
	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	1/46

CRT-310 V3.0 读卡器通讯协议

目 录

1. 通讯格式	2
2. 通讯控制方法	2
3. 通讯控制字符	2
4. 通讯命令结构	2
5. 控制控制命令结构	2
6. 通讯过程描述	3
7. 通讯操作	4
8. CRT310 V3 读卡器卡机操作例程	6
9. CRT310 V3 读卡器卡操作例程	13
9.1 Mefare one 射频卡操作	13
9.2 24CXX 系列存贮卡操作	18
9.3 接触式 CPU 卡操作	20
9.4 SLE4442 卡操作	22
9.5 SLE4428 卡操作	25
9.6 AT88SC102 卡操作	28
9.7 AT88S1604 卡操作	33
9.8. AT45D041 卡操作	35
9.9. SIM 卡操作	36
9.10 磁卡操作	38
9.11 AT88SC1608 卡操作	41

注意：本文档内容绝大部分都兼容 V2.0 版的 CRT-310，请对比使用。

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	2/46

1. 通讯格式:

波特率 (BPS): 可由主控制器设定 (缺省 9600 BPS) (1200/2400/4800/9600/192000/38400BPS)

通信类型: 异步通信

传输类型: 半双工

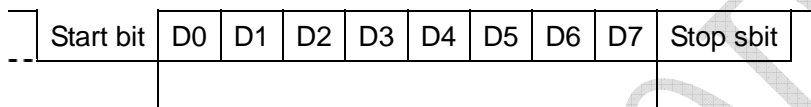
数据帧结构:

起始位: 1 位

数据位: 8 位

校验位: 无

停止位: 1 位



2. 通讯控制方法:

卡机是从动部分, 接收到主机发送有效命令后方能进行操作。

3. 通讯控制字符:

STX (0X02)	通讯文本起始字符
ETX (0X03)	通讯文本结束字符
ENQ (0X05)	发送请求命令 (主机->读卡器)
ACK (0X06)	肯定应答 (读卡器->主机)
NAK (0X15)	否定应答 (读卡器->主机)
EOT (0X04)	取消通信

4. 通讯命令结构: (命令和返回信息的数据包格式)

STX(0x02)	命令包	ETX(0x03)	BCC
-----------	-----	-----------	-----

BCC 使用异或校验, $BCC = STX \oplus \text{命令包} \oplus ETX$ (\oplus 为异或运算符)


例: 复位命令

0x02	0x00	0x02	0x30	0x30	0x03	BCC
------	------	------	------	------	------	-----

$BCC = 0x02 \oplus 0x00 \oplus 0x02 \oplus 0x30 \oplus 0x30 \oplus 0x03$

5. 控制控制命令结构

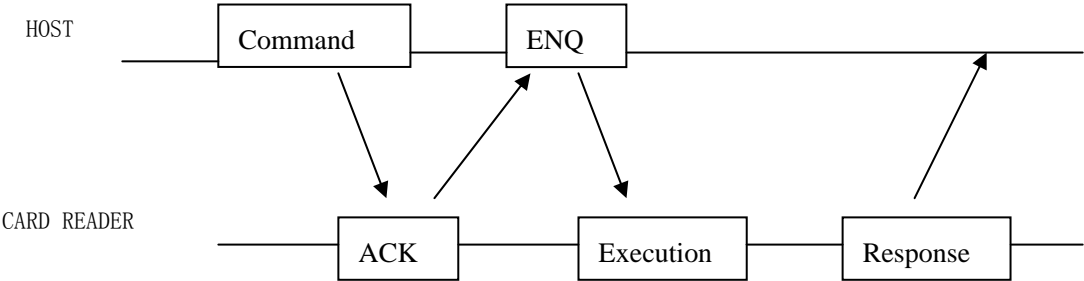
A C K	N A K	E N Q	E O T
-------------	-------------	-------------	-------------

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	3/46

6. 通讯过程描述:

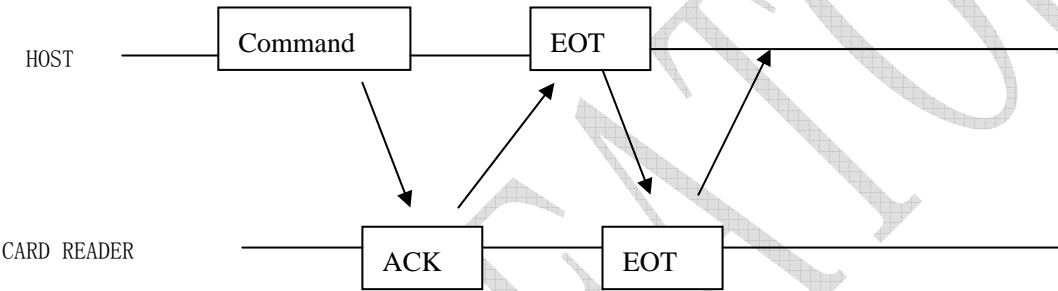
6.1 正常通讯过程:(命令操作)

A. 命令操作



HOST 发送命令，READER 收到并校验 BCC 正确，回 ACK 后，HOST 再发 ENQ 后，READER 将按命令执行相应的操作，并根据命令返回相应操作信息给 HOST。

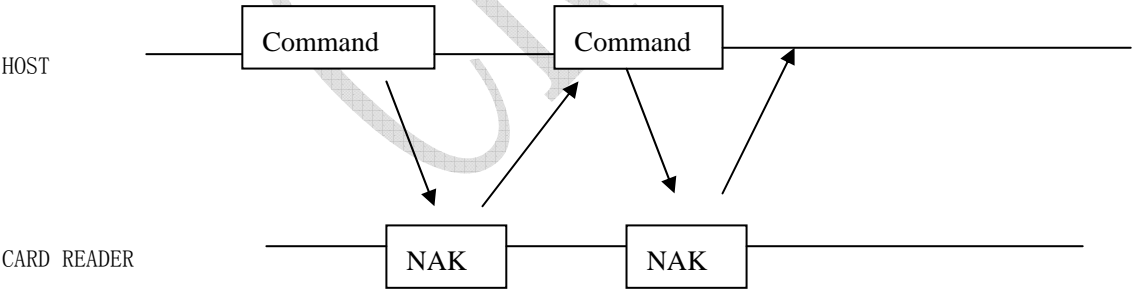
B. 取消命令操作




主机发 EOT 后，CARD READER 结束当前命令状态，返回 EOT ，重新进入等待接收 HOST 命令状态。

6.2 非正常通讯过程:

6. 2. 1 发送包 Command 包 BCC 错误:

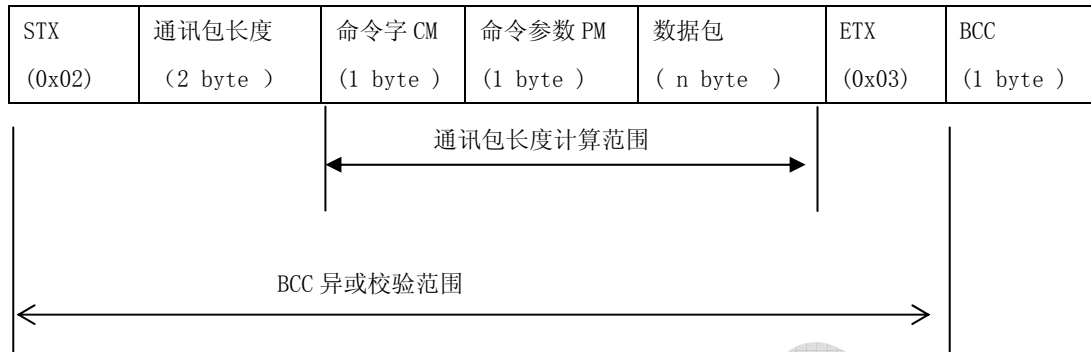


CARD READER 收到一个通讯包出现 BCC 校验出错时，将回应 NAK 给 HOST，表明收到通讯包 BCC 校验错，上位机 (HOST) 需检查发送通讯包 BCC 校验是否有错，无错后再重发当前 CARD READER 只有收到通讯包 BCC 校验是正确时才返回 ACK 给 HOST。

	SPECIFICATION		Model No.	CRT-310 读卡器
			Date	2007/4/1
	通讯协议		Ver.	3.0
			Page	4/46

7. 通讯操作

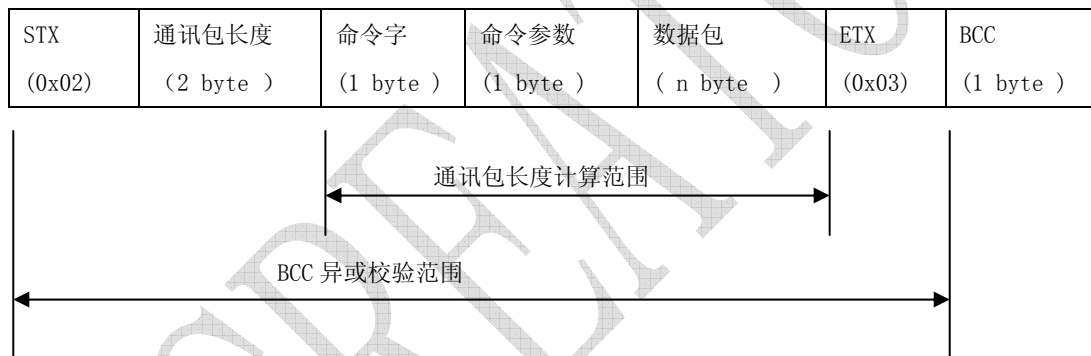
7.1 发送命令通讯包格式:



- 其中数据包中 n byte 最大为 264 byte , 最小为 0 byte.
- 通讯包长度两个字节传送, 前一个字节为高字节, 后一个为低字节。

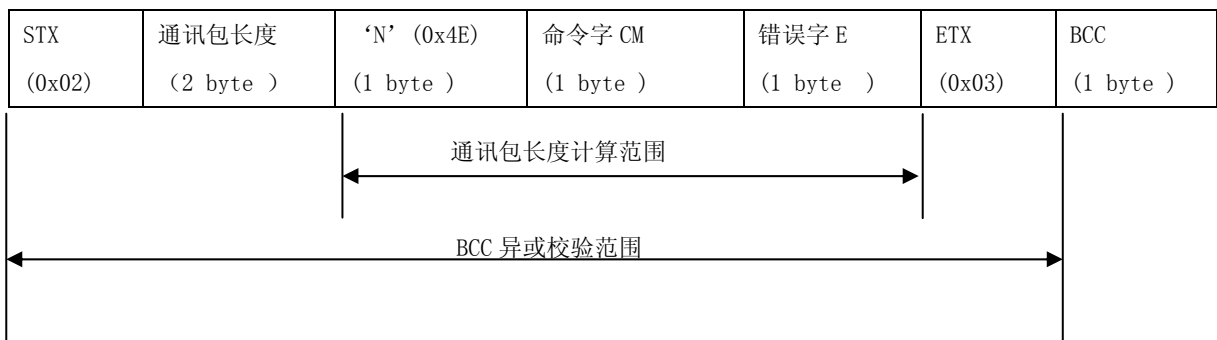
7.2 返回信息通讯包格式


7.2.1 正常返回



- 其中数据包中 n byte 最大为 268 byte , 最小为 0 byte.
- 返回的命令字、命令参数为 HOST 发送到 READER 执行的命令、命令参数。

7.2.2 非正常返回




	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	5/46

错误字 E 含义:

错误字 E	描叙
0x00	命令字错误, 发送的通讯包中有不符合通讯协议规定的命令字 CM
0x01	命令参数错误, 发送的通讯包中有不符合通讯协议规定的命令参数 PM
0x02	命令不能被执行, 发送的命令受限制不能执行该命令。
0x04	命令数据包错误, 发送的通讯包中数据包部分有不符合通讯协议规定的的数据。
0x05	输入电源电压不在卡机工作范围内, 提供给读卡器电源超出读卡器工作电源范围 低于 10.8V 或高于 14.5V , 读卡器处于电源保护状态。
0x06	读卡器内有异常长度的非标准长度的卡, 提示上位机需要处理这些卡片。
0x07	读卡器主电源掉电, 备用电源在工作, 不能执行其它命令操作

