INTERFACE SPECIFICATION

Type Name :

ICT3K5-3R6940

Spec. No.	ASL-NP-09085-01

Notes :

ISSUED
AUG. 17 2004
ENG.DIV
SANKYOSEIKI MFG.CO.,LTD.

SGH	1									
Distribution	No. of sheet									
			Sym.	Revision		Page	Cha. No.	Date	By	Appr.
						Reference Document				
	Custody		Design	T.Shiomi	May.31,2004					
			Det-che	F.Akahane	May.31,2004					
		Type Name	Appro.	Y.Uemura	Jun.01,2004	SANKYO SEIKI MFG.CO.,LTD. JAPAN				

REGISTERED JUN.3.2004 ENG.DIV

No. S39Z-032-00-02B

Revision History

Rev.	Date	Author	Description
A	May 31, 2004	T.Shiomi	First Edition

This page left intentionally blank.

Function implementation table

This model implements the following functions in the specification.

Hard Ware Functions		Function (**V**:Available)
Magnetic Stripe Read	ISO Track #1	**V**
	ISO Track #2	**V**
	ISO Track #2	**V**
	JIS **II** Track	**-**
Contact IC Card	T=0,T=1, Memory Card (SLE4442/4428,4406,I2C)	**V**
Contactless IC Card		**-**
Mechanism	Capture Mechanism	**V**
	Shutter Type (Full Shutter or Pin Shutter)	**Full**

Section	Command	cm	pm	Details of operation	Function (**V**:Available)
5.Command list of Supervisor program code area					
5.1	INITIALIZE	30H	30H	Designate communication format	**V**
5.2	REVISION	41H	30H	Send the revision of Supervisor program code area	**V**
5.3	DOWNLOAD	4AH	30H	Erase the User program code area	**V**
			31H	Execute download	**V**
			32H	Confirm User program code area	**V**
			33H	Inquire download count	**V**
5.4	SWITCH	4BH	30H	Switch to the User program code area	**V**
7.Command list of User program code area					
7.1	INITIALIZE	30H	30H	Initialize and designate ICRW and eject a card	**V**
			31H	Initialize and designate ICRW and capture a card	**V**
			32H	Initialize and designate ICRW and re-positioning a card	**V**
			33H	Initialize and designate ICRW with no card operation	**V**
			38H	Initialize parameter report	**V**
7.2	STATUS REQUEST	31H	30H	Report presence of card and its position	**V**
			31H	Report presence of sensor status in detail	**V**
7.3	ENTRY	32H	30H	Card Entry (Mag-Track read)	**V**
7.4	CARD CARRY	33H	30H	Move card to Gate from inside of ICRW	**V**
			31H	Capture card to rear side of ICRW	**V**
7.5	RETRIEVE	34H	30H	Retrieve card from eject position	**V**
7.6	LED	35H	30H	All Color LED Off	**V**
			31H	Green On from All Off or directly from Other Color On	**V**
			32H	Red On from All Off or directly from Other Color On	**V**
			33H	Orange On from All Off or directly from Other Color On	**V**
7.7	Mag-Track READ	36H	31H	ISO Track #1 reads Transmit read data	**V**
			32H	ISO Track #2 reads Transmit read data	**V**
			33H	ISO Track #3 reads Transmit read data	**V**
			34H	JIS II Track reads Transmit read data	**-**
			35H	Transmit All channel data	**V**
			37H	Data buffer status read	**V**
			39H	ISO Track #1 another reads Transmit read data	**V**
			3AH	ISO Track #2 another reads Transmit read data	**V**
			3BH	ISO Track #3 another reads Transmit read data	**V**
			3CH	JIS II Track another reads Transmit read data	**-**
	Mag-Track READ with DATA ENCRYPTION	36H	41H	ISO Track #1 reads Transmit read data	**V**
			42H	ISO Track #2 reads Transmit read data	**V**
			43H	ISO Track #3 reads Transmit read data	**V**
			44H	JIS II Track reads Transmit read data	**-**
			45H	Transmit All channel data	**V**
			49H	ISO Track #1 another reads Transmit read data	**V**
			4AH	ISO Track #2 another reads Transmit read data	**V**
			4BH	ISO Track #3 another reads Transmit read data	**V**
			4CH	JIS II Track another reads Transmit read data	**-**

Section	Command	cm	pm	Details of operation	Function (**V**:Available)
7.8	ENABLE / DISABLE	3AH	30H	Enable card entry	**V**
			31H	Disable card entry	**V**
7.9	PORT IN / OUT	3DH	30H	Enter maintenance mode	**V**
			31H	Release maintenance mode	**V**
			32H	Check operation of a motor and solenoid	**V**
			33H	Check operation of a sensor	**V**
7.10	SENSOR LEVEL TRANSMIT	3EH	30H	Transmit the sensor A/D level on normal condition	**V**
			31H	Transmit the sensor A/D level on adjust condition	**V**
7.11	REVISION	41H	31H	Revision of User program code area	**V**
			32H	Revision of ICC control code area	**V**
			33H	Transmit the EMV approval number	**V**
			34H	Transmit the GIE-CB approval number	**V**
			35H	Transmit the IFM number of the EMV approval	**V**
7.12	COUNTER	43H	32H	Inquire of card pass count	**V**
			33H	Inquire of card capture count	**V**
			34H	Set capture alert count	**V**
7.13	IC CARD CONTROL	49H	30H	Activate ICC	**V**
			31H	Deactivate ICC	**V**
			32H	Inquire of ICC status	**V**
			33H	ICC communication T=0	**V**
			34H	ICC communication T=1	**V**
			35H	ICC extended communication 1	**V**
			36H	ICC extended communication 2	**V**
			37H	ICC extended communication 3	**V**
			38H	ICC Warm reset	**V**
			39H	ICC automatic communication	**V**
	OFFLINE PIN VERIFICATION	49H	53H	ICC communication T=0 using Triple DES	**V**
			54H	ICC communication T=1 using Triple DES	**V**
			59H	ICC automatic communication using Triple DES	**V**
			63H	ICC communication T=0 using Single DES	**V**
			64H	ICC communication T=1 using Single DES	**V**
			69H	ICC automatic communication using Single Triple DES	**V**
7.14	SAM CONTROL	49H	40H	Activate to SAM	**V**
			41H	Deactivate SAM	**V**
			42H	Inquire of SAM status	**V**
			43H	SAM communication T=0	**V**
			44H	SAM communication T=1	**V**
			45H	SAM extended communication 1	**V**
			46H	SAM extended communication 2	**V**
			47H	SAM extended communication 3	**V**
			48H	SAM Warm reset	**V**
			49H	SAM automatic communication	**V**
			50H	Select SAM	**V**
7.15	SWITCH	4BH	30H	Switch to Supervisor program code area	**V**

Section	Command	cm	pm	Details of operation	Function (**V**:Available)
7.16	Siemens Memory Card Control	52H	30H	Power Supply and Activate to Siemens card	**V**
			31H	Deactivate to Siemens card	**V**
			32H	Inquire of ICR status for Siemens card	**V**
			33H	Exchange data for SLE4442 card	**V**
			34H	Exchange data for SLE4428 card	**V**
			35H	Exchange data for SLE4406 card	**V**
7.17	I2C MEMORY CONTROL	53H	30H	To activate I2C and To close the shutter	**V**
			31H	To deactivate I2C	**V**
			32H	To inquire status of I2C	**V**
			33H	To exchange data between I2C	**V**
7.18	Contactless IC CARD CONTROL	5AH	33H	Contactless ICRW control	**-**
			34H	Exchange data with IC card by T=CL protocol	**-**
			35H	Transmit chaining data to contactless IC card by T=CL protocol	**-**
			36H	Transmit Last chaining data to contactless IC card by T=CL protocol	**-**
			37H	Require of chaining data by T=CL	**-**
			38H	Reset Contactless ICRW	**-**
7.19	SECURITY	47H	30H	Device authentication data exchange and key exchange key loading	**V**
			31H	Key loading for the magnetic data	**V**
			32H	Key loading for the Plaintext offline PIN verification	**V**
		-----	-----	New master exchange key loading	**V**
9	RAS Function	Power on / Reset		RAS function	**V**
ANNEX 1				Calculation method of CRCC	**V**
ANNEX 2, 3, 4, 5,6				Additional explanation of ICC control function	**V**

Contents

1. Logic level 4
1.1 Transmission / Control Specification 4
1.2 Transmission control method 4
1.3 Transmission Control Characters 4
1.4 Transmission Format 4
2. Transmission / Control protocol 5
2.1 Timing chart 5
2.2 Cancel of command 6
2.3 Protocol 6
2.3.1 Ordinary operation 6
2.3.2 Irregular operation and back-up 7
2.3.3 State transition matrix 8
3. Command /Response 10
3.1 Text format 10
3.2 Structure of Firmware areas 11
4. Supervisor program code area 12
4.1 Command list 12
4.2 Status code 12
4.3 Error code 12
5. Command explanation of Supervisor program code area 13
5.1 Initialize command 13
5.2 Revision command 13
5.3 Download command 14
5.4 Switch command 17
6. User program code area 18
6.1 Command list 18
6.2 Status code 21
6.3 Error code 21
7. Command explanation of User program code area 24
7.1 Initialize command 24
7.2 Status request command 26
7.3 Entry command 27
7.4 Card carry command 28
7.5 Retrieve command 28
7.6 LED command 29
7.7 Mag-Track Read command 30
7.8 Enable/Disable command 32
7.9 Port In/Out command 33
7.10 Sensor Level transmit command 35
7.11 Revision command 35
7.12 Counter command 36

7.13 IC Card control command 37
7.13.1 Activate ICC command 37
7.13.2 Deactivate ICC command 38
7.13.3 Inquire ICC status command 39
7.13.4 ICC communication T=0 40
7.13.5 ICC communication T=1 41
7.13.6 ICC extended communication 1 43
7.13.7 ICC extended communication 2 44
7.13.8 ICC extended communication 3 45
7.13.9 ICC warm reset 46
7.13.10 ICC automatic communication 47
7.13.11 Plaintext offline PIN verification 48
7.14 SAM (Secure Application Module) control command 49
7.14.1 Activate SAM command 49
7.14.2 Deactivate SAM command 50
7.14.3 Inquire SAM status command 51
7.14.4 SAM communication T=0 52
7.14.5 SAM communication T=1 53
7.14.6 SAM extended communication 1 55
7.14.7 SAM extended communication 2 56
7.14.8 SAM extended communication 3 57
7.14.9 SAM warm reset 58
7.14.10 SAM automatic communication 59
7.14.11 Select SAM 60
7.15 Switch command 61
7.16 Siemens memory card control command 62
7.16.1 Siemens memory card Power on 62
7.16.2 Siemens memory card Power off 63
7.16.3 Inquire Status of Siemens memory card 64
7.16.4 Communicate with SLE4442 65
7.16.4.1 Data read from main memory on SLE4442 65
7.16.4.2 Data read from protection memory on SLE4442 66
7.16.4.3 Data read from security memory on SLE4442 66
7.16.4.4 Data write to main memory on SLE4442 67
7.16.4.5 Data write to protection memory on SLE4442 68
7.16.4.6 Data write to security memory on SLE4442 69
7.16.4.7 Verification data present to SLE4442 70
7.16.5 Communicate with SLE4428 71
7.16.5.1 Data Reading of main-memory of SLE4428 71
7.16.5.2 Condition data reading of protection-bit of SLE4428 72
7.16.5.3 Data writing to main-memory of SLE4428 73
7.16.5.4 Data writing to main-memory of SLE4428 (with protecting it) 73
7.16.5.5 Protection-bit is written by the completion of the verification 74
7.16.5.6 Verification data present to SLE4428 75
7.16.6 Communicate with SLE4406 76
7.16.6.1 Verification data present to SLE4406 76
7.16.6.2 Data Reading of memory of SLE4406 77
7.16.6.3 Data writing to memory of SLE4406 78
7.16.6.4 Reloading to counter stage of SLE4406 79

7.17 I2C memory card control command 80
7.17.1 I2C Power on 80
7.17.2 I2C Power off 81
7.17.3 Inquire Status of I2C 82
7.17.4 I2C Communication 83
7.17.4.1 Read data from I2C 84
7.17.4.2 Write data into I2C 85
7.18 Contactless IC card control 86
7.18.1 Contactless ICRW control 86
7.18.2 Contactless IC card communication 1 87
7.18.3 Contactless IC card communication 2 88
7.18.4 Contactless IC card communication 3 88
7.18.5 Contactless IC card communication 4 89
7.18.6 Contactless IC card reset 89
7.18.7 Example 90
7.19 Security command 91
7.19.1 Device authentication data exchange and key exchange key loading 91
7.19.2 Key loading for the magnetic data 91
7.19.3 Key loading for the Plaintext offline PIN verification 92
7.19.4 New master exchange key loading 92
8. Explanation of error code 94
8.1 Error in communication soft 94
8.2 Error at card feeding 94
8.3 Error in reading card 95
8.4 Other error codes 95
9. RAS (Reliability, Availability, and Serviceability) Function 96
9.1 The power on / reset boot mode 96
9.2 The boot check items and result 96
9.3 The condition for boot on RAS mode 96
9.4 The finish condition of RAS mode 97
9.5 The overview of RAS operation 97
9.6 The check items and the error indications of RAS 97
9.7 The not checked functions by RAS 97
9.8 The flow chart of RAS operation 98
ANNEX 1 Calculation method of CRCC 99
ANNEX 2 Values of ATR parameter (TA1 and TA2) 100
ANNEX 3 Values of ATR parameter 102
ANNEX 4 C-APDU Format 103
ANNEX 5 Sequence of activating IC card / SAM 104
ANNEX 6 Method of IC card communication 110

1. Logic level

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 can not be switched to another protocol during communication.

1.1 Transmission / Control Specification

1) Synchronous method : Asynchronous
2) Transmission method : Half duplex
3) Baud rate : 9600, 19200, 38400, 115200 BPS (automatic recognition)

note) Baud rate is recognized and set up by STX of the first time command after a power-on / reset, and it is cleared by power-off/reset.
Therefore, baud rate recognition and a setup are not performed for every initialization command.
The parity check result of the following data of STX is also made into recognition conditions as a measure against an incorrect recognition.

4) Data length : 8bit + 1 parity

ST	b0	b1	b2	b3	b4	b5	b6	b7	P	SP

5) Stop bit : 1 bit
6) Character Code : ASCII 8 bit code
7) Parity check method : Vertical (Even) parity check

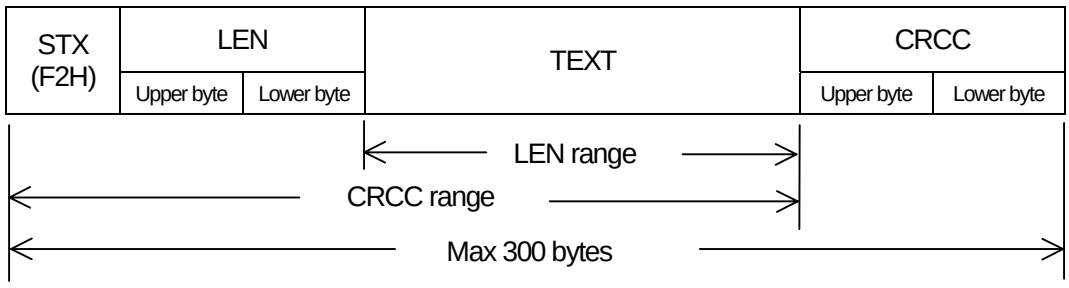
1.2 Transmission control method

Command / Response method
ICRW executes particular operation according to text (command) received from HOST then reports result of execution to HOST.

1.3 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 (2bytes)	Text length.
TEXT	Command or response.
CRCC (2bytes)	Cyclic redundancy code. Polynomial X16+X12+X5+1. Initial value is 0000H.

1.4 Transmission Format



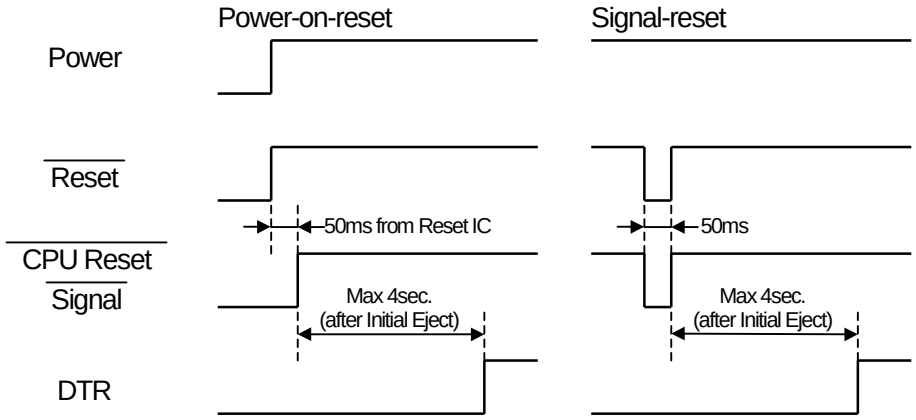
Notes 1.Gap between characters STX to CRCC is less than 250 msec.

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.
At the time of RAS mode operation, “DTR” is not turned on until ICRW ends RAS operation and changes to the normal mode. “DTR” is turned off while detecting the fall of power supply voltage.



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 characters data is completed.

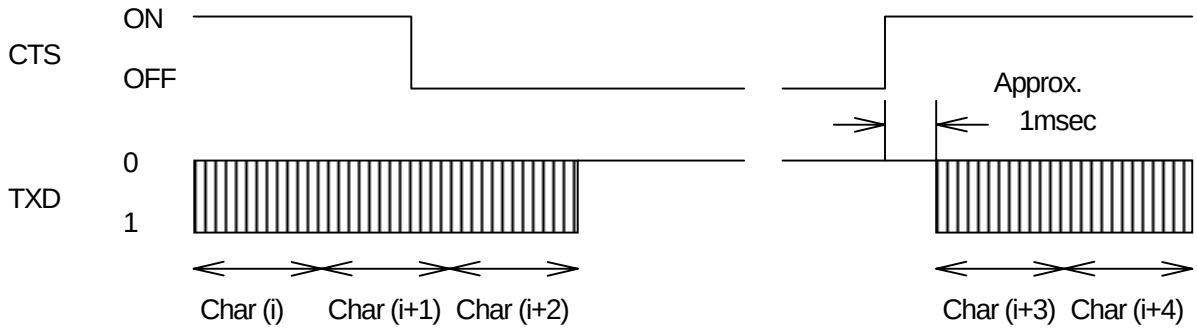
4) Monitoring state of HOST

ICRW is monitoring "DTR" from HOST.
When "DTR" is off, ICRW considers that the state of HOST is not normal and interrupts the command under execution.
It depends on specification by initialize command whether a card ejects after that.

5) Cancel/Resume of transmission (User program code area only)

During text transmission from ICRW, when CTS signal goes OFF, ICRW stops its transmission with Max 2 characters' delay.

After CTS is turned on, text transmission is resumed within about 1msec.



6) Eject Operations (User program code area only)

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.

Therefore, the eject2 command is not necessary to 8bit mode.

2.2 Cancel of command

(User program code area only)

When ICRW receives "DLE,EOT", ICRW will interrupt execution of a command immediately.

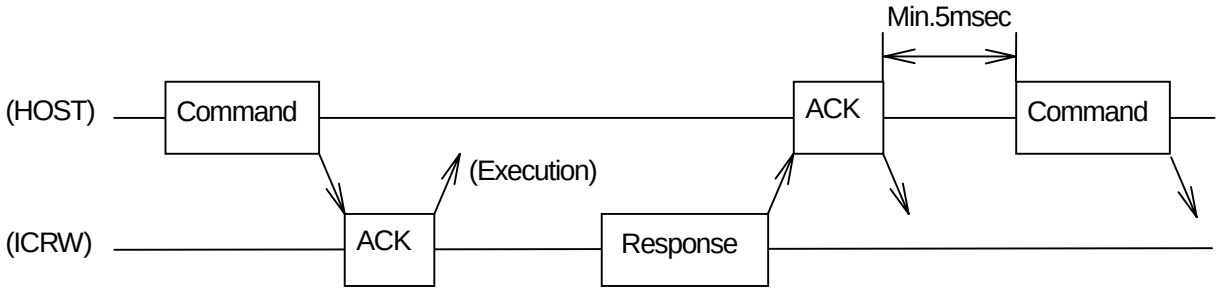
And then ICRW transmits "DLE,EOT" and waits for the following command.

