to the HOST.

ATR	TS	T0	TA1	TB1	...	TCK
-----	----	----	-----	-----	-----	-----

When a power failure is detected while a power supply is supplied to the SAM, the error code "60"(36h,30h) is returned.

If the ATR receive error is occurred, the ICRW initiate the deactivation sequence, and sends the error

code " 61"(36h,31h), "63"(36h,33h) or "64"(36h,34h).

When the Vcc parameter "0"(30h) is selected and the ATR value is not based on the EMV2000 ver.4.0, the ICRW initiate the deactivation sequence, and sends the error code " 69"(36h,39h).

When the Vcc parameter "3"(33h), "5"(35h) or "6"(36h) are selected and the ATR value is not supported by the ICRW, the ICRW initiates the deactivation sequence, and sends the error code " 66"(36h,36h).

The Vcc parameter is not related to the SAM communication. The SAM communication complies with the EMV version 4.2

The activation command "CI@@ " (Vcc=@"(40h)) is only for the MONEO application with the MONEO card. For the other application (CB, EMV and others) with the MONEO card, the activation commands "CI@0", "CI@3", "CI@5" , "CI@6" or "CI@8" are available.

Please refer the time chart of the SAM activating sequence to related standard (ISO7816 or EMV)

5.16.2 Deactivate SAM command

Command	"C" (43h)	"I" (49h)	"A" (41h)		
Positive response	"P" (50h)	"I" (49h)	"A" (41h)	st1	st0
Negative response	"N" (4Eh)	"I" (49h)	"A" (41h)	e1	e0

This command deactivates the SAM.

Please refer the time chart of the SAM deactivating sequence to related standard (ISO7816 or EMV)

5.16.3 Inquire SAM status command

Command	“C” (43h)	“I” (49h)	“B” (42h)				
Positive response	“P” (50h)	“I” (49h)	“B” (42h)	st1	st0	sti (1byte)	stj (1 byte)
Negative response	“N” (4Eh)	“I” (49h)	“B” (42h)	e1	e0		

The ICRW reports the state of the SAM in the sti of the positive response

sti

b7	b6	b5	b4	b3	b2	b1	b0	Content
0	1	0	X	-	-	-	-	V18
0	1	0	0	-	-	-	-	- VCC is defined by V5V3
0	1	0	1	-	-	-	-	-VCC=1.8V
0	1	0	-	X	X	-	-	CLK frequency
0	1	0	-	0	0	-	-	- No clock
0	1	0	-	0	1	-	-	-CLK=3.58MHz
0	1	0	-	1	0	-	-	-CLK=7.16MHz
0	1	0	-	1	1	-	-	- Reserve
0	1	0	-	-	-	X	-	V5V3
0	1	0	-	-	-	0	-	- VCC=5V if V18=0
0	1	0	-	-	-	1	-	- VCC=3V if V18=0
0	1	0	-	-	-	-	X	Active
0	1	0	-	-	-	-	0	- Inactive
0	1	0	-	-	-	-	1	- Active

And also, ICRW reports the number of the selected SAM with stj. Before selecting SAM number, ICRW responds that ICRW selects SAM1 as default.

	b7							b0	
stj=	0	0	1	1	0	X	X	X	(binary)
	XXX: Selected number								
	000: SAM1								
	001: SAM2								
	002: SAM3								
	003: SAM4								

While a power supply is supplied to the SAM, the ICRW monitors the VCC (the power supply line of the SAM). The error "60"(36h,30h) is returned when a power failure is detected.

5.16.4 SAM Communication T=0

Command	"C" (43h)	"T" (49h)	"C" (43h)	C-APDU (Binary max 261bytes)	
Positive response	"P" (50h)	"T" (49h)	px	st1	st0 R-APDU (Binary max 258bytes)
Negative response	"N" (4Eh)	"T" (49h)	"C" (43h)	e1	e0

This command exchanges data with the SAM using protocol T=0. In this command, the HOST has to set the "C-APDU" data.

C-APDU	CLA	INS	P1	P2	Lc	Data1	...	Data(Lc)	Le
--------	-----	-----	----	----	----	-------	-----	----------	----

The ICRW returns the "R-APDU" data to the HOST.

R-APDU	Data1					Data(Licc)	SW1	SW2
--------	-------	--	--	--	--	------------	-----	-----

px = "C"(43h) The received data from SAM is 258 bytes or less.

px = "E"(45h) The received data from SAM is 259 bytes or more.
The ICRW requires the following R-APDU data receiving.
The HOST has to receive the remaining R-APDU data using the "CIG" command.

The maximum data size which can be handled with the ICRW is 261 bytes. If the ICRW receives 262 bytes data from the HOST, the ICRW sends the error code "04"(30h,34h) to the HOST. The maximum length of the R-APDU in the positive response is 258 bytes. If the R-APDU length from the SAM is 259 bytes or more, the ICRW returns the response with the parameter px="E"(45h) and first 258 bytes data. The remaining R-APDU data are sent as the positive response data of the command "CIG".

While a power supply is supplied to the SAM, the ICRW monitors the VCC (the power supply line of the SAM).

The ICRW is returned the error code "60"(36h,30h) when a power failure is detected.

If the protocol type of the SAM is not T=0, the error code "62"(36h,32h) is sent.

If the SAM does not respond within WWT(Working Wait Time), the ICRW deactivates the SAM and the error code "63"(36h,33h) is sent.

If any other protocol error occurs, the ICRW deactivates the SAM and the error code "64"(36h,34h) is sent.

If the HOST tries to communicate before the SAM activation, the error code "65"(36h,35h) is sent.

Note) Licc is the data length which the SAM returns. Please refer to the specifications of the SAM about Licc.

5.16.5 SAM communication T=1

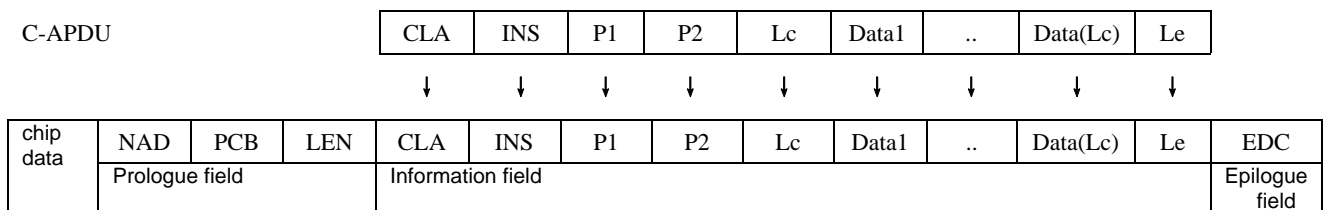
Command	“C” (43h)	“T” (49h)	“D” (44h)	C-APDU (Binary max 261bytes)	
Positive response	“P” (50h)	“T” (49h)	px	st1	st0
Negative response	“N” (4Eh)	“T” (49h)	“D” (44h)	e1	e0

R-APDU
(Binary max 258bytes)

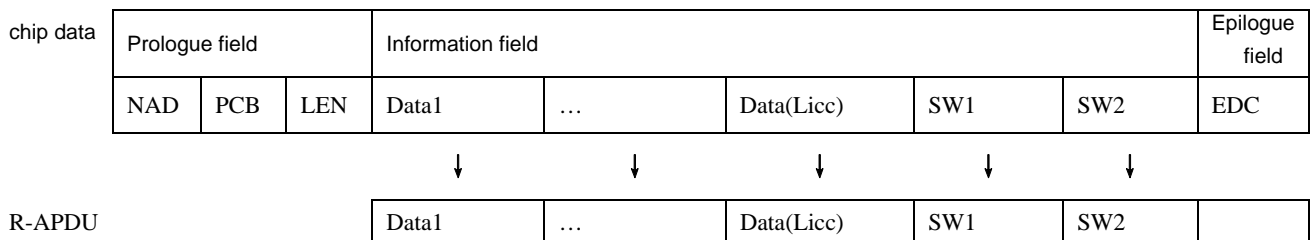
This command exchanges data with the SAM using the protocol T=1.

In this command, the HOST has to set the "C-APDU" data. The ICRW adds the Prologue field and the Epilogue field to the "C-APDU", and sends to the SAM.

If the C-APDU length is greater than the information field size for the SAM (IFSC), the ICRW divides the C-APDU into several consecutive blocks.。



The ICRW sets the R-APDU information field which received from the SAM into the positive response, and transmits to the HOST.



px = “D”(44h) The received R-APDU from the SAM is 258 bytes or less.。

px = “E”(45h) The received R-APDU from the SAM is 259 bytes or more.

The ICRW requires the following R-APDU receiving to the HOST.

The HOST has to receive the remaining R-APDU data using "CIG" command.

px = “O”(4Fh) The ICRW received the S(ABORTrequest) block from the SAM, suspended the data transmission to the SAM, and deactivated the SAM. The HOST has to stop the following data transmitting.

The maximum data size which can be handled by the ICRW is 261 bytes. If the ICRW receives 262 bytes data from the HOST, the ICRW sends the error code "04"(30h,34h) to the HOST.

When the C-APDU data size is 262 bytes or more, the HOST has to transmit the C-APDU exceeding 261 bytes using the command "CIE" and "CIF".

The maximum length of the R-APDU in the positive response is 258 bytes. If the R-APDU length from the SAM is 259 bytes or more, ICRW returns the response with the parameter px="5"(35h) and first 258 bytes data. The remaining R-APDU data are sent as the positive response data of the command "CIG".

While a power supply is supplied to the SAM, the ICRW monitors the VCC (the power supply line of the SAM). The error "60"(36h,30h) is returned when a power failure is detected.

If the protocol type of the SAM is not T=1, the error code "62"(36h,32h) is sent.

If the SAM does not respond within BWT(Block Waiting Time) or CWT(Character Waiting Time), the ICRW deactivates the SAM and the error code "63"(36h,33h) is sent.。

If any other protocol error occurs, the CRW deactivates the SAM and the error code "64"(36h,34h) is sent.