注: 非正常返回数据包出现, 是对 HOST 所发的通讯包中命令字, 命令参数, 及卡机出现异常情况一个返回。


1. 错误字 E=0x00 表明 HOST 发送的通讯包中的命令字是通讯协议没有定义的命令字, 是非法的命令。
2. 错误字 E=0x01 表明 HOST 发送的通讯包中的命令参数是通讯协议没有定义的命令字, 是一条非法命令。出现这种情况请详细核对通讯协议的中命令参数字节定义范围, 特别是对 IC 卡操作时, 命令的参数(操作地址, 操作长度)取值范围, 不能超出 IC 卡所规定的操作地址空间范围。否则读卡器进行报错处理。
3. 错误字 E=0x02 表明 HOST 发送的通讯包是本机型不能支持的功能, 不能执行, 进行报错, 返回这种报错请核对读卡器型号, 如是无磁卡的机型, 发送磁卡通讯包时, 读卡器将返回命令不能执行的报错处理。同理, 无射频卡机型发射频卡操作通讯包也时报命令不能执行的报错处理。请注意通讯协议中提到命令不能执行说明部分。
4. 错误字 E=0x04 表明 HOST 发送的通讯包中的数据包是不符合通讯协议要求, 数据包中的格式有错, 不能执行, 进行报错处理。出现情况是在 CPU 卡的 A-PDU 命令操作中进行检测处理。
5. 错误字 E=0x05 表明供给读卡器的直流电源已经超出了工作范围(读卡器电源的工作范围: 10.5V-14.5V, 建议使用 12V), 读卡器处于电源保护状态, 不能执行命令操作及其它进卡, 走卡的动作, 只响应通讯操作。
6. 错误字 E=0x06 表明读卡器内停有异常长度的卡, 超出 ISO 标准长度卡(长卡, 短卡, 残卡等)进入读卡器后, 收到 HOST 发送通讯包后, 读卡器向 HOST 返回报错, 提示要对读卡器的异常卡进行清理。
7. 错误字 E=0x07 表明读卡器使用主电源+备用电源方式进行供电, 当主电源掉电后, 备用电源在工作, 收到 HOST 发送通讯包后, 读卡器向 HOST 返回错误进行报错处理。

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	6/46

8. CRT-310 读卡器卡机操作命令:

8. 操作命令列表

命令	命令字 CM	命令参数 PM	描述
持卡位置设置	0x2E	Pm	卡机进卡读完磁卡后持卡位置设定
进卡使能控制	0x2F	Pm1, Pm2	前后端进卡方式使能，禁能
复位	0x30	0x30	复位卡机，返回卡机软件版本信息
		0x31	复位卡机，弹出卡机内的卡到前端，返回卡机软件版本信息
		0x32	复位卡机，弹出卡机内的卡到后端，返回卡机软件版本信息
读写序列号 （仅 V3.0）	0x30	0x3A	读读卡器的序列号
		0x3B	写读卡器的序列号
查状态	0x31	0x2F	查卡机各传感器的状态信息
		0x30	查卡机状态（卡机内有无卡等）信息
测 IC 卡类型	0x31	0x31	自动测 IC 卡的类型
卡机卡走位操作	0x32	0x2E	将停在持卡位置或卡机内位置的卡进卡到卡机内
		0x2F	将停在持卡位置或卡机内位置的卡进卡到 IC 卡的操作位置上，进卡完成后可进行 IC 卡 R/W 的操作
		0x30	将卡从前端弹出，不持卡
		0x31	将卡从前端弹出，并持卡
		0x32	将卡从后端弹出，并持卡
		0x33	将卡从后端弹出，不持卡
IC 卡上下电	0x33	0x30	IC 卡上电
		0x31	IC 卡下电
SIM 卡下电	0x4A	0x31	SIM 卡下电
设置串口波特率	0x34	0x30	UART=1200 BPS
		0x31	UART=2400 BPS
		0x32	UART=4800 BPS
		0x33	UART=9600 BPS
		0x34	UART=192000 BPS
		0x35	UART=384000 BPS
各类操作请见命令详解			

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	7/46

8.1 卡机复位类

8.1.1 卡机复位

Host 发送: (Pm=0x30, 0x31, 0x32)

0x02	0x00	0x02	0x30	Pm	0x03	BCC
------	------	------	------	----	------	-----

Pm=0x30 卡机复位, 上传读卡器版本信息

Pm=0x31 卡机复位, 上传读卡器版本信息, 并将卡弹在前端不持卡

Pm=0x32 卡机复位, 上传读卡器版本信息, 并将卡从后端弹出不持卡

Reader 返回:

0x02	0x00	0x0F	0x30	Pm	读卡器版本信息字 SV	0x03	BCC
------	------	------	------	----	-------------	------	-----

读卡器版本信息: CRT310 读卡器 SV= "CRT 310 V3.0 "

8.1.2 读 CRT310 读卡器的序列号

Host 发送:

0x02	0x00	0x02	0x30	0x3A	0x03	BCC
------	------	------	------	------	------	-----

Reader 操作成功返回: 操作状态字 P= 'Y' (0x59)

0x02	通讯包长度 2 byte	0x30	0x3A	操作状态字 P	序列号数据包	0x03	BCC
------	--------------	------	------	---------	--------	------	-----

序列号数据默认为 "CRT 310 V3.0 "

Reader 操作失败返回: 操作状态字 P= 'N' (0x4E)

0x02	0x00	0x03	0x30	0x3A	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

8.1.3 写 CRT310 读卡器的序列号

Host 发送:

0x02	通讯包长度 2 byte	0x30	0x3A	N byte 序列号数据包	0x03	BCC
------	--------------	------	------	---------------	------	-----

Reader 操作返回:

0x02	0x00	0x03	0x30	0x3A	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'Y' (0x59)

P= 'N' (0x4E)

N byte 序列号数据包: 要写入序列号数据, 其中 N = 0x01—0x10 (序列号数据最小为 1 byte, 最大为 16 byte)

以 HEX 代码写入。

8.2 CRT310 卡机进卡使能、停卡位置设置控制操作

8.2.1 CRT310 读卡器进卡方式控制设置命令操作

Host 发送:

0x02	0x00	0x03	0x2F	Pm1	Pm2	0x03	BCC
------	------	------	------	-----	-----	------	-----


Pm1=0x31 禁止前端进卡

Pm1=0x32 磁卡方式 (磁信号+开关同时有效) 进卡使能, 只允许磁卡从前端开闸门进卡

Pm1=0x33 开关方式进卡使能, 允许磁卡, IC 卡, Mefare 1 射频卡, 双界面卡从前端开闸门进卡

Pm1=0x34 磁信号方式进卡, 针对薄磁卡等一些纸卡进卡

Pm2=0x30 允许后端进卡

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	8/46

Pm2=0x31 禁止后端进卡

Reader 返回:

0x02	0x00	0x04	0x2F	Pm1	Pm2	卡机状态字 S	0x03	BCC
------	------	------	------	-----	-----	---------	------	-----

S= 'N' (0x4E) 设置失败

S= 'Y' (0x59) 设置成功

读卡器在上电或执行复位命令后默认的前端进卡方式是开关方式进卡使能，后端允许进卡。

注：对于无电控门的机型，只能响应开关方式进卡，不能设置成磁卡方式进卡和磁信号方式进卡，否则将提示“命令不能执行”。

8.2.2 CRT310 停卡位置设置（当卡机进卡读完磁卡后所停的位置进行设置）

其中卡机上电或执行复位后，默认停卡位置是停在卡机内位置上。

Host 发送:

0x02	0x00	0x02	0x2E	Pm	0x03	BCC
------	------	------	------	----	------	-----

Pm=0x30 进卡后停卡在前端位置，不持卡。

Pm=0x31 进卡后停卡在前端位置，并持卡。

Pm=0x32 进卡后停卡在卡机内位置，但是 IC 卡触点没有与卡接触，M1 射频卡可以进行读写操作。

Pm=0x33 进卡后停卡在卡机内位置，同时将 IC 卡座触点与卡接触，直接可进行 IC 卡操作和 M1 射频卡进行操作。

Pm=0x34 进卡后停卡在后端位置，并持卡。

Pm=0x35 进卡后将卡从后端弹出，不持卡。

Reader 返回:

0x02	0x00	0x03	0x2E	Pm	卡机状态字 S	0x03	BCC
------	------	------	------	----	---------	------	-----

S= 'N' (0x4E) 设置失败

S= 'Y' (0x59) 设置成功

注：无 IC 卡机型执行设定进卡后停卡在 IC 卡操作位时，读卡器将返回“命令不能执行”的信息，设定停卡位为 IC 操作位将无效。

8.3 CRT310 卡机状态信息

8.3.1 CRT310 卡机查状态

Host 发送:

0x02	0x00	0x02	0x31	0x30	0x03	BCC
------	------	------	------	------	------	-----

Reader 返回

0x02	0x00	0x05	0x31	0x30	卡机状态字 S1	卡机状态字 S2	卡机状态字 S3	0x03	BCC
------	------	------	------	------	----------	----------	----------	------	-----


S1=0x46 卡机内有长卡(卡的长度长于标准卡长度)

S1=0x47 卡机内有短卡(卡的长度短于标准卡长度)

S1=0x48 卡机前端，不持卡位置有卡（相当于在前端完全弹出了卡）。

S1=0x49 卡机前端持卡位置有卡。

S1=0x4A 卡机内停卡位置有卡。

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	9/46

- S1=0X4B 卡机内 IC 卡操作位置有卡，并且 IC 卡触电已下落。
- S1=0X4C 卡机后端持卡位置有卡。
- S1=0X4D 卡机后端不持卡位置有卡（相当于在后端完全弹出了卡，没收了卡）。
- S1=0x4E 卡机内无卡。
-
- S2=0X49 卡机允许磁卡方式进卡，只允许磁卡开闸门进卡。
- S2=0X4A 卡机允许开关方式进卡，允许磁卡，IC 卡，M1 射频卡，双界面卡进卡。
- S2=0X4B 卡机允许磁信号方式进卡，允许纸磁卡，薄卡进卡。
- S2=0x4E 卡机禁止进卡。
-
- S3=0X4A 卡机允许后端进卡，允许磁卡，IC 卡，M1 射频卡，双面卡进卡。
- S3=0x4E 卡机禁止后端进卡。

8.3.2 CRT310 传感器详细状态检测(与 V2 版本兼容):

Host 发送：卡机执行自动侦测各传感器状态(5 个红外传感器，闸门状态，开关进卡传感器状态)

0x02	0x00	0x02	0x31	0x2F	0x03	BCC
------	------	------	------	------	------	-----

Reader 返回:

0x02	0x00	0x09	0x31	0x2F	PSS1	PSS2	PSS3	PSS4	PSS5	CTSW	KSW	0x03	BCC
------	------	------	------	------	------	------	------	------	------	------	-----	------	-----

- PSS1—PSS5: 红外传感器状态 PSS (1...5) =0X30 表示此传感器位置上未探测到卡片;
PSS (1...5) =0X31 表示探测到有卡片。
- CTSW: 闸门状态信息 CTSW=0X30 表示闸门已关闭;
CTSW=0X31 表示闸门已打开。
- KSW: 开关进卡传感器状态 KSW=0X30 表示开关没有检测到卡片插入闸门信号;
KSW=0X31 表示开关检测到有卡片插入闸门。

8.3.3 CRT310 传感器详细状态检测(仅 V3.0):


Host 发送：卡机执行自动侦测各传感器状态(6 个红外传感器，闸门状态，开关进卡传感器状态)