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

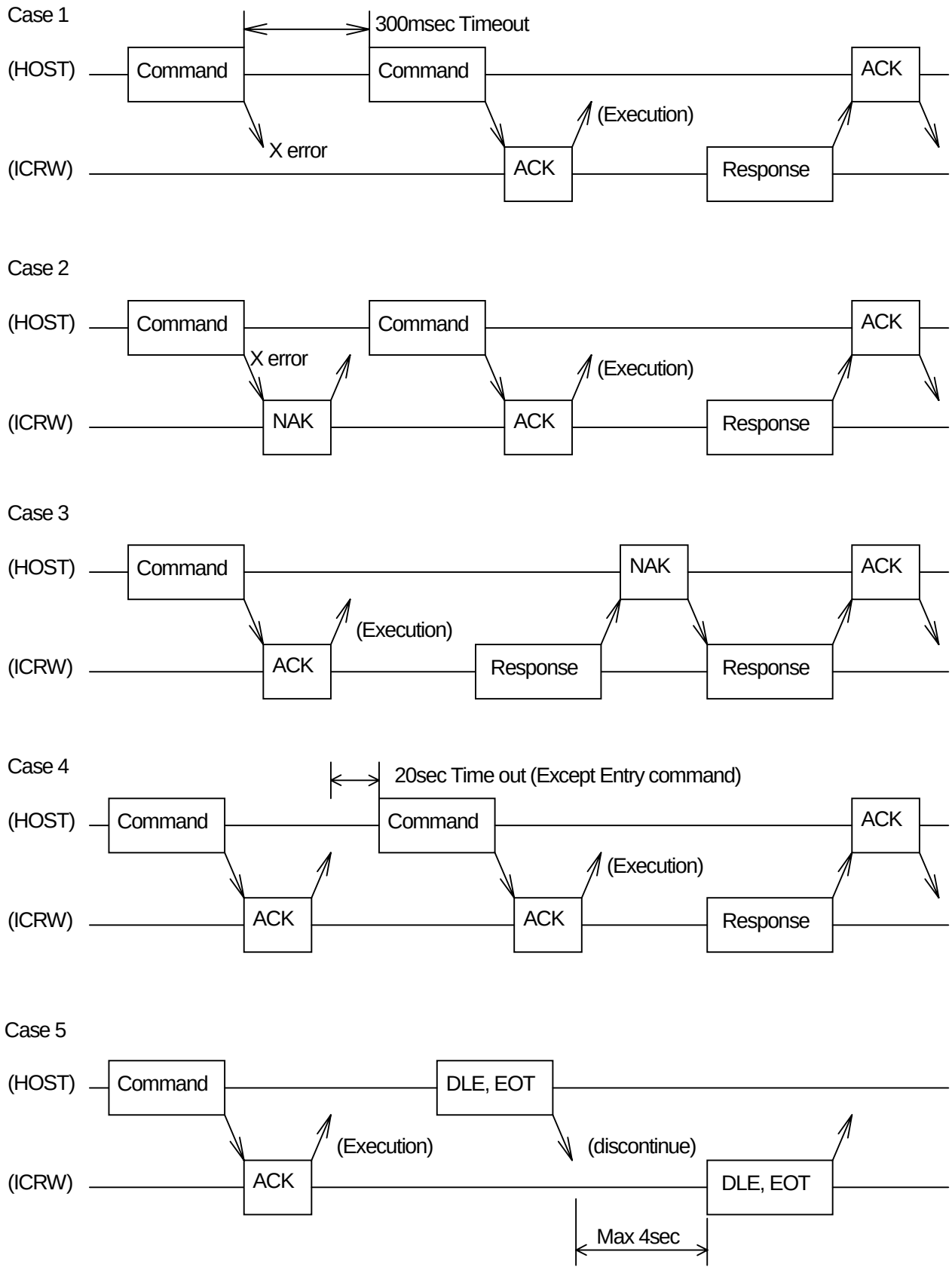
If "DLE,EOT" is received for the entry, retrieve, and eject commands at the time of execution, each operation will be interrupted and a card will be ejected.

2.3 Protocol

2.3.1 Ordinary operation



2.3.2 Irregular operation and back-up



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)* (except Entry)	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 in the Length. Receive the Length bytes then go to (5)				Send NAK Go to (2)	250msec
(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)	250msec

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

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 send 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 send DLE,EOT	Ignore	go to (1)	300msec

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

3. Command /Response

HOST sends command to ICRW and instruct operation.
Command is followed by data necessary for operation.
ICRW sends result of execution as response.
Command must be transmitted more than 5msec after sending ACK to the response from ICRW.

3.1 Text format

An ASCII code is expressed as shown in "C", and a binary code is shown like 30H (= "0") by hexadecimal.
Command and response format is as follows.

"C"	30H	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"	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 commands with data part and without data part.

2) Positive response format (ICRW -> HOST)

"P"	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 values which were received with command transmission.
(pm : except for IC card control)

3) Negative response format (ICRW -> HOST)

"N"	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 “N”(=4EH).
There are negative responses with data part and without data part.
In this format cm and pm returns the same values which were received with command transmission.
(pm : except for IC card control)

3.2 Structure of Firmware areas

Firmware of ICRW is divided into two parts.

(1) Supervisor program code area
To execute the download and rewrite the firmware of a user part with directions of HOST.
HOST can not rewrite this area.

(2) User program code area
This area usually performs control of the function of ICRW.
HOST can reprogram this area (under 100 times).
If the firmware is downloaded normally in this area, ICRW executes the program in it after power-on.
So HOST usually doesn't care Supervisor program code area.

In case error response "02" arises in initialize command, User program code area is abnormal condition.
This state shows that ICRW executes Supervisor program code area.
And it needs to perform user part program rewriting by the download from HOST.

Switch command is to switch Supervisor program code area and User program code area.
Initialize command shall be executed when after Switch command is executed.

In addition to this, the firmware holds the sensor adjustment value for card detection,
the download counter of user program code area, and the path counter, as non-volatility data.
Moreover, since a firmware does not have the function of execution record of a command,
or memory dumping, it needs the communication log of HOST for the analysis of an error.

4. Supervisor program code area

4.1 Command list

cm: Command code pm: Parameters

Command	cm	Function	pm	Details of operation
INITIALIZE	30H	Initialize ICRW	30H	Designate communication format
REVISION	41H	Revision	30H	Send the revision of Supervisor program code area
DOWNLOAD	4AH	Download	30H	Erase the User program code area
			31H	Execute download
			32H	Confirm User program code area
			33H	Inquire download count
SWITCH	4BH	Area switch	30H	Switch to the User program code area

Notes. Example 30H present ASCII code, "0", "01" present ASCII character.
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"	always "00" in Supervisor program code area.

4.3 Error code

e1, e0 : error code

error code	Meaning
"00"	A given command code is unidentified
"01"	Parameter is not correct
"02"	Command execution is impossible. Under Supervisor program code area
"04"	Command data error
"70"	F-ROM write error
"71"	CRC error of user program code area
"B0"	Not received Initialize command

5. Command explanation of Supervisor program code area

5.1 Initialize command

Command	"C"	30H	30H	30H	30H	30H	30H	fm

Positive response Nothing

Negative response	"N"	30H	30H	30H	32H

Execute this command whenever power is turned on or after switch from User program code area.

fm : Not use. Always 30H.

A positive response is not transmitted to HOST with the initialization command of Supervisor program code area.
A response is surely set to negative response and returns the error code “02” to HOST.

5.2 Revision command

Command	"C"	41H	30H			
Positive response	"P"	41H	30H	30H	30H	Supervisor code area revision (ASCII 8bytes)
Negative response	"N"	41H	30H	e1	e0	

Eight characters that show firmware revision of Supervisor program code area
are added to an positive response, and it transmits to HOST.
Ex) "1234-01A"

5.3 Download command

Command	"C"	4AH	pm	Download Data(ASCII 176bytes)		
Positive response	"P"	4AH	pm	30H	30H	Download Count (ASCII 3bytes)
Negative response	"N"	4AH	pm	e1	e0	

Execution of this command rewrites program in the User program code area by downloading from HOST.
This command is used in case to write latest firmware.

pm=30H: Erase current User program code area.
Need to execute first to execute download.
Error "70" arise in case Erase isn't executed normally.
This error relates to board degradation. Need to change the board.

pm=31H: Write download data (Fixed length 176bytes).
HOST use this command write the date of download data file, Sankyo supplies, per each line.
Download is completed when all download data file is sent.
Error "70" arise in case Write isn't executed normally.
Repeat the download again (from pm=30H).

pm=32H: Execute the CRC check of User program code area and confirm it's condition.
Error "71" arise in case CRC check is wrong.
Repeat the download again (from pm=30H).

pm=33H: Inquire download count
This command reports the download count as three digit of ASCII decimal number.
100 times download is guaranteed by CPU on ICRW.

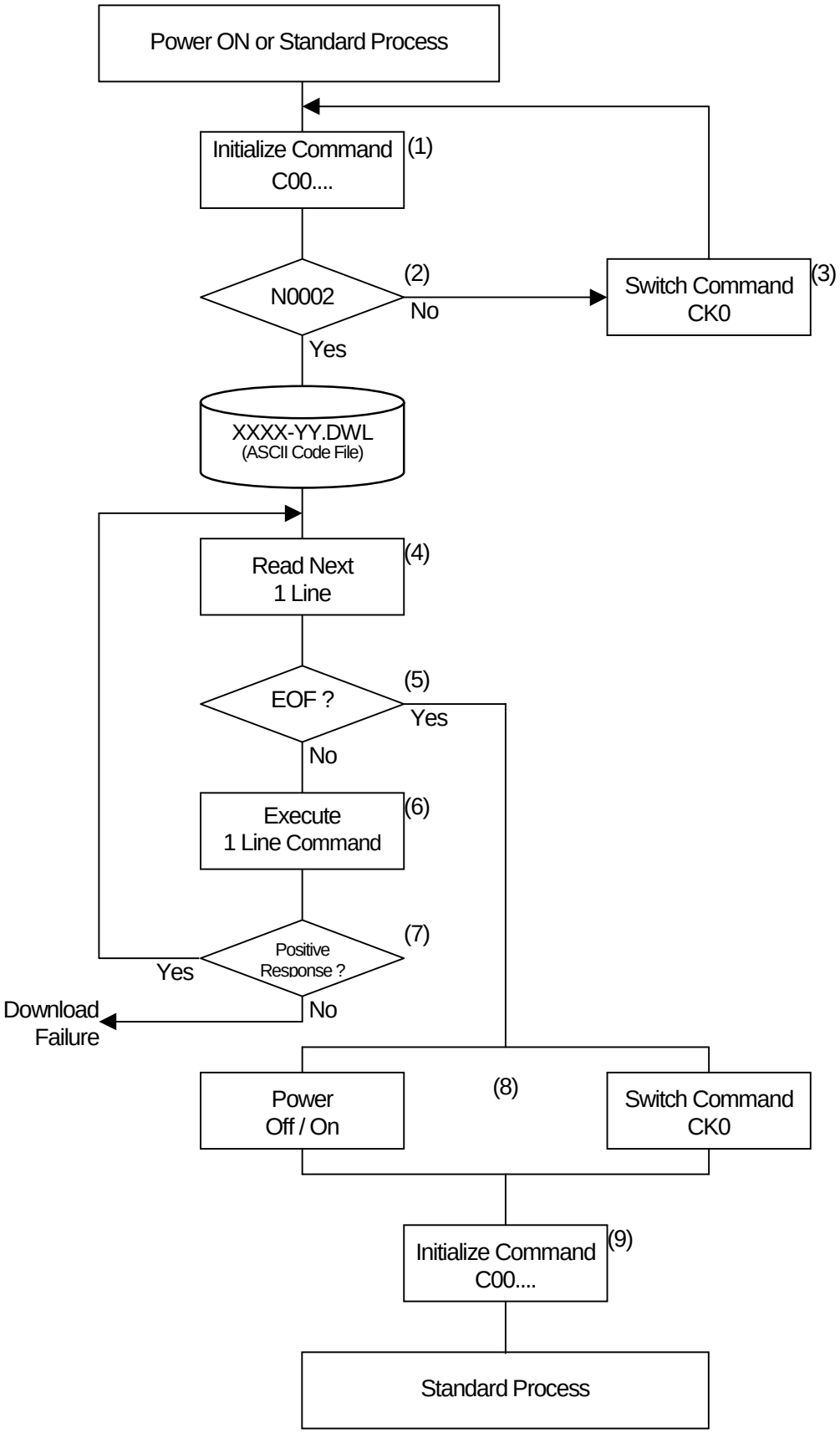
Structure of the file for downloading

```
Rev1234-01A [CRLF]                                          <= Sankyo revision Header
CJ0 [CRLF]                                                  <= Erase command.
CJ1xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx(176bytes) [CRLF]  <= transmit download data
    :                                                           :
CJ1xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx(176bytes) [CRLF]      :
CJ2[CRLF]                                                   <= CRC check command
(EOF)                                                       <= End of File
    (CTRL-Z(1AH) code is not added at the EOF)
```

Explanation of the download procedure

(1) Execute the Initialize command.
(2) If response is "N0002", the program in "Supervisor Program Area" is executed and goes to (4).
(3) If response is not "N0002", move to the "Supervisor Program Area" using "Switch command" and restart from (1).
(4) Characters are read from the 2nd line of the Download file except of CRLF that Sankyo supplies for line by line.
(5) If Host finds EOF then goes to (8). Downloading is completed.
(6) The characters read by (3) are sent to ICRW as a command.
(7) If ICRW detected positive response, goes to (4).
If ICRW detected negative response, downloading is failure.
(8) Reboot or change to "User Area Command" using "Switch command".
(9) Execute "Initialize command" and execute standard process.

The flow chart of the download procedure



5.4 Switch command

Command	"C"	4BH	30H		
Positive response	"P"	4BH	30H	30H	30H
Negative response	"N"	4BH	30H	e1	e0

Execute the CRC check of User program code area.
Switch the control to User program code area from Supervisor program code area in case of normal.
Error “71” arise and not switch to the User program code area, in case the CRC check is wrong.
Repeat the download again.

Note : Start from Initialize command of User program code area after the switch is completed.

ex) Under the supervisor program code area operation

↓

Switch command “CK0”

↓

Switch the control to User program code area

↓

Execute initialize command of user program code area

↓

Usual operation

6. User program code area

6.1 Command list

List1 cm: Command code pm: Parameters

Command	cm	Function	pm	Details of operation
INITIALIZE	30H	Initialize ICRW	30H	Initialize and designate ICRW and eject a card
			31H	Initialize and designate ICRW and capture a card
			32H	Initialize and designate ICRW and re-positioning a card
			33H	Initialize and designate ICRW with no card operation
			38H	Initialize parameter report
STATUS REQUEST	31H	Inquire status	30H	Report presence of card and its position
			31H	Report presence of sensor status in detail
ENTRY	32H	Card Entry	30H	Card Entry (Mag-Track read)
CARD CARRY	33H	Eject	30H	Move card to Gate from inside of ICRW
		Capture	31H	Capture card to rear side of ICRW
RETRIEVE	34H	Retrieve	30H	Retrieve card from eject position
LED	35H	LED Off	30H	All Color LED Off
		LED Green On	31H	Green On from All Off or directly from Other Color On
		LED Red On	32H	Red On from All Off or directly from Other Color On
		LED Orange On	33H	Orange On from All Off or directly from Other Color On
Mag-Track READ	36H	ISO #1 read	31H	ISO Track #1 reads Transmit read data
		ISO #2 read	32H	ISO Track #2 reads Transmit read data
		ISO #3 read	33H	ISO Track #3 reads Transmit read data
		JIS II read	34H	JIS II Track reads Transmit read data
		All tracks read	35H	Transmit All channel data
		Read Status	37H	Data buffer status read
		ISO#1 another read	39H	ISO Track #1 reads Transmit read data
		ISO#2 another read	3AH	ISO Track #2 reads Transmit read data
		ISO#3 another read	3BH	ISO Track #3 reads Transmit read data
		JIS II another read	3CH	JIS II Track reads Transmit read data
Mag-Track READ with DATA ENCRYPTION	36H	ISO #1 read	41H	ISO Track #1 reads Transmit read data
		ISO #2 read	42H	ISO Track #2 reads Transmit read data
		ISO #3 read	34H	ISO Track #3 reads Transmit read data
		JIS II read	44H	JIS II Track reads Transmit read data
		All tracks read	45H	Transmit All channel data
		ISO#1 another read	49H	ISO Track #1 reads Transmit read data
		ISO#2 another read	4AH	ISO Track #2 reads Transmit read data
		ISO#3 another read	4BH	ISO Track #3 reads Transmit read data
		JIS II another read	4CH	JIS II Track reads Transmit read data

List 2 cm: Command code pm: Parameters

Command	cm	Function	pm	Details of operation
ENABLE / DISABLE	3AH	Enable	30H	Enable card entry
		Disable	31H	Disable card entry
PORT IN / OUT	3DH	Mode Change	30H	Enter maintenance mode
			31H	Release maintenance mode
		Output port	32H	Check operation of a motor and solenoid.
		Input port	33H	Check operation of a sensor.
SENSOR LEVEL TRANSMIT	3EH	NORMAL check	30H	Transmit the sensor A/D level on normal condition
		for ADJUST	31H	Transmit the sensor A/D level on adjust condition
REVISION	41H	Revision	31H	Revision of User program code area
			32H	Version of EMV2000 code area
			33H	Transmit the EMV approval number
			34H	Transmit the GIE-CB approval number
			35H	Transmit the IFM number of the EMV approval
COUNTER	43H	Pass Counter Read	32H	Inquire of card pass count
		Capture Counter Read	33H	Inquire of card capture count
		Capture Alert Count Set	34H	Set capture alert count
SECURITY	47H	Device Authentication and Key Exchange Key Load	30H	Device authentication data exchange and key exchange key loading
		Key Loading for Magnetic Data	31H	Key loading for the magnetic data
		Key Loading for Offline PIN Verification	32H	Key loading for the offline PIN verification
	- - - -	New Master Exchange Key Loading	- - -	New master exchange key loading
IC CARD CONTROL	49H	Activate	30H	Activate ICC
		Deactivate	31H	Deactivate ICC
		Inquire Status	32H	Inquire of ICC status
		Communication T=0	33H	ICC communication T=0
		Communication T=1	34H	ICC communication T=1
		Communication 1	35H	ICC extended communication 1
		Communication 2	36H	ICC extended communication 2
		Communication 3	37H	ICC extended communication 3
		Warm Reset	38H	ICC Warm reset
		Automatic Communication	39H	ICC automatic communication
OFFLINE PIN VERIFICATION	49H	communication T=0 using Triple DES	53H	ICC communication T=0 using Triple DES
		communication T=1 using Triple DES	54H	ICC communication T=1 using Triple DES
		Automatic communication using Triple DES	59H	ICC automatic communication using Triple DES
		communication T=0 using Single DES	63H	ICC communication T=0 using Single DES
		communication T=1 using Single DES	64H	ICC communication T=1 using Single DES
		Automatic communication using Single DES	69H	ICC automatic communication using Single Triple DES

List 3 cm: Command code pm: Parameters

Command	cm	Function	pm	Details of operation
SAM CONTROL	49H	Activate	40H	Activate SAM
		Deactivate	41H	Deactivate SAM
		Inquire Status	42H	Inquire of SAM status
		Communication T=0	43H	SAM communication T=0
		Communication T=1	44H	SAM communication T=1
		Communication 1	45H	SAM extended communication 1
		Communication 2	46H	SAM extended communication 2
		Communication 3	47H	SAM extended communication 3
		Warm Reset	48H	SAM Warm reset
		Automatic Communication	49H	SAM automatic communication
		Select SAM	50H	Select SAM
SWITCH	4BH	Area switch	30H	Switch to Supervisor program code area.
Siemens Memory Card Control	52H	Power on	30H	Power Supply and Activate to Siemens card
		Power off	31H	Deactivate to Siemens card
		Status request	32H	Inquire status of Siemens card
		Communication	33H	Exchange data for 4442 card
		Communication	34H	Exchange data for 4428 card
		Communication	35H	Exchange data for 4406 card
I2C MEMORY CONTROL	53H	Activate I2C	30H	To activate I2C and To close the shutter
		Deactivate I2C	31H	To deactivate I2C
		Status of I2C	32H	To inquire status of I2C
		Communication	33H	To exchange data between I2C
Contactless IC CARD CONTROL	5AH	Contactless ICRW	33H	Contactless ICRW control
		Communication 1	34H	Exchange data with IC card by T=CL protocol
		Communication 2	35H	Transmit chaining data to IC card by T=CL protocol
		Communication 3	36H	Transmit Last chaining data to IC card by T=CL protocol
		Communication 4	37H	Require of chaining data by T=CL
		Reset	38H	Reset Contactless ICRW

Notes. Example 30H present ASCII code, "0", "01" present ASCII character.
Initialize command includes fixed original data.
Do not use any other codes than those shown by this table.