If the HOST tries to communicate before the SAM activation, the error code "65"(36h,35h) is sent.

In case there is any trouble in sequence of command receiving, the error code "02"(30h,32h) is sent. If the error code "02"(30h,32h) is sent, please re-start from activation.

Note) The Licc is data length which the SAM returns. Please refer to specifications of the SAM about length of Licc.

5.16.6 SAM extended communication 1

Command	"C" (43h)	"I" (49h)	"E" (45h)	C-APDU (Binary max 261bytes)	
Positive response	"P" (50h)	"I" (49h)	px	st1	st0
Negative response	"N" (4Eh)	"I" (49h)	"E" (45h)	e1	e0

This command transmits the C-APDU exceeding 261 bytes to the SAM. The HOST has to divide the C-APDU into 261 bytes or less and transmits using this command repeatedly.

px = "G"(47h)

The ICRW requires the following C-APDU data to the SAM. There is no data portion of the positive response. The HOST has to transmit the remaining C-APDU data using the command "CIE" or "CIF".

px = "O"(4Fh)

The ICRW received the S(ABORTrequest) block from the SAM, suspended the data transmission to the SAM, and deactivated the SAM. The HOST has to stop the following data transmitting.

While a power supply is supplied to the SAM, the ICRW monitors the VCC (the power supply line of the SAM). The error code "60"(36h,30h) is returned when a power failure is detected.

If the protocol type of the SAM is not T=1, the error code "62"(36h,32h) is sent.

If the SAM does not respond within BWT(Block Waiting Time) or CWT(Character Waiting Time), the ICRW deactivates the SAM and error code "63"(36h,33h) is sent.

If any other protocol error occurs, the ICRW deactivates the SAM and the error code "64"(36h,34h) is sent.

If the HOST tries to communicate before the SAM activation, the error code "65"(36h,35h) is sent.

5.16.7 SAM extended communication 2

Command	“C” (43h)	“T” (49h)	“F” (46h)	C-APDU (Binary max 261bytes)	
Positive response	“P” (50h)	“T” (49h)	px	st1	st0
Negative response	“N” (4Eh)	“T” (49h)	“F” (46h)	e1	e0

R-APDU
(Binary max 258byte)

This command is used for transmitting the last part of the divided C-APDU. The size of the last data which can be transmitted is 261 bytes or less.

px = “D”(44h) The received R-APDU from the SAM is 258 bytes or less.

px = “E”(45h) The received R-APDU from the SAM is 259 bytes or more.
 The ICRW requires the following R-APDU data receiving.
 The HOST has to receive the remaining R-APDU data using the "CIG" command.

px = “O”(4Fh) The ICRW received the S(ABORTrequest) block from the SAM, suspended the data transmission to the SAM, and deactivated the SAM. The HOST has to stop the following data transmitting.

While a power supply is supplied to the card, the ICRW monitors the VCC (the power supply line of the SAM). The error "60"(36h,30h) is returned when a power failure is detected.

If protocol type of the SAM is not T=1, the error code "62"(36h,32h) is sent.

If the SAM does not respond within BWT(Block Waiting Time) or CWT(Character Waiting Time), the ICRW deactivates the SAM and error code "63"(36h,33h) is sent.

If any other protocol error occurs, the ICRW deactivates the SAM and the error code "64"(36h,34h) is sent.

If the HOST tries to communicate before the SAM activation, the error code "65"(36h,35h) is sent.

5.16.8 SAM extended communication 3

Command	“C” (43h)	“T” (49h)	“G” (47h)		
Positive response	“P” (50h)	“T” (49h)	px	st1	st0
Negative response	“N” (4Eh)	“T” (49h)	“G” (47h)	e1	e0

R-APDU
(Binary max 258bytes)

This command is used for receiving the divided R-APDU exceeding 258 bytes. The HOST has to receive all of the remaining R-APDU data using this command repeatedly until the response of this command becomes px="F"(46h).

px = “E”(45h) The received R-APDU from the SAM is 259 bytes or more.
 The ICRW requires the following R-APDU data receiving.

The HOST has to receive the remaining R-APDU data using "CIG" command.

px = "F"(46h) here is no remaining R-APDU data from the SAM.

px = "O"(4Fh) The ICRW received the S(ABORTrequest) block from the SAM, suspended the data transmission to the SAM, and deactivated the SAM. The HOST has to stop the following data transmitting.

While a power supply is supplied to the SAM, the ICRW monitors the VCC (the power supply line of the SAM). The error "60"(36h,30h) is returned when a power failure is detected.

If the SAM does not respond within WWT(T=0), BWT(T=1) or CWT(T=1), the ICRW deactivates the SAM and the error code "63"(36h,33h) is sent.

If any other protocol error occurs, the ICRW deactivates the SAM and the error code "64"(36h,34h) is sent.

If the HOST tries to communicate before the SAM activation, the error code "65"(36h,35h) is sent.

5.16.9 SAM warm reset

Command	"C" (43h)	"I" (49h)	"H" (48h)			
Positive response	"P" (50h)	"I" (49h)	"H" (48h)	st1	st0	ATR (Binary max 65bytes)
Negative response	"N" (4Eh)	"I" (49h)	"H" (48h)	e1	e0	ATR (Binary max 65bytes)

The ICRW sends a reset pulse, keeping the state where the SAM is activated (VCC,CLK), and receives the ATR from the SAM again (Warm Reset).

If the ATR is not supported by the ICRW with the selected condition at the activate command, the ICRW initiate the deactivation sequence, and sends the error code "66"(36h,36h) or "69"(36h,39h) with the ATR.

If the ATR receive error is occurred, the ICRW initiate the deactivation sequence, and sends the error code "61"(36h,31h), "63"(36h,33h) or "64"(36h,34h).

The ICRW returns error code "65"(36h,35h) if the SAM does not activated.

While a power supply is supplied to the SAM, the ICRW monitors the VCC (the power supply line of the SAM). The error code "60"(36h,30h) is returned when a power failure is detected.

5.16.10 SAM automatic communication

Command	"C" (43h)	"I" (49h)	"I" (49h)	C-APDU (Binary max 261 bytes)		
Positive response	"P" (50h)	"I" (49h)	px	st1	st0	R-APDU (Binary max 258bytes)
Negative response	"N" (4Eh)	"I" (49h)	"I" (49h)	e1	e0	

This command exchanges data with the SAM using the protocol T=0 or T=1. These protocols are selected

automatically by the ICRW. In this command, the HOST has to set "C-APDU" data. Other functions are same as "CIC" or "CID".

px = "D"(44h) The received R-APDU from the SAM is 258 bytes or less.

px = "E"(45h) The received R-APDU from the SAM is 259 bytes or more.
The ICRW requires the following R-APDU data receiving.
The HOST has to receive the remaining R-APDU data using "CIG" command.

px = "O"(4Fh) The ICRW received the S(ABORTrequest) block from the SAM, suspended the data transmission to the SAM, and deactivated the SAM. The HOST has to stop the following data transmitting.

While a power supply is supplied to the SAM, the ICRW monitors VCC (the power supply line of the SAM). The ICRW is returned the error code "60"(36h,30h) when a power failure is detected.

If the SAM does not respond within WWT(T=0), BWT(T=1) or CWT(T=1), the ICRW deactivates the SAM and error code "63"(36h,33h) is sent.

If any other protocol error occurs, the ICRW deactivates the SAM and the error code "64"(36h,34h) is sent.

If the HOST tries to communicate with this command before the SAM activation, the error code "65"(36h,35h) is sent.

When the protocol is T=1 and C-APDU data is 262 bytes or more, the HOST has to use "CI5" and "CI6" to send the following C-APDU data.

5.16.11 Select SAM

Command	"C" (43h)	"I" (49h)	"P" (50h)	Sel (1byt)
Positive response	"P" (50h)	"I" (49h)	"P" (50h)	st1 st0
Negative response	"N" (4Eh)	"I" (49h)	"P" (50h)	e1 e0

This command selects the SAM 2,3,4.

These SAMs are available by connecting the external SAM board (option).

Sel = "0"(30h) : Select SAM1。

Sel = "1"(31h) : Select SAM2。

Sel = "2"(32h) : Select SAM3。

Sel = "3"(33h) : Select SAM4。

The SAM commands for each SAM are available after selecting the SAM by this command.

Before using this command, SAM1 is the default selection.

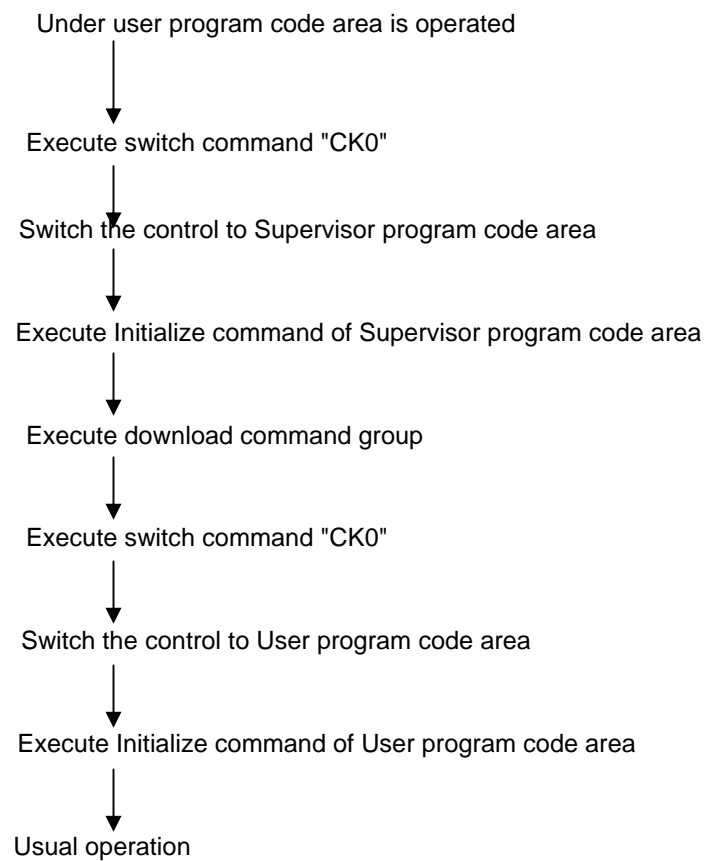
5.17 Switch command

Command	"C" (43h)	"K" (4Bh)	"O" (30h)	Sel (1byte)	
Positive response	"P" (50h)	"K" (4Bh)	"O" (30h)	st1	st0
Negative response	"N" (4Eh)	"K" (4Bh)	"O" (30h)	e1	e0

Switch the control to supervisor program code area from user program code area.