0x02	0x00	0x02	0x31	0x2E	0x03	BCC
------	------	------	------	------	------	-----

Reader 返回:

0x02	0x00	0x0A	0x31	0x2E	PSS0	PSS1	PSS2	PSS3	PSS4	PSS5	CTSW	KSW	0x03	BCC
------	------	------	------	------	------	------	------	------	------	------	------	-----	------	-----

- PSS0—PSS5: 红外传感器状态: PSS (0...5) =0X30 表示此传感器位置上未探测到卡片;
PSS (0...5) =0X31 表示探测到有卡片。
- CTSW: 闸门状态信息 CTSW=0X30 表示闸门已关闭;
CTSW=0X31 表示闸门已打开。
- KSW: 开关进卡传感器状态 KSW=0X30 表示开关没有检测到卡片插入闸门信号;
KSW=0X31 表示开关检测到有卡片插入闸门。

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	10/46

8.4 CRT310 自动测 IC 卡类型:

Host 发送: 卡机执行自动侦测卡片类型, 并返回寻到卡类型

0x02	0x00	0x02	0x31	0x31	0x03	BCC
------	------	------	------	------	------	-----

Reader 返回:

0x02	0x00	0x04	0x31	0x31	卡类型状态字 S1	卡类型状态字 S2	0x03	BCC
------	------	------	------	------	-----------	-----------	------	-----

类型状态字 S1, S2:

卡类型状态字 S1	卡类型状态字 S2	卡类型说明
'N'	'0'	卡机内无卡
	'1'	未知卡类型
	'2'	卡不在允许操作的位置上
'0'	'0'	卡为非接触式 M1 射频卡
'1'	'0'	卡为接触式 T=0 的 CPU 卡
	'1'	卡为接触式 T=1 的 CPU 卡
'2'	'0'	卡为 24C01 卡
	'1'	卡为 24C02 卡
	'2'	卡为 24C04 卡
	'3'	卡为 24C08 卡
	'4'	卡为 24C16 卡
	'5'	卡为 24C32 卡
	'6'	卡为 24C64 卡
'3'	'0'	卡为 SL4442 卡
	'1'	卡为 SL4428 卡
'4'	'0'	卡为 AT88S102 卡
	'1'	卡为 AT88S1604 卡
	'2'	卡为 AT45D041 卡
	'3'	卡为 AT88SC1608 卡

注: 自动测卡型, 只支持检测 Mafare one 射频卡, 接触式 IC 卡, 不能做双界面卡检测, 对于接触式 IC 卡, 可能受卡片触点清洁程度影响, 可能会造成测卡型不准确, 所以自动测卡型中接触式 IC 卡只能作参考。

8.5 CRT310 卡机卡走位控制操作

将停在持卡位置或卡机内位置的卡重新进行走卡到新的持卡位置操作。

Host 发送:


0x02	0x00	0x02	0x32	Pm	0x03	BCC
------	------	------	------	----	------	-----

Pm=0x2E 将卡重新走位到卡机内位置,操作成功后可进行 M1 射频卡操作。

Pm=0x2F 将卡重新走位到卡机内位置, 并将 IC 卡触点落下, 操作成功后可进行接触式 IC 卡操作。

Pm=0x30 将卡重新走位到前端位置, 不持卡。

Pm=0x31 将卡重新走位到前端位置, 并持卡。

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	11/46

Pm=0x32 将卡重新走位到后端位置，并持卡。

Pm=0x33 将卡重新走位后端位置，不持卡。

Pm=0x34 将异常长度卡（短卡，长卡）清出卡机内，将卡向后端弹卡，对于短卡还需人工在卡口插正常卡辅助操作。

（该指令可用于清洁卡机内部的作用）

Reader 返回：

0x02	0x00	0x03	0x32	Pm	操作状态字 P	0x03	BCC
------	------	------	------	----	---------	------	-----

P= 'Y' (0x59) 操作成功。

P= 'N' (0x4E) 操作失败。

P= 'E' (0x45) 卡机内无卡。

P= 'W' (0x57) 卡不在允许操作的位置上。

注：当卡不在有持卡位置上或不在卡机内时再执行其它的进、弹卡命令时，将返回“卡不在允许操作位置”的信息上。

无 IC 卡机型执行走卡到 IC 卡操作位时，读卡器将返回“命令不能执行”的信息,进行走卡到 IC 卡操作位无效。

8.6 IC 卡、SIM 卡 上/下电操作

8.6.1 接触式 IC 卡上/下电

Host 发送：

0x02	0x00	0x02	0x33	Pm	0x03	BCC
------	------	------	------	----	------	-----

Pm=0x30 IC 卡上电

Pm=0x31 IC 卡下电

Reader 返回：

0x02	0x00	0x03	0x33	Pm	操作状态字 P	0x03	BCC
------	------	------	------	----	---------	------	-----

操作状态字 P= 'Y' (0x59) 操作成功

P= 'N' (0x4E) 操作失败

P= 'E' (0x45) 卡机内无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

注：当卡不在有持卡位置上或不在卡机内时再执行 IC 卡上/下电命令时，将返回“卡不在允许操作位置”的信息上。

无 IC 卡机型执行 IC 卡上/下电命令时，读卡器将返回“命令不能执行”的信息,进行 IC 卡上/下电操作位无效。

8.6.2 SIM 卡下电操作

Host 发送：

0x02	0x00	0x02	0x4A	0x31	0x03	BCC
------	------	------	------	------	------	-----

Pm=0x31 SIM 卡下电

Reader 返回：


0x02	0x00	0x03	0x4A	Pm	操作状态字 P	0x03	BCC
------	------	------	------	----	---------	------	-----

操作状态字 P= 'Y' (0x59) 操作成功

P= 'N' (0x4E) 操作失败

注：SIM 卡的上电操作由 SIM 卡的复位操作时来完成的。

无 SIM 卡机型执行 SIM 卡上/下电命令时，读卡器将返回“命令不能执行”的信息,进行 SIM 卡上/下电操作位无效。

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	12/46

8.7 闸门指示灯控制操作

8.7.1 亮灭指示灯操作

Host 发送:

0x02	0x00	0x02	0x46	Pm	0x03	BCC
------	------	------	------	----	------	-----

Pm=0x30 亮指示灯

Pm=0x31 灭指示灯

Reader 返回:

0x02	0x00	0x03	0x46	Pm	操作状态字 P	0x03	BCC
------	------	------	------	----	---------	------	-----

操作状态字 P= 'Y' (0x59) 操作成功

8.7.2 闪烁指示灯操作 (闪烁周期可调)

Host 发送:

0x02	0x00	0x03	0x49	Pm1	Pm2	0x03	BCC
------	------	------	------	-----	-----	------	-----

Pm1: 亮指示灯时间值 (Pm1 值为 0x00-0xFF, 时间值为 0.25 秒 X Pm1)

Pm2: 灭指示灯时间值 (Pm2 值为 0x00-0xFF, 时间值为 0.25 秒 X Pm2)

Reader 返回:

0x02	0x00	0x04	0x49	Pm1	Pm2	操作状态字 P	0x03	BCC
------	------	------	------	-----	-----	---------	------	-----

操作状态字 P= 'Y' (0x59) 操作成功

指示灯闪烁一次的时间周期= Pm1 时间 + Pm2 时间。闪烁最小时间周期值为 0.5 秒 (Pm1=0x01, Pm2=0x01)。

当 Pm1=0x00, Pm2 为任意时间值, 指示灯常灭; 当 Pm2=0x00, Pm1=0x01-0xFF, 指示灯常亮。

注: 在上电复位或执行复位命令后, 闸门指示灯将熄灭。执行 10.7.1 亮灭灯操作, 闪烁灯操作退出, 此时灯的状态由亮灭指示灯的命令操作的决定。

8.8 设置串口通讯波特率:

Host 发送:

0x02	0x00	0x02	0x34	Pm	0x03	BCC
------	------	------	------	----	------	-----

Pm=0x30 uart=1200bps

Pm=0x31 uart=2400pbs

Pm=0x32 uart=4800bps

Pm=0x33 uart=9600bps

Pm=0x34 uart=19200bps

Pm=0x35 uart=38400bps


Reader 返回:

0x02	0x00	0x03	0x33	Pm	操作状态字 P	0x03	BCC
------	------	------	------	----	---------	------	-----

操作状态字 P= 'Y' (0x59) 操作成功

操作状态字 P= 'N' (0x4E) 操作失败

Host 收到卡机返回操作成功信息后, 读卡器将按新的波特率对读卡器串口重新设置, 并保存在读卡器 EEPROM 中存储, 直至有新的波特率更改。Host 也要相应地进入按设定的波特率重新串口设置, 才能进行通讯。

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	13/46

8.9 第三方通讯接口使能禁能:

Host 发送:

0x02	0x00	0x02	0xFA	Pm	0x03	BCC
------	------	------	------	----	------	-----

Pm = 0x30 使能第三方通讯接口

Pm = 0x31 禁能第三方通讯接口

Reader 返回:

0x02	0x00	0x03	0xFA	Pm	操作状态字 P	0x03	BCC
------	------	------	------	----	---------	------	-----

操作状态字 P= 'Y' (0x59) 操作成功

操作状态字 P= 'N' (0x4E) 操作失败

第三方通讯接口, 允许第三方设备的串口与 CRT310 读卡器串口并接一起分时使用, 使能第三方通讯接口后, CRT310 将处于监听状态, 不作任何通回应, 直至收到主机发送禁止第三方通讯操作命令时才回应, 此时主机发第三方通讯操作命令就能操作第三方设备。

9. CRT310 V3 读卡器读写卡操作规程

9.1. Mefare one 射频卡操作 (支持读写 S50, S70 的卡片)

9.1.1 寻射频卡

HOST 发送:

0x02	0x00	0x02	0x35	0x30	0x03	BCC
------	------	------	------	------	------	-----

READER 返回:

0x02	0x00	0x03	0x35	0x30	操作状态 P	0x03	BCC
------	------	------	------	------	--------	------	-----

操作状态字 P= 'Y' (0x59) 寻卡成功

P= 'N' (0x4E) 寻卡不成功

P= 'E' (0x45) 卡机内无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

9.1.2 获取 Mefare1 卡序列号

HOST 发送:

0x02	0x00	0x02	0x35	0x31	0x03	BCC
------	------	------	------	------	------	-----

READER 操作返回:

0x02	0x00	0x07	0x35	0x31	操作状态 P	4 byte hex 卡序列号	0x03	BCC
------	------	------	------	------	--------	-----------------	------	-----

操作状态字 P= 'Y' (0x59) 获取卡序列号成功, 并返回卡序列号

P= 'N' (0x4E) 获取卡序列号失败, 并返回空序列号 (0x00, 0x00, 0x00, 0x00)


P= 'E' (0x45) 卡机内无卡

4byte 卡序列号用十六进制传送: 如 "C6B272AE"

例: 上传的通讯包为: 0x02 0x00 0x06 0x35 0x31 0xC6 0xB2 0x72 0xAE 0x03 BCC

9.1.3 验证扇区操作密码: 对指定扇区指定 Key_A 或 Key_B 的密码来验证操作密码。

9.1.3.1 验证 Key_A 密码:

	SPECIFICATION		Model No.	CRT-310 读卡器
			Date	2007/4/1
	通讯协议		Ver.	3.0
			Page	14/46

HOST 发送:

0x02	0x00	0x09	0x35	0x32	扇区号	6 byte hex 密码	0x03	bcc
------	------	------	------	------	-----	---------------	------	-----

READER 操作返回:

0x02	0x00	0x04	0x35	0x32	扇区号	操作状态字 P	0x03	bcc
------	------	------	------	------	-----	---------	------	-----