6.2 Status code

st1, st0 : ICRW status code

status code	Meaning
"00"	No card detected within ICRW (including card gate)
"01"	Card locates at card Gate
"02"	Card locates inside ICRW (Transport)

6.3 Error code

List 1 e1, e0 : error code

error code	Meaning
"00"	A given command code is unidentified
"01"	Parameter is not correct
"02"	Command execution is impossible.
"03"	Function is not implemented.
"04"	Command data error
"05"	
"06"	Key for decrypting is not received
"07"	
"08"	
"09"	
"10"	Card jam
"11"	Shutter error
"12"	
"13"	Irregular card length (LONG)
"14"	Irregular card length (SHORT)
"15"	Flash Memory Parameter Area CRC error
"16"	Card position Move (and Pull out error)
"17"	Jam error at retrieve
“18”	Two card error
"19"	

List 2 e1, e0 : error code

error code	Meaning
"20"	Read Error (Parity error (VRC error))
"21"	Read Error (Start sentinel error, end sentinel error or LRC error)
"22"	
"23"	Read Error (No data contents, only start sentinel, end sentinel and LRC)
"24"	Read Error (No magnetic stripe or not encorded)
"25"	
"26"	
"27"	
"28"	
"29"	
"30"	Power Down
"31"	DSR signal was turned to OFF
"32"	
"33"	
"34"	
"35"	
"36"	
"37"	
"38"	
"39"	Electric fan breaks down.

List 3 e1, e0 : error code

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

7. Command explanation of User program code area

7.1 Initialize command

* * * * =>See Notes 1

Command	"C"	30H	pm	33H	32H	34H	31H	fm	Pd	Ty	Ds	Cc	Re	30H	30H	Ce
Positive response	"P"	30H	pm	st1	st0	Type recognizing code (ASCII 16bytes)										
Negative response	"N"	30H	pm	e1	e0											

This command set the operation conditions for ICRW and initializes ICRW.
Execute this command whenever power on, reset and code area change from supervisor program to user program by switch command.
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.

Notes 1. * These parameters have no meaning, but remained for the command format compatibility to the command format of the other models. The parameter codes 30H to 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.
- 30H: Eject the card to the gate portion and finish the command even if the card is not taken out.
- 31H: Capture the card to the rear side.
- 32H: Re-position the card to the home position in the ICRW.
- 33H: Don't move the card.
- 38H: Initialize parameter report command

fm : Not used. Always 30H. (This code is not omissible.)

Pd : Power down card control
- 30H : The ICRW ejects the card in the ICRW. (Default value at omit this code)
- 31H : The ICRW keeps the card in the ICRW.

Ty : Reader type recognition code control

30H: No data is contained in the response. (Default value at omit this code)

31H: Response includes type recognition code.

Type recognition code (16bytes)	ISO#1	ISO#2	ISO#3	JIS II	IC contact	RF	Pinpad	Capture	Fan	Full Shutter	"0"	SAM1	SAM2	SAM3	SAM4	SAM5
	Magnetic Head : "0" = Not Available "1" = Available				Function : "0" = Not Available "1" = Available							SAM Information : "0" = Socket is not mounted "1" = Socket is empty "2" = SAM is inserted "3" = SAM is inserted but Vcc error				

Ds : DSR off card control

30H : ICRW ejects the card in ICRW (Default value at omit this code)

31H : ICRW keeps the card in ICRW

Cc : Capture counter control

30H : Turn off the capture counter (Default value at omit this code)

31H : Turn on the capture counter

Re : Reset eject control

This code sets on / off of the card eject function after power on and reset. The setting is memorized and is available after the next reset condition.

30H : Turn on the reset eject function. The ICRW eject the card to the gate after reset.

31H : Turn off the reset eject function. The ICRW don't eject the card after reset.

Omit : The previous value is valid.

Default : If the value has never been set, the ICRW control the card according to the following default value.

ICRW without the capture function : 30H (The ICRW ejects the card)

ICRW with the capture function : 31H (The ICRW don't eject the card)

Ce : Transparent card eject control

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

30H : Turn off the transparent card detect function. (Default value at omit this code)
The ICRW can not detect the transparent card.

31H : Turn on the transparent card detect function.
The ICRW detects and ejects the transparent card.

Omit : The previous set value is valid.

Default : If the value has never been set, the default value is 30H.

Notes Pd, Ty, Ds, Cc, Re and Ce are omissible. When Pd, Ty, Ds or Cc are not set, these are set "0" as a default value.

When Re is 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.

7.2 Status request command

Command	"C"	31H	pm			
Positive response	"P"	31H	pm	st1	st0	Se
Negative response	"N"	31H	pm	e1	e0	

Negative response is sent against Status request command if mechanical failure remains from the prior operation.

pm=30H :Report current status of after execution of previous command ICRW.
pm=31H :Response is returned in form of “Se”, with the status information obtained.
“Se” is added also in the time of negative response transmission.

The locations of sensor are referred to appearance drawing.

	b7							b0	
Se=	0	X	X	X	X	X	X	X	(binary)

Card Width Sensor (full shutter model) or PD1 (pin shutter model)
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 Close, 0: Shutter Open
PI2 1: IC Contact is set, 0: IC Contact is not set
(The IC contact is set mechanically at the card entry)
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 no mount.)

7.3 Entry command

Command	"C"	32H	pm	mg	
Positive response	"P"	32H	pm	st1	st0
Negative response	"N"	32H	pm	e1	e0

This is to accept to carry the card inside ICRW. This command doesn't 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" to HOST.
If another card already stays inside ICRW, ICRW sends error "02" 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, ICRW sends 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=30H : To accept the card
When receiving the command with this parameter, ICRW becomes card insertion waiting mode.
After detecting 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" will be transmitted to HOST.

mg=30H : Mag data detect Off
ICRW executes card accept operation without mag data detection. "mg" is omissible and this value is default.

mg=31H : Mag data detect On
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" (No mag error) .
The point of mag data detection is approx. 34mm from card front edge.

7.4 Card carry command

Command	"C"	33H	pm		
Positive response	"P"	33H	pm	st1	st0
Negative response	"N"	33H	pm	e1	e0

pm=30H : EJECT

ICRW moves the card from inside of ICRW to Gate with roller on position.
After executing this command, ICRW can execute a retrieve command.
After card was ejected, ICRW executes a status request command, and when the status code is "00", it is shown that the card was completely pull out from the gate.
It takes a maximum of 7sec after ICRW receives a command until it returns a response.
If a card is not in ICRW, ICRW does not executes the card move operation and returns positive response.

pm=31H : CAPTURE

ICRW moves the card from inside of ICRW to rear side.
After card was captured, ICRW executes a status request command and when its status code is "00", it is shown that the card was completely discharged from the ICRW.
It takes a maximum of 7sec after ICRW receives a command until it returns a response.
If a card is not in ICRW, ICRW sends error "02" to HOST against receipt of this command.

7.5 Retrieve command

Command	"C"	34H	30H		
Positive response	"P"	34H	30H	st1	st0
Negative response	"N"	34H	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.

7.6 LED command

Command	"C"	35H	pm		
Positive response	"P"	35H	pm	st1	st0
Negative response	"N"	35H	pm	e1	e0

This function controls the LED on front bezel of ICRW. LED On commands for every color are able to change directly from the condition of other color on.

pm=30H : LED Off
pm=31H : LED Green On
pm=32H : LED Red On
pm=33H : LED Orange On

7.7 Mag-Track Read command

Command	"C"	36H	pm			
Positive response	"P"	36H	pm	st1	st0	Read Data (ASCII Max 219bytes (pm=35H))
Negative response	"N"	36H	pm	e1	e0	Read Data (ASCII Max 104bytes (pm=3BH))

pm=31H : read data on ISO Track #1
pm=32H : read data on ISO Track #2
pm=33H : read data on ISO Track #3
pm=34H : read data on JIS II

When ICRW takes in a card, the magnetic data read into the buffer is edited and is converted into an ASCII code. If this data is normal, it will transmit to HOST as read data.
The data transmitted to HOST excepts 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" is no magnetic track).
When the card has a track with the sentinels but no data, ICRW sends negative response (error code"23")

EX) ISO Track #1 (Max 76bytes)

bit	5 4 3 2 1 0		
data=0	0 1 0 0 0 0	->	30H
data=A	1 0 0 0 0 1	->	41H

ISO Track #2 (Max 37bytes)

bit	3 2 1 0		
data=0	0 0 0 0	->	30H
data=9	1 0 0 1	->	39H

ISO Track #3 (Max 104char)

bit	3 2 1 0		
data=0	0 0 0 0	->	30H
data=9	1 0 0 1	->	39H

JIS II Track (Max 69bytes)

bit	6 5 4 3 2 1 0		
data=0	0 1 1 0 0 0 0	->	30H
data=A	1 0 0 0 0 0 1	->	41H

pm=35H : All tracks simultaneous read and transmit.
The contents of read data are the order of track 1 data, track 2 data, track 3 data, and JIS II track 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","21","23" or "24" is sent to HOST.

Ex)

Track 1 Data	7EH	Track 2 Data	7EH	Track 3 Data

(Max 219bytes)

pm=37H : Indicates in response if track is encoded/not encoded.
ICRW doesn’t carry the card.
ISO#1: 30H: ISO #1 is not encoded. 31H: ISO #1 is encoded.
ISO#2: 30H: ISO #2 is not encoded. 31H: ISO #2 is encoded.
ISO#3: 30H: ISO #3 is not encoded. 31H: ISO #3 is encoded.
JIS II : 30H: JIS II is not encoded. 31H: JIS II is encoded.

ISO#1	ISO#2	ISO#3	JIS II

30H : 31H :

pm=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.
pm=3CH : read data on JIS II by another way.
The above parameters differ from pm=31H, 32H, 33H and 34H 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 doesn’t read data.

Mag-track read with data encryption command :

pm=41H : read data on ISO Track #1
pm=42H : read data on ISO Track #2
pm=43H : read data on ISO Track #3
pm=44H : read data on JIS II
pm=45H : All three tracks simultaneous read and transmit.
pm=49H : read data on ISO Track #1 by another way
pm=4AH : read data on ISO Track #2 by another way
pm=4BH : read data on ISO Track #3 by another way
pm=4CH : read data on JIS II by another way.
The commands with these pm encrypt the read data in the form of Single DES-CBC and transmit data.
Other processing are the same as pm=31H to 3CH.
In case of pm=45H, ICRW encrypts whole data including separator “7EH”.
Before using these pm, execution of "Security command" is necessary.
A 0x80 and some 0x00 code are padded in the end of read data, HOST must ignore after 0x80.
In case of pm=45H, a 0x80 and some 0x00 code are padded in the end of the data connected with separator “7EH”.
If ICRW has not obtain the key for these command by the “Key loading for the magnetic data”, ICRW sends an error code "06".

Ex) Original data : 0x31 0x32 0x33 0x34 0x35 0x36 0x37 0x38 0x39 0x30
Transmit data : 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x??
Decrypted data : 0x31 0x32 0x33 0x34 0x35 0x36 0x37 0x38 0x39 0x30 0x80 0x00 0x00 0x00 0x00 0x00
Ex) Original data : 0x31 0x32 0x33 0x34 0x7E 0x35 0x36 0x37 0x7E 0x38 0x39 0x30 (pm=45H)
Transmit data : 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x?? 0x??
Decrypted data : 0x31 0x32 0x33 0x34 0x7E 0x35 0x36 0x37 0x7E 0x38 0x39 0x30 0x80 0x00 0x00 0x00

7.8 Enable/Disable command

Command	"C"	3AH	pm	mg	
Positive response	"P"	3AH	pm	st1	st0
Negative response	"N"	3AH	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 entry command becomes impossible at the time of enable command execution, combined use of the enable command and the entry command cannot be performed.

pm=30H : Enable to accept card . (Enable mode)
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.

pm=31H : Disable to accept card. (Disable mode)
It changes into a prohibition state from the permission state of accepting a card.

mg=30H : Mag data detect Off
ICRW executes card accept operation without mag data detection.
"mg" is omissible and this value is default.

mg=31H : Mag data detect On
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". (No mag error)
The point of mag data detection is approx. 34mm from card front edge.

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 DSR signal off.

7.9 Port In/Out command

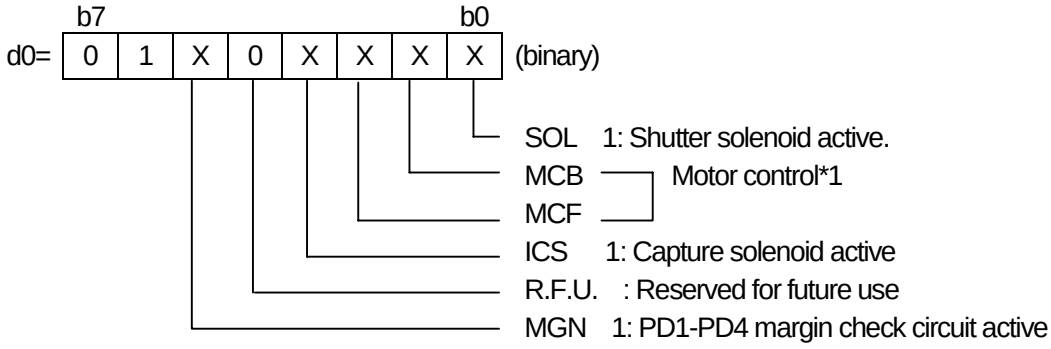
Command	"C"	3DH	pm	d0	
Positive response	"P"	3DH	pm	st1	st0	Se0
Negative response	"N"	3DH	pm	e1	e0	

This is to check ICRW in maintenance. Operation checks can be done by this command for the motor, the solenoids, the switch, and the sensors.

pm=30H : To enter maintenance mode.
In this mode, no commands other than initialize or switch command can be executed.
After executing initialize or switch command, ICRW will usually return from maintenance mode to Normal mode automatically.

pm=31H : To release maintenance mode.
ICRW is returned from maintenance mode to normal mode.
Eject the card if it is within the reader transport.

pm=32H :To output port.
To designate the operation for the motor and solenoids.

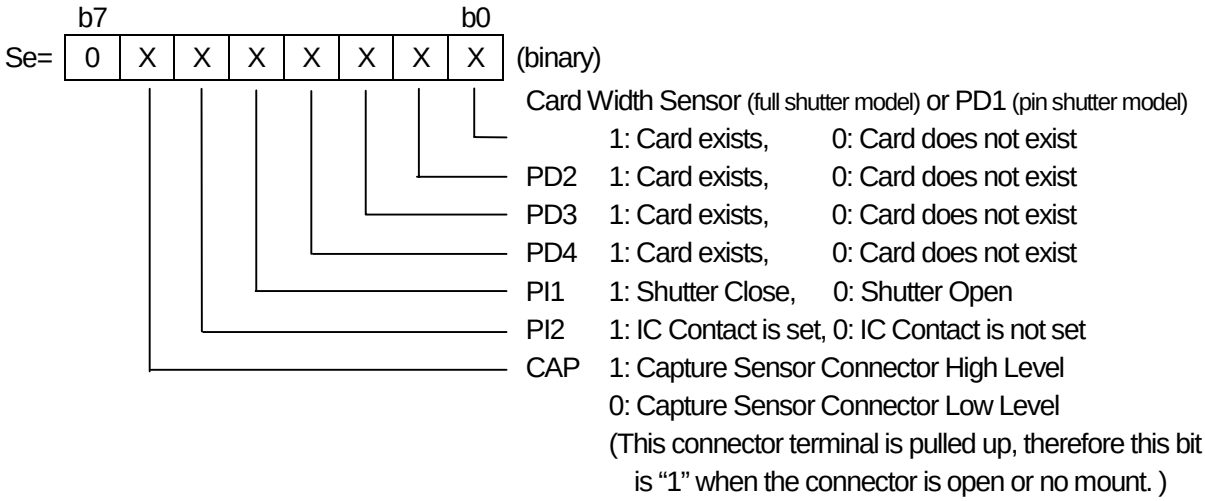


*1 MCB:1 MCF:1 BRAKE MCB:1 MCF:0 FWD MCB:0 MCF:1 BWD MCB:0 MCF:0 BRAKE

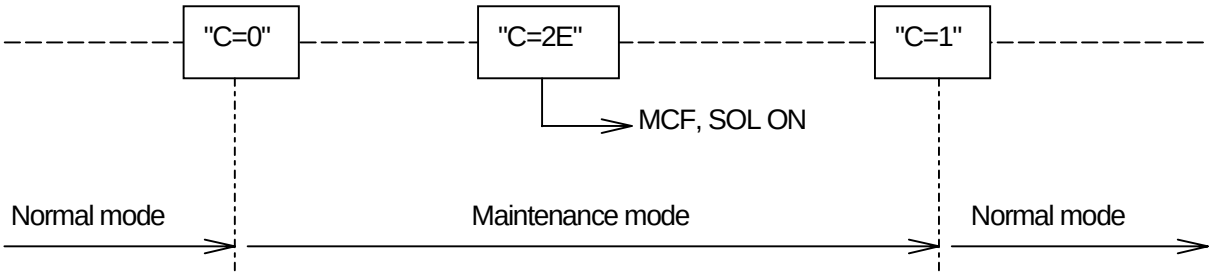
Note: Every function can not be simultaneously performed.

pm=33H : To input port.

To input the status on the switch and the sensors.



** Basic flow (example)



The normal mode shows command modes other than the maintenance mode.
The method of going into the maintenance mode from the normal mode is only transmitting "C=0" command shown in the above figure.
In order to return from the maintenance mode to the normal mode, please transmit "C=1" command shown in the above figure.
However, Initialize command is executed, after returning to the normal mode, when transmitting Initialize command into the maintenance mode.

7.10 Sensor Level transmit command

Command	"C"	3EH	pm										
Positive response	"P"	3EH	pm	st1	st0	v1h	v1l	v2h	v2l	v3h	v3l	v4h	v4l
Negative response	"N"	3EH	pm	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 30H added respectively.

Ex) : A/D data=E5(H)
Convert to the Voltage data.
E5H = 229 (DEC) => 5[V] × (229/255) = 4.5[V] => vih=34H, vil=35H
Comparison of vi and each sensor is as follows;
v1: PD1 , v2: PD2 , v3: PD3 , v4: PD4

pm=30H: Emission amount of LED is normal level. If sensor voltage is less than 4.2V without any presence of card on sensor, the sensor cleaning must be done as soon as possible. (Attention)
If sensor voltage is less than 3.0V, maintenance such as sensor cleaning must be done immediately (Warning) .

pm=31H: Emission amount of LED is around one fifth of normal level.
Objective of voltage measurement with this parameter is to verify sensor work in maintenance.
If sensor voltage is more than 1.5V without any presence of card on sensor,
the sensor is normal. In the case of the full shutter model, the voltage of PD1 has no mean.

7.11 Revision command

Command	"C"	41H	pm			
Positive response	"P"	41H	pm	st1	st0	Revision data (ASCII 8bytes) Approval Number(ASCII 20,21bytes)
Negative response	"N"	41H	pm	e1	e0	

pm=31H : Indicates User program code area revision in positive response. (Data length = 8)
ex) "2490-04B"
pm=32H : Indicates EMV2000 controller's firmware revision in positive response. (Data length = 8)
ex) "2491-02A"
pm=33H : Sends the EMV approval number to HOST. (Data length = 21)
ex) "11711 1203 400 20 FIM"
pm=34H : Sends the GIE-CB approval number to HOST. (Data length = 22)
ex) "131 C04 2003 (SNK 008)" (The "SNK 008" is the ATM protcol number.)
pm=35H : Sends the IFM number of the EMV approval to HOST. (Data length = 11)
ex) " IFM0K0-0101"

7.12 Counter command

Command	"C"	43H	pm	Counter value (ASCII Max 3bytes)		
Positive response	"P"	43H	pm	st1	st0	Counter value (ASCII Max 3bytes)
Negative response	"N"	43H	pm	e1	e0	

pm=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=33H : This command is for the capture counter function.
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'.
If a capture command is executed when the capture count number is over the alert count set by the bellow function, the capture operation performs to usual and transmits the capture counter overflow error"50" to the HOST.

pm=34H : This command is for the capture counter function.
This command 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'.

7.13 IC Card control command

7.13.1 Activate ICC command

Command	"C"	49H	30H	Vcc		
Positive response	"P"	49H	30H	st1	st0	ATR (Binary max 65bytes)
Negative response	"N"	49H	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=30H:The ICRW supplies +5V to the VCC and activates according to the EMV2000 ver.4.0.

Vcc=33H:The ICRW supplies +5V to the VCC and activates according to the ISO/IEC7816-3:1997.

Vcc=35H:The ICRW supplies +3V to the VCC and activates according to the ISO/IEC7816-3:1997.

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

Vcc=36H:The ICRW supplies with +5V to the VCC and activates according to the ISO/IEC7816-3:1997/Amd.1:2001. After receiving the ATR, the ICRW changes the voltage to the VCC in accordance with the T=15 value of the ATR.

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 30H.