Note: Start from initialize command of supervisor program code area after the switch is completed.

For example:



5.18 Simons memory card control command

5.18.1 Simens memory card power on and activate

Command	“C” (43h)	“R” (52h)	“0” (30h)			
Positive response	“P” (50h)	“R” (52h)	“0” (30h)	st1	st0	ATR (Binary 4 byte)
Negative response	“N” (4Eh)	“R” (52h)	“0” (30h)	e1	e0	

This command activates the memory card. ICRW supply power (Vcc) and clock (CLK), and assert reset (RST) signal. Then, the memory card is activated and returns ATR.

ICRW returns a negative response when proper ATR isn't received from the memory card.

An error code “60” (36h, 30h) is returned when a power failure is recognized while a power supply is supplied to the card.

Card reader judges card type automatically according to ATR. Refer to the following table for the judgement:

ATR		Memory card
H1	H2	
A2	13	SLE4442/4432
92	23	SLE4428/4418

5.18.2 Simens meomory card power off

Command	“C” (43h)	“R” (52h)	“1” (31h)			
Positive response	“P” (50h)	“R” (52h)	“1” (31h)	st1	st0	
Negative response	“N” (4Eh)	“R” (52h)	“1” (31h)	e1	e0	

This command deactivates the meomory card.

ICRW asserts reset (RST) signal, and stop clock(CLK) and power supply(Vcc), then ,the meomory card is deactivated.

5.18.3 Inquire status of Simens memory card

Command	“C” (43h)	“R” (52h)	“2” (32h)			
Positive response	“P” (50h)	“R” (52h)	“2” (32h)	st1	st0	str
Negative response	“N” (4Eh)	“R” (52h)	“2” (32h)	e1	e0	

This command report the status of Simens meomory card in “str” byte.

While a power supply is supplied to the card, the ICRW monitors VCC (The power supply line of the card). An error “60”(36h,30h) is returned when a power failure is detected.

	b7				b0				
str=	0	1	0	0	0	X	X	Y	(binary)

Y(VCC) 1:Active 0: Inactive
 XX(type) 01:SLE4428/4418 00: SLE4442/4432

5.18.4 Communicate with SLE4442

The SLE4442 meomory card has no protocol handler in it. So, ICRW builds in protocol handler to control the memory card. when a usual IC card is controlled, ICRW doesn't check the contents of the data.(aA message is transmitted and received between ICRW and the IC card) Then, the data that it was received from host are transmitted through ICRW to the IC card.

About SLE4442, ICRW must control the signal line of the memory card directly about each data transmission by hardware. Therefore, some functions to control SLE4442 were prepared in ICRW. These functions are specified by a command data from like C-APDU which format is based on ISO/IEC 7816-3 T=0 standard.

Therefore, ICRW recognizes the meaning of command data, and carries out the treatment related to the card by controlling hardware.

After the command was executed properly, ICRW returns a positive response with response data 9000h like from the IC card.

When an error occurs during the communication with SLE4442, ICRW returns a positive response with status information in response data “SW1+SW2” which is based on the ISO/IEC7816-3 T=0 standard.

When a power supply is supplied to the card, the ICRW monitors VCC (the power supply line of the card). An error “60” is returned when a power failure is detected.

5.18.4.1 Data read from main memory on SLE4442

Command	“C” (43h)	“R” (52h)	“3” (33h)	00B000 h + ab h + cd h		
Positive response	“P” (50h)	“R” (52h)	“3” (33h)	st1	st0	Data
Negative response	“N” (4Eh)	“R” (52h)	“3” (33h)	e1	e0	

This command is recognized as follows:

ab h: The start address to read data in the main memory

cd h: The number of bytes of data to read.

ICRW reads data from the main memory of SLE4442, and transmits data on cdh bytes from the ICRW reads data from the main memory is 256 bytes. The byte number “00”(30h,30h) of data to address ab h. the capacity of the main memory is 256 bytes. All the contents of the main memory can be read with the following command.

“CR3” + 00B0000000 h

While a power supply is supplied to the card, the ICRW monitors VCC (the power supply line of the card). An error “60” (36h,30h) is returned when a power failure is detected.

5.18.4.2 Data read from protection memory on SLE4442

Command	“C” (43h)	“R” (52h)	“3” (33h)	00B001 h + ab h + cd h		
Positive command	“P” (50h)	“R” (52h)	“3” (33h)	st1	st0	Data
Negative Command	“N” (4Eh)	“R” (52h)	“3” (33h)	e1	e0	

This command is recognized as follows:

ab h: The start address to read data in the protection memory

cd h: The number of bytes of data to read.

ICRW handles the data of all 32bits in the protection memory as the data on 4bytes. The contents (32bits) of protection memory can be read with the following command.

“CR3” + 00B0010004 h

ICRW reads data from the protection memory of SLE4442, and transmits data on cd h bytes from the address ab h.

While a power supply is supplied to the card, the ICRW monitors VCC (the power supply line of the card). An error “60” (36h,30h) is returned when a power failure is detected.

5.18.4.3 Data read from security memory on SLE4442

Command	“C” (43h)	“R” (52h)	“3” (33h)	00B002 h + ab h + cd h		
Positive response	“P” (50h)	“R” (52h)	“3” (33h)	st1	st0	Data
Negative response	“N” (4Eh)	“R” (52h)	“3” (33h)	e1	e0	

This command is recognized as follows:

ab h: The start address to read data in the security memory

cd h: The number of bytes of data to read.

The security code inside the security memory can't be read properly if the check of PSC (programmable security code) isn't finished normally. ICRW returns four bytes of 00h. ICRW reads four bytes security memory data of SLE4442.

The contents of the security memory can be read with the following command:

“CR3” + 00B0020004 h

ICRW reads data from the security memory of SLE4442, and transmits data on cd h bytes from the address ab h.

While a power supply is supplied to the card , the ICRW monitors VCC (the power supply line of the card). An error “60” (36h, 30h) is returned when a power failure is detected.

5.18.4.4 Data write to main memory on SLE4442

Command	“C” (43h)	“R” (52h)	“3” (33h)	00D000 h + ab h + cd h + ef h + ...		
Positive Command	“P” (50h)	“R” (52h)	“3” (33h)	st1	st0	Data
Negative Command	“N” (4Eh)	“R” (52h)	“3” (33h)	e1	e0	

This command is recognized as follows:

ab h: The start address to write data in the main memory

cd h: The number of bytes of data to write.

ef h: The data to write first (cd h bytes)

ICRW writes data in the main memory. ICRW returns a result after written data are checked. Before doing this operation, PSC (programmable security Code) check must be done.

The capacity of the main memory is 256bytes. The byte number “00” of data to write means 256 bytes.
the contents of the whole memory area is shown in the following:

“CR3” + 00D0000000 h + Write data (256byte)

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

If the address data on main memory is protected by the protection memory, the writing operation is not available.

While power supply is supplied to the card, the ICRW monitors VCC (the power supply line of the card). an error “60” (36h, 30h) is returned when a power failure is detected.

5.18.4.5 Data write to protection memory on SLE4442

Command	“C” (43h)	“R” (52h)	“3” (33h)	00D001 h + ab h + cd h + ef h + ...		
Positive Command	“P” (50h)	“R” (52h)	“3” (33h)	st1	st0	Data
Negative Command	“N” (4Eh)	“R” (52h)	“3” (33h)	e1	e0	

This command is recognized as follows:

ab h: The start address of the protection of the main memory

cd h: The number of bytes that it is protected continuously

ef h: The contents of data to protect (cd h bytes)

ICRW can set up writing protection in a part of the main memory which can be protected. Once it is set up, the protection can't be cancelled. Before doing this operation, PSC(Programmable Security Code) check must be done.

The address of the main memory that the protection is possible from 00h to 1Fh. They are controlled by 4bytes (32bits) of protection data. For example, if bit0 of protection memory byte0 is “0”, data on the address 00h of the main memory are protected.

The contents of data must be presented to protect data in main memory. Therefore, the contents of the protection memory can't be operated directly.

For example, protection is set up with the next command when the value of the address 10h of the main memory is 20h and protection isn't set up in the bit address 10h of the protection memory.

“CR3” + 00D001100120h

After command execution, ICRW returns response 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 a time in the data which continued in the main memory.

While a power supply is supplied to the card, the ICRW monitors VCC (the power supply line of the card). An error “60”(36h, 30h) is returned when a power failure is detected.

5.18.4.6 Data write to security memory on SLE4442

Command	“C” (43h)	“R” (52h)	“3” (33h)	00D002 h + ab h + cd h + ef h + ...		
Positive Command	“P” (50h)	“R” (52h)	“3” (33h)	st1	st0	Data
Negative response	“N” (4Eh)	“R” (52h)	“3” (33h)	e1	e0	

This command is recognized as follows:

- ab h: The start address to write data in the security memory
- cd h: The number of bytes of data to write.
- ef h: The data to write first (cd h bytes)

After a PSC check is finished normally, the reference-data area of 4 bytes can be changed.

For example, the following command can change security code into 123456h:

“CR3” + 00D0020103123456h

After command execution, ICRW returns response with 9000h or sw1+sw2.

While a power supply is supplied to the card, the ICRW monitors VCC (the power supply line of the card). An error “60” (36h, 30h) is returned when a power failure is detected.