操作状态字 P= 'Y' (0x59) 下载密码成功
P= '0' (0X30) 寻不到射频卡
P= '3' (0X33) 密码错误
P= 'E' (0x45) 卡机内无卡
P= 'W' (0x57) 卡不在允许操作的位置上。

9.1.3.2 验证 Key_B 密码:

HOST 发送:

0x02	0x00	0x09	0x35	0x39	扇区号	6 byte hex 密码	0x03	bcc
------	------	------	------	------	-----	---------------	------	-----

READER 操作返回:

0x02	0x00	0x04	0x35	0x39	扇区号	操作状态字 P	0x03	bcc
------	------	------	------	------	-----	---------	------	-----

操作状态字 P= 'Y' (0x59) 验证密码成功
P= '0' (0X30) 寻不到射频卡
P= '3' (0X33) 密码错误
P= 'E' (0x45) 卡机内无卡
P= 'W' (0x57) 卡不在允许操作的位置上。

注: 扇区号= 0x00 ~0x28 (其中 S50 卡片扇区号是 0x00 ~0x0F, S70 卡片扇区号是 0x00 ~0x28)

块号= 0x00 ~0x0F (其中 S50 卡片每个扇区有 4 个地块, 块号分别是 0x00 0x01 0x02 0x03, S70 卡片第 0-31

扇区中每一扇区有 4 个块, 块号分别是 0x00 0x01 0x02 0x03, 第 32-39 扇区每一扇区有 16 个块, 块号分别是 0x00~0x0F)

要对扇区块数据进行读、写、值操作必须验证该扇区密码成功后才能进行。

9.1.4 读扇区块数据

HOST 发送:

0x02	0x00	0x04	0x35	0x33	扇区号	块号	0x03	BCC
------	------	------	------	------	-----	----	------	-----

当卡片为 S50 时, 扇区号= 0x00~0x0F (S50 卡有 16 个扇区)

当卡片为 S70 时, 扇区号= 0x00~0x28 (S70 卡有 40 个扇区)

块号= 0x00 0x01 0x02 0x03 (S50 卡片块号, S70 卡片的块号=0x00~0x0F)

READER 读数据块操作成功返回: P= 'Y' (0x59)


0x02	0x00	0x15	0x35	0x33	扇区号	块号	操作状态字 P	16 byte hex 数据	0x03	BCC
------	------	------	------	------	-----	----	---------	----------------	------	-----

读扇区块数据成功, 并上传 16BYTE 读出的数据

READER 读扇区块操作错误返回:

0x02	0x00	0x05	0x35	0x33	扇区号	块号	操作状态字 P	0x03	BCC
------	------	------	------	------	-----	----	---------	------	-----

操作状态字 P= '0' (0X30) 寻不到 RF 卡
P= '1' (0X31) 操作扇区号错 (不是验证密码后的扇区)

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	15/46

P= '2' (0X32) 操作的卡序列号错

P= '3' (0X33) 密码验证错

P= '4' (0X34) 读数据错

P= 'E' (0x45) 卡机内无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

注： 扇区号= 0x00 ~0x28 （其中 S50 卡片扇区号是 0x00~0x0F， S70 卡片扇区号是 0x00~0x28）

块号= 0x00 ~0x0F （其中 S50 卡片每个扇区有 4 个地块，块号分别是 0x00 0x01 0x02 0x03， S70 卡片第 0-31 扇区中每一扇区有 4 个块，块号分别是 0x00 0x01 0x02 0x03， 第 32-39 扇区每一扇区有 16 个块，块号分别是 0x00~0x0F）

9.1.5 写扇区块数据

HOST 发送：

0x02	0x00	0x14	0x35	0x34	扇区号	块号	16 byte hex 数据	0x03	BCC
------	------	------	------	------	-----	----	----------------	------	-----

READER 写数据块操作成功返回：

0x02	0x00	0x15	0x35	0x34	扇区号	块号	操作状态字 P	16 byte hex 数据	0x03	BCC
------	------	------	------	------	-----	----	---------	----------------	------	-----

操作状态字：P= 'Y' (0x59)

写扇区块数据成功, 并上传 16BYTE 成功写入后再读出的数据

READER 写扇区块操作错误返回：

0x02	0x00	0x05	0x35	0x33	扇区号	块号	操作状态字 P	0x03	BCC
------	------	------	------	------	-----	----	---------	------	-----

操作状态字 P= '0' (0X30) 寻不到 RF 卡

P= '1' (0X31) 操作扇区号错（不是验证密码后的扇区）

P= '2' (0X32) 操作的卡序列号错

P= '3' (0X33) 密码验证错

P= '4' (0X34) 校验写入块数据错

P= 'E' (0x45) 卡机内无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

注： 扇区号= 0x00~0x28 （其中 S50 卡片扇区号是 0x00~0x0F， S70 卡片扇区号是 0x00~0x28）


块号= 0x00~0x0F （其中 S50 卡片每个扇区有 4 个地块，块号分别是 0x00 0x01 0x02 0x03， S70 卡片第 0-31 扇区中每一扇区有 4 个块，块号分别是 0x00 0x01 0x02 0x03， 第 32-39 扇区每一扇区有 16 个块，块号分别是 0x00~0x0F）

S50, S70 第 0-31 扇区中每个扇区的第 0X03 块, S70 第 32-40 扇区中第 0X0F 块是 KEYA、控制字、KEYB 的存储区域，对其进行写操作可能会遭成卡片锁死报废，需要谨慎操作，详见飞利浦 M1 卡片技术资料。

9.1.6 更改密码：执行该命令只能对 KEYA 的密码更改操作，并对 KEYB 密码的改写成：“0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF”同时控制字写成：“0xFF, 0x07, 0x80, 0x69” (卡片出厂的默认值)。

HOST 发送：

0x02	0x00	0x09	0x35	0x35	扇区号	6 byte hex 密码	0x03	bcc
------	------	------	------	------	-----	---------------	------	-----

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	16/46

扇区号= 0x00~0x28 （其中 S50 卡片扇区号是 0x00~0x0F，S70 卡片扇区号是 0x00 ~0x28）

READER 返回:

0x02	0x00	0x04	0x35	0x35	扇区号	操作状态字 P	0x03	bcc
------	------	------	------	------	-----	---------	------	-----

操作状态字 P= ‘Y’ (0x59) 更改密码成功
P= ‘0’ (0x30) 寻不到 RF 卡
P= ‘1’ (0x31) 操作扇区号错（不是验证密码后的扇区）
P= ‘2’ (0x32) 操作的卡序列号错
P= ‘3’ (0x33) 密码验证错
P= ‘E’ (0x45) 卡机内无卡
P= ‘W’ (0x57) 卡不在允许操作的位置上。

要完全对扇区操作密码 (KeyA 或 KeyB) 和扇区存取控制字修改, 在验证操作密码成功后对每扇区的块 3 进行写扇区块数据命令操作来完成。其格式如下 (详见飞利浦 M1 卡片技术资料):

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
6 byte KeyA 密码字节						4 byte 扇区存取控制字				6 byte KeyB 密码字节					

9.1.7 增值操作

HOST 发送:

0x02	0x00	0x08	0x35	0x37	扇区号	块号	4 byte hex 数据	0x03	BCC
------	------	------	------	------	-----	----	---------------	------	-----

4 byte hex 数据为指定的扇区的指字块的值要增加的值 (低字节在前高字节在后)。如第 5 扇区块 0 要增加 0x10, 发送的

4 byte hex 数据为: “0x10, 0x00, 0x00, 0x00”

READER 返回:

0x02	0x00	0x05	0x35	0x37	扇区号	块号	操作状态字 P	0x03	BCC
------	------	------	------	------	-----	----	---------	------	-----

操作状态字 P= ‘0’ (0x30) 寻不到 RF 卡
P= ‘1’ (0x31) 操作扇区号错（不是验证密码后的扇区）
P= ‘2’ (0x32) 操作的卡序列号错
P= ‘3’ (0x33) 密码验证错
P= ‘4’ (0x34) 块数据格式错误（该块存储数据没有写成值数据形式）
P= ‘5’ (0x35) 增值溢出
P= ‘E’ (0x45) 卡机内无卡
P= ‘Y’ (0x59) 操作成功
P= ‘W’ (0x57) 卡不在允许操作的位置上。

扇区号= 0x00~0x28 （其中 S50 卡片扇区号是 0x00 ~0x0F，


S70 卡片扇区号是 0x00 ~0x28）

块号= 0x00 ~0x0E （其中 S50 卡片块号范围是 0x00 0x01 0x02，

S70 卡片第 0-31 扇区块号范是 0x00 0x01 0x02，

第 32-39 扇区块号范围是 0x00 ~0x0E）

每一扇区的最后一块不能进行增减值操作。

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	17/46

9.1.8 减值操作

HOST 发送:

0x02	0x00	0x08	0x35	0x38	扇区号	块号	4 byte hex 数据	0x03	BCC
------	------	------	------	------	-----	----	---------------	------	-----

4 byte hex 数据为指定的扇区的指字块的值要减的值（低字节在前高字节在后）。不允许为 0 值，否则操作不成功。

READER 返回:

0x02	0x00	0x05	0x35	0x38	扇区号	块号	操作状态字 P	0x03	BCC
------	------	------	------	------	-----	----	---------	------	-----

操作状态字	P= '0' (0X30)	寻不到 RF 卡
	P= '1' (0X31)	操作扇区号错（不是验证密码后的扇区）
	P= '2' (0X32)	操作的卡序列号错
	P= '3' (0X33)	密码验证错
	P= '4' (0X34)	块数据格式错误（该块存储数据没有写成值数据形式）
	P= '5' (0X35)	减值溢出
	P= 'E' (0x45)	卡机内无卡
	P= 'Y' (0x59)	操作成功
	P= 'W' (0x57)	卡不在允许操作的位置上。

扇区号= 0x00 ~0x28 （其中 S50 卡片扇区号是 0x00 0x01 0x020x0F, S70 卡片扇区号是 0x00 0x01 0x020x28）

块号= 0x00 ~0x0E （其中 S50 卡片块号范围是 0x00 0x01 0x02, S70 卡片第 0-31 扇区块号范是 0x00 0x01 0x02, 第 32-39 扇区块号范围是 0x00 ~0x0E）,每一扇区的最后一块不能进行增减值操作。

9.1.9 初始化值: 用写扇区块数据命令来执行, 按 MIFARE 值段数据格式进入写入 16 byte 数据, 其格式如下:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Value				/Value				Value				Adr	/Adr	Adr	/Adr

Value: 要初始化 4 byte 值, 注值的低字节在前, 高字节在后

/Value: 要初始化 4 byte 值取反

Adr: 所要初始化值的块地址:

Adr= 扇区号 X 4 + 块号 (S50 卡片第 0-15 扇区, S70 卡片第 0-31 扇区块值操作地址计算)

Adr= (扇区号 - 32) X 16 + 128 + 块号 (S70 卡片第 32-39 扇区块值操作地址计算)

/Adr: 所要初始化值的块地址的取反

每一扇区的最后一块不能进行初始化值操作。


如: 将第 5 扇区块 0 初始化值为 10, 所要写入 16 byte 扇区块数据为:

“ 0x0A, 0x00, 0x00, 0x00, 0xF0, 0xFF, 0xFF, 0xFF, 0x0A, 0x00, 0x00, 0x00, 0x14, 0xEB, 0x14, 0xEB ”

S70 卡第 39 扇区块 0 初始化值为 10, 所要写入 16 byte 扇区块数据为:


“ 0x0A, 0x00, 0x00, 0x00, 0xF0, 0xFF, 0xFF, 0xFF, 0x0A, 0x00, 0x00, 0x00, 0xF0, 0x0F, 0xF0, 0x0F ”

9.1.10 读值: 用读扇区块数据命令执行, 对返回 16 byte 数据格式要校验是 MIFARE 卡值数据格式, 校验是 MIFARE 卡值数据格式作读值处理, 否则应报读值错误（数据格式错）。