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

ATR	TS	TO	TA1	TB1	…	TCK

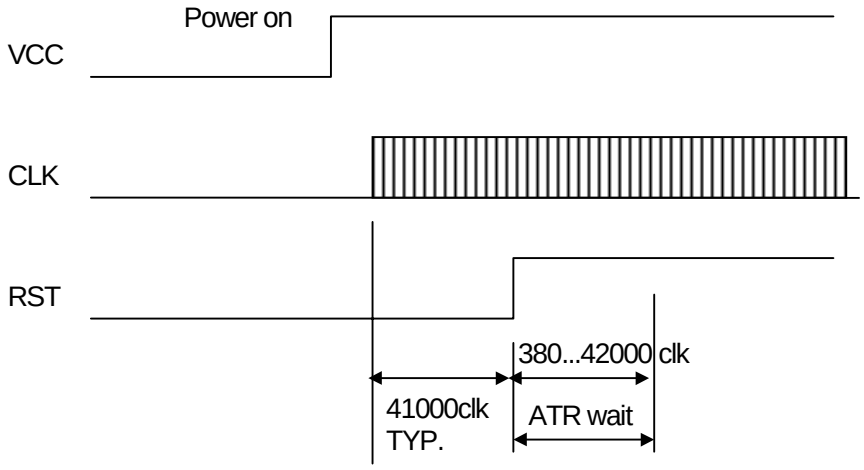
When a power failure is detected while a power supply is supplied to the IC card, the error code "60" is returned. If the activation error is occurred, the ICRW initiate the deactivation sequence, and sends the error code " 61", "63" or "64". When the Vcc parameter 30H is selected and the ATR value is not based on the EMV2000 ver.4.0, the ICRW initiate the deactivation sequence, and sends the error code " 69". When the Vcc parameter 33H, 35H or 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".

The Vcc parameter is not related to the IC card communication. The IC card communication complies with the EMV2000 ver.4.0.

The activation command "CI0@" (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 "CI00","CI03","CI05" or "CI06" are available.

The IC card automatic communication command "CI9" must be used after the ICC activation by "CI0@".

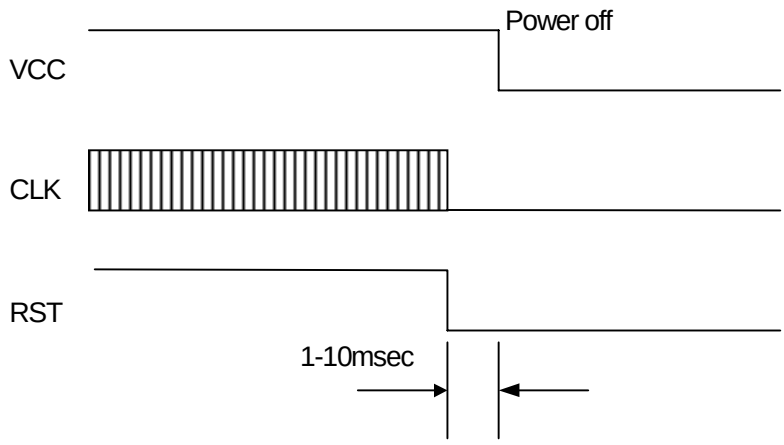
The timing chart of ICC activation



7.13.2 Deactivate ICC command

Command	"C"	49H	31H		
Positive response	"P"	49H	31H	st1	st0
Negative response	"N"	49H	31H	e1	e0

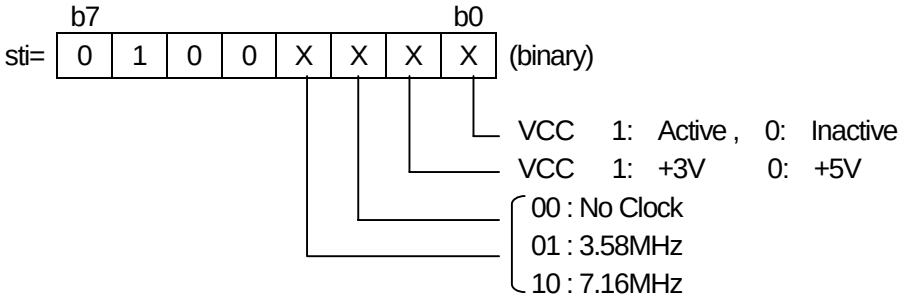
This command deactivates the IC card.
The time chart of the IC card deactivating sequence is as follows.



7.13.3 Inquire ICC status command

Command	"C"	49H	32H			
Positive response	"P"	49H	32H	st1	st0	sti
Negative response	"N"	49H	32H	e1	e0	

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



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” is returned when a power failure is detected.

7.13.4 ICC communication T=0

Command	"C"	49H	33H	C-APDU (Binary max 261bytes)		
Positive response	"P"	49H	px	st1	st0	R-APDU (Binary max 258bytes)
Negative response	"N"	49H	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-APDU” data to the HOST.

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

px=33H : The received data from the IC card is 258 bytes or less.
px=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" 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” 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=35H and first 258 bytes data. The remaining R-APDU data are sent as the positive response data of the command “CI7”.

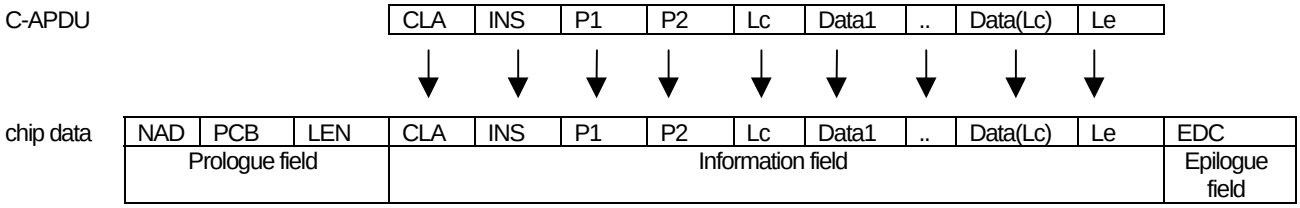
While a power supply is supplied to the IC card, the ICRW monitors the VCC (the power supply line of the IC card). The ICRW is returned the error code “60” when a power failure is detected.
If the protocol type of the IC card is not T=0, error code “62” is sent.
If IC card does not respond within WWT(Working Wait Time), the ICRW deactivates the IC card and the error code “63” is sent.
If any other protocol error occurs, the ICRW deactivates the IC card and the error code "64" is sent.
If HOST tries to communicate before the IC card activation, the error code “65” is sent.

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

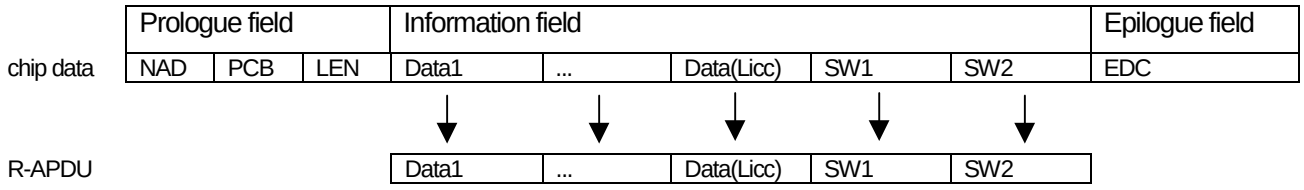
7.13.5 ICC communication T=1

Command	"C"	49H	34H	C-APDU (Binary max 261bytes)		
Positive response	"P"	49H	px	st1	st0	R-APDU (Binary max 258bytes)
Negative response	"N"	49H	34H	e1	e0	

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.



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



px=34H : The received R-APDU from the IC card is 258 bytes or less.
px=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(ABTreq) 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” 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” and “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=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” is returned when a power failure is detected.
If the protocol type of IC card is not T=1, the error code “62” 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” is sent.
If any other protocol error occurs, the ICRW deactivates the IC card and the error code "64" is sent.
If the HOST tries to communicate before the IC card activation, the error code “65” is sent.
In case there is any trouble in the sequence of command receiving, the error code "02" is sent.
If the error code "02" 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.

7.13.6 ICC extended communication 1

Command	"C"	49H	35H	C-APDU (Binary max 261bytes)	
Positive response	"P"	49H	px	st1	st0
Negative response	"N"	49H	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=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(ABTreq) 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” 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” is sent.
If any other protocol error occurs, the ICRW deactivates the IC card and the error code "64" is sent.
If the HOST tries to communicate before the IC card activation, the error code “65” is sent.

7.13.7 ICC extended communication 2

Command	"C"	49H	36H	C-APDU (Binary max 261bytes)		
Positive response	"P"	49H	px	st1	st0	R-APDU (Binary max 258bytes)
Negative response	"N"	49H	36H	e1	e0	

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=34H : The received R-APDU from the IC card is 258 bytes or less.

px=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(ABTreq) 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” is returned when a power failure is detected.
If protocol type of the IC card is not T=1, the error code “62” 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” is sent.
If any other protocol error occurs, the ICRW deactivates the IC card and the error code "64" is sent.
If the HOST tries to communicate before the IC card activation, the error code “65” is sent.

7.13.8 ICC extended communication 3

Command	"C"	49H	37H			
Positive response	"P"	49H	px	st1	st0	R-APDU (Binary max 258bytes)
Negative response	"N"	49H	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=36H".

px=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=36H : There is no remaining R-APDU data from the IC card.
px=3FH : The ICRW received the S(ABTreq) 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” 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” is sent.
If any other protocol error occurs, the ICRW deactivates the IC card and the error code "64" is sent.
If HOST tries to communicate before an IC card activation, the error code “65” is sent.

7.13.9 ICC warm reset

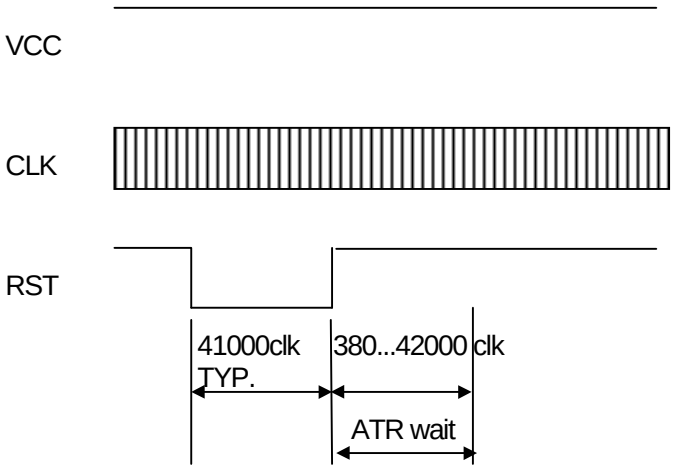
Command	"C"	49H	38H			
Positive response	"P"	49H	38H	st1	st0	ATR (Binary max 65bytes)
Negative response	"N"	49H	38H	e1	e0	ATR (Binary max 65bytes)

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” or “69” with the ATR. If the ATR receive error is occurred, the ICRW initiate the deactivation sequence, and sends the error code “ 61”, “63” or “64”. The ICRW returns error code "65" 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” is returned when a power failure is detected.

The time chart of the warm reset sequence is as follows.



7.13.10 ICC automatic communication

Command	"C"	49H	39H	C-APDU (Binary max 261bytes)		
Positive response	"P"	49H	px	st1	st0	R-APDU (Binary max 258bytes)
Negative response	"N"	49H	39H	e1	e0	

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 “CI3” or “CI4”.

px=34H : The received R-APDU from the IC card is 258 bytes or less.

px=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=3FH : The ICRW received the S(ABTreq) 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” 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” is sent. If any other protocol error occurs, the ICRW deactivates the IC card and the error code "64" is sent. If the HOST tries to communicate with this command before the IC card activation, the error code “65” 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 sends the following C-APDU data.

7.13.11 Plaintext offline PIN verification

Command	"C"	49H	pm	C-APDU (Verify command)(13byte)							
				CLA 0xH	INS 20H	P1 00H	P2 80H	Lc 08H	Encrypted offline PIN block (8byte)		
Positive response	"P"	49H	px	st1	st0	R-APDU					
Negative response	"N"	49H	pm	er1	er0						

This command decrypts offlince PIN block of C-APDU and changes into plaintext verify command, then transmits to an IC card.
This function intends the plain text offline PIN block (8bytes fixed) defined by the verify command which P2 value is 80H to transmit ICRW safely.

pm = 53H: Communication T=0 using "Triple-DES-ECB"
pm = 54H: Communication T=1 using "Triple-DES-ECB"
pm = 59H: Automatic communication using "Triple-DES-ECB"
pm = 63H: Communication T=0 using "Single-DES-ECB"
pm = 64H: Communication T=1 using "Single-DES-ECB"
pm = 69H: Automatic communication using "Single-DES-ECB"

The Key for decrypting PIN is set by "Key loading for the Plaintext offline PIN verification" command.
If "Device authentication data exchange and key exchange key loading" command or "Key loading for the Plaintext offline PIN verification" command are not completed, error code "06" is sent.

px=33H: T=0 protocol IC card's response.
px=34H : T=1 protocol IC card's response.
px=3FH :ICRW receive the S(ABTreq) block from the IC card, so the communication is suspended and the IC card deactivated. (Only T=1 protocol).

Reference:
The plaintext offline PIN block shall be formatted as follows:

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

Where

	Name	Value
C	Control field	Binary 2 (hex. 0010)
N	PIN length	4-bit binary number with permissible values of hex. 0100 to hex. 1100
P	PIN digit	4-bit field with permissible values of hex. 0000 to hex. 1001
P/F	PIN / filler	Determined by PIN length
F	Filler	4-bit binary number with value of hex. 1111

(Reference: EMV2000 Integrated Circuit Card Specification for Payment Systems Version 4.0 May 31, 1998
Part II Data Elements and Commands)

7.14 SAM (Secure Application Module) control command

7.14.1 Activate SAM command

Command	"C"	49H	40H	Vcc		
Positive response	"P"	49H	40H	st1	st0	ATR (Binary max 65bytes)
Negative response	"N"	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=30H:The ICRW supplies +5V to the VCC and activates according to the EMV2000 ver.4.0.

Vcc=33H:The ICRW supplies +5V to the VCC and activates according to the ISO/IEC7816-3:1997.

Vcc=35H:The ICRW supplies +3V to the VCC and activates according to the ISO/IEC7816-3:1997.

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

Vcc=36H:The ICRW supplies with +5V to the VCC and activates according to the ISO/IEC7816-3:1997/Amd.1:2001. After receiving the ATR, the ICRW changes the voltage to the VCC in accordance with the T=15 value of the ATR.

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 30H.

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

ATR	TS	TO	TA1	TB1	…	TCK

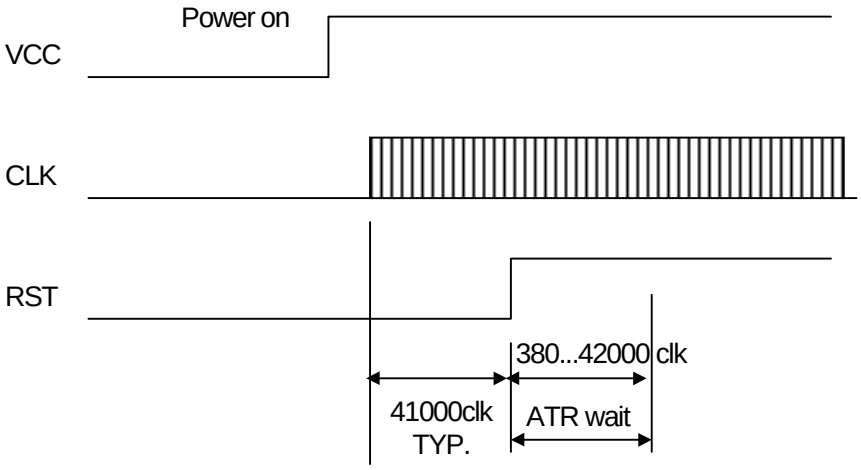
When a power failure is detected while a power supply is supplied to the SAM, the error code "60" is returned. If the ATR receive error is occurred, the ICRW initiate the deactivation sequence, and sends the error code " 61", "63" or "64". When the Vcc parameter 30H is selected and the ATR value is not based on the EMV2000 ver.4.0, the ICRW initiate the deactivation sequence, and sends the error code " 69". When the Vcc parameter 33H, 35H or 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".

The Vcc parameter is not related to the SAM communication. The SAM communication complies with the EMV2000 ver.4.0.

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" or "CI@6" are available.

The SAM automatic communication command "CII" must be used after the SAM activation by "CI@@".

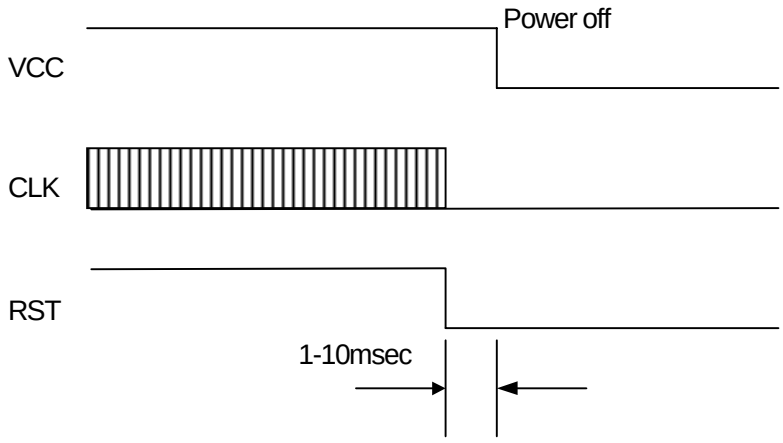
The time chart of the SAM activating sequence is as follows



7.14.2 Deactivate SAM command

Command	"C"	49H	41H		
Positive response	"P"	49H	41H	st1	st0
Negative response	"N"	49H	41H	e1	e0

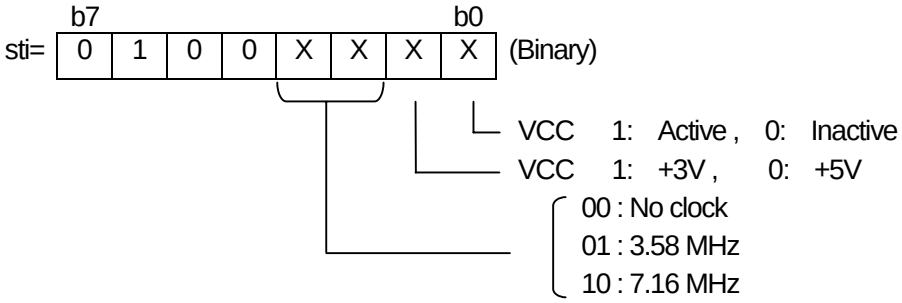
This command deactivates the SAM.
The time chart of the SAM deactivating sequence is as follows.



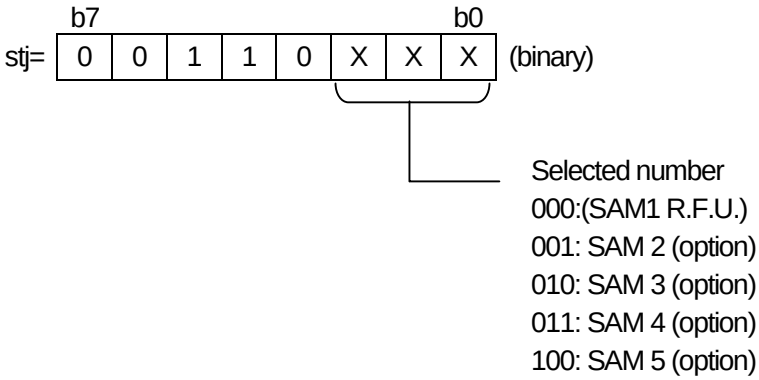
7.14.3 Inquire SAM status command

Command	"C"	49H	42H				
Positive response	"P"	49H	42H	st1	st0	sti	stj
Negative response	"N"	49H	42H	e1	e0		

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



And also, ICRW reports the number of the selected SAM with stj.
Before selecting SAM number, ICRW responds that ICRW selects SAM2.



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

7.14.4 SAM communication T=0

Command	"C"	49H	43H	C-APDU (Binary max 261bytes)		
Positive response	"P"	49H	px	st1	st0	R-APDU (Binary max 258bytes)
Negative response	"N"	49H	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=43H : The received data from SAM is 258 bytes or less.
px=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" 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=45H and first 258 bytes data. The remaining R-APDU data are sent as the positive response data of the command "CIG".

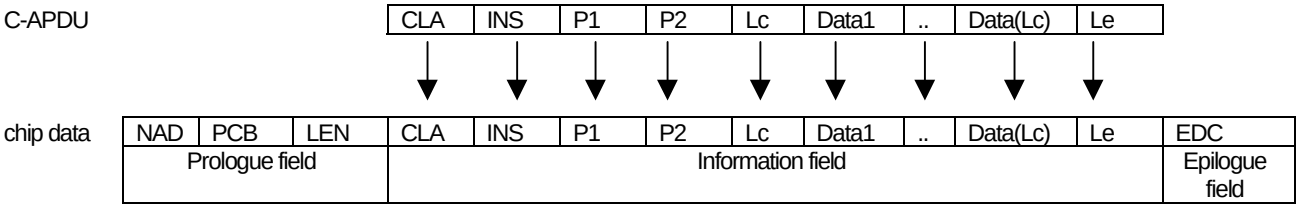
While a power supply is supplied to the SAM, the ICRW monitors the VCC (the power supply line of the SAM).
The ICRW is returned the error code "60" when a power failure is detected.
If the protocol type of the SAM is not T=0, the error code "62" is sent.
If the SAM does not respond within WWT(Working Wait Time), the ICRW deactivates the SAM and the error code "63" is sent.
If any other protocol error occurs, the ICRW deactivates the SAM and the error code "64" is sent.
If the HOST tries to communicate before the SAM activation, the error code "65" is sent.