Note: It is only writing though data writing to error-counter is always possible. Therefore, be careful of writing to error-counter. Otherwise, the card can't be written any more. Error-counter is controlled when PSC is checked.

5.18.4.7 Verification data present to SLE4442

Command	“C” (43h)	“R” (52h)	“3” (33h)	0020 h + 03 h + 01 h + 03 h + ef h...		
Positive command	“P” (50h)	“R” (52h)	“3” (33h)	st1	st0	Data
Negative Command	“N” (4Eh)	“R” (52h)	“3” (33h)	e1	e0	

This command is recognized as follows:

- 03 h: Fixed value (the maximum value of the error counter)
- 01 h: Fixed value (the start address of security code in the security memory)
- c3 h: Fixed value (the number of bytes of data to compare)

ef h: The data to compare (3bytes)

Before writing operation, PSC (Programmable Security Code) must be checked properly with SLE4442.

For example, the following command can verify whether security code is valid:

“CR3” + 0020030103XXXXXXh (XXXXXXh: 3bytes security code)

If verification succeed, writing treatment becomes effective until a power supply is turned off when a check is finished normally.

The writing function of the card is lost when the command is carried out continuously three times with the wrong code.

When a power supply is supplied to the card, the ICRW monitors VCC(the power supply line of the card). An error “60”(36h, 30h) is returned when a power failure is detected.

5.18.5 Communicate with SLE4428

The SLE4428 memory card has no protocol handler in it, so, ICRW also builds in protocol handler to control SLE4428.

The control method of SLE4428 is done in the same way as SLE4442. refer to SLE4442 for the details of the contents.

While a power supply is supplied to the card, the ICRW monitors VCC (the power supply line of the card). An error “60” (36h, 30h) is returned when a power failure is detected.

5.18.5.1 Data reading of main-memory of SLE4428

Command	“C” (43h)	“R” (52h)	“4” (34h)	00B0 h + 0a h + bc h + de h		
Positive response	“P” (50h)	“R” (52h)	“4” (34h)	st1	st0	Data
Negative response	“N” (4Eh)	“R” (52h)	“4” (34h)	e1	e0	

This command is recognized as follows:

abc h: The start address to read data in the main memory

de h: The number of bytes of data to read.

ICRW reads data from the main memory of SLE4428, and transmits data on de h bytes from the address abch. The capacity of the main memory is 1024bytes. The byte number 00h of data to read means 256bytes. The head part of main memory can be read with the following command.

“CR4” + 00B0000000 h

While a power supply is supplied to the card, the ICRW monitors VCC (the power supply line of the card). An error “60”(36h,30h) is returned when a power failure is detected.

5.18.5.2 Condition data reading of protection-bit of SLE4428

Command	“C” (43h)	“R” (52h)	“4” (34h)	00B0 h + 10 h + ab h + cd h		
Positive response	“P” (50h)	“R” (52h)	“4” (34h)	st1	st0	Data
Negative response	“N” (4Eh)	“R” (52h)	“4” (34h)	e1	e0	

This command is recognized as follows:

- 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 data on 1024bits, and it is read. 1024bits is equivalent to 128bytes. (1024=128x8). Data to read first become protection information to address 007 h from address 000 h of main memory in the case of abh=00 h. the contents of the whole protection image can be read with the following command.:

“CR4” + 00B0100080 h

ICRW reads data as the protection image of SLE4428, and transmits data on cd h bytes from the address ab h.

While a power supply is supplied to the card, the ICRW monitors VCC (the power supply line of the card). An error “60”(36h, 30h) is returned when a power failure is detected.

5.18.5.3 Data writing to main-memory of SLE4428

Command	“C” (43h)	“R” (52h)	“4” (34h)	00D0 h + 0a h + bc h + de h + fg h + ...		
Positive response	“P” (50h)	“R” (52h)	“4” (34h)	st1	st0	Data
Negative response	“N” (4Eh)	“R” (52h)	“4” (34h)	e1	e0	

This command is recognized as follows:

- abc h: The start address of write dat in the main memory
- de h: The number of bytes of data to write
- fg h: The data to write first (de h bytes)

ICRW writes data in the main memory. ICRW returns a result after written data are checked. Before doing this operation, PSC (Programmable Security Code) check must be done (SLE4428). The capacity of the main memory

is 1024bytes. The byte number 00h of data to write means 256bytes. The example that data are written in from the address 100h is shown in the following.

“CR4” + 00D0010000 h + write data (256byte)

After command execution, ICRW returns response with 9000h or sw1+sw2. if the addressed data on main memory is protected, the write operation is not available. While a power supply is supplied to the card, the ICRW monitors VCC(the power supply line of the card). An error “60” (36h, 30h) is returned when a power failure is detected.

5.18.5.4 Data writing to main-memory of SLE4428 (with protecting it)

Command	“C” (43h)	“R” (52h)	“4” (34h)	00D0 h + 1a h + bc h + de h + fg h + ...		
Positive response	“P” (50h)	“R” (52h)	“4” (34h)	st1	st0	Data
Negative response	“N” (4Eh)	“R” (52h)	“4” (34h)	e1	e0	

This command is recognized as follows:

abc h : 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)

ICRW writes data in the main memory. ICRW returns a result after written data are checked.

Before doing this operation, PSC (Programmable Security Code) check must be done (SLE4428).

This command is the same as data writing except for Protect's being done at the same time with writing. Renewal becomes impossible when data are written with this command.

5.18.5.5 Protection-bit is written by the completion of the verification

Command	“C” (43h)	“R” (52h)	“4” (34h)	00D0 h + 2a h + bc h + de h + fg h + ...		
Positive response	“P” (50h)	“R” (52h)	“4” (34h)	st1	st0	Data
Negative response	“N” (4Eh)	“R” (52h)	“4” (34h)	e1	e0	

This command is recognized as follows.

abc h : the start address of the protection of the main memory

de h : the number of bytes that it is protected continuously

fg h : the contents of data to protect (de h bytes)

ICRW can set up writing protection in a part of the main memory which can be protected. Once it is set up, the protection can't be canceled. Before doing this operation, PSC (Programmable Security Code) check must be done.

The contents of data must be presented to protect data in main memory.

For example, protection is set up with the next command when the value of the address 010 h of the main memory is 20 h and protection isn't set up.

"CR4" + 00D020100120h

After command execution, ICRW returns response 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 a time in the data which continued in the main memory.

While a power supply is supplied to the card, the ICRW monitors VCC (the power supply line of the card). An error "60"(36h,30h) is returned when a power failure is detected.

5.18.5.6 Verification data present to SLE4428

Command	"C" (43h)	"R" (52h)	"4" (34h)	00200000 h + 02 h + ef h...		
Positive response	"P" (50h)	"R" (52h)	"4" (34h)	st1	st0	Data
Negative response	"N" (4Eh)	"R" (52h)	"4" (34h)	e1	e0	

This command is recognized as follows.

02 h : Fixed value (the number of bytes of data to compare)
ef h : the data to compare (2bytes)

Before changing data, PSC(Programmable Security Code) must be checked properly with SLE4428. Because this function should be made effective, the issue of the next command is necessary.

ex). "CR4"+ 0020000002xxxx h (xxxx : security code 2bytes)

The presented data are compared with internal Reference-Data by SLE4428 card itself. Writing treatment becomes effective until a power supply is turned off when a check is finished normally.

The writing function of the card is lost when the command is carried out continuously eight times with wrong code.

While a power supply is supplied to the card, the ICRW monitors VCC (the power supply line of the card). An error "60"(36h,30h) is returned when a power failure is detected.

5.18.5.7 SLE4428 Change Password

Command	“C” (43h)	“R” (52h)	“4” (34h)	00240100 h + 02 h + abh + cdh...		
Positive response	“P” (50h)	“R” (52h)	“4” (34h)	st1	st0	Data
Negative response	“N” (4Eh)	“R” (52h)	“4” (34h)	e1	e0	

This command is recognized as follows:

ab h, cd h: Need to set up password (total 2bytes)

Before changing password, SLE4428 needs to make process of password check.

While a power supply is supplied to the card, the ICRW monitors VCC (the power supply line of the card). An error "60"(36h,30h) is returned when a power failure is detected.

5.19 I2C memory card control command

5.19.1 I2C Power on

Command	“C” (43h)	“S” (53h)	“0” (30h)	Vcc (1byte)	Wrd (1byte)
Positive response	“P” (50h)	“S” (53h)	“0” (30h)	st1	st0
Negative response	“N” (4Eh)	“S” (53h)	“0” (30h)	e1	e0

To activate an I2C memory card, ICRW supplies a power supply (Vcc) to the card. After that, ICRW initializes the card inside. An error code "60"(36h,30h) is returned when a power failure is recognized while a power supply is supplied to the card.

Vcc: The choice of a power supply voltage to supply

Vcc = “0”(30h) ICRW supplies with +5V to VCC and activates the card.

Vcc = “1”(31h) ICRW supplies with +3V to VCC and activates the card.

Wrd: The number of bytes of the word address of an I2C memory card to use

Wrd="1"(31h) : ICRW accesses an I2C memory card in the Word address of 1byte.

Wrd="2"(32h) : ICRW accesses an I2C memory card in the Word address of 2bytes.

5.19.2 I2C Power off

Command	“C” (43h)	“S” (53h)	“1” (31h)		
Positive response	“P” (50h)	“S” (53h)	“1” (31h)	st1	st0
Negative Response	“N” (4Eh)	“S” (53h)	“1” (31h)	e1	e0

When this command is received, ICRW deactivates an I2C card. ICRW suspends the supply of the power supply (Vcc). An I2C memory card is deactivated as a result.