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	18/46

注：在进行值操作时，S50，S70 第 0-31 扇区中每个扇区的第 3 块，S70 第 32-39 扇区中第 15 块是 KEYA、控制字、KEYB 的存储区域，是不能作值段数据存贮。初始化值，增值，减值，读值时应注意操作扇区块地址范围。

CREATOR

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	19/46

9.2. 24CXX 系列存贮卡操作：（24C01、24C02、24C04、24C08、24C16、24C32、24C64）

9.2.1 设置卡类型

HOST 发送：

0x02	0x00	0x03	0x36	0x30	卡类型 N	0x03	BCC
N=0x30	设置卡为 24C01	128BYTE	ADR=0x0000—0x007F				
N=0x31	设置卡为 24C02	256BYTE	ADR=0x0000—0x00FF				
N=0x32	设置卡为 24C04	512BYTE	ADR=0x0000—0x01FF				
N=0x33	设置卡为 24C08	1K BYTE	ADR=0x0000—0x03FF				
N=0x34	设置卡为 24C16	2K BYTE	ADR=0x0000—0x07FF				
N=0x35	设置卡为 24C32	4K BYTE	ADR=0x0000—0x0FFF				
N=0x36	设置卡为 24C64	8K BYTE	ADR=0x0000—0x1FFF				

Reader 返回：

0x02	0x00	0x04	0x36	0x30	卡类型 N	操作状态字 P	0x03	BCC
操作状态字	P= 'N' (0x4E)	设置卡不成功						
	P= 'Y' (0x59)	设置卡成功						
	P= 'E' (0x45)	卡机无卡						
	P= 'W' (0x57)	卡不在允许操作的位置上。						

9.2.2 读卡

HOST 发送：

0x02	0x00	0x06	0x36	0x31	卡类型 N	操作首地址 2byte	操作长度 L	0x03	BCC
------	------	------	------	------	-------	-------------	--------	------	-----

其中操作长度 L=0x01—0x80，最小长度为 1 BYTE，最大长度为 128 BYTE

操作首地址 2BYTE：有效地址由卡片的容量来决定。

Reader 返回：

读卡成功返回： P= 'Y' (0x59)


0x02	通讯包长度 Length (2 byte)	0x36	0x31	卡类型 N	操作状态字 P	操作首地址 2byte	操作 长度 L	读卡数据 n byte	0x03	BCC
------	--------------------------	------	------	----------	------------	----------------	------------	----------------	------	-----

通讯包长度 Length= 7 + 操作长度 L

读卡不成功返回：

Reader 读卡不成功返回：

0x02	0x00	0x04	0x36	0x31	卡类型 N	操作状态字 P	0x03	BCC
操作状态字	P= 'N' (0x4E)	读卡不成功						
	P= 'E' (0x45)	卡机无卡						
	P= 'W' (0x57)	卡不在允许操作的位置上。						

	SPECIFICATION		Model No.	CRT-310 读卡器
			Date	2007/4/1
	通讯协议		Ver.	3.0
			Page	20/46

9.2.3 写卡

9.2.3.1 不带校验写卡

HOST 发送:

0x02	通讯包长度 Length(2 byte)	0x36	0x32	卡类型 N	操作首地址 2byte	操作长度 L	写卡数据 n byte	0x03	BCC
------	-------------------------	------	------	-------	----------------	--------	-------------	------	-----

通讯包长度 Length= 6 + 操作长度 L

其中操作长度 L=0X01—0X80, 最小长度为 1 BYTE, 最大长度为 128 BYTE

Reader 返回:

0x02	0x00	0x04	0x36	0x32	卡类型 N	操作状态字 P	0x03	BCC
------	------	------	------	------	-------	---------	------	-----

操作状态字 P= 'Y' (0x59) 写卡成功

P= 'N' (0x4E) 写卡不成功

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

9.2.3.2 带校验写卡

HOST 发送:

0x02	通讯包长度 Length(2 byte)	0x36	0x33	卡类型 N	操作首地址 2byte	操作长度 L	写卡数据 n byte	0x03	BCC
------	-------------------------	------	------	-------	----------------	--------	-------------	------	-----

注: 通讯包长度 Length= 6 + 操作长度 L

其中操作长度 L=0X01—0X80 , 最小长度为 1 BYTE, 最大长度为 128 BYTE

Reader 返回:

写卡成功带校验返回

0x02	通讯包长度 Length (2 byte)	0x36	0x33	卡类型 N	操作状态 字 P	操作首地址 2byte	操作长 度 L	读出写入卡数据 n byte	0x03	BCC
------	-----------------------------	------	------	----------	-------------	----------------	------------	-------------------	------	-----

通讯包长度 Length= 7 + 操作长度 L

写卡校验不成功返回


Reader 返回:

0x02	0x00	0x04	0x36	0x33	卡类型 N	操作状态字 P	0x03	BCC
------	------	------	------	------	-------	---------	------	-----

操作状态字 P= 'N' (0x4E) 写卡不成功

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	21/46

9.3. 接触式 CPU 卡操作

9.3.1 CPU 卡冷复位

HOST 发送:

0x02	0x00	0x02	0x37	0x30	0x03	BCC
------	------	------	------	------	------	-----

Reader 操作成功返回: T=0 CPU 卡复位成功返回操作状态字 P= 'Y' (0x59)

0x02	通讯包长度 2 byte	0x37	0x30	操作状态字 P	复位数据包长度 2 byte	复位数据 n byte	0x03	BCC
------	--------------	------	------	---------	----------------	-------------	------	-----

通讯包长度=5+ 复位数据长度 n

Reader 操作成功返回: T=1 CPU 卡复位成功返回操作状态字 P= 'Z' (0x5A)

0x02	通讯包长度 2 byte	0x37	0x30	操作状态字 P	复位数据包长度 2 byte	复位数据 n byte	0x03	BCC
------	--------------	------	------	---------	----------------	-------------	------	-----

通讯包长度=5+ 复位数据长度 n

Reader 操作失败返回:

0x02	0x00	0x03	0x37	0x30	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'N' (0x4E) 复位不成功

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

9.3.2 CPU 卡热复位

HOST 发送:

0x02	0x00	0x02	0x37	0x2F	0x03	BCC
------	------	------	------	------	------	-----

Reader 操作成功返回: T=0 CPU 卡复位成功返回操作状态字 P= 'Y' (0x59)

0x02	通讯包长度 2 byte	0x37	0x2F	操作状态字 P	复位数据包长度 2 byte	复位数据 n byte	0x03	BCC
------	--------------	------	------	---------	----------------	-------------	------	-----

通讯包长度=5+ 复位数据长度 n

Reader 操作成功返回: T=1 CPU 卡复位成功返回操作状态字 P= 'Z' (0x5A)

0x02	通讯包长度 2 byte	0x37	0x2F	操作状态字 P	复位数据包长度 2 byte	复位数据 n byte	0x03	BCC
------	--------------	------	------	---------	----------------	-------------	------	-----

通讯包长度=5+ 复位数据长度 n

Reader 操作失败返回:

0x02	0x00	0x03	0x37	0x2F	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'N' (0x4E) 复位不成功

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

9.3.3 T=0 CPU 卡 C-APDU 命令操作


HOST 发送:

0x02	通讯包长度 2 byte	0x37	0x31	C-APDU 包长度 2 byte	C-APDU 包 n byte	0x03	BCC
------	--------------	------	------	-------------------	-----------------	------	-----

通讯包长度=4+ C-APDU 包长度 n (n 最大值为 262byte)

Reader 操作成功返回: 操作状态字 P= 'Y' (0x59)

0x02	通讯包长度 byte	0x37	0x31	操作状态字 P	C-APDU 操作返回包长度 2 byte	C-APDU 操作返回包 n byte	0x03	BCC
------	---------------	------	------	------------	--------------------------	------------------------	------	-----

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	22/46

通讯包长度=5+ C-APDU 返回包长度 n (n 最大值 257byte)

Reader 操作失败返回:

0x02	0x00	0x03	0x37	0x31	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'N' (0x4E) 操作不成功

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

对 CPU 卡 C-APDU 操作时应根据 CPU 卡复位返回 T=0, T=1 时卡类型进行选择 T=0, T=1 的 C-APDU 命令来操作.

9.3.4 T=1 CPU 卡 C-APDU 命令操作

HOST 发送:

0x02	通讯包长度 2 byte	0x37	0x32	C-APDU 包长度 2 byte	C-APDU 包 n byte	0x03	BCC
------	--------------	------	------	-------------------	-----------------	------	-----

通讯包长度=4+ C-APDU 包长度 n (n 最大值为 262byte)

Reader 操作成功返回: 操作状态字 P= 'Y' (0x59)

0x02	通讯包长度 2 byte	0x37	0x32	操作状态字 P	C-APDU 操作返回包 长度 2 byte	C-APDU 操作 返回包 n byte	0x03	BCC
------	--------------	------	------	---------	---------------------------	-------------------------	------	-----

通讯包长度=5+ C-APDU 返回包长度 n (n 最大值 257byte)

Reader 操作失败返回:

0x02	0x00	0x03	0x37	0x32	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----


操作状态字 P= 'N' (0x4E) 操作不成功

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

对 CPU 卡 C-APDU 操作时应根据 CPU 卡复位返回 T=0, T=1 时卡类型进行选择 T=1 的 C-APDU 命令来操作.

接收链接 C-APDU 包: (当返回 C-APDU 包的 DATA 长度超出 256 时,

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	23/46

9.4. SLE4442 卡操作

9.4.1 SLE4442 CARD 复位操作

HOST 发送:

0x02	0x00	0x02	0x38	0x30	0x03	BCC
------	------	------	------	------	------	-----

Reader 操作成功返回: 操作状态字 P= 'Y' (0x59)

0x02	0x00	0x07	0x38	0x30	操作状态字 P	复位数据包 4 byte	0x03	BCC
------	------	------	------	------	---------	--------------	------	-----

Reader 操作失败返回:

0x02	0x00	0x03	0x38	0x30	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'N' (0x4E) 复位不成功

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

9.4.2 读 4442 主存贮区

HOST 发送:

0x02	0x00	0x04	0x38	0x31	读取首地址 ADR 1 byte	读取长度 L 1 byte	0x03	BCC
------	------	------	------	------	------------------	---------------	------	-----

ADR=0x00-0xFF

L =0x01-0x80

其中操作长度 L=0x01-0x80 , 最小长度为 1 BYTE, 最大长度为 128 BYTE

4442 主存贮区只有 256 byte 使用时应注意操作地址和长度在它允许的范围

Reader 操作成功返回: 操作状态字 P= 'Y' (0x59)

0x02	通讯长度 2 byte	0x38	0x31	操作状态字 P	读取首地址 ADR	读取长度 L	读取数据 L byte	0x03	BCC
------	-------------	------	------	---------	-----------	--------	-------------	------	-----

通讯长度=5+ 读取长度 L

Reader 操作失败返回:

0x02	0x00	0x05	0x38	0x31	操作状态字 P	读取首地址 ADR	读取长度 L	0x03	BCC
------	------	------	------	------	---------	-----------	--------	------	-----

P= 'N' (0x4E) 读不成功

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

9.4.3 读 4442 保护位区

HOST 发送:

0x02	0x00	0x02	0x38	0x32	0x03	BCC
------	------	------	------	------	------	-----

Reader 操作成功返回: 操作状态字 P= 'Y' (0x59)


0x02	0x00	0x23	0x38	0x32	操作状态字 P	32 byte 保护位状态字	0x03	BCC
------	------	------	------	------	---------	----------------	------	-----

保护位状态字每一字节对应一个主存贮区每一单元的写保护状态, 地址从低到高排列

保护位状态字=0x00 表示该字节写保护有效不能写该单元

保护位状态字=0x01 表示该字节写保护无效可以写该单元

读保护位区将 4442 卡 32 Byte 保护位状态一次全读出。

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	24/46

Reader 操作失败返回:

0x02	0x00	0x03	0x38	0x32	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'N' (0x4E) 读不成功

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

9.4.4 读 4442 PSC 区

HOST 发送:

0x02	0x00	0x02	0x38	0x33	0x03	BCC
------	------	------	------	------	------	-----

Reader 操作成功返回: 操作状态字 P= 'Y' (0x59)

0x02	0x00	0x07	0x38	0x33	操作状态字 P	安全区数据包 4 byte	0x03	BCC
------	------	------	------	------	---------	---------------	------	-----

安全区数据包第一字节为: 密码错误计数器数据

安全区数据包第二字节为: 密码数据 1

安全区数据包第三字节为: 密码数据 2

安全区数据包第四字节为: 密码数据 3

密码错误计数器=0x07 (验证密码错误错为 0), 0x06 (错误数为 1), 0x04 (错误数为 2), 0x00 (错误码数为 1, 卡已报废)

Reader 操作失败返回:

0x02	0x00	0x03	0x38	0x33	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'N' (0x4E) 读不成功

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

9.4.5 验证密码

HOST 发送:

0x02	0x00	0x05	0x38	0x34	密码数据 3 byte	0x03	BCC
------	------	------	------	------	-------------	------	-----

Reader 操作返回:

0x02	0x00	0x03	0x38	0x34	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'Y' (0x59) 验证密码正确

P= 'N' (0x4E) 验证密码错误

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

9.4.6 写主存贮区: (00H-FFH)


HOST 发送:

0x02	通讯长度 2 byte	0x38	0x35	写首地址 ADR(1byte)	写长度 L	写数据 L byte	0x03	BCC
------	-------------	------	------	-----------------	-------	------------	------	-----

通讯长度= 4+ 写长度 L

其中操作长度 L=0x01—0x80, 最小长度为 1 Byte, 最大长度为 128 Byte.

Reader 操作返回:

	SPECIFICATION				Model No.	CRT-310 读卡器
					Date	2007/4/1
	通讯协议				Ver.	3.0
					Page	25/46

0x02	0x00	0x05	0x38	0x35	操作状态字 P	写首地址 ADR	写长度 L	0x03	BCC
------	------	------	------	------	---------	----------	-------	------	-----

操作状态字 P= 'Y' (0x59) 写入成功
 P= 'N' (0x4E) 写入错误
 P= 'E' (0x45) 卡机无卡
 P= 'W' (0x57) 卡不在允许操作的位置上。

9.4.7 写保护区：(ADR: 0x00-0x1f 共 32 BYTE 有写保护位功能单元进行指字起始地址，指定长度的进行写保护)

HOST 发送：

0x02	通讯包长度 L	0x38	0x36	Adr	len	Len byte 写保护数据	0x03	BCC
------	---------	------	------	-----	-----	----------------	------	-----

说明： 通讯包长度 L= 4 + len

Adr : 要进行写保护的字节首地址 ADR:0x00——0x1F

Len : 要进行写保护的字节长度 0x01——0x20

Sbyte : 要进行写保护的单元状态字节包

Len byte 写保护数据：是要进行写保护的数据。当写保护的数据与原存贮单元的数据相同时，执行写保护才能成功，要写保护的数据与原数据不相同，进行写保护位将操作失败。

更改写保护区：只能对 00H-31H 这些存贮单元更改，一旦写保护有效将永久有效不能取消写保护。进行操作时应确定 Adr, len 在规定的范围。可进行单字节进行写保护。

Reader 操作返回：

0x02	0x00	0x03	0x38	0x36	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'Y' (0x59) 写入成功
 P= 'N' (0x4E) 写入错误
 P= 'E' (0x45) 卡机无卡
 P= 'W' (0x57) 卡不在允许操作的位置上。

9.4.8 更改密码


HOST 发送：

0x02	0x00	0x05	0x38	0x37	密码数据 3 byte	0x03	BCC
------	------	------	------	------	----------------	------	-----

Reader 操作返回：

0x02	0x00	0x03	0x38	0x37	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'Y' (0x59) 更改密码成功
 P= 'N' (0x4E) 更改密码失败
 P= 'E' (0x45) 卡机无卡
 P= 'W' (0x57) 卡不在允许操作的位置上

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	26/46

9.5. SLE4428 卡操作

9.5.1 复位

HOST 发送:

0x02	0x00	0x02	0x39	0x30	0x03	BCC
------	------	------	------	------	------	-----

Reader 操作成功返回: 操作状态字 P= 'Y' (0x59)

0x02	0x00	0x07	0x39	0x30	操作状态字 P	复位数据包 4 byte	0x03	BCC
------	------	------	------	------	---------	--------------	------	-----

Reader 操作失败返回:

0x02	0x00	0x03	0x39	0x30	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'N' (0x4E) 复位不成功

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

9.5.2 读 4428 存储区: (不带保护位读)

HOST 发送:

0x02	0x00	0x05	0x39	0x31	读取首地址 ADR 2 byte	读取长度 L 1 byte	0x03	BCC
------	------	------	------	------	------------------	---------------	------	-----

ADR=0000-03FF

L =0x01—0x80

其中操作长度 L=0x01—0x80 , 最小长度为 1 BYTE, 最大长度为 128 BYTE

4428 存储区只有 1K byte 使用时应注意操作地址和长度在它允许的范围

Reader 操作成功返回: 操作状态字 P= 'Y' (0x59)

0x02	通讯长度 2 byte	0x39	0x31	操作状态字 P	读取首地址 2byte	读取长度 L 1byte	读取数据 L byte	0x03	BCC
------	----------------	------	------	---------	-------------	--------------	-------------	------	-----

通讯长度=6+ 读取长度 L

Reader 操作失败返回:

0x02	0x00	0x06	0x39	0x31	操作状态字 P	读取首地址 2byte	读取长度 L 1byte	0x03	BCC
------	------	------	------	------	---------	-------------	--------------	------	-----

操作状态字 P= 'N' (0x4E) 读卡不成功

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

9.5.3 读 4428 保护位

HOST 发送:

0x02	0x00	0x05	0x39	0x32	读取首地址 ADR 2 byte	读取长度 L 1 byte	0x03	BCC
------	------	------	------	------	------------------	---------------	------	-----

ADR=0000-03FF

L =0x01—0x80


其中操作长度 L=0x01—0x80 , 最小长度为 1 BYTE, 最大长度为 128 BYTE

4428 存储区只有 1K byte 使用时应注意操作地址和长度在它允许的范围

保护位状态字每一字节对应一个主存储区每一单元的写保护状态 地址从低到高排列。

保护位状态字=0x00 表示该字节写保护有效不能写该字节

保护位状态字=0x01 表示该字节写保护无效可以写该字节

	SPECIFICATION		Model No.	CRT-310 读卡器
			Date	2007/4/1
	通讯协议		Ver.	3.0
			Page	27/46

Reader 操作成功返回： 操作状态字 P= 'Y' (0x59)

0x02	通讯长度	0x39	0x32	操作状态字 P	读取首地址 2byte	读取长度 L 1byte	保护位数 据 L byte	0x03	BCC
	2 byte								

通讯长度=6+ 读取长度 L

Reader 操作失败返回：

0x02	0x00	0x06	0x39	0x32	操作状态字 P	读取首地址 2byte	读取长度 L 1byte	0x03	BCC
------	------	------	------	------	---------	-------------	--------------	------	-----

操作状态字 P= 'N' (0x4E) 读不成功

P= 'E' (0x45) 卡机无卡.

P= 'W' (0x57) 卡不在允许操作的位置上。

9.5.4 验证密码

HOST 发送：

0x02	0x00	0x04	0x39	0x33	密码数据 2 byte	0x03	BCC
------	------	------	------	------	-------------	------	-----

Reader 操作返回：

0x02	0x00	0x03	0x39	0x33	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'Y' (0x59) 验证密码正确

P= 'N' (0x4E) 难证密码错误

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

9.5.5 写数据（不带写保护位写）

HOST 发送：

0x02	通讯长度 2 byte	0x39	0x34	写首地址 ADR 2byte	写长度 L 1byte	写数据 L byte	0x03	BCC
------	-------------	------	------	----------------	-------------	------------	------	-----

通讯长度= 5+ 写长度 L

地址范围=0x0000—0x03FF;

其中操作长度 L=0x01—0x80，最小长度为 1 BYTE，最大长度为 128 BYTE

应注意：4428 卡的最后 3 个存储位单元 (0x03FD, 0x3FE, 0x03FF) 是密码错误计数器，在写数据时操作中不要輕易操作防止造成卡报废

Reader 操作返回：

0x02	0x00	0x06	0x39	0x34	操作状态字 P	写首地址 ADR 2byte	写长度 L 1byte	0x03	BCC
------	------	------	------	------	---------	----------------	-------------	------	-----

操作状态字 P= 'Y' (0x59) 写入成功

P= 'N' (0x4E) 写入错误

P= 'E' (0x45) 卡机无卡


P= 'W' (0x57) 卡不在允许操作的位置上。

9.5.6 写数据（带写保护位写）

HOST 发送：

0x02	通讯长度 2 byte	0x39	0x35	写首地址 ADR 2byte	写长度 L 1byte	写数据 L byte	0x03	BCC
------	-------------	------	------	----------------	-------------	------------	------	-----

通讯长度= 5+ 写长度 L

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	28/46

地址范围=0x0000—0x03FF（整张卡的任何一个单元均可进行写保护）

操作长度 L=0x01—0x80，最小长度为 1 BYTE，最大长度为 128 BYTE

写入数据 L byte：是要进行写保护的数据。

应注意：一旦进行带写保护位写数据后的存贮单元将不能再进行写操作。

4428 卡的最后 3 个存贮位单元（0x03FD, 0x03FE, 0x03FF）分别是密码错误计数器、密码字节 1，密码字节 2。在写数据时操作中不要輕易操作防止造成卡报废。一旦进行写保护位后的这三个单元将不能再进行写操作。

Reader 操作返回：

0x02	0x00	0x06	0x39	0x35	操作状态字 P	写首地址 ADR 2byte	写长度 L 1byte	0x03	BCC
------	------	------	------	------	---------	----------------	-------------	------	-----

操作状态字 P= 'Y' (0x59) 写入成功

P= 'N' (0x4E) 写入错误

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

9.5.7 更改密码

HOST 发送：

0x02	0x00	0x06	0x39	0x36	原密码数据 2 byte	新密码数据 2 byte	0x03	BCC
------	------	------	------	------	--------------	--------------	------	-----

Reader 操作返回：


0x02	0x00	0x03	0x39	0x36	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'Y' (0x59) 更改密码成功

P= 'N' (0x4E) 更改密码失败

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

	SPECIFICATION		Model No.	CRT-310 读卡器
			Date	2007/4/1
	通讯协议		Ver.	3.0
			Page	29/46

9.6. AT88SC102 卡操作

9.6.1 复位

HOST 发送:

0x02	0x00	0x02	0x3A	0x30	0x03	BCC
------	------	------	------	------	------	-----

Reader 操作返回:

0x02	0x00	0x03	0x3A	0x30	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'Y' (0x59) 复位成功
P= 'N' (0x4E) 复位不成功
P= 'E' (0x45) 卡机无卡
P= 'W' (0x57) 不在允许操作的位置上。

9.6.2 验证主密码: 主密码(2byte), 擦除密码一(6byte), 擦除密码二(4byte)

HOST 发送:

0x02	0x00	0x04	0x3A	0x31	密码数据包 2 byte	0x03	BCC
------	------	------	------	------	--------------	------	-----

Reader 操作返回:

0x02	0x00	0x04	0x3A	0x31	密码区号	操作状态字 P	0x03	BCC
------	------	------	------	------	------	---------	------	-----