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

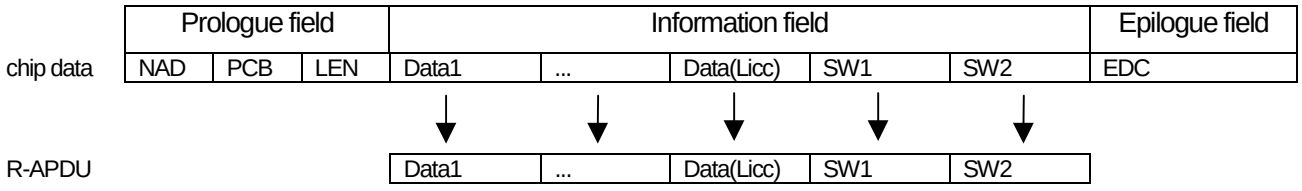
7.14.5 SAM communication T=1

Command	"C"	49H	44H	C-APDU (Binary max 261bytes)		
Positive response	"P"	49H	px	st1	st0	R-APDU (Binary max 258bytes)
Negative response	"N"	49H	44H	e1	e0	

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=44H : The received R-APDU from the SAM is 258 bytes or less.
px=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=4FH : The ICRW received the S(ABTreq) 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" 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=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” is returned when a power failure is detected.
If the protocol type of the SAM is not T=1, the error code “62” 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” is sent.
If any other protocol error occurs, the CRW deactivates the SAM and the error code "64" is sent.
If the HOST tries to communicate before the SAM activation, the error code “65” is sent.
In case there is any trouble in sequence of command receiving, the error code "02" is sent.
If the error code "02" 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.

7.14.6 SAM extended communication 1

Command	“C”	49H	45H	C-APDU (Binary max 261bytes)	
Positive response	“P”	49H	px	st1	st0
Negative response	“N”	49H	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=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=4FH : The ICRW received the S(ABTreq) 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” is returned when a power failure is detected.
If the protocol type of the SAM is not T=1, the error code “62” 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” is sent.
If any other protocol error occurs, the ICRW deactivates the SAM and the error code "64" is sent.
If the HOST tries to communicate before the SAM activation, the error code “65” is sent.

7.14.7 SAM extended communication 2

Command	"C"	49H	46H	C-APDU (Binary max 261bytes)		
Positive response	"P"	49H	px	st1	st0	R-APDU (Binary max 258bytes)
Negative response	"N"	49H	46H	e1	e0	

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=44H : The received R-APDU from the SAM is 258 bytes or less.

px=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=4FH : The ICRW received the S(ABTreq) 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" is returned when a power failure is detected.
If protocol type of the SAM is not T=1, the error code "62" 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" is sent.
If any other protocol error occurs, the ICRW deactivates the SAM and the error code "64" is sent.
If the HOST tries to communicate before the SAM activation, the error code "65" is sent.

7.14.8 SAM extended communication 3

Command	“C”	49H	47H			
Positive response	“P”	49H	px	st1	st0	R-APDU (Binary max 258bytes)
Negative response	“N”	49H	47H	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=46H".

px=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=46H : There is no remaining R-APDU data from the SAM.
px=4FH : The ICRW received the S(ABTreq) 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” 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” is sent.
If any other protocol error occurs, the ICRW deactivates the SAM and the error code "64" is sent.
If the HOST tries to communicate before the SAM activation, the error code “65” is sent.

7.14.9 SAM warm reset

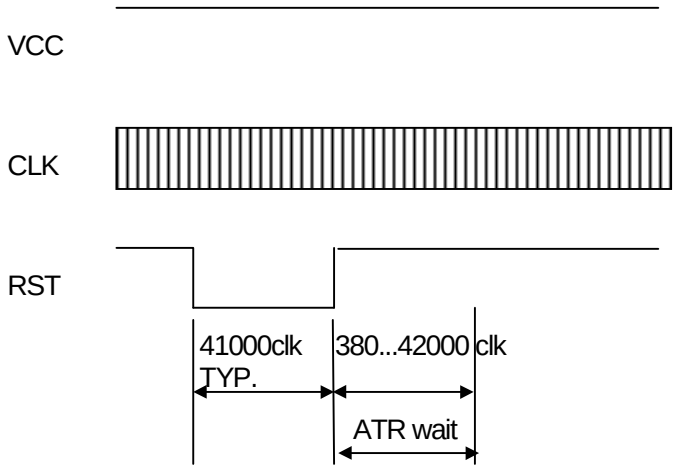
Command	"C"	49H	48H			
Positive response	"P"	49H	48H	st1	st0	ATR (Binary max 65bytes)
Negative response	"N"	49H	48H	e1	e0	ATR (Binary max 65bytes)

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" or "69" with the ATR. If the ATR receive error is occurred, the ICRW initiate the deactivation sequence, and sends the error code " 61", "63" or "64". The ICRW returns error code "65" 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" is returned when a power failure is detected.

The time chart of the warm reset sequence is as follows.



7.14.10 SAM automatic communication

Command	“C”	49H	49H	C-APDU (Binary max 261bytes)		
Positive response	“P”	49H	px	st1	st0	R-APDU (Binary max 258bytes)
Negative response	“N”	49H	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=44H : The received R-APDU from the SAM is 258 bytes or less.

px=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=4FH : The ICRW received the S(ABTreq) 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” 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” is sent. If any other protocol error occurs, the ICRW deactivates the SAM and the error code "64" is sent. If the HOST tries to communicate with this command before the SAM activation, the error code “65” 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 sends the following C-APDU data.

7.14.11 Select SAM

Command	"C"	49H	50H	Sel	
Positive response	"P"	49H	50H	st1	st0
Negative response	"N"	49H	50H	e1	e0

This command selects the SAM 2,3,4 or 5. The SAM 1 is reserved for future use(R.F.U).
These SAMs are available by connecting the external SAM board (option).

Sel = 30H:(SAM 1(R.F.U.))
Sel = 31H: SAM 2. (option)
Sel = 32H: SAM 3. (option)
Sel = 33H: SAM 4. (option)
Sel = 34H: SAM 5. (option)

The SAM commands for each SAM are available after selecting the SAM by this command.
The SAM2 is the default value before selecting the SAM using this command.

7.15 Switch command

Command	"C"	4BH	30H		
Positive response	"P"	4BH	30H	st1	st0
Negative response	"N"	4BH	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.

Ex) Under user program code area is operated

↓

Execute switch command “CK0”

↓

Switch the control to Supervisor program code area

↓

Execute Initialize command of Supervisor program code area

↓

Execute download command group

↓

Execute switch command “CK0”

↓

Switch the control to User program code area

↓

Execute Initialize command of User program code area

↓

Usual operation

7.16 Siemens memory card control command

7.16.1 Siemens memory card Power on

Command	"C"	52H	30H	type		
Positive response	"P"	52H	30H	st1	st0	ATR
Negative response	"N"	52H	30H	er1	er0	

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 return ATR. ICRW returns a negative response when proper ATR isn't received from the memory card. An error code "60" is returned when a power failure is recognized while a power supply is supplied to the card.

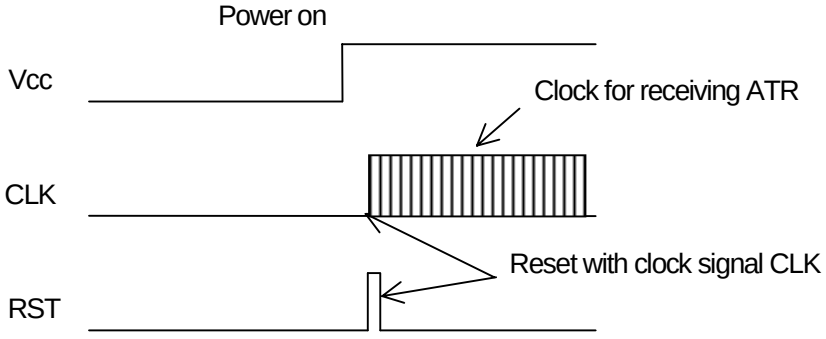
type :31H

This is for the case to select SLE4406.
No ATR data check is executed, and return ATR.
If the card is activated properly with this command,
only SLE4406 command can be executed

: No definition or 30H

This is for the case to select all memory cards.
ICRW automatically judges the type of memory card by ATR data.
If the card is activated properly, the command of the memory card
of the judged kind can be executed.
Refer to the following table for the judgement.

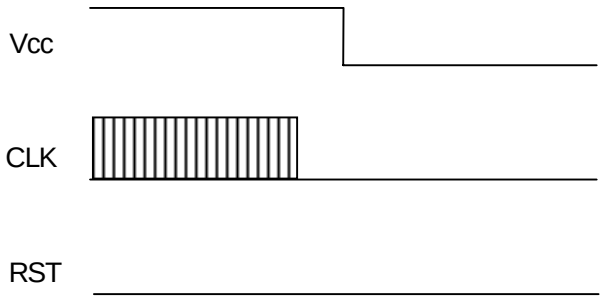
ATR		memory card
H1	H2	
A2	13	SLE4442/4432
92	23	SLE4428/4418
19	04	SLE4406
99	04	



7.16.2 Siemens memory card Power off

Command	"C"	52H	31H		
Positive response	"P"	52H	31H	st1	st0
Negative response	"N"	52H	31H	er1	er0

This command deactivates the memory card.
ICRW asserts reset (RST) signal, and stops clock (CLK) and power supply (Vcc).
Then, the memory card is deactivated.



7.16.3 Inquire Status of Siemens memory card

Command	"C"	52H	32H			
Positive response	"P"	52H	32H	st1	st0	str
Negative response	"N"	52H	32H	er1	er0	

This command report the status of Siemens memory 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” is returned when a power failure is detected.

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

VCC 1: Active , 0: Inactive
Sort 01: SLE4428 / 4418 , 00: SLE4442 / 4432
10:SLE4406

7.16.4 Communicate with SLE4442

The SLE4442 memory 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. (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 SLE4442, ICRW must control the signal line of the memory card directly about each data transmission by the hardware. Therefore, some functions to control SLE4442 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 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.

While 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.

7.16.4.1 Data read from main memory on SLE4442

Command	"C"	52H	33H	00B000H + abH + cdH		
Positive response	"P"	52H	33H	st1	st0	Data
Negative response	"N"	52H	33H	er1	er0	

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 address abH. The capacity of the main memory is 256 bytes. The byte number "00" of data to read means 256bytes. All the contents of the main memory can be read with the following command.

ex). "CR3"+00B0000000

While 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.

7.16.4.2 Data read from protection memory on SLE4442

Command	"C"	52H	33H	00B001H + abH + cdH		
Positive response	"P"	52H	33H	st1	st0	Data
Negative response	"N"	52H	33H	er1	er0	

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

ex). "CR3"+00B0010004

ICRW reads data from the protection memory of SLE4442, and transmits data on cdH bytes from the address abH.

While 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.

7.16.4.3 Data read from security memory on SLE4442

Command	"C"	52H	33H	00B002H + abH + cdH		
Positive response	"P"	52H	33H	st1	st0	Data
Negative response	"N"	52H	33H	er1	er0	

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 three bytes of 00H as the security code

ICRW handles the data of all 32bits in the security memory as the data on 4bytes.

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

ex). "CR3"+00B0020004

ICRW reads data from the security memory of SLE4442, and transmits data on cdH bytes from the address abH.

While 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.

7.16.4.4 Data write to main memory on SLE4442

Command	"C"	52H	33H	00D000H + abH + cdH + efH + ...		
Positive response	"P"	52H	33H	st1	st0	Data
Negative response	"N"	52H	33H	er1	er0	

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 256 bytes. The byte number "00" of data to write means 256bytes.
The example that data are written in the whole area of the main memory is shown in the following.

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

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

If the addressed data on main memory is protected by the protection memory, 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” is returned when a power failure is detected.

7.16.4.5 Data write to protection memory on SLE4442

Command	"C"	52H	33H	00D001H + abH + cdH + efH		
Positive response	"P"	52H	33H	st1	st0	Data
Negative response	"N"	52H	33H	er1	er0	

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

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

The 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.

ex). "CR3" + 00D001100120

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” is returned when a power failure is detected.

7.16.4.6 Data write to security memory on SLE4442

Command	"C"	52H	33H	00D002H + abH + cdH + efH		
Positive response	"P"	52H	33H	st1	st0	Data
Negative response	"N"	52H	33H	er1	er0	

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 3byte can be changed.

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

ex). "CR3"+ 00D0020103123456

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

While 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.

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

7.16.4.7 Verification data present to SLE4442

Command	"C"	52H	33H	0020H + 03H + 01H + 03H + efH		
Positive response	"P"	52H	33H	st1	st0	Data
Negative response	"N"	52H	33H	er1	er0	

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 the security code in the security memory)

03 H : Fixed value (the number of bytes of data to compare)

ef H : the data to compare (3bytes)

Before changing data, PSC(Programmable Security Code) must be checked properly with SLE4442. Because this function should be made effective, the issue of the next command is necessary.

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

The presented data are compared with internal Reference-Data by SLE4442 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 three times with the wrong code. A user must know PSC at least when a user wants to rewrite the data on SLE4442 card.

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

While 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.

7.16.5 Communicate with SLE4428

Same as SLE4442, 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” is returned when a power failure is detected.

7.16.5.1 Data Reading of main-memory of SLE4428

Command	"C"	52H	34H	00B0H + 0aH + bcH + deH		
Positive response	"P"	52H	34H	st1	st0	Data
Negative response	"N"	52H	34H	er1	er0	

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 deH bytes from the address abcH.
The capacity of the main memory is 1024bytes. The byte number "00" of data to read means 256bytes.
The head part of the main memory can be read with the following command.
ex). "CR4"+00B0000000

While 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.

7.16.5.2 Condition data reading of protection-bit of SLE4428

Command	"C"	52H	34H	00B0H + 10H + abH + cdH		
Positive response	"P"	52H	34H	st1	st0	Data
Negative response	"N"	52H	34H	er1	er0	

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 the data on 1024bits, and it is read. 1024bits is equivalent to 128bytes. (1024 = 128 x 8)

Data to read first become protection information to address007H from address000H of main-memory in the case of abH=00H. The contents of the whole protection image can be read with the following command.

ex). "CR4"+00B0100080

ICRW reads data as the protection image of SLE4428, and transmits data on cdH bytes from the address abH.

While 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.

7.16.5.3 Data writing to main-memory of SLE4428

Command	"C"	52H	34H	00D0H + 0aH + bcH + deH + fgH + ...		
Positive response	"P"	52H	34H	st1	st0	Data
Negative response	"N"	52H	34H	er1	er0	

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).

The capacity of the main memory is 1024 bytes. The byte number "00" of data to write means 256bytes.
The example that data are written in from the address 100H is shown in the following.
ex). "CR4"+ 00D0010000 + Write Data (256byte)
After command execution, ICRW returns response with 9000H or sw1+sw2 as the result.

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

While 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.

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

Command	"C"	52H	34H	00D0H + 1aH + bcH + deH + fgH + ...		
Positive response	"P"	52H	34H	st1	st0	Data
Negative response	"N"	52H	34H	er1	er0	

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.

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

Command	"C"	52H	34H	00D0H + 2aH + bcH + deH + fgH + ...		
Positive response	"P"	52H	34H	st1	st0	Data
Negative response	"N"	52H	34H	er1	er0	

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 010H of the main memory is 20H and protection isn't set up.
ex). "CR4" + 00D020100120
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” is returned when a power failure is detected.

7.16.5.6 Verification data present to SLE4428

Command	"C"	52H	34H	00200000H + 02H + efH		
Positive response	"P"	52H	34H	st1	st0	Data
Negative response	"N"	52H	34H	er1	er0	

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 (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 the wrong code. A user must know PSC at least when a user wants to rewrite the data on SLE4428 card.

Error-Counter can be reset in the zero if PSC is given to SLE4428 card properly if the value of Error-Counter is 7 or less.

While 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.

7.16.6 Communicate with SLE4406

Same as SLE4442, The SLE4406 memory card has no protocol handler in it.
So, ICRW also builds in protocol handler to control SLE4406.
The control method of SLE4406 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” is returned when a power failure is detected.

7.16.6.1 Verification data present to SLE4406

Command	"C"	52H	35H	002000H + 0aH + 03H + TCB1+TCB2+TCB3		
Positive response	"P"	52H	35H	st1	st0	Data
Negative response	"N"	52H	35H	er1	er0	

This command is recognized as follows.
0aH : Fixed value
03H : Fixed value
TCB1,TCB2,TCB3 : Transport Code Byte (3byte)

TCB1	TCB2	TDB3
D7----------D0	D15---------D8	D23---------D16

Write operation is performed at an error counter (72bit~76bit), and TCB is presented to Transport code area.
Verification is not performed when an error counter is 0.
The presented data are compared with internal Reference-Data by SLE4406 card itself. The writing function of the card is lost when the command is carried out five times with the wrong code. Error counter can not be reset to the 0.

After verification, writing the bit64 in the memory changes the card state from Issuer Mode to the User Mode.
This command is not required for card in User Mode.

While 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.

7.16.6.2 Data Reading of memory of SLE4406

Command	"C"	52H	35H	00B000H + abH + cdH		
Positive response	"P"	52H	35H	st1	st0	Data
Negative response	"N"	52H	35H	er1	er0	

This command is recognized as follows.

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

cd H : the number of bytes of data to read

ICRW reads data from the memory of SLE4406, and transmits data on cdH bytes from the address abH.

The capacity of the memory is 128bits.

128bits is equivalent to 16bytes.

The contents of the whole data of memory can be read with the following command.

ex) Command

"CR5"+00B000010

Bit	0123 4567	89…..			127
Data	0100 1000	0010 1100	0110 1010	0001 1110 …	1111 1111
Address	00H	01H	02H	03H	0FH

Response

"PR5"+12345678….FF9000

16byte

While 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.

7.16.6.3 Data writing to memory of SLE4406

Command	"C"	52H	35H	00D000H + abH + cdH + efH ...	
Positive response	"P"	52H	35H	st1	st0
Negative response	"N"	52H	35H	er1	er0

This command is recognized as follows.
ab H : the start address to write data in the memory
cd H : the number of bytes of data to write
ef H… : the data to write first (cd H bytes)

Write data	Memory data	operation
“0”	“1”	Write operation is executed. Write bit to “0”.
“0”	“0”	Not executed. *
“1”	“1” or ”0”	Ignore.

* : Data write does not perform when a memory data before writing is 0. In this case processing is interrupted.

ICRW write processing is performed from a low rank bit.
Under command execution if a verification error occurs processing is interrupted.

The capacity of the memory is 128bits(=16bytes). However, ROM area is also contained. Refer to the specification of SLE4406 for details of writable area in memory. ICRW does not distinguish ROM area and PROM/EEPROM area.

While 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.

7.16.6.4 Reloading to counter stage of SLE4406

Command	"C"	52H	35H	00D001H + abH + cdH	
Positive response	"P"	52H	35H	st1	st0
Negative response	"N"	52H	35H	er1	er0

This command is recognized as follows.
ab H : counter number.
cd H : bits number.

		bit number
		7 0
counter number	5	bit71-------bit64
	4	bit79-------bit72
	3	bit87-------bit80
	2	bit95-------bit88
	1	bit103-----bit96

ICRW performs reloading cycle operation to counter stage of SLE4406.
Reloading cycle does not perform, when a data is 0.

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

ICRW does not perform the check after reloading cycle operation.
A result of command execution can be checked by reading of the counter data.

While 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.

7.17 I2C memory card control command

7.17.1 I2C Power on

Command	"C"	53H	30H	Vcc	Wrd
Positive response	"P"	53H	30H	st1	st0
Negative response	"N"	53H	30H	e1	e0

To close the shutter, then 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" 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=30H : ICRW supplies with +5V to VCC and activates the card.
Vcc=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=31H : ICRW accesses an I2C memory card in the Word address of 1byte.
Wrd=32H : ICRW accesses an I2C memory card in the Word address of 2bytes.

7.17.2 I2C Power off

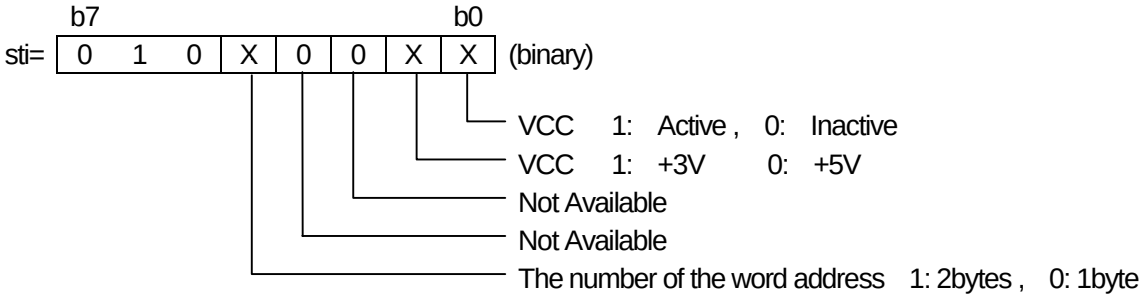
Command	"C"	53H	31H		
Positive response	"P"	53H	31H	st1	st0
Negative response	"N"	53H	31H	e1	e0

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.