5.19.3 Inquire Status of I2C

Command	“C” (43h)	“S” (53h)	“2” (32h)			
Positive command	“P” (50h)	“S” (53h)	“2” (32h)	st1	st0	sti
Negative Command	“N” (4Eh)	“S” (53h)	“2” (32h)	e1	e0	

When this command is received, ICRW reports the condition of an I2C memory card by byte of stj. While a power supply is supplied to the card, the ICRW monitors VCC (the power supply line of the card). An error "60"(36h,30h) is returned when a power failure is detected.

str=

b7	b0						
0	1	0	X	0	0	Y	Z

 (binary)

Z(VCC) 1: Active 0: Inactive

Y(VCC) 1: 3V 0: 5V

X(The number of the word address) 1: 2bytes 0: 1byte

5.19.4 I2C Communication

The I2C memory card has no protocol handler in it. So, ICRW builds in protocol handler to control this. When a usual IC card is controlled, ICRW doesn't check the contents of the data. (A message is transmitted and received between ICRW and the IC card)Then, the data that it was received from HOST are transmitted through ICRW to the IC card.

About the I2C memory card, ICRW must control the signal line of the I2C memory card directly about each data transmission by the hardware. Therefore, some functions to control an I2C memory card were prepared in ICRW. These functions are specified by a command data form like C-APDU which format is based on ISO/IEC 7816-3 T=0 standard.

Therefore, ICRW recognizes the meaning of the command data, and carries out the treatment related to the card by controlling hardware.

After a command is carried out properly, ICRW returns 9000h by the positive response as if it was just received from the IC card.

When an error occurs during the communication with the I2C memory card, ICRW returns a positive response with status information in response data “SW1+SW2” which is based on T=0 standard of ISO/IEC7816-3.

While a power supply is supplied to the card, the ICRW monitors VCC (the power supply line of the card). An error "60"(36h,30h) is returned when a power failure is detected.

5.19.4.1 Read data from I2C

Command	“C” (43h)	“S” (53h)	“3” (33h)	00B0 h + ab h + cd h + ef h		
Positive response	“P” (50h)	“S” (53h)	“3” (33h)	st1	st0	Data
Negative response	“N” (4Eh)	“S” (53h)	“3” (33h)	e1	e0	

This command is recognized as follows:

ab h : The upper address of head address which begins to read data

cd h : The lower address of head address which begins to read data

ef h : The number of bytes of data to read

ICRW reads data from the I2C memory card, and transmits data on ef h bytes from the address abcd h. The value established with ef h bytes is the value which makes the value which it can access without striding over a page by an I2C memory card to use an upper limit

For example, the following command reads the first 8bytes of memory card:

“CS3” + 00B0000008 h

Note: It doesn't change to the next page automatically when it tries to read it by the bigger value than the page size of the used I2C memory card or when it changes in the next page from the middle of the page. Therefore, access it not to cross the boundary of the page. If it is not so, it isn't finished normally.

While a power supply is supplied to the card, the ICRW monitors VCC (the power supply line of the card). An error "60"(36h,30h) is returned when a power failure is detected.

5.19.4.2 Write data into I2C

Command	“C” (43h)	“S” (53h)	“3” (33h)	00D0 h + ab h + cd h + ef h + gh h + ...		
Positive response	“P” (50h)	“S” (53h)	“3” (33h)	st1	st0	Data
Negative response	“N” (4Eh)	“S” (53h)	“3” (33h)	e1	e0	

This command is recognized as follows:

ab h: The upper address of head address which begins to write data

cd h: The lower address of head address which begins to write data

ef h: The number of bytes of data to write

gh h: the data to write first (the head data of the data on ef h bytes)

ICRW writes data in the I2C memory card. ICRW returns a result after written data are checked.

For example, the following command make the first 8bytes write into memory card.

“CS3” + 00D0000008 h + write data (8bytes)

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

Note: It doesn't change to the next page automatically when it tries to write it by the bigger value than the page size of the used I2C memory card or when it changes in the next page from the middle of the page. Therefore, access it not to cross the boundary of the page. If it is not so, it isn't finished normally.

While a power supply is supplied to the card, the ICRW monitors VCC (the power supply line of the card). An error "60"(36h,30h) is returned when a power failure is detected.

5.20 command for Contactless card

5.20.1 Reset activated

Command	"C"	"Z"	"0"	1 st	2 nd	3 rd
	(43h)	(5Ah)	(30h)	type	type	type

Mifare, TypeA

Positive response	"P"	"Z"	"0"	st1	st0	type	ATQA	UID	SAK	ATS	PPSS
	(50h)	(5Ah)	(30h)			1 byte	2 byte	4-12 bytes	1 byte	1-254 byte	1 byte

Negative response	"N"	"Z"	"0"	e1	e0	type	ATQA	UID	SAK	ATS	PPSS
	(4Eh)	(5Ah)	(30h)			1 byte	2 byte	4-12 bytes	1 byte	1-254 byte	1 byte

Type B

Positive response	"P"	"Z"	"0"	st1	st0	type	PUPI	App.Data	Protocol Info	CID
	(50h)	(5Ah)	(30h)			1 byte	4 byte	4 bytes	3 bytes	1 byte

Negative response	"N"	"Z"	"0"	e1	e0	type	PUPI	App.Data	Protocol Info	CID
	(4Eh)	(5Ah)	(30h)			1 byte	4 byte	4 bytes	3 bytes	1 byte

This command is used to activate contactless card. Now support card type: ISO/IEC 14443 TypeA and ISO/IEC14443 TypeB.

ICRW executes reset/activate to the card, the procedure is as following activating sequence:

Mifare and 14443 Type A

- 1) Request A(REQA) / Answer Request A (ATQA)
- 2) Anticollision
- 3) Select(SEL) / Unique Identifier(UID) & Select Acknowledge(SAK)

14443 Type A only

- 4) Request for answer to select (RATS) / Answer to Select(ATS)
- 5) Protocol and parameter selection request(PPSR) / PPS start(PPSS)

ISO14443 Type B

1. Request B (REQB) / Answer to REQB(ATQB)
2. Attribute (ATTRIB) / Answer to ATTRIB

When Mifare card is activated, ICRW will return positive response of ATQA, UID and SAK. If the card is ISO/IEC14443 TypeA card, ATR include ATS and PPSS. If SAK bit 6 is 1, the activated card is compatible to ISO/IEC 14443 part4.

If the error occurs in activation, ICRW will respond negative response including error code and returning data.

Type B is same as above.

For Mifare series cards, only executing 1)~3), for the other TypeA cards, executing 1)~5).

If it's activated successfully, responses following data in ordinary answers:

In all ordinary answers, the types of cards activated by type:

type A = (41h) the current cards are compliant to ISO14443 TypeA, not Mifare series cards.

Type M = (4Dh) the current cards are Mifare series cards.

Type B = (42h) the current cards are compliant to ISO14443 TypeB.

“0”(30h = no type)

5.20.2 Contactless card deactive / release

Command	“C” (43h)	“Z” (5Ah)	“1” (31h)		
Positive	“P” (50h)	“Z”(5 Ah)	“1” (31h)	st1	st0
Negative	“N” (4Eh)	“Z”(5 Ah)	“1” (31h)	e1	e0

Close interface of contactless card, close power supply for reading module.

5.20.3 Inquiry status of contactless card

Command	“C” (43h)	“Z” (5Ah)	“2” (32h)				
Positive	“P” (50h)	“Z”(5 Ah)	“2” (32h)	st1	st0	sti	stj
Negative	“N” (4Eh)	“Z”(5 Ah)	“2” (32h)	e1	e0		

Respond the card activation in status.

status = 0x40 no activation

status = 0x43 activated

5.20.4 Mifare card communication

5.20.4.1 Mifare standard card communication

Command	“C” (43h)	“Z” (5Ah)	“3” (33h)	Function code (ASCII 1byte)		parameter, data (HEX)	
Positive response	“P” (50h)	“Z” (5Ah)	“3” (33h)	st1	st0	Status code (HEX, 1byte)	Return data (HEX)
Negative response	“N” (4Eh)	“Z” (5Ah)	“3” (33h)	e1	e0		

This command is executed to making communication conform to Mifare Classic protocol and Mifare standard card.

Refer to Mifare specification about specified card function.

If the executed result isn't 'OK' (=00h), ICRW returns the executed status in normal response.

Load Key function

Function code = “L” (4Ch)

parameter (total 8 bytes) = key choice (1 byte, HEX, key A=00h, key B=01h) +
sector serial number (1 byte, HEX, 00-0Fh, 10-27h*) +
no coding key (6 bytes, HEX)

ATR data = status code (1 byte, HEX, OK = 00h)

Save key in non volatile memory, be auto-selected in card validation. This function can be executed in anytime without card operation.

note:

- 1) For the safe reason, suggest loading the key before using ICRW.
- 2) Due to the key in sector 10-27h (Mifare standard 4K card) stored in flash of CPU, so don't frequently re-write the key, it will damage CPU (not over 100 times).

Validation function

Function code = “A” (41h)

Parameter (total 2 byte) = key choice (1 byte, HEX, key A=00h, key B=01h) +
no coding key (6 bytes, HEX)

ATR data = status code (1 byte, HEX, OK = 00h)

Use previous loaded key to validate the sector.

The key is auto-selected according to the sector number by validation function.

Read function

Function code = “R” (52h)

INTERFACE SPECIFICATION	CRT-310-NU01	71/90
-------------------------	--------------	-------

parameter (total 1 byte) = block serial No. (1 byte, HEX, 00-3Hh, 40-FFh*)**
ATR data (total 17 bytes) = status code (1 byte, HEX, OK = 00h) +
Reading data (16 bytes, HEX)

Read 16 bytes data from a validated block.

Write function

Function code = "W" (57h)
Parameter (total 17 bytes) = block s/n (1byte, Hex, 00-3Hh, 40-FFh*)** +
Prepared written data (16 byte, Hex)
response = status code (1byte, Hex, OK = 00h)

write 16 bytes data into a certified block of a card.

Increament transmit function

Function code = "I" (49h)
parameter (total 6 bytes) = source block S/N (1byte, Hex, 00-3Hh, 40-FFh*)** +
target block S/N (1byte, Hex, 00-3Hh, 40-FFh*)** +
increament value (4 bytes, Hex)***
response = status code (1 byte, Hex, OK = 00h)

transmit the value in original source block increased to the specified value to the target block. Source block and target block must be data block format.