操作状态字 P= 'Y' (0x59) 密码验证成功
P= 'N' (0x4E) 密码验证失败
P= 'E' (0x45) 卡机无卡
P= 'F' (0x46) 卡已报废 (密码验证失败超过允许次数后卡锁死报废)
P= 'W' (0x57) 卡不在允许操作的位置上。

在安全级别 1 模式下验证主密码后所有单元均可读出。

在安全级别 2 模式下验证主密码成功除密码存贮单元读不出外, 其余单元均可读出。

9.6.3 读存贮区 (应用区 1, 应用区 2, 控制区)

HOST 发送:

0x02	0x00	0x05	0x3A	0x32	区号	读应用区首地址 adr 1 byte	读应用区长度 len 1 byte	0x03	BCC
------	------	------	------	------	----	--------------------	-------------------	------	-----

注: 区号=0x30 控制区 (除应用区 1, 应用区 2 以外的单元为控制区)

=0x31 应用区 1 (64 byte 地址范围 0x16-0x55)

=0x32 应用区 2 (64 byte 地址范围 0x5C-0x9B)

Reader 操作成功返回: 操作状态字 P= 'Y' (0x59)


0x02	通讯长度 L 2 byte	0x3A	0x32	区号	操作状态字 P	读应用区首地址 adr 1 byte	读应用区长 度 len 1 byte	读数据 Len byte	0x03	BCC
------	------------------	------	------	----	---------	-----------------------	--------------------------	-----------------	------	-----

通讯长度 L=5+ 读应用区长度 len

Reader 操作失败返回:

0x02	0x00	0x04	0x3A	0x31	区号	操作状态字 P	0x03	BCC
------	------	------	------	------	----	---------	------	-----

操作状态字 P= 'N' (0x4E) 读不成功
P= 'E' (0x45) 卡机无卡

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	30/46

P= 'W' (0x57) 卡不在允许操作的位置上。

9.6.4 擦除存储区 (作写存卡准备, 要进行写入数据之前, 一定先要执行擦除操作才能正确写入)

9.6.4.1 安全模式 1 下擦除应用区

HOST 发送:

0x02	0x00	0x05	0x3A	0x33	区号 B	擦除存储区首地址 adr 1 byte	擦除存储区长度 len 1 byte	0x03	BCC
------	------	------	------	------	------	---------------------	--------------------	------	-----

区号 B= 0x30 安全模式 1 下擦除控制区

B= 0x31 安全模式 1 下擦除应用区 1

B= 0x32 安全模式 1 下擦除应用区 2

Reader 操作返回:

0x02	0x00	0x04	0x3A	0x33	区号	操作状态字 P	0x03	BCC
------	------	------	------	------	----	---------	------	-----

操作状态字 P= 'Y' (0x59) 擦除成功

P= 'N' (0x4E) 擦除失败

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上

9.6.4.2 安全模式二下擦除应用区一

HOST 发送:

0x02	0x00	0x09	0x3A	0x33	0x33	擦除密码数据包 6 byte	0x03	BCC
------	------	------	------	------	------	----------------	------	-----

Reader 操作返回:

0x02	0x00	0x04	0x3A	0x33	区号	操作状态字 P	0x03	BCC
------	------	------	------	------	----	---------	------	-----

操作状态字 P= 'Y' (0x59) 擦除成功

P= 'N' (0x4E) 擦除失败

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

9.6.4.3 安全模式二下擦除应用区二

HOST 发送:

0x02	0x00	0x08	0x3A	0x33	0x34	EC2	擦除密码数据包 4 byte	0x03	BCC
------	------	------	------	------	------	-----	----------------	------	-----

擦除熔丝状态操作字 EC2 = 0x30 擦除熔丝未熔断应用区二擦除

= 0x31 擦除熔丝已熔断应用区二擦除

Reader 操作返回:

0x02	0x00	0x04	0x3A	0x33	区号	操作状态字 P	0x03	BCC
------	------	------	------	------	----	---------	------	-----

操作状态字 P= 'Y' (0x59) 擦除成功

P= 'N' (0x4E) 擦除失败


P= 'E' (0x45) 卡机无卡

P= 'F' (0x46) 二区已报废, 只能读不能再进行擦写。

P= 'W' (0x57) 卡不在允许操作的位置上。

(EC2 熔丝未熔断超过允许擦除次数(128 次)后卡不能再擦写报废)

注: 在安全模式 2 下进行擦除应用一、二区操作时是分别输入一、二区的密码, 密码验证成功后将对该应用区整区进行

	SPECIFICATION		Model No.	CRT-310 读卡器
			Date	2007/4/1
	通讯协议		Ver.	3.0
			Page	31/46

擦除。

9.6.5 写存储区（应用区 1，应用区 2，控制区）

HOST 发送：

0x02	通讯长度	0x3A	0x34	区号	写存储区地址 adr	1	写存储区长度 len	写数据 Len	0x03	BCC
	L 2 byte				byte		1 byte	byte		

通讯长度 L=5+写数据长度 len

Reader 操作返回：

0x02	0x00	0x04	0x3A	0x34	区号	操作状态字 P	0x03	BCC
------	------	------	------	------	----	---------	------	-----

操作状态字

P= 'Y' (0x59) 写卡成功

P= 'N' (0x4E) 写卡不成功

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

注：在安全模式 1 下只要验证主密码后所有单元可进行擦除写入。控制区单元一些数据不能随意写入，以防更改到密码存储单元，造成密码被改写验证密码失败造成卡报废。

在安全模式 2 下只能擦除写入应用区，所有控制区单元将不能擦除写入。应用区只有验证主密码成功再验证擦除密码成功后才能进行写入。

9.6.6 修改密码：（控制区密码，应用区一密码，应用区二密码）

HOST 发送：

0x02	通讯长度 L 2 byte	0x3A	0x35	区号	新密码数据 Len	byte	0x03	BCC
------	---------------	------	------	----	-----------	------	------	-----

通讯长度 L=3+新密码数据长度 len

区号 =0x30 修改控制区密码 密码数据为 2 byte

=0x31 修改应用区一密码 密码数据为 6 byte

=0x32 修改应用区二密码 密码数据为 4 byte

Reader 操作返回：

0x02	0x00	0x04	0x3A	0x35	区号	操作状态字 P	0x03	BCC
------	------	------	------	------	----	---------	------	-----

操作状态字

P= 'Y' (0x59) 修改密码成功

P= 'N' (0x4E) 修改密码失败

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

注：修改密码只能在安全模式 1 下验证主密码后才能修改，进入安全模式 2 后不能再修改所有密码，只能验证。

9.6.7 个人化操作，使卡进入安全级别模式 2


HOST 发送：

0x02	0x00	0x03	0x3A	0x36	操作模式 F	0x03	BCC
------	------	------	------	------	--------	------	-----

操作模式 F=0x30 使卡模拟进入安全级别模式 2，可供测试，

F=0x31 使模拟进入安全级别模式 2 的卡恢复到安全级别模式 1。

F=0x32 使卡完全进入安全级别模式 2，一旦将卡操作成安全模式 2，

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	32/46

将无法再恢复到安模式 1。

Reader 操作返回：

0x02	0x00	0x04	0x3A	0x36	操作模式 F	操作状态字 P	0x03	BCC
------	------	------	------	------	--------	---------	------	-----

操作状态字 P= 'Y' (0x59) 个人化操作成功
 P= 'N' (0x4E) 个人化操作失败
 P= 'E' (0x45) 卡机无卡
 P= 'W' (0x57) 卡不在允许操作的位置上。

进入安全模式 2 前一定设定好应用区一，二的密码，应用区一第一字节 (0x16)

应用区二第一字节 (0x5C) 不能轻易修改，是控制这些区单元的读写使能。

进入安全模式 2 后要写这些应用区，卡进行擦除操作时是对这些应用区整块擦除，应注意

写入新数据前应先读出保存，以防数据丢失。同时这些应用区受熔丝计数器的控制。使熔丝计数器有效则写入 128 次后不能再写入。使其无效则写入次数为卡的最大有效操作数 (100, 000 次)。

9.6.8 二区擦除计数器操作字 EC2 设置成无效操作。

HOST 发送：

0x02	0x00	0x02	0x3A	0x37	0x03	BCC
------	------	------	------	------	------	-----

Reader 操作返回：


0x02	0x00	0x03	0x3A	0x37	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'Y' (0x59) 操作成功
 P= 'N' (0x4E) 操作失败
 P= 'E' (0x45) 卡机无卡
 P= 'W' (0x57) 卡不在允许操作的位置上。

注： 要使卡在安全模式 2 下应用区二擦除次数不受限则要在进入个人化操作前执行此操作。

否则在卡设置完成模式 2 后，卡默认应用区二在模式 2 下擦除次数受限有效(只能擦除 128 次)。若要取消应用二区擦写不受限，则无法取消二区擦除受限次数 (128 次)。

同样设置成卡在模式 2 下擦写次数不受限后不能再设置成擦写受限。同时用户也要对 EC2 操作状态保存，卡在模式 2 下应用时要擦写应用区二时 (验证应用区二的擦除密码) 应注意相应的参数。

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	33/46

9.7 AT88S1604 卡操作

9.7.1 复位

HOST 发送:

0x02	0x00	0x02	0x3B	0x30	0x03	BCC
------	------	------	------	------	------	-----

Reader 操作返回:

0x02	0x00	0x03	0x3B	0x30	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'Y' (0x59) 复位成功
 P= 'N' (0x4E) 复位不成功
 P= 'E' (0x45) 卡机无卡
 P= 'W' (0x57) 卡不在允许操作的位置上。

9.7.2 验证密码

HOST 发送:

0x02	0x00	0x05	0x3B	0x31	密码区号 1 byte	密码数据 2 byte	0x03	BCC
------	------	------	------	------	-------------	-------------	------	-----

Reader 操作返回:

0x02	0x00	0x04	0x3B	0x31	密码区号	操作状态字 P	0x03	BCC
------	------	------	------	------	------	---------	------	-----

操作状态字 P= 'Y' (0x59) 验证密码成功
 P= 'N' (0x4E) 验证密码失败
 P= 'F' (0x46) 卡已报废或应用块报废
 P= 'E' (0x45) 卡机无卡
 P= 'W' (0x57) 卡不在允许操作的位置上。

其中密码区号: = 0x30 验证主密码
 = 0x31 验证应用一区密码
 = 0x32 验证应用一区擦除密码
 = 0x33 验证应用二区密码
 = 0x34 验证应用二区擦除密码
 = 0x35 验证应用三区密码
 = 0x36 验证应用三区擦除密码
 = 0x37 验证应用四区密码
 = 0x38 验证应用四区擦除密码

9.7.3 读数据

HOST 发送:


0x02	0x00	0x06	0x3B	0x32	区号 1 byte	操作地址 2 byte	操作长度 1 byte	0x03	BCC
------	------	------	------	------	-----------	-------------	-------------	------	-----

Reader 操作成功返回: P= 'Y' (0x59)

0x02	通讯长度 L	0x3B	0x32	区号	操作状态字 P	操作地址 2 byte	操作长度 1 byte	数据 n byte	0x03	BCC
	2 byte									

通讯长度: L= 7 + n byte

Reader 操作失败返回:

	SPECIFICATION					Model No.	CRT-310 读卡器
						Date	2007/4/1
	通讯协议					Ver.	3.0
						Page	34/46

0x02	0x00	0x07	0x3B	0x32	区号	操作状态字 P	操作地址 2 byte	操作长度 1 byte	0x03	BCC
------	------	------	------	------	----	---------	-------------	-------------	------	-----

操作状态字 P= 'N' 读卡失败
 P= 'E' 卡机无卡
 P= 'W' (0x57) 卡不在允许操作的位置上。

操作地址范围: 0x000—0x7FF

操作长度范围: 0x01—0x80

区号: = 0x30 一区(0x020 — 0x21A)
 = 0x31 二区(0x21B — 0x420)
 = 0x32 三区(0x421 — 0x621)
 = 0x33 四区(0x622 — 0x7F5)
 = 0x34 其它区(除一, 二, 三, 区以外的区域)