7.17.3 Inquire Status of I2C

Command	"C"	53H	32H			
Positive response	"P"	53H	32H	st1	st0	sti
Negative response	"N"	53H	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” is returned when a power failure is detected.



7.17.4 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” is returned when a power failure is detected.

7.17.4.1 Read data from I2C

Command	"C"	53H	33H	00B0H + ab H + cd H + ef H		
Positive response	"P"	53H	33H	st1	st0	Data
Negative response	"N"	53H	33H	e1	e0	

This command is recognized as follows.

Value
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 efH bytes from the address abcdH.
The value established with efH 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

When the following command is transmitted, data can be read from the I2C memory card.
ex). "CS3"+00B0000008

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” is returned when a power failure is detected.

7.17.4.2 Write data into I2C

Command	"C"	53H	33H	00D0 H + ab H + cd H + ef H + gh H + ...		
Positive response	"P"	53H	33H	st1	st0	Data
Negative response	"N"	53H	33H	e1	e0	

This command is recognized as follows.

abH : The upper address of head address which begins to write data
cdH : The lower address of head address which begins to write data
efH : The number of bytes of data to write
ghH : the data to write first (the head data of the data on efH bytes)

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

The example which data on 8bytes are written in by the continuance from the head address of the I2C memory card is shown in the following.

ex). "CS3"+ 00D0000008 + 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” is returned when a power failure is detected.

7.18 Contactless IC card control

This model is supported to contactless ICRW module defined by ISO14443 TypeB, and supplies the function based on this.

7.18.1 Contactless ICRW control

Command	"C"	5AH	33H	Contactless ICRW command (Binary max 259byte)							
				CLA	INS	P1	P2	[Lc]	[Data]	[Le]	
Positive response	"P"	5AH	33H	st1	st0	Contactless ICRW response (Binary max 258byte)					
				[Data]					SW1	SW2	
Negative response	"N"	5AH	33H	e1	e0						

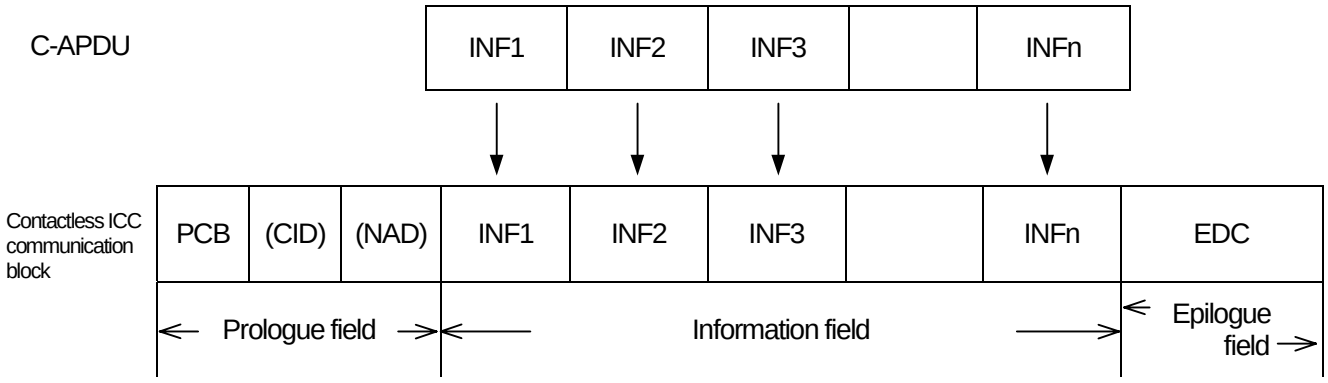
This exchanges data between Contactless IC card by protocol T=CL.
ICRW executes the following command based on "Proximity Communication Interface Implementation Specifications" which "New Media Development Association" defined.
Refer to the agreement document for the details of the parameter of each command.

CLA : 00H Fixed
INS : 01H Contactless ICRW reset
03H Contactless ICRW information acquisition
05H Contactless IC card communication information acquisition
11H Career control
13H Contactless IC card communication information setting
31H Request all B
33H Attribute
39H Halt B
3BH Wake-up all B
F1H Contactless ICRW self diagnosis

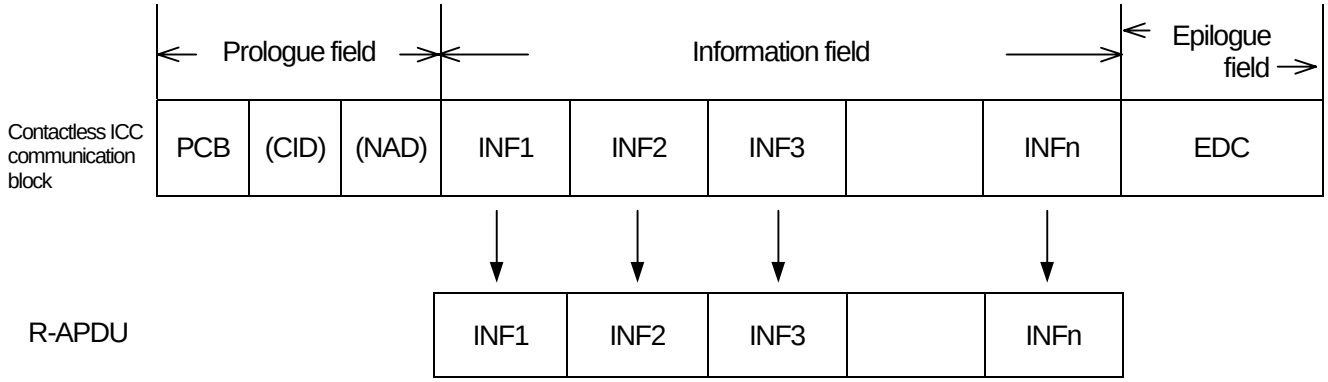
7.18.2 Contactless IC card communication 1

Command	"C"	5AH	34H	C-APDU (Binary max 261bytes)		
Positive response	"P"	5AH	px	st1	st0	R-APDU (Binary max 258bytes)
Negative response	"N"	5AH	34H	e1	e0	

This exchanges data between Contactless IC card by protocol T=CL.
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.
px=34H : The received data from contactless IC card is 258 bytes or less.
px=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.

7.18.3 Contactless IC card communication 2

Command	“C”	5AH	35H	C-APDU (Binary max 261bytes)	
Positive response	“P”	5AH	px	st1	st0
Negative response	“N”	5AH	35H	e1	e0

In the protocol T=CL, in case the transmitted data to contactless IC card is 262 bytes or more, this command is used repeatedly.

px=37H : ICRW requires receiving following 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.

7.18.4 Contactless IC card communication 3

Command	“C”	5AH	36H	C-APDU (Binary max 261bytes)		
Positive response	“P”	5AH	px	st1	st0	R-APDU (Binary max 258bytes)
Negative response	“N”	5AH	36H	e1	e0	

In the protocol T=CL, this command is used when the last data are transmitted.

px=34H : The received data from contactless IC card is 258 bytes or less.
px=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.

7.18.5 Contactless IC card communication 4

Command	“C”	5AH	37H			
Positive response	“P”	5AH	px	st1	st0	R-APDU (Binary max 258bytes)
Negative response	“N”	5AH	37H	e1	e0	

This command is used when receiving the followed data from ICRW.
HOST should send this command repeatedly till the response "px=46H".

px=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.
px=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.

7.18.6 Contactless IC card reset

Command	“C”	5AH	38H		
Positive response	“P”	5AH	38H	st1	st0
Negative response	“N”	5AH	38H	e1	e0

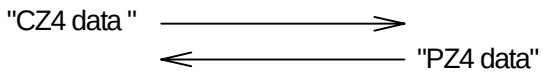
Reset of contactless IC card reader/writer.

Reset time is for 200msec.
ICRW completes reset and returns a response after the 200msec of time when the firmware of a contactless read/write function spends on starting

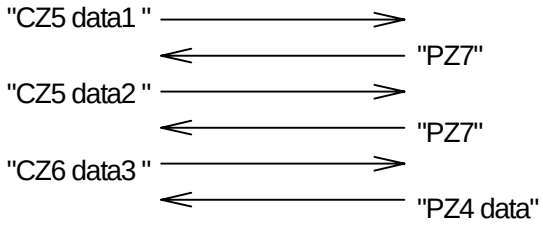
7.18.7 Example

HOST ICRW

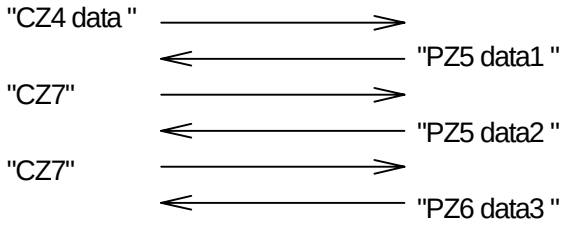
(exp.1) Transmit data 259 bytes or less of data.
Receive 259 bytes or less of data.



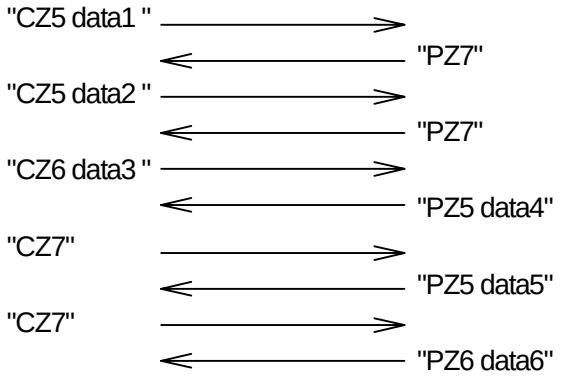
(exp.2) Transmit data by command chaining(Each data size is 259 bytes or less)
Receive 259 bytes or less of data



(exp.3) Transmit 259 bytes or less of data
Receive data by command chaining (Each data size is 259 bytes or less)



(exp.4) Transmit data by command chaining (Each data size is 259 bytes or less)
Receive data by command chaining (Each data size is 259 bytes or less)



7.19 Security command

This command loads the key for “Magnetic data encrypt / decrypt command”
and “Plaintext offline PIN verification command”
Detail of the encrypted data format is defined in the additional document to keep security.

7.19.1 Device authentication data exchange and key exchange key loading

Command	“C”	47H	30H	Encrypted data A (32 bytes : binary value)		
Positive response	“P”	47H	30H	st1	st0	Encrypted data B (16 bytes : binary value)
Negative response	“N”	47H	30H	e1	e0	

This command is for the preparation procedure of the encrypted data communication between ICRW and HOST.
ICRW decrypts the “Encrypted data A” of the command using the master exchange key which is the fixed secret key and obtains the device authentication data and the key exchange key for "Key loading for the magnetic data" and "Key Loading for the Plaintext offline PIN verification".
ICRW encrypts the authentication data using the key exchange key and transmits to the HOST as the “Encrypted data B” of the positive response. HOST checks the result of the authentication from the “Encrypted data B”. These encrypting and decrypting processes use Triple DES-ECB.

If the key exchange key is weak key or semi weak key, ICRW sends the error code "04".
If the first 8 bytes and the second 8 bytes of the key exchange key are the same data, ICRW sends the error code “04”.

7.19.2 Key loading for the magnetic data

Command	“C”	47H	31H	Encrypted data (16 bytes : binary value)	
Positive response	“P”	47H	31H	st1	st0
Negative response	“N”	47H	31H	e1	e0

This command is for loading the key for the ICRW for the “Magnetic data encrypt / decrypt command”.
ICRW decrypts the “Encrypted data” of the command using the key exchange key which is obtained by the command with pm=30H. This decrypting process uses Triple DES-ECB.
And ICRW obtains the key and initialization vector (IV) for "Magnetic data encrypt / decrypt command" from the decrypted data.

If the obtained key is weak key or semi weak key, ICRW sends an error code "04".
If ICRW has not obtain the key exchange key, ICRW sends and error code “06”.

7.19.3 Key loading for the Plaintext offline PIN verification

Command	“C”	47H	32H	Encrypted data (16 bytes : binary value)	
Positive response	“P”	47H	32H	st1	st0
Negative response	“N”	47H	32H	e1	e0

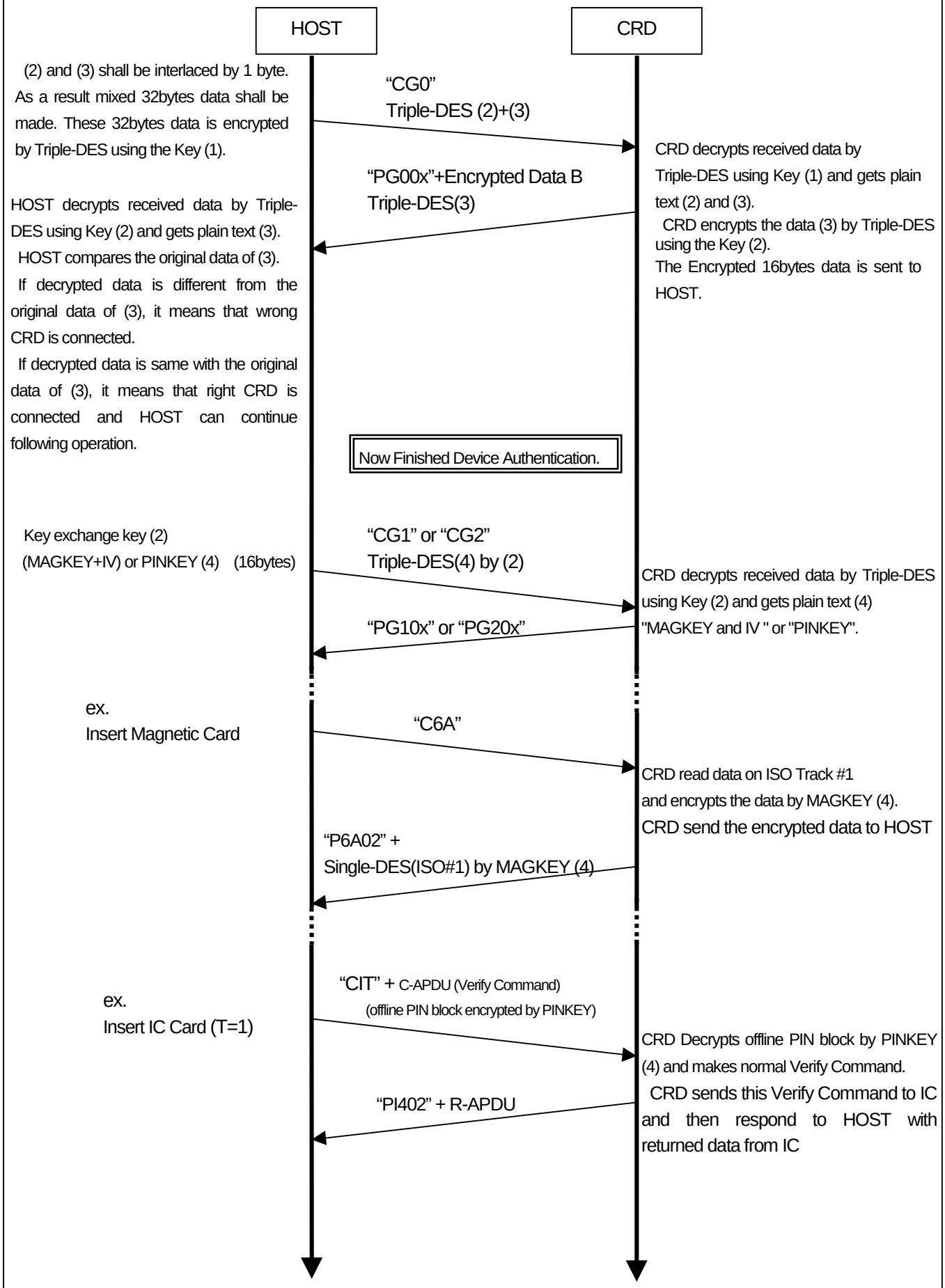
This command is for loading the key for the ICRW for the “Plaintext offline PIN verification command”.
ICRW decrypts the encrypted data of the command using the key exchange key which is obtained by pm=30H. This decrypting process uses Triple DES-ECB.
And ICRW obtains the key for “Plaintext offline PIN verification command” from the decrypted data.
When the Plaintext offline PIN verification command is used with the Single DES-ECB mode, the key is only 8bytes and should be set in first 8bytes of the encrypted data. And second 8bytes should not be same data to the first 8bytes.

If the obtained key is weak key or semi weak key, ICRW sends an error code "04".
If the first 8 bytes and the second 8 bytes are the same data, ICRW sends an error code “04”.
If ICRW has not obtain the key exchange key, ICRW sends and error code “06”.

7.19.4 New master exchange key loading

This command loads the new master exchange key.
The detail of this command’s specification is described in the separated confidential volume of the interface specification.

Master exchange key (1) : 16bytes
Key exchange key (2) : 16bytes
Authenticate Data (3) : 16bytes



8. Explanation of error code

Every error status can be cleared by procedure of (Re-Start by initialize to complete normal).
Also, eliminating the cause (i.e.: taking card out of ICRW) clear the error status.
In this case, uses Status request command and confirm before next step that no error code remain.

8.1 Error in communication soft

"00" Meaning : To shows that received command was undefined.

Clear : Cleared by receiving correct commands.

"01" Meaning : To show command parameter error.

Clear : Cleared by receiving command with correct parameter.

"02" Meaning : To show that ICRW executes Supervisor program code area.
(Supervisor) (Initialize command only on supervisor mode)
Meaning : To show that un-executable command was received.
(User) Cf. Receiving read command while card is not staying inside the ICRW.

Clear : Cleared by receiving executable command.

"03" Meaning : The function (hardware) required for execution of a command is not carried.
The function may not be carried or be out of order.
(The existence of each function is automatically recognized by the firmware.)
Clear : The check of hardware is needed.

"04" Meaning : To show that error data was included in command.

Clear : Cleared by receiving command including correct data.

"06" Meaning : The key for the cipher function command is not received.

Clear : Cleared by the executing the key exchange procedure.

"B0" Meaning : Other commands were received before performing initialize command after a power supply injection, reset or switch command execution.
Clear : Execute Initialize command.

8.2 Error at card feeding

"10" Meaning : 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.
Clear : 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" Meaning : To show that the full shutter does not close when the card entry is completed.

Clear : 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" Meaning : To show that the card longer than 88.5mm is inserted into ICRW.

Clear : Cleared in case card is returned to card gate by eject command.

"14" Meaning : To show that the card shorter than 83.5mm is inserted into ICRW.

Clear : Cleared in case card is returned to card gate by eject command.

"16" Meaning : To show that card staying inside the ICRW was moved up to the point where status request information changes.

Clear : Cleared in the case card is ejected.

"17" Meaning : 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.

Clear : 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" Meaning : ICRW detected that two cards were inserted, and ejected it.

Clear : Remove ejected card from a gate.

"40" Meaning : To show that card is pulled out against card feed in operation.

Clear : Command execution is normally possible continuously.

8.3 Error in reading card

The following errors may be recovered if ICRW re-take in and read a card.
When an error is not recovered after this operation, it is unrecoverable since magnetic record of a card is unusual

"20" Meaning : To show that parity error exists in read error.

"21" Meaning : To show that other read error than "20", "23" and "24" (cf : no start sentinel is recorded in the card).

"23" Meaning : To show that only start sentinel, end sentinel, LRC are contained in the card. There are no contents of data.

"24" Meaning : To show that the card has no magnetic track. For entry and enable command with mag check, this code is used to indicate error.

8.4 Other error codes

"30" Meaning : 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.

Clear : Cleared when a card is ejected and pulled out after a power supply recovery.

"31" Meaning : To show that DSR signal was turned to OFF (communication is cut).

Clear : Cleared when a card is ejected and pulled out after DSR signal recovery.

9. RAS (Reliability, Availability, and Serviceability) Function

9.1 The power on / reset boot mode

The ICRW selects the boot modes by the shade conditions of the card detect sensors after the power on or hardware reset. The boot modes are the standard mode for normal operation and RAS mode to check their functions and report the results by LED.

9.2 The boot check items and result

The ICRW checks the following items with this order before booting as the standard mode or RAS mode.