Decrement transmit function

Function code = "D" (44h)
parameter (total 6 bytes) = source block S/N (1byte, Hex, 00-3Hh, 40-FFh*)** +
target block S/N (1byte, Hex, 00-3Hh, 40-FFh*)** +
decrease value (4 bytes, Hex)***
response = status code (1 byte, Hex, OK = 00h)

transmit the value in original source block decreased to the specified value to the target block. Source block and target block must be data block format.

* these value is only used for Mifare standard 4K card.

** block S/N counting, for example:

Sector 1 block 0: block S/N = $1*4 + 0 = 04h$
Sector 2 block 1: block S/N = $2*4 + 1 = 09h$
Sector 3 block 2: block S/N = $3*4 + 2 = 0Eh$
Sector 15 block 3: block S/N = $15*4 + 3 = 3Fh$
Sector 35 block 10: block S/N = $(35-32)*16 + 32*4 + 10 = BAh$

*** Data is transmitted in a high byte priority order, for example: increase 0x12345678 to source block 5 then transmit to target block 6:

"C" "Z" "3" "I" 05h 06h 12h 34h 56h 78h

5.20.4.2 Mifare Ultraligh card communication

Command	"C"	"Z"	"3"	Function code	Parameter, data
---------	-----	-----	-----	---------------	-----------------

INTERFACE SPECIFICATION	CRT-310-NU01	72/90
--------------------------------	--------------	-------

(43h)	(5Ah)	(33h)	(ASCII 1byte)	(Hex)
-------	-------	-------	---------------	-------

Positive	“P” (50h)	“Z” (5Ah)	“3” (33h)	st1	st0	Status code (Hex, 1 byte)	Return data (Hex)
-----------------	--------------	--------------	--------------	-----	-----	------------------------------	----------------------

Negative	“N” (4Eh)	“Z” (5Ah)	“3” (33h)	e1	e0
-----------------	--------------	--------------	--------------	----	----

This command is used to communicate with MifareUltralight card.

Refer to Mifare specification about specified card function.

If the execution result is not ‘OK’ (=00h), reader returns execution status in positive response.

Read function

Function code = “R” (52h)
 Parameter (total 1 byte) = page S/N (1 byte, Hex, 00-0Fh)
 Response data (total 17 bytes) = status code (1 byte, Hex, OK = 00h) +
 Read data (16 bytes, Hex)
 Read 16 bytes data from a page of card (consicutive 4 pages) .

Write function

Function code = “W” (57h)
 parameter (total 5 bytes) = page S/N (1byte, Hex, 00-0Fh) +
 Prepared written data (4 bytes, Hex)
 Response data = status code (1 byte, Hex, OK = 00h)

Write 4 byte data into a page of the card.

Compatible of writing function

Function code = “W” (57h)
 parameter (total 17 bytes) = page S/N (1 byte, Hex, 00-0Fh) +
 Prepared written data (16 bytes, Hex)
 Response data = status code (1 byte, Hex, OK = 00h)

Same as write function, only write forward 4 bytes data.

5.20.4.3 Mifare status code

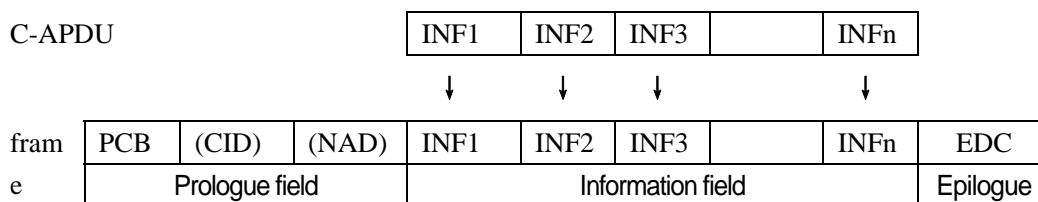
Status code	Error name	Description
FFh	NOTAGERR	No card in operation field or no response
FEh	CRCERR	CRC error of the card
FCh	AUTHERR	No card certified

FBh	PARITYERR	Card parity error
FAh	CODEERR	Receive NAK
F6h	NOTAUTHERR	Sector no certified
F5h	BITCOUNTERR	Received bit count error
F4h	BYTECOUNTERR	Received byte count error
F1h	WRITEERR	Receive NAK after writting
EDh	OVFLERR	FIFO overflow
EBh	FRAMINGERR	RF interface frame error, start bit invalid
E8h	COLLERR	RF data transmit on conflict
E5h	ACCESSTIMEOUT	IC respond time out
E1h	CODINGERR	Received abnormal data
90h	RECBUF_OVERFLOW	Receiving buffer area overflow
84h	VALERR	Data block format error

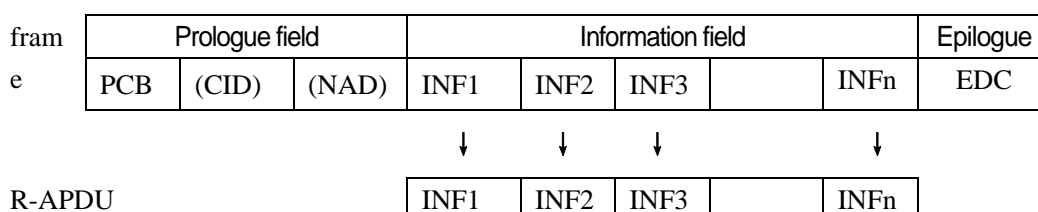
5.20.5 Contactless Type A,B card APDU communication

Command	“C” (43h)	“Z” (5Ah)	“4” (34h)	C-APDU (Binary max 261bytes)		
Positive	“P” (50h)	“Z” (5Ah)	px	st1	st0	R-APDU (Binary max 258bytes)
Negative	“N” (4Eh)	“Z” (5Ah)	“4” (34h)	e1	e0	

This command is compliant to ISO/IEC 14443-4, ICRW sets C-APDU to information field and transmits to contactless IC card.



ICRW sets to R-APDU Information field which received from contactless IC card, and transmits to HOST.



Maximum size of data ICRW can handle is 261 bytes. If exceeds 261 bytes, it needs “CZ5” and “CZ6” commands.

px = “4”(34h) : The received data from contactless IC card is 258 bytes or less.

px = “5”(35h) : The received data from contactless IC card is 259 bytes or more.

ICRW requires transmitting following data.

HOST needs to receive remaining data using "CZ7" command.

If ICRW cannot recover the communication hang-up to ICC, error code "63" is sent. If any other protocol error occurs, error code "64" is sent.

If ICC is not activated, error code "65" is sent.

5.20.6 Contactless Type A, B extend communication 1

Command	“C” (43h)	“Z” (5Ah)	“5” (35h)	C-APDU (Binary max 261bytes)	
Positive	“P” (50h)	“Z” (5Ah)	px	st1	st0
Negative	“N” (4Eh)	“Z” (5Ah)	“5” (35h)	e1	e0

The transmitted data to contactless IC card is 262 bytes or more of C-APDU.

px = “7”(37h) ICRW requires receiving following C-APDU data. There is no data portion.
When the length of data is 262 bytes or more, the remaining data is transmitted to ICRW using this command. And the length of data is 261 bytes or less, the remaining data is transmitted to ICRW using “CZ6” command.

If ICRW cannot recover the communication hang-up to ICC, error code "63" is sent. If any other protocol error occurs, error code "64" is sent.

If ICC is not activated, error code "65" is sent.

5.20.7 Contactless Type A, B extend communication 2

Command	“C” (43h)	“Z” (5Ah)	“6” (36h)	C-APDU (Binary max 261bytes)	
Positive	“P” (50h)	“Z” (5Ah)	px	st1	st0
					R-APDU (Binary max 258bytes)
Negative	“N” (4Eh)	“Z” (5Ah)	“6” (36h)	e1	e0

INTERFACE SPECIFICATION	CRT-310-NU01	75/90
-------------------------	--------------	-------

(4Eh)	(5Ah)	(36h)		
-------	-------	-------	--	--

this command is used when the last data which the length of C-APDU data is 262 bytes or more are transmitted.

px = "4"(34h) The received data from contactless IC card is 258 bytes or less.
px = "5"(35h) The received data from contactless IC card is 259 bytes or more.
HOST needs to receive remaining data using "CZ7" command

If ICRW cannot recover the communication hang-up to ICC,
error code "63" is sent. If any other protocol error occurs, error
code "64" is sent.

If ICC is not activated, error code "65" is sent.

5.20.8 Contactless Type A, B extend communication 3

Command	"C" (43h)	"Z" (5Ah)	"7" (37h)			
Positive	"P" (50h)	"Z" (5Ah)	px	st1	st0	R-APDU (Binary max 258bytes)
Negative	"N" (4Eh)	"Z" (5Ah)	"7" (37h)	e1	e0	

px = "5"(35h) The received data from contactless IC card is 259 bytes or more.
HOST needs to receive remaining data using "CZ7" command.

px = "6"(36h) ICRW does not have more transmit contactless IC card data.

If ICRW cannot recover the communication hang-up to ICC,
error code "63" is sent. If any other protocol error occurs, error
code "64" is sent.

If ICC is not activated, error code "65" is sent.

5.20.9 Contactless card reset

Command	"C" (43h)	"Z" (5Ah)	"8" (38h)		
Positive	"P" (50h)	"Z" (5Ah)	"8" (38h)	st1	st0
Negative	"N" (4Eh)	"Z" (5Ah)	"8" (38h)	e1	e0

INTERFACE SPECIFICATION	CRT-310-NU01	76/90
--------------------------------	--------------	-------

(4Eh)	(5Ah)	(38h)		
-------	-------	-------	--	--

Reset of contactless IC card reader/writer and reset IC card

5.20.10 Level 3 Transparent transfer timeout setting

Command	“C” (43h)	“Z” (5Ah)	“A” (41h)	time_out (2 bytes)
----------------	--------------	--------------	--------------	-----------------------

Positive	“P” (50h)	“Z” (5Ah)	“A” (41h)	st1	st0
-----------------	--------------	--------------	--------------	-----	-----

Negative	“N” (4Eh)	“Z” (5Ah)	“A” (41h)	e1	e0
-----------------	--------------	--------------	--------------	----	----

When activated to ISO14443-3, the transparent transmission mode will be used to fill data.