Check Items	Result
User Program Area CRC Check	The ICRW work only on the supervisor program area (The Initialize command response is always "N0002")
Flash ROM Parameter Area CRC Check	The functions of the user program area are not available. (The Initialize command response is always "N0015")
EEPROM Read Check	The functions of user program area are not available. (The Initialize command response is always "N0073")
Remained Card Eject and Card Jam Check	The functions of user program area are not available. (The Initialize command response is always "N0010")
Implemented Functions Self Recognition (Magnetic Head and the available tracks, IC Contact and Contactless Read / Write Module~~*1~~)	The result of the implemented functions self recognition are able to be confirmed by the initialize command response. The commands using not implemented functions are not available. (The command response using not implemented function is "Nxx02")

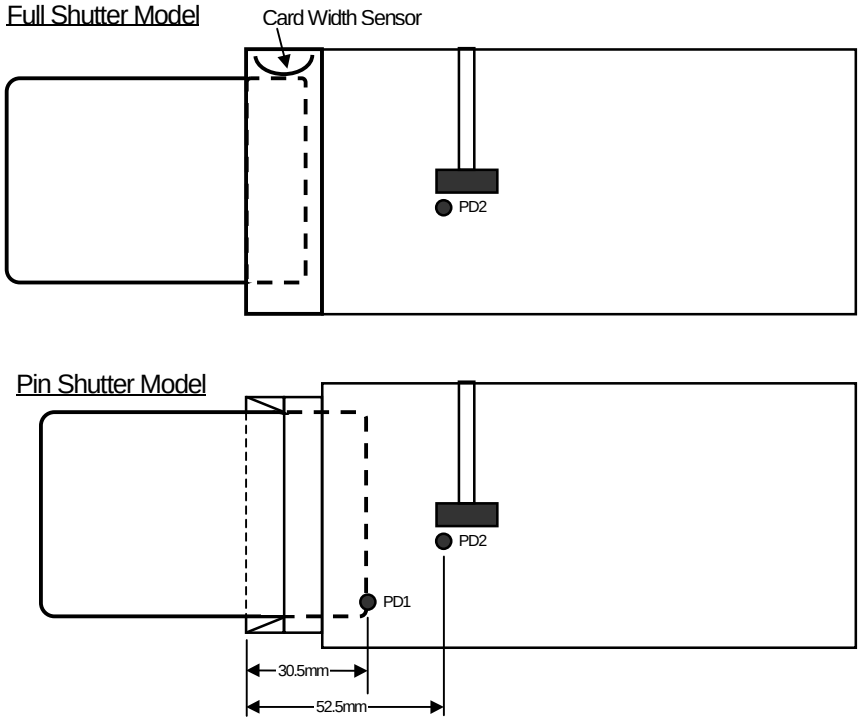
9.3 The condition for boot on RAS mode

The ICRW boots on RAS mode when the card shades only the card witdth sensor (full shutter model) or the PD1 (pin shutter model) and the power supply is turned on or the ICRW is reset.

The ICRW starts the card entry motion after booting on RAS mode.

The entry motion tries while 2 seconds with rotating the motor and retries 2 times.

If the card is not inserted while the entry motion, the ICRW finishes the RAS mode and starts the standard mode.



9.4 The finish condition of RAS mode

In the RAS mode, the ICRW finishes the RAS mode and start standard mode when the card is pulled out to PD1 open position. And when the abnormal conditions which discontinue the RAS function is detected, the RAS function stops and finishes the RAS mode when the card is pulled out.

9.5 The overview of RAS operation

1). When the ICRW enter the RAS mode, the ICRW checks the basic functions for RAS operation. If the basic functions are not normal condition, the ICRW stops the RAS operation, indicate orange LED and finishes the RAS mode.
2). The ICRW executes the card entry motion. When the ICRW detects the card transport error, the ICRW stop the RAS operation, indicate orange LED and finishes the RAS mode.
3). While the ICRW executes the card entry, the ICRW read the magnetic stripe data on the card. After finishing the card entry, the ICRW activate the contact IC card and execute the request B command for contactless IC card. Each functions are executed only when the functions are implemented on the ICRW.
4). After the ICRW checks the results of the executions, the ICRW ejects the card. When the ICRW detects the card transport error, the ICRW stop the RAS operation, indicate orange LED and finishes the RAS mode.
5). The ICRW indicates the check results by LED blinking three times after ejecting the card properly.
6). The RAS operations are repeatable. If the card turn on the card width sensor or PD1 after LED indicating the result of previous checking, the ICRW executes the card entry again.
7). If the card is pulled out after LED indicating the result of previous checking, the ICRW finishes the RAS mode and starts the standard mode.

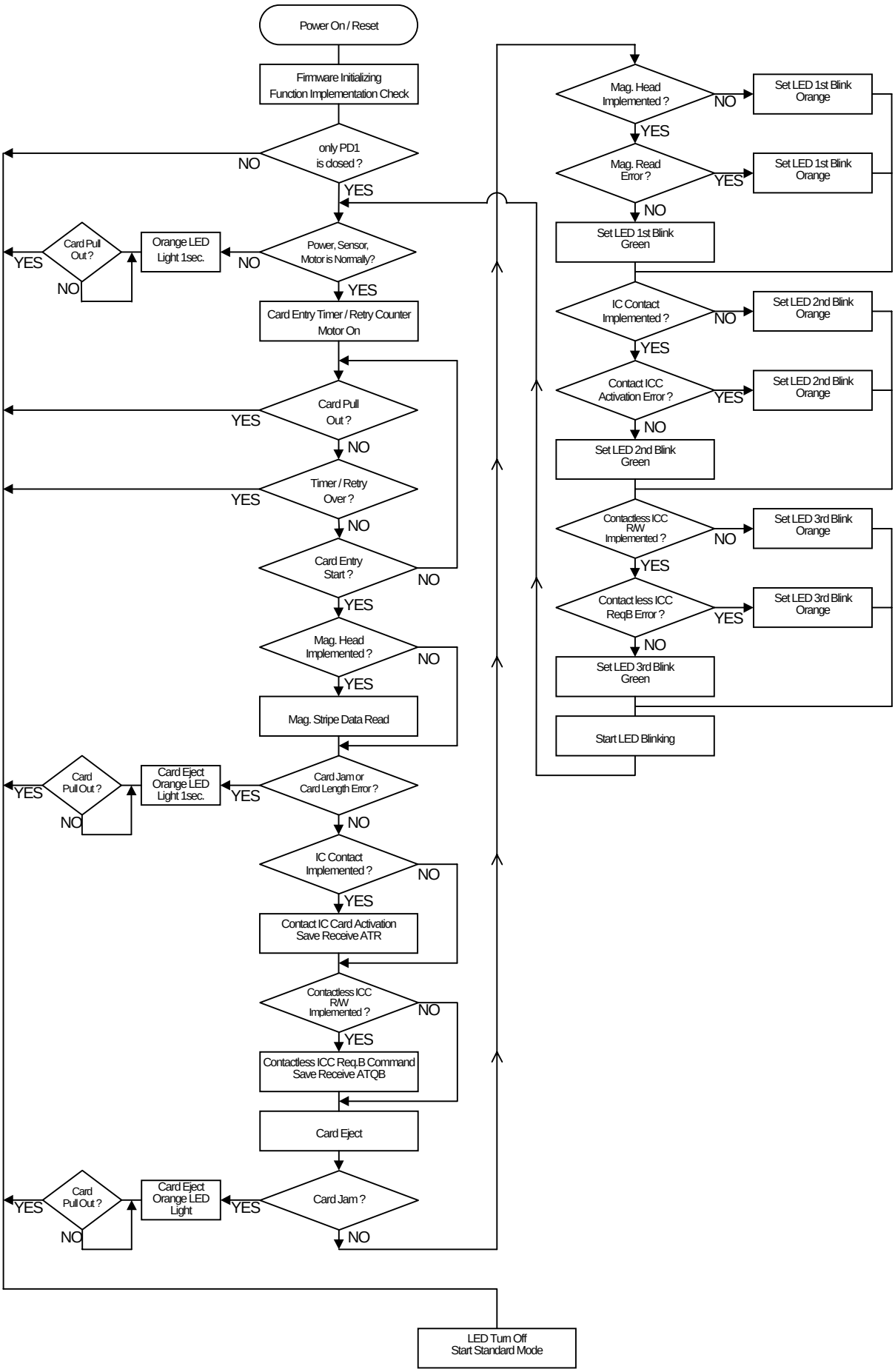
9.6 The check items and the error indications of RAS

check items	check function	LED indications	LED indication color		
			normal	abnormal	not implemented
basic functions	power supply , sensor, motor	light 1sec. and turn off		orange	
card transport	card jam or abnormal card length are detected	light 1sec. and turn off		orange	
magnetic stripe data read	read error (except for not encoded)	1st blink	green	orange	green
contact IC card activation	receive ATR properly	2nd blink	green	orange	green
contactless IC card request B command	receive ATQB properly	3rd blink	green	orange	green

9.7 The not checked functions by RAS

1). CPU functions
2). LED lighting
3). Very low power supply voltage
4). Shutter solenoid
5). Interface to the HOST (While the RAS operation, the interface is not available)

9.8 The flow chart of RAS operation



ANNEX 1 Calculation method of CRCC

CRCC(X16+X12+X5+1) is made by the following method.

```
/*
        [data]
        hex     0xF2, 0x00, 0x08, 0x43, 0x30, 0x30, 0x33, 0x32, 0x34, 0x30, 0x30
        CRC     0xFACE
*/
#define INIT            0x0000      /* Initial value */
#define POLINOMIAL      0x1021      /* Polynomial X16+X12+X5+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) ^ POLINOMIAL;
        }
        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;         /*lengthof(STX+LEN+TEXT) */
    unsigned short crc;                     /* CRC */

    crc = GetCRC(TransCommand, TextLength);
    TransCommand[11] = (crc >> 8) & 0xFF;
    TransCommand[12] = crc & 0xFF;

    return 0;
}
```

ANNEX 2 Values of ATR parameter (TA1 and TA2)

Table1: Supportable TA1 values

Vcc	Condition	Support (Yes/No)	Communication speed (F,D)
30H 33H 35H 36H	TA1 = '11' and TA2=none	Yes	9622bps (F=372, D=1)
	TA1 = 'any' and TA2=none (Not including TA1='11')	Yes	If TA1 is shown in Table2, ICRW sends PPS request. Communication speed depends on PPS response. If TA1 is not shown in Table2, ICRW does not sends PPS request. Communication speed is 9622bps (F=372, D=1).
	TA1 = 'any' and TA2.b5 = 0	Yes (*1)	Comply with Table3
	TA1='any' and TA2.b5=1	No(Vcc=30H)	-
		Yes(Vcc=ELSE)	9622bps (F=372, D=1)
40H	TA1 = 'any' and TA2=none (Including TA1='11')	Yes	9622bps (F=372, D=1)
	TA1='any' and TA2.b5=0	Yes	Comply with Table3
	TA1='any' and TA2.b5=1	Yes	9622bps (F=372, D=1)

A meaning of Vcc parameter please refer "activate ICC command".

(*1) When TA1 exists in table3, ICRW supports its TA1.

Table2: TA1 values that ICRW sends PPS request

TA1	02, 12, 03, 13, 32, 33, 53, 54, 92, 93, B2, B3, D3, D4

Table 3: Supported TA1 values in specific mode

D= / F=	1	2	4	8	16	CLK frequency
372	01 (9622)	02 (19244)	03 (38490)	-	-	3.58MHz
372	11 (9622)	12 (19244)	13 (38490)	-	-	3.58MHz
558	-	-	-	-	-	-
744	31 (9622)	32 (19244)	33 (38490)	-	-	7.16MHz
1116	-	-	-	-	-	-
1488	-	52 (9622)	53 (19244)	54 (38490)	-	7.16MHz
1860	-	-	-	-	-	-
512	91 (6991)	92 (13983)	93 (27965)	-	-	3.58MHz
768	-	-	-	-	-	-
1024	B1 (6991)	B2 (13983)	B3 (27965)	-	-	7.16MHz
1536	-	-	-	-	-	-
2048	-	D2 (6991)	D3 (13983)	D4 (27965)		7.16MHz

Upper row: TA1 value
(Lower row): Communication speed (bps)

ANNEX 3 Values of ATR parameter

Table4: Supported values of ATR

ATR \ Vcc	30H	33H	35H	36H	40H
	Supported values				
TS	'3F', '3B'				
T0	any value				
TA1	See Table1				
TB1	'00' (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	Table1 and TA2 l.s.nibble = TD1 l.s.nibble	See Table1			
TB2	None (prohibit)	any value (*1)			
TC2	'01'… 'FF'				
TD2	m.s. nibble : any value l.s. nibble : '1','E'	m.s. nibble : any value l.s. nibble : any value			
NOT T=15					
TA3,TA4	'10'...'FE'	'01' ... 'FE'			
TB3,TB4	m.s. nibble : '0'...'4' and l.s. nibble : '0'...'5' and $2^{CWI} > (N+1)$	m.s. nibble : '0'...'9' and l.s. nibble : '0'...'15' and $2^{CWI} > (N+1)$			
TC3,TC4	'00'	any value			
TD3,TD4	any value	any value			
T=15					
TA3	(*2)	b1=1	b2=1 or b1=1		any value
TB3,TC3, TD3	(*2)	any value			
TA4	b1=1	b1=1	b2=1 or b1=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.

ANNEX 4 C-APDU Format

The C-APDU consists of a mandatory header of four consecutive bytes denoted CLA, INS, P1 andP2, 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.

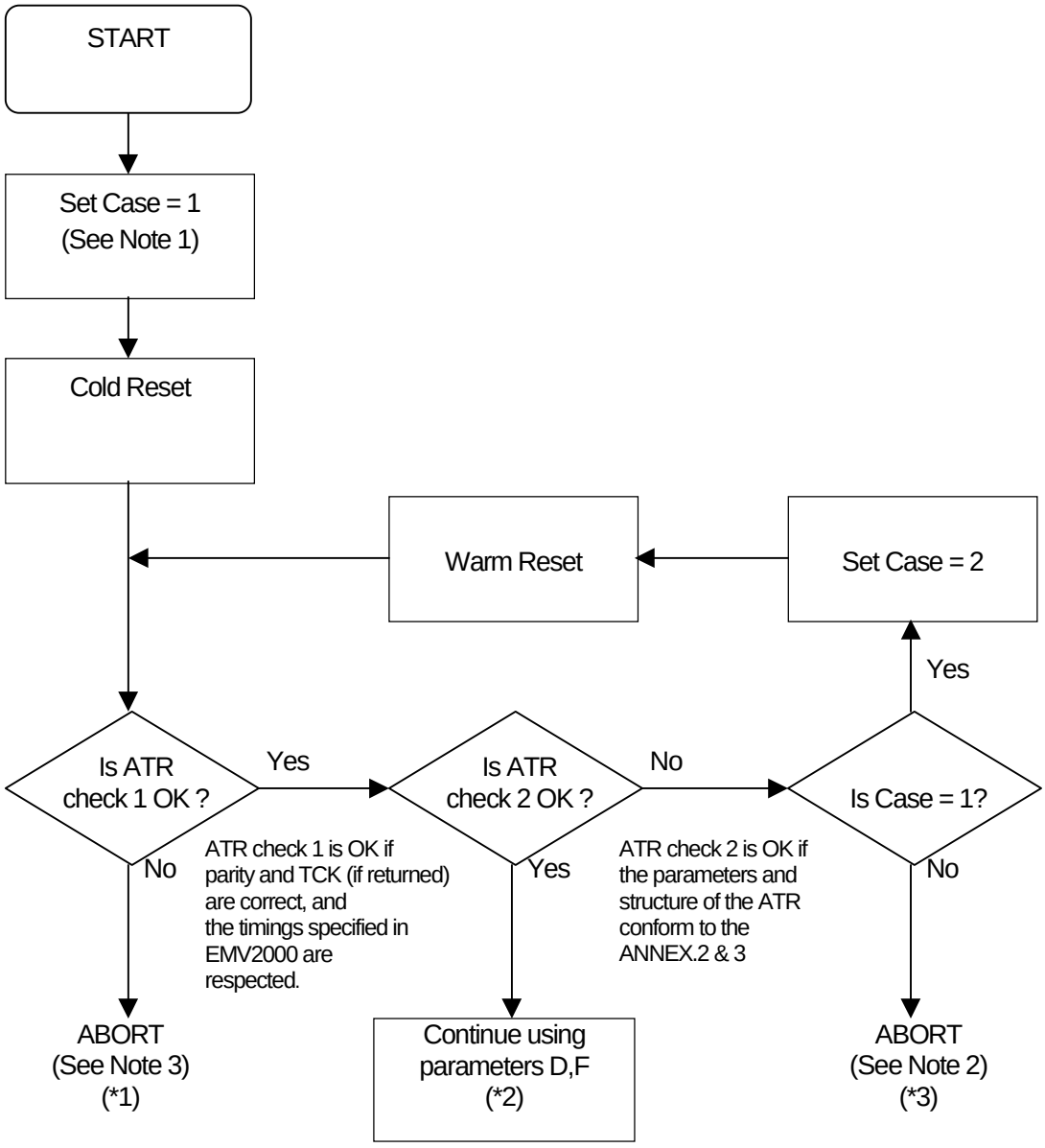
The C-APDU structure has following four cases.

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 Case1, 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.

ANNEX 5 Sequence of activating IC card / SAM

1. In case of Vcc=30H



'Case' is a process variable used to indicate whether a cold or warm reset is operative.
Case = 1 for a cold reset, and Case = 2 for a warm reset.

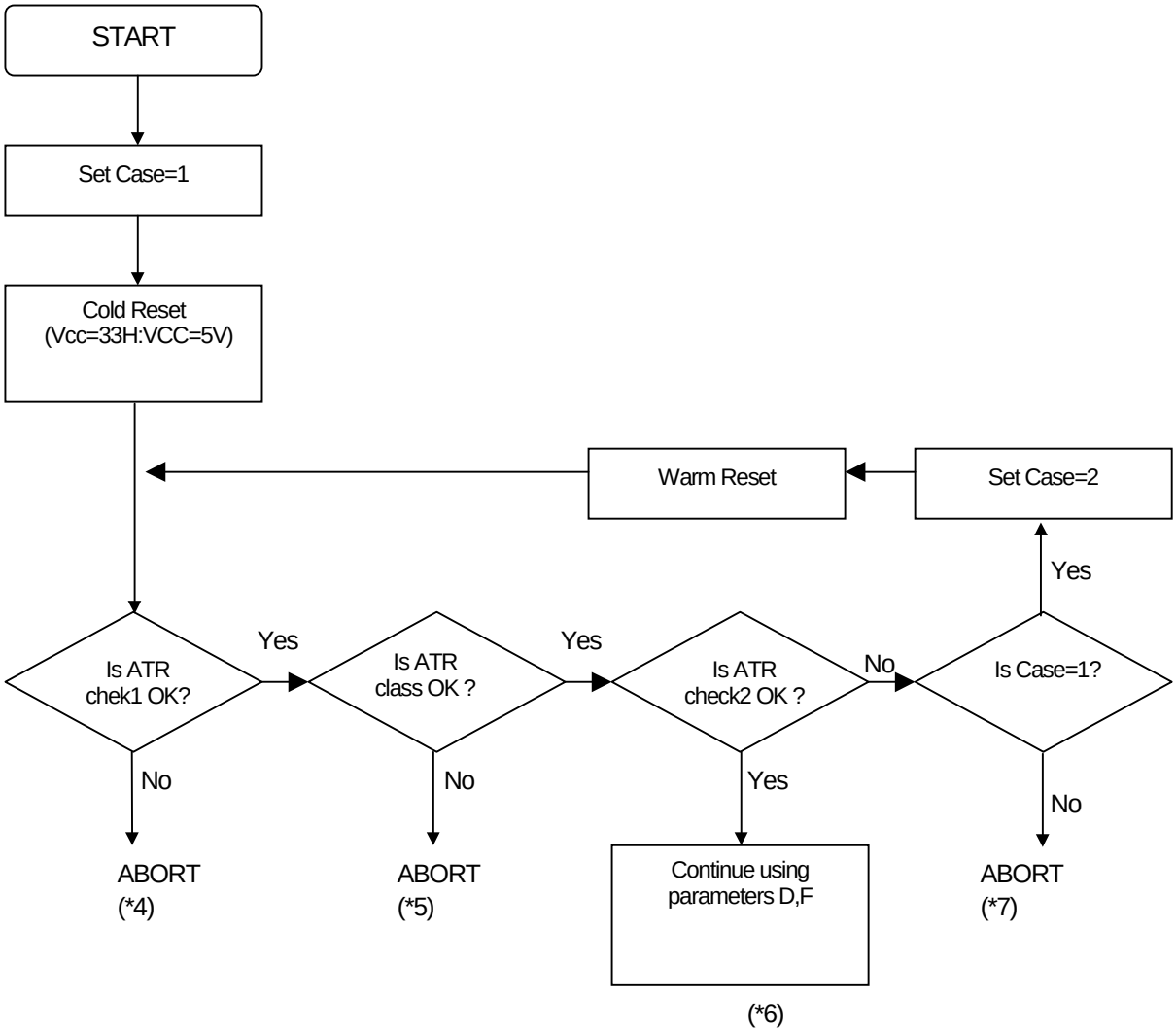
(*1)ICRW initiates the deactivation of ICC, and sends back error code " 61".

(*2)After ICRW received ATR which shows T=1 protocol, ICRW transmits S (IFSreq) to ICC. If S (IFSresp) can't be received properly from ICC, ICRW initiates the deactivation of ICC, and sends back error code " 63" or "64". When S (IFSresp) is received properly in the above or when ATR is not T=1 protocol, ICRW transmits the contents of ATR which is received from ICC to HOST.

(*3)When ATR content is not based on such protocol, which is supported by ICRW, error code "69" with ATR data will be sent back and ICRW will deactivate the IC card.

(Reference: EMV 2000 Integrated Circuit Card Specification for Payment Systems. version 4.0 December 2000)

2. In case of Vcc=33H



(*4)ICRW initiates the deactivation of ICC, and sends back error code " 61".

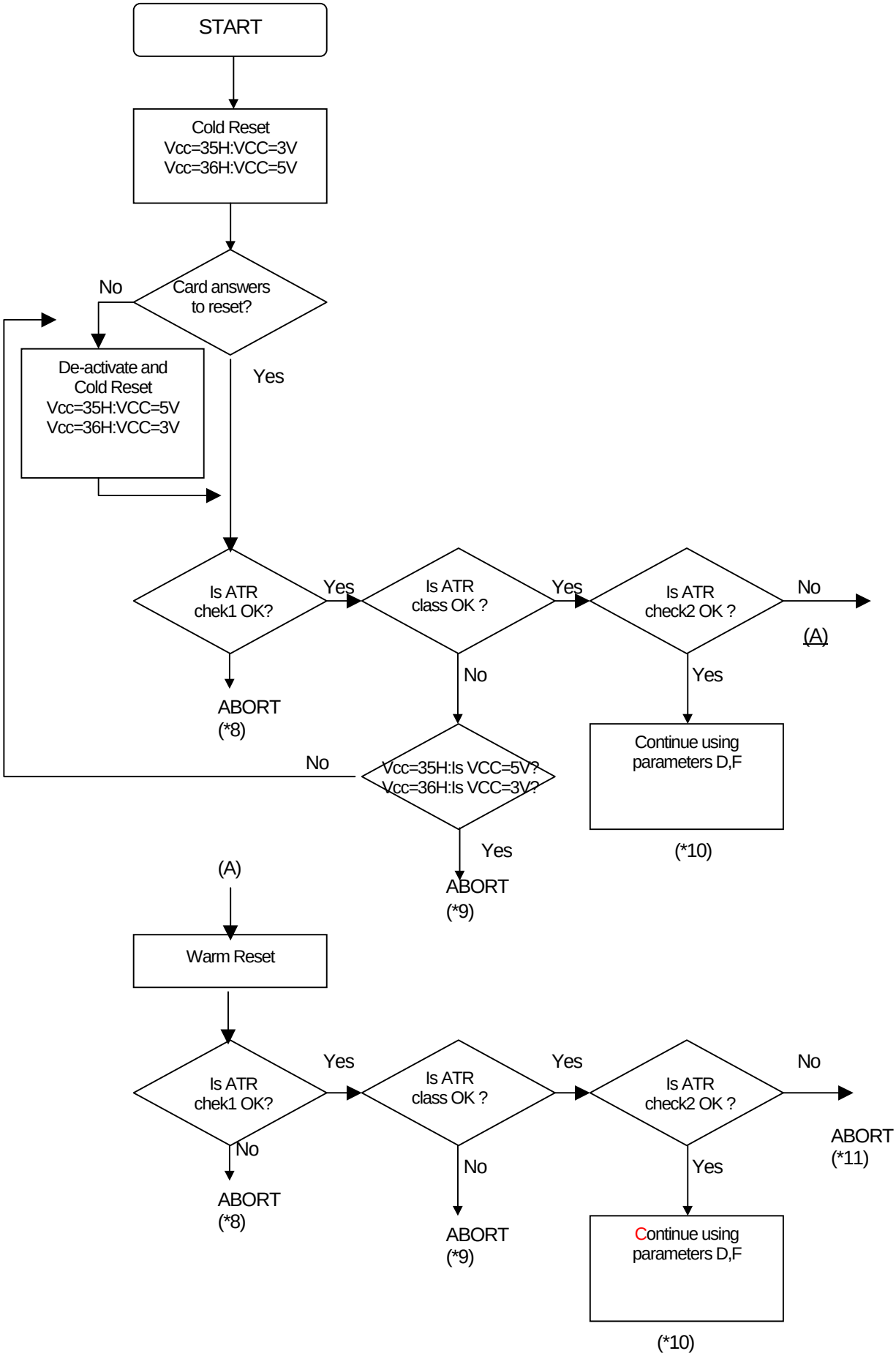
(*5)ICRW checks IC-card's class indicator, which is not supported by ICRW, error code "66" with ATR data will be sent back and ICRW will deactivate the IC card.

(*6) After ICRW received ATR which shows T=1 protocol, ICRW transmits S (IFSreq) to ICC. If S (IFSresp) can't be received properly from ICC, ICRW initiates the deactivation of ICC, and sends back error code " 63" or "64". When S (IFSresp) is received properly in the above or when ATR is not T=1 protocol, ICRW transmits the contents of ATR which is received from ICC to HOST.

(*7)When ATR content is not based on such protocol, which is supported by ICRW, error code "66" with ATR data will be sent back and ICRW will deactivate the IC card.

(Reference: ISO/IEC 7816-3:1997)

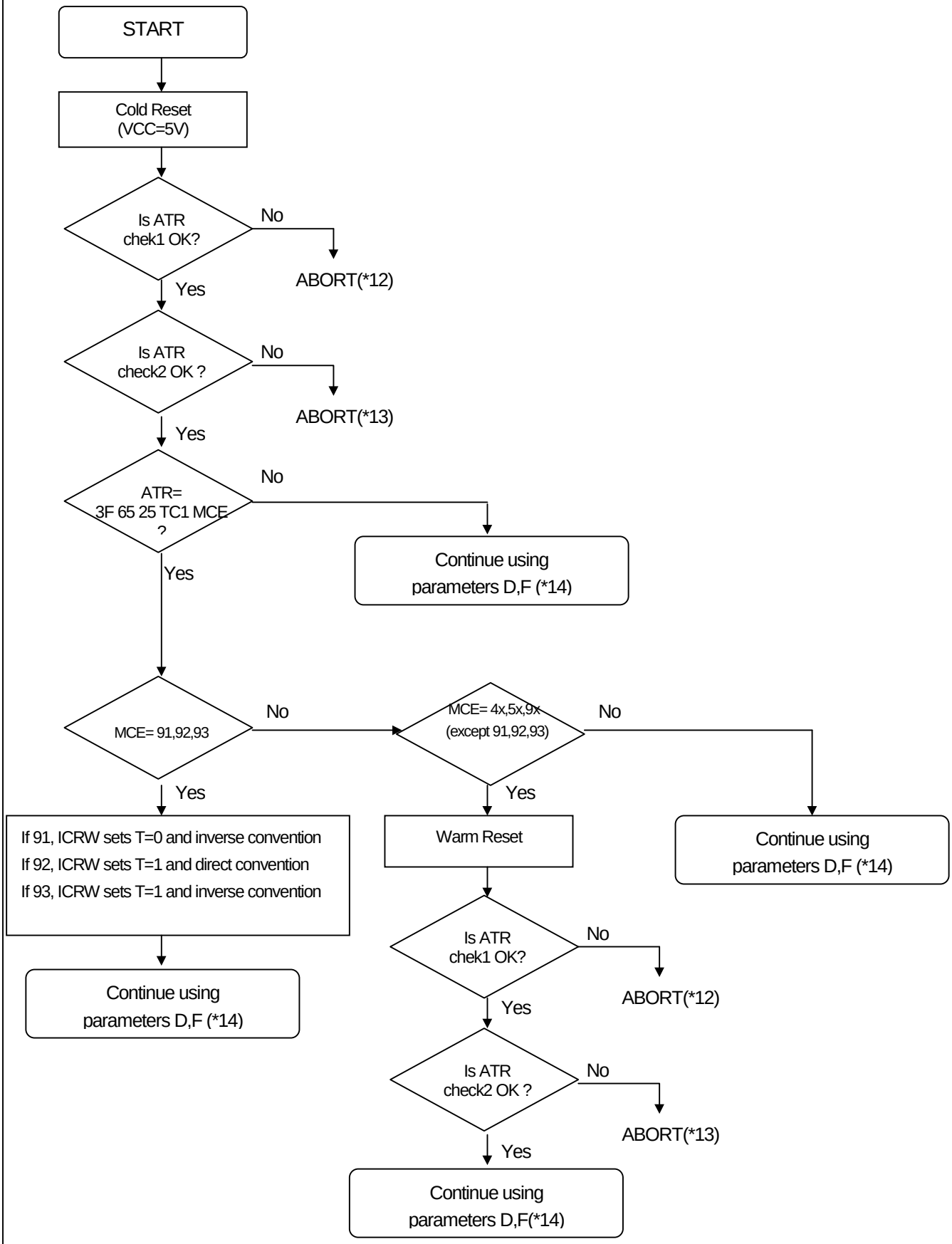
3. In case of Vcc=35H or 36H



(*8)ICRW initiates the deactivation of ICC, and sends back error code " 61".
(*9)ICRW checks IC-card's class indicator, which is not supported by ICRW, error code "66" with ATR data will be sent back and ICRW will deactivate the IC card.
(*10)After ICRW received ATR which shows T=1 protocol, ICRW transmits S (IFSreq) to ICC. If S (IFSresp) can't be received properly from ICC, ICRW initiates the deactivation of ICC, and sends back error code " 63" or "64". When S (IFSresp) is received properly in the above or when ATR is not T=1 protocol, ICRW transmits the contents of ATR which is received from ICC to HOST.
(*11)When ATR content is not based on such protocol, which is supported by ICRW, error code "66" with ATR data will be sent back and ICRW will deactivate the IC card.

(Reference: ISO/IEC 7816-3:1997/Amd.1: 2001)

4. In case of Vcc=40H



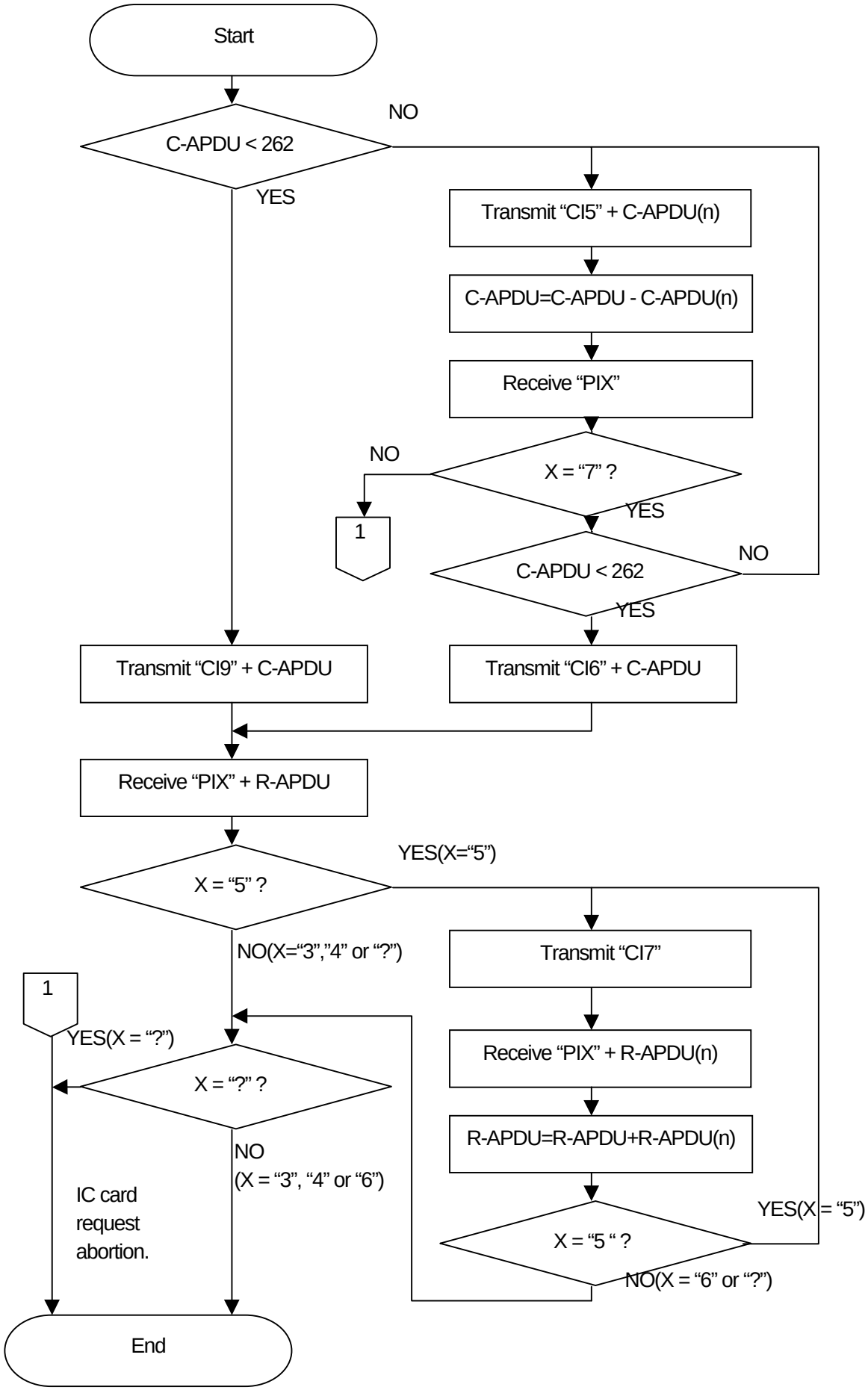
(*12)ICRW initiates the deactivation of ICC, and sends back error code " 61".

(*13)ICRW checks IC-card's class indicator, which is not supported by ICRW, error code "66" with ATR data will be sent back and ICRW will deactivate the IC card.

(*14)After ICRW received ATR which shows T=1 protocol, ICRW transmits S (IFSreq) to ICC. If S (IFSresp) can't be received properly from ICC, ICRW initiates the deactivation of ICC, and sends back error code " 63" or "64". When S (IFSresp) is received properly in the above or when ATR is not T=1 protocol, ICRW transmits the contents of ATR which is received from ICC to HOST.

ANNEX 6 Method of IC card communication

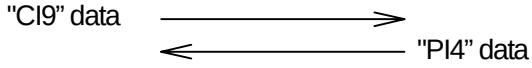
IC card communication flow



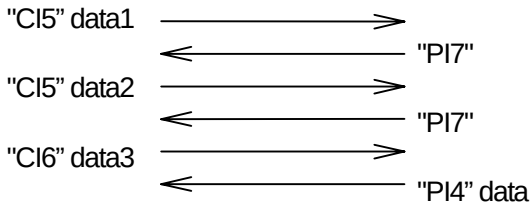
Example

HOST ICRW

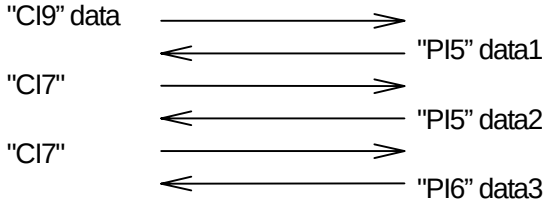
(exp.1) Transmit 261 bytes or less of data.
Receive 258 bytes or less of data.



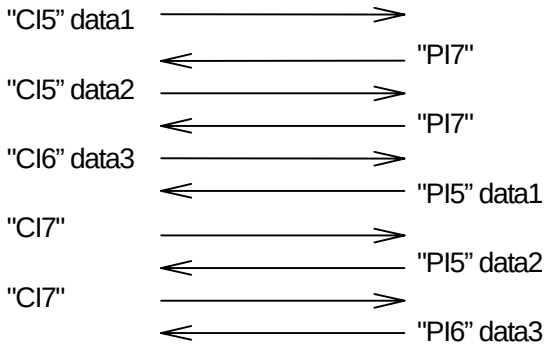
(exp.2) Transmit data by command chaining(Each data size is 261 bytes or less)
Receive 258 bytes or less of data



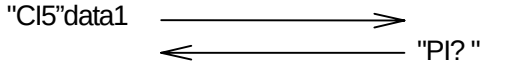
(exp.3) Transmit 261 bytes or less of data
Receive data by command chaining (Each data size is 258 bytes or less)



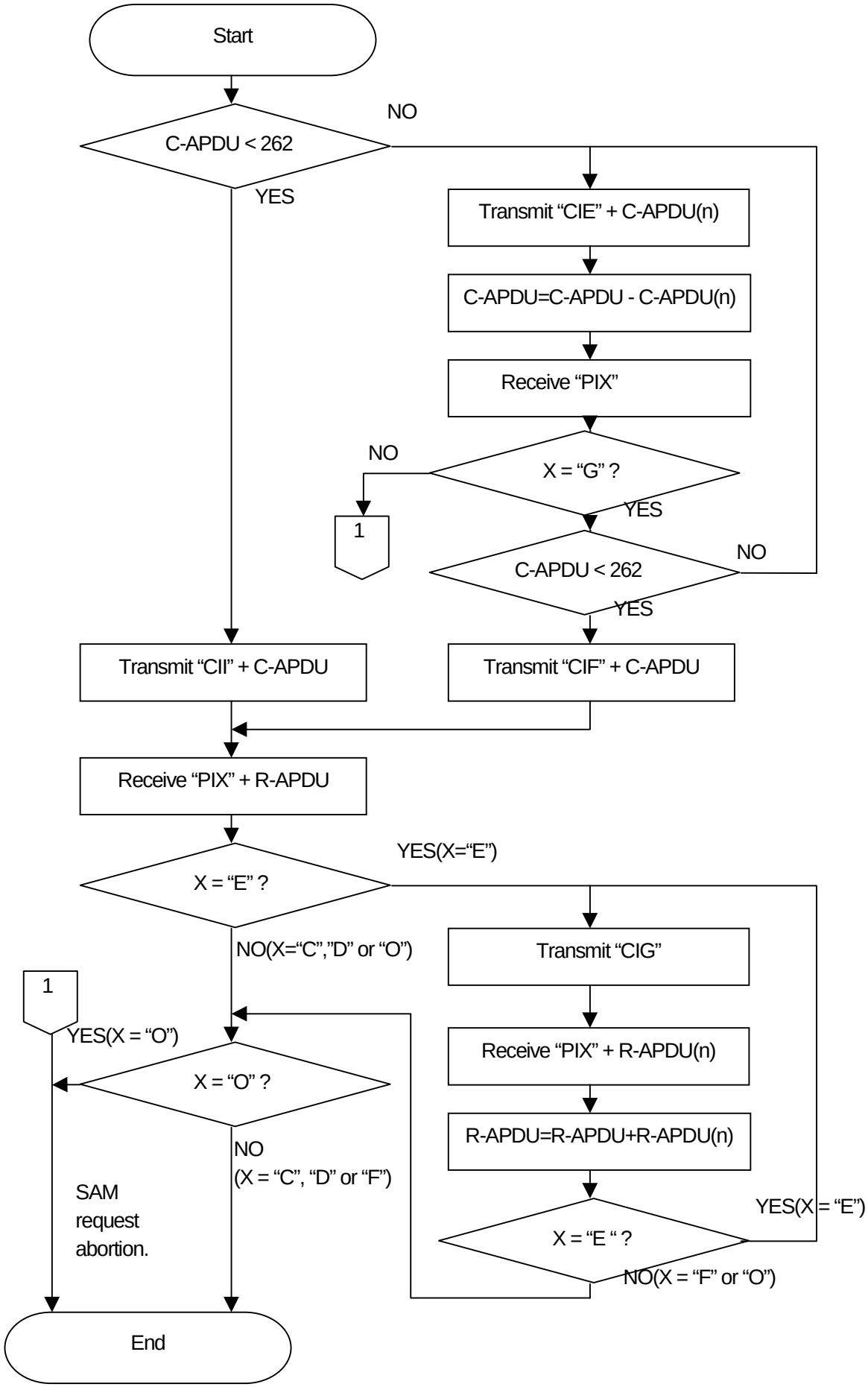
(exp.4) Transmit data by command chaining (Each data size is 261 bytes or less)
Receive data by command chaining (Each data size is 258 bytes or less)



(exp.5) Interruption with receipt of ABORT request



SAM communication flow



Example

HOST ICRW

(exp.1) Transmit data 261 bytes or less of data.
Receive 258 bytes or less of data.

"CII" data →
← "PID" data

(exp.2) Transmit data by command chaining(Each data size is 261 bytes or less)
Receive 258 bytes or less of data

"CIE" data1 →
← "PIG"
"CIE "data2 →
← "PIG"
"CIF" data3 →
← "PID" data

(exp.3) Transmit 261 bytes or less of data
Receive data by command chaining (Each data size is 258 bytes or less)

"CII" data →
← "PIE" data1
"CIG" →
← "PIE" data2
"CIG" →
← "PIF" data3

(exp.4) Transmit data by command chaining (Each data size is 261 bytes or less)
Receive data by command chaining (Each data size is 258 bytes or less)

"CIE" data1 →
← "PIG"
"CIE" data2 →
← "PIG"
"CIF" data3 →
← "PIE" data1
"CIG" →
← "PIE" data2
"CIG" →
← "PIF" data3

(exp.5) Interruption with receipt of ABORT request

"CIE" data1 →
← "PIO"

This page is the end of the document.