This command sets the delay time for transparent transferring.

This command is used for some cards need transparent transferring on ISO14443-3 level (for example: Mifare Plus card) .

time_out 2 bytes wait for delaying, unit:ms, high byte is in front.

For example: 01 00, delaying time is 256ms.

5.20.11 Level 3 transparent transferring

Command	“C” (43h)	“Z” (5Ah)	“B” (42h)	Send_Data (binary, Max 1024 bytes)
----------------	--------------	--------------	--------------	---------------------------------------

Positive	“P” (50h)	“Z” (5Ah)	“B” (42h)	st1	st0	Recv_Data (binary, Max 1024 bytes)
-----------------	--------------	--------------	--------------	-----	-----	---------------------------------------

Negative	“N” (4Eh)	“Z” (5Ah)	“B” (42h)	e1	e0
-----------------	--------------	--------------	--------------	----	----

When activated to ISO14443-3, the transparent transmission mode will be used to fill data.

This command is used for some cards need transparent transferring on ISO14443-3 level (for example: Mifare Plus card) .

Send_Data data waiting to be sent, length is Max 1024 bytes.

Recv_Data received returning data, length is Max 1024 bytes.

5.20.12 Mifare Plus card operation instruction

According to Mifare Plus DataSheet, Mifare Plus is able to activated to ISO14443-3 or ISO14443-4.

Activated to ISO14443-3 is able to use “RF card reset” command and the first parameter is “M” .

On Level 3, transparent transferring function can be used for data changing, refer to “Level 3 transparent transfer time out set command” and “Level 3 transparent transfer” command.

Activated to ISO14443-4 is able to use “RF reset activating ” command, and the first parameter is “A” .

On Level4, communication operation is same as Type A CPU card, refer to “contactless Type A,B card APDU communication” command.

5.20.13 Mifare DESFire card operation instruction

Mifare DESFire is Type A CPU card. So it's OK to use related commands of Type A CPU card to activate and communicate.

Activation is able to use “RF card reset activated” command, and the first parameter is “A” .

Communication operation is same as Type A CPU card, refer to “contactless Type A,B card APDU communication” command.

5.21 Automatically test the type of IC card / contactless card

Command	“C” (43h)	90h	pm				
Positive	“P” (50h)	90h	pm	st1	st0	c_type0 (1 byte)	c_type1 (1 byte)
Negative	“N” (4Eh)	90h	pm	e1	e0		

pm = “0”(30h) automatically check the type of IC card.

Once ICRW receives this command, at first, moves the card inside to IC card position, then do reset operation on the card, judge the type of the card by ATR. This command is exactly suitable for integrated dealing with working of multi-IC cards.

Automatically success to test the type of the card, deactivate the IC card, again do operation for the IC card, reset command is must be done.

When getting unknown type of the card in automatic testing, again moves to the IC card position, again do auto-test once.

pm = “2”(32h) automatically test the type of contactless card

ICRW automatically moves card in front of the Mag-Head (operational position of contactless IC card), and do card type auto-test, responds the type of card. If it's positive, then deactivate contactless IC card, again do the same operation previously to activate/search the contactless IC card.

c_type0	c_type1	Type of IC card	Type of RF card
“0”	“0”	Unknown type	Unknown type
“1”	“0”	T=0 CPU Card	Mifare one S50 card
	“1”	T=1 CPU Card	Mifare one S70 card
	“2”	-	Mifare one UL card
“2”	“0”	-	Type A CPU card
	“1”	24C01 Card	-
	“2”	24C02 Card	-
	“3”	24C04 Card	-
	“4”	24C08 Card	-
	“5”	24C16 Card	-
	“6”	24C32 Card	-
	“7”	24C64 Card	-
	“8”	24C128 Card	-
	“9”	24C256 Card	-
“3”	“0”	-	Type B CPU card
	“1”	SLE4442 Card	-
	“2”	SLE4428 Card	-

5.22 Command for the counting of Shutter, Contact, Magnetic Head working

Command	“C” (43h)	A1h	pm	type (1 byte)	w_data (8 byte)
Positive	“P” (50h)	A1h	pm	st1 st0	r_data (8 byte)
Negative	“N” (4Eh)	A1h	pm	e1 e0	

This command is used for reading or setting the count of wearing parts.

pm control reading or writing to count value.

 “0”(30h) read relevant count of operation

 “1”(31h) write relevant count of operation

type set command for the counting type

 “0” (30h) count of shutter opening

 “1” (31h) count of moving over the magnetic head

 “2” (32h) count of operation of the IC card

w_data count value to be set

 8 bit ASCII for decimal representation

 For example, count is 12345678 times, then w_data = “31h 32h 33h 34h 35h 36h 37h 38h”

r_data count value to be read. The format is same as w_data.

5.23 Read S/N of ICRW

Command	“C” (43h)	A2h	pm			
Positive	“P” (50h)	A2h	pm	st1	st0	sn (1-18 byte)
Negative	“N” (4Eh)	A2h	pm	e1	e0	

This command is used to get S/N of the ICRW (unique code for ICRW production/maintenance)

pm read S/N
“0”(30h) read S/N

sn read to get S/N
18bit ASCII for string presentation.

For example: 2013/12/17 produced CRT-310-(020)MR-LDN, sn should be S310020MR131217001, its label should be: S121217001

The meaning of the first letter:

- S: S/N presentation generated in production
- F: first time repairing
- U: second time repairing
- W: third time repairing

Repairing only changes the label on the body of ICRW, no changing ‘SN.

310: present the type of ICRW, for example: 310/284/288/530/540 etc;

020: present the version of ICRW, as the content of ‘(XXX)’ in CRT-310- (010) MR-LDN;

MR: present the specific main function of ICRW;

131217001: present production date, means the first ICRW produced in 2013/12/17.

6 Explanation of error code

6.1 Error in communication

Error code	Meaning	Clear Conditions
"00" (30h,30h)	To shows that received command was undefined	Cleared by receiving correct commands
"01" (30h,31h)	To show command parameter error	Cleared by receiving command with correct parameter.
"02" (30h,32h)	Supervisor: To show that ICRW executes Supervisor program code area. User: To show that un-executable command was received.	Cleared by receiving executable command
"03" (30h,33h)	The function may not be carried or be out of order.	The check of hardware is needed.
"04" (30h,34h)	To show that error data was included in command.	Cleared by receiving command including correct data.
"06" (30h,36h)	The key for the cipher function command is not received.	Cleared by the executing the key exchange procedure.
"B0" (42h,30h)	Other commands were received before performing initialize command after a power supply injection, reset or switch command ececution.	Execute initialize command.

6.2 Error at card feeding

Error code	Meaning	Clear Conditions
"10" (31h,30h)	To show that the card was not carried to the specific location after specified number of trial for specified time duration during execution of command of carrying card in various ways	To execute a command again and a card is conveyed in a normal position. Or, cleared when the card is taken out from the card reader manually. In this case, confirm the recovery by Status request command.
"11" (31h,31h)	To show that the full shutter does not close when the card entry is completed.	Cleared in case card is returned to card gate by eject command. After the card is inserted, the unexpected objects are inserted into the gate or the full shutter is not work collect. Please conform those condition.
"13" (31h,33h)	To show that the card longer than 88.5mm is inserted into ICRW.	Cleared in case card is returned to card gate by eject command.

INTERFACE SPECIFICATION	CRT-310-NU01	83/90
--------------------------------	--------------	-------

"14" (31h,34h)	To show that the card shorter than 83.5mm is inserted into ICRW.	Cleared in case card is returned to card gate by eject command.
"16" (31h,36h)	To show that card staying inside the ICRW was moved up to the point where status request information changes.	Cleared in the case card is ejected.
"17" (31h,37h)	To show that the card was not carried to the specific location after specified number of trial for specified time duration during execution of Retrieve command.	To execute a Retrieve command again and a card is normally taken in. Or, cleared when the card is taken out from the card reader manually. Confirm the recovery by Status request command in this case.
"18" (31h,38h)	ICRW detected that two cards were inserted, and ejected it.	Remove ejected card from a gate.
"40" (34h,30h)	To show that card is pulled out against card feed in operation.	Command execution is normally possible continuously.

6.3 Error in reading card

The following errors may be recovered if ICRW re-take in and read a card.

Error code	Meaning	Clear Conditions
"20" (32h,30h)	To show that parity error exists in read error.	When an error is not recovered after this operation, it is unrecoverable since magnetic record of a card is unusual.
"21" (32h,31h)	To show that other read error than "20""22" "23"	
"23" (32h,33h)	To show that only start sentinel, end sentinel, LRC are contained in the card. There are no contents of data	
"24" (32h,34h)	To show that the card has no magnetic track. For entry and enable command. with mag check, this code is used to indicate error.	

6.4 Other error codes

Error code	Meaning	Clear Conditions
"30" (33h,30h)	To show that power down (or power cut in short instant) is detected(or being detected).It is to be recognized as normal power down if back up power supply goes down below +12V.	Cleared when a card is ejected and pulled out after a power supply recovery.
"31" (33h,31h)	To show that DSR signal was turned to off (communication is cut)	Cleared when a card is ejected and pulled out after DSR signal recovery.

7 ANNEX

7.1 ANNEX 1 Calculation method of CRCC

CRCC($X_{16}+X_{12}+X_5+1$) is made by the following method.

```

/*
    [data]
    hex0xF2, 0x00, 0x08, 0x43, 0x30, 0x30, 0x33, 0x32, 0x34, 0x30, 0x30
    CRC0xFACE
*/
#define INIT0x0000/* Initial value */
#define POLYNOMIAL 0x1021/* Polynomial  $X_{16}+X_{12}+X_5+1$  */
unsigned short calc_crc(unsigned short crc,unsigned short ch);
unsigned short GetCRC(unsigned char *p,unsigned short n);

unsigned short calc_crc(unsigned short crc,unsigned short ch)
{
    unsigned short i;
    ch <= 8;
    for (i = 8; i > 0; i--) {
        if ((ch ^ crc) & 0x8000) {
            crc = (crc << 1) ^ POLYNOMIAL;
        }
        else {
            crc <= 1;
        }
        ch <= 1;
    }
    return crc;
}
/* Generate GetCRC */
unsigned short GetCRC(unsigned char *p,unsigned short n)
{
    unsigned char ch;
    unsigned short i;
    unsigned short crc = INIT;
    for (i = 0; i < n; i++) {
        ch = *p++;
        crc = calc_crc(crc,(unsigned short)ch);
    }
    return crc;
}
int main(void)
{
    /* Transmission command
    STX : F2H  LEN : 00 08H  TEXT: Initialize command ("C0032400")
    unsigned char TransCommand[13]   ={0xF2,0x00,0x08,0x43,0x30,0x30,0x33,0x32,0x34,0x30,
    0x30,0x00,0x00};
    unsigned short TextLength = 11;    /* length of (STX+LEN+TEXT) */
    unsigned short crc;    /* CRC */
    crc = GetCRC(TransCommand, TextLength); TransCommand[11] = (crc >> 8) & 0xFF;
    TransCommand[12] = crc & 0xFF;
    return 0; }

```

7.2 Annex2 : Supportable TA1 & TA2 values

Vcc	Condition	Support	Communication speed (F, D)
"0"(30h)	TA1='any' and TA2=none (Negotiable mode)	Yes	Comply with table A2-2
	TA1='any' and TA2.b5=0(Specific mode)	Yes (*1)	Comply with table A2-4
	TA2.b5=1	No	
30h 33h 35h 36h	TA1='any' and TA2=none (Negotiable mode)	Yes	Comply with table A2-3
	TA1='any' and TA2.b5=0(Specific mode	Yes(*1)	Comply with table A2-4
	TA1='any' and TA2.b5=1	Yes	9622bps(F=372,D=1)
"@ " (40h)	TA1='any' and TA2=none (Negotiable mode)	Yes	9622bps(F=372,D=1)
	TA1='any' and TA2.b5=0 (Specific mode)	Yes(*1)	Comply with table A2-4
	TA1='any' and TA2.b5=1	Yes	9622bps(F=372,D=1)

Vcc is defined by Activate ICC(SAM) command.

(*1) When TA1 exists in following tables, ICRW supports its TA1.

Table A2-2 – Supportable TA1 values and PPS request in EMV mode

ATR			PPS request			Transmission speed
TA1	F	D	PPS1	F	D	
02h	372	2	02h	372	2	Transmission speed depends on PPS response of PPS1
03h	372	4	03h	372	4	
12h	372	2	12h	372	2	
13h	372	4	13h	372	4	
32h	744	2	32h	744	2	
33h	744	4	33h	744	4	
48h	1116	12	48h	1116	12	
53h	1488	4	43h	1488	4	
54h	1488	8	54h	1488	8	
55h	1488	16	55h	1488	16	
69h	1860	20	69h	1860	20	
92h	512	2	92h	512	2	
93h	512	4	93h	512	4	

INTERFACE SPECIFICATION	CRT-310-NU01	86/90
-------------------------	--------------	-------

B2h	1024	2	B2h	1024	2	
B3h	1024	4	B3h	1024	4	
B4h	1024	8	B4h	1024	8	
C8h	1536	12	C8h	1536	12	
D3h	2048	4	D3h	2048	4	
D4h	2048	8	D4h	2048	8	
D5h	2048	16	D5h	2048	16	
All other values of TA1			none			f=3.58MHZ Transmission speed(bps)=9622bps

Note: If the card returns echoing PPS1, transmission speed is changed to table A2-4. If the card doesn't transmit PPS1, transmission speed is default (not changed).

Table A2-3-Supportable TA1 values and PPS request in ISO mode

ATR			PPS request			Transmission speed
TA1	F	D	PPS1	F	D	
02h	372	2	02h	372	2	Transmission speed depends on PPS response of PPS1
03h	372	4	03h	372	4	
04h	372	8				
05h	372	16				
06h	372	32				
07h	372	64				
08h	372	12				
09h	372	20				
12h	372	2	12h	372	2	
13h	372	4	13h	372	4	
14h	372	8				
15h	372	16				
16h	372	32				
17h	372	64				
18h	372	12				
19h	372	20				
32h	744	2	32h	744	2	
33h	744	4	33h	744	4	
34h	744	8				
35h	744	16				
36h	744	32				
37h	744	64				
38h	744	12				
39h	744	20				
48h	1116	12	48h	1116	12	

INTERFACE SPECIFICATION	CRT-310-NU01	87/90
-------------------------	--------------	-------

53h	1488	4	53h	1488	4	
54h	1488	8	54h	1488	8	
55h	1488	16	55h	1488	16	
56h	1488	32				
57h	1488	64				
58h	1488	12				
59h	1488	20				

ATR			PPS request			Transmission speed
TA1	F	D	PPS1	F	D	
69h	1860	20	69	1860	20	Transmission speed depends on PPS response of PPS1
92h	512	2	92h	512	2	
93h	512	4	93h	512	4	
94h	512	8				
95h	512	16				
96h	512	32				
97h	512	64				
98h	512	12				
99h	512	20				
B2h	1024	2	B2h	1024	2	
B3h	1024	4	B3h	1024	4	
B4h	1024	8	B4h	1024	8	
B5h	1024	16				
B6h	1024	32				
B7h	1024	64				
B8h	1024	12				
B9h	1024	20				
C8h	1536	12				
D3h	2048	4	D3h	2048	4	
D4h	2048	8	D4h	2048	8	
D5h	2048	16	D5h	2048	16	
D6h	2048	32				
D7h	2048	64				
D8h	2048	12				
D9h	2048	20				
All other values of TA1			None			F=3.58MHz, Transmission speed (bps)=9622bps

Note: If the card returns echoing PPS1, transmission speed is changed to table A2-4. If the card doesn't transmit PPS1, transmission speed is default (not changed).

Table A2-4-Supportable TA1 in case of specific mode

TA1	F	D	F(MHz)	Transmission speed (bps) =1 / (current etu) current etu =F/ (D*F)
-----	---	---	--------	--

INTERFACE SPECIFICATION

CRT-310-NU01

88/90

01h	372	1	3.58	9622
02h	372	2	3.58	19245
03h	372	4	3.58	38490
11h	372	1	3.58	9622
12h	372	2	3.58	19245
13h	372	4	3.58	38490
31h	744	1	7.16	9622
32h	744	2	7.16	19245
33h	744	4	7.16	38490
34h	744	8	3.58	38490
48h	1116	12	3.58	38490
52h	1488	2	7.16	9622
53h	1488	4	7.16	19245
54h	1488	8	7.16	38490
55h	1488	16	3.58	38490
69h	1860	20	3.58	38490
91h	512	1	3.58	6991
92h	512	2	3.58	13983
93h	512	4	3.58	27965
B1h	1024	1	7.16	6991
B2h	1024	2	7.16	13983
B3h	1024	4	7.16	27965
B4h	1024	8	3.58	27965
C8h	1536	12	3.58	27965
D2h	2048	2	7.16	6991
D3h	2048	4	7.16	13983
D4h	2048	8	7.16	27965
D5h	2048	16	3.58	27965

7.3 ANNEX3 Values of ATR parameter

Table4: Supported values of ATR

Vcc \ ATR	30h		33h	35h	36h	38h	40h
	Supported values						
TS	3Fh, 3Bh						
T0	See ANNEX2						
TA1	See ANNEX2						
TB1	00h (cold reset) any value (warm reset) (*1)		Any value (*1)				
TC1	Any value						
TD1	m. s. nibble : any value l. s. nibble : 0 or 1						
TA2	ANNEX2 and TA2 l.s. nibble = TD1 l.s .nibble		See ANNEX2				
TB2	None(prohibit)		Any value				
TC2	01h ... FFh						
TD2	m. s. nibble: any value l.s. nibble: 1,14		m. s. nibble : any value l.s. nibble :any value				
NOT T=15	10h ... FEh		01h ... FEh				
TA3,TA4							
TB3,TB4			m .s .nibble :0...4 and l.s. nibble :0...5 and 2 ^{CW} >(N+1)				
TC3,TC4			Any value				
TD3,TD4			Any value				
T=15	(*2)						
TA3			b1 =1	b2 = 1 or b1 = 1	b1 =1 or b2 =1or b3 = 1	Any value	
TB3,TC3, TD3			Any value				
TA4			b1 = 1	b1 =1	b2 = 1 or b1 = 1	b1 =1 or b2=1or b3 = 1	Any value
TB4,TC4, TD4			Any value				

A meaning of Vcc parameter please refer 'activate ICC command;.

(*1) ICRW does not generate Vpp.

(*2)'F'=(T=15) is prohibited in TD2 l. s. nibble.

7.4 ANNEX 4 C-APDU Format

The C-APDU consists of a mandatory header of four consecutive bytes denoted CLA, INS, P1 and P2, followed by a conditional body of variable length. The meanings of every byte are below.

	byte	Meanings
Mandatory Header	CLA	Instruction class
	INS	Instruction code
	P1	Instruction Parameter 1
	P2	Instruction Parameter 2
Conditional Body	Lc	Byte length of Data Field
	Data	Data Field
	Le	Byte Length of Expected Response Length.

About the details of each byte, refer to specifications of every card's standard.

The C-APDU structure has following four cases.

Case	Structure							
1	CLA	INS	P1	P2				
2	CLA	INS	P1	P2	Le			
3	CLA	INS	P1	P2	Lc	Data		
4	CLA	INS	P1	P2	Lc	Data	Le	

The host shall transmit the command of case 1, case2, case3 and case4 correctly.

Especially for the case 1 on T=0 protocol, ICRW adds '00' internally as the fifth byte of the command to the card.