9.7.4 擦数据

HOST 发送:

0x02	0x00	0x06	0x3B	0x33	区号 1 byte	操作地址 2 byte	操作长度 1 byte	0x03	BCC
------	------	------	------	------	-----------	-------------	-------------	------	-----

Reader 操作返回:

0x02	0x00	0x04	0x3B	0x33	区号	操作状态字 P	0x03	BCC
------	------	------	------	------	----	---------	------	-----

操作状态字 P= 'Y' (0x59) 擦除成功
 P= 'N' (0x4E) 擦除失败
 P= 'E' (0x45) 卡机无卡
 P= 'W' (0x57) 卡不在允许操作的位置上。

操作地址范围: 0x000—0x7FF

操作长度范围: 0x01—0x80

9.7.5 写数据

HOST 发送:

0x02	通讯长度 L 2 byte	0x3B	0x34	区号 1 byte	操作地址 2 byte	操作长度 1 byte	写数据 n byte	0x03	BCC
------	-----------------	------	------	-----------	-------------	-------------	------------	------	-----

通讯长度 L = 6 + n byte

Reader 操作返回:


0x02	0x00	0x04	0x3B	0x34	区号	操作状态字 P	0x03	BCC
------	------	------	------	------	----	---------	------	-----

操作状态字 P= 'Y' (0x59) 写数据成功
 P= 'N' (0x4E) 写数据失败
 P= 'E' (0x45) 卡机无卡
 P= 'W' (0x57) 卡不在允许操作的位置上。

操作地址范围: 0x000—0x7FF

操作长度范围: 0x01—0x80

区号: = 0x30 一区(0x020 --- 0x21A)
 = 0x31 二区(0x21B --- 0x420)
 = 0x32 三区(0x421 ---- 0x621)

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	35/46

= 0x33 四区(0x622 ---- 0x7F5)

= 0x34 其它区(除一, 二, 三, 区以外的区域)

9.7.6 模式 1 下修改密码

HOST 发送:

0x02	0x00	0x05	0x3B	0x35	密码类型号 1 byte	密码数据 2 byte	0x03	BCC
------	------	------	------	------	--------------	-------------	------	-----

Reader 操作返回:

0x02	0x00	0x04	0x3B	0x35	密码区号	操作状态字 P	0x03	BCC
------	------	------	------	------	------	---------	------	-----

操作状态字 P= 'Y' (0x59) 修改密码成功

P= 'N' (0x4E) 修改密码失败

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

其中: 密码类型号:

= 0x30 修改主密码

= 0x31 修改应用一区密码

= 0x32 修改应用一区擦除密码

= 0x33 修改应用二区密码

= 0x34 修改应用二区擦除密码

= 0x35 修改应用三区密码

= 0x36 修改应用三区擦除密码

= 0x37 修改应用四区密码

= 0x38 修改应用四区擦除密码

修改密码只能在安全模式 1 下修改, 安全模式 2 下只能验证不能修改任何密码。

9.7.7 个人化操作 (卡进入安全模式 2)

HOST 发送:

0x02	0x00	0x03	0x3B	0x36	操作号	0x03	BCC
------	------	------	------	------	-----	------	-----

操作号 = 0x30 软个人化操作 (模拟个人化操作使卡进入安全模式 2, 供测试)

= 0x31 退出软个人化操作

= 0x32 完全个人化操作不可再恢复

Reader 操作返回:


0x02	0x00	0x04	0x3B	0x36	操作号	操作状态字 P	0x03	BCC
------	------	------	------	------	-----	---------	------	-----

操作状态字 P= 'Y' (0x59) 操作成功

P= 'N' (0x4E) 操作失败

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	36/46

9.8. AT45D041 卡操作：2048 页，每页 264 byte

9.8.1 复位

HOST 发送：

0x02	0x00	0x02	0x3C	0x30	0x03	BCC
------	------	------	------	------	------	-----

Reader 操作返回：

0x02	0x00	0x03	0x3C	0x30	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'Y' (0x59) 复位成功
 P= 'N' (0x4E) 复位不成功
 P= 'E' (0x45) 卡机无卡
 P= 'W' (0x57) 卡不在允许操作的位置上。

9.8.2 读数据：只支持页读(264 byte)

HOST 发送：

0x02	0x00	0x04	0x3C	0x31	页地址 2 byte	0x03	BCC
------	------	------	------	------	------------	------	-----

Reader 操作成功返回：P= 'Y' (0x59) 读卡成功

0x02	0x01	0x0D	0x3C	0x31	操作状态字 P	页地址 2 byte	264 byte 卡数据	0x03	BCC
------	------	------	------	------	---------	------------	--------------	------	-----

Reader 操作失败返回：

0x02	0x00	0x05	0x3C	0x31	操作状态字 P	页地址 2 byte	0x03	BCC
------	------	------	------	------	---------	------------	------	-----

操作状态字 P= 'N' (0x4E) 读卡失败
 P= 'E' (0x45) 卡机无卡
 P= 'W' (0x57) 卡不在允许操作的位置上。

页地址: 0x0000—0x07FF

9.8.3 写数据：只支持页写(264 byte)


HOST 发送：

0x02	0x01	0x0C	0x3C	0x31	页地址 2 byte	264 byte 卡数据	0x03	BCC
------	------	------	------	------	------------	--------------	------	-----

Reader 操作返回：

0x02	0x00	0x05	0x3C	0x31	操作状态字 P	页地址 2 byte	0x03	BCC
------	------	------	------	------	---------	------------	------	-----

操作状态字 P= 'Y' (0x59) 写卡成功
 P= 'N' (0x4E) 写卡失败
 P= 'E' (0x45) 卡机无卡
 P= 'W' (0x57) 卡不在允许操作的位置上。

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	37/46

9.9. SIM 卡操作：（对有 SIM 卡模块机型）

9.9.1 复位 SIM 卡：（对 1.8V ， 3.0V ， 5.0V 的 SIM 卡进行复位）

HOST 发送：

0x02	0x00	0x03	0x3D	Pm	SIM 卡座号	0x03	BCC
------	------	------	------	----	---------	------	-----

Pm= 0x2E 对工作电压是 1.8 V 的 SIM 卡进行复位操作

Pm= 0x2F 对工作电压是 3.0 V 的 SIM 卡进行复位操作

Pm= 0x30 对工作电压是 5.0 V 的 SIM 卡进行复位操作

Reader 操作成功返回： T=0 SIM 卡复位成功返回操作状态字 P= ‘Y’（0x59）

0x02	通讯包长度 2 byte	0x3D	Pm	SIM 卡 座号	操作状 态字 P	复位数据包长 度 2 byte	复位数据 n byte	0x03	BCC
------	-----------------	------	----	-------------	-------------	--------------------	----------------	------	-----

通讯包长度=6+ 复位数据长度 n

Reader 操作成功返回： T=1 SIM 卡复位成功返回操作状态字 P= ‘Z’（0x5A）

0x02	通讯包长度 2 byte	0x3D	Pm	SIM 卡 座号	操作状 态字 P	复位数据包长 度 2 byte	复位数据 n byte	0x03	BCC
------	-----------------	------	----	-------------	-------------	--------------------	----------------	------	-----

通讯包长度=6+ 复位数据长度 n

SIM 卡座号=0x30 操作 SIM 卡 1

=0x31 操作 SIM 卡 2

=0x32 操作 SIM 卡 3

=0x33 操作 SIM 卡 4

=0x34 操作 SIM 卡 5

=0x35 操作 SIM 卡 6

=0x36 操作 SIM 卡 7

=0x37 操作 SIM 卡 8

Reader 操作失败返回：

0x02	0x00	0x04	0x3D	0x30	SIM 卡座号	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	---------	------	-----

操作状态字 P= ‘N’（0x4E） 复位不成功

注：对 SIM 卡进行操作，只有复位成功后才能进行 C-APDU 包操作。使用 SIM 卡时请核对 SIM 卡工作电压，否则有可能损坏 SIM 卡。

9.9.2 T=0 SIM 卡 C-APDU 命令操作

HOST 发送：


0x02	通讯包长度 2 byte	0x3D	0x31	SIM 卡座号	C-APDU 包长度 2 byte	C-APDU 包 n byte	0x03	BCC
------	--------------	------	------	---------	-------------------	-----------------	------	-----

通讯包长度=5+ C-APDU 包长度 n （n=4—263byte）

Reader 操作成功返回： 操作状态字 P= ‘Y’（0x59）

0x02	通讯包长度 2 byte	0x3D	0x31	SIM 卡 座号	操作状态 字 P	C-APDU 操作返回包长 度 2 byte	C-APDU 操作返回包 n byte	0x03	BCC
------	-----------------	------	------	-------------	-------------	---------------------------	------------------------	------	-----

通讯包长度=6+ C-APDU 返回包长度 n （n=4--263byte）

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	38/46

9.9.3 T=1 SIM 卡 C-APDU 命令操作

0x02	通讯包长度 2 byte	0x3D	0x32	SIM 卡座号	C-APDU 包长度 2 byte	C-APDU 包 n byte	0x03	BCC
------	--------------	------	------	---------	-------------------	-----------------	------	-----

通讯包长度=5+ C-APDU 包长度 n (n=4--263byte)

Reader 操作成功返回: 操作状态字 P= 'Y' (0x59)

0x02	通讯包长度 2 byte	0x3D	0x32	SIM 卡座号	操作状态字 P	C-APDU 操作返回包长度 2 byte	C-APDU 操作返回包 n byte	0x03	BCC
------	--------------	------	------	---------	---------	-----------------------	---------------------	------	-----


通讯包长度=6+ C-APDU 返回包长度 n (n=4—263byte)

Reader 操作失败返回:

0x02	0x00	0x04	0x3D	0x32	SIM 卡座号	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	---------	------	-----

操作状态字 P= 'N' (0x4E) 操作不成功

CREATOR

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	39/46

9.10. 磁卡操作

读卡器上电初始化读磁卡方式为 ASCII 码读一二三轨，卡机执行复位操作，也将卡机设置成读磁卡方式为 ASCII 码读一二三轨。

9.10.1 按指定方式读指字轨道磁卡数据

HOST 发送：

0x02	0x00	0x04	0x45	0x30	读卡模式	指定轨道号	0x03	BCC
------	------	------	------	------	------	-------	------	-----

读卡模式： 0x30 以 ASCII 码读卡数据

0x31 以二进制码读卡数据

指定轨道号： 0x30 磁卡三轨都不读

0x31 读磁卡一轨

0x32 读磁卡二轨

0x33 读磁卡三轨

0x34 读磁卡一二轨

0x35 读磁卡二三轨

0x36 读磁卡一三轨

0x37 读磁卡一二三轨

操作返回：

0x02	通讯长度 N byte	0x45	0x30	读 卡 模 式	指 定 轨 道 号	一轨数据包 n byte + 二轨数据包 n byte + 三轨数据包 n byte	0x03	BCC
------	----------------	------	------	------------	--------------	---	------	-----

通讯长度：N = 4 + 三轨数据长度

读卡模式：

=0x30 卡机已设置成 ASCII 码读卡，上传卡数据为 ASCII 码编码

=0x31 卡机已设置成二进制码读卡，上传卡数据为二进制码编码形式

注意：二进制读卡传送的数据格式是：

一轨：b0,b1,b2,b3,b4,P

二轨,三轨：b0,b1,b2 b3,P

其中每轨数据包格式如下：

轨道数据起始字 + 读卡状态字 + 卡轨道数据

轨道起始字： 0x1F

读卡状态字： 0x59 读该轨数据读正确，卡轨道数据为该轨信息数据

0x4E 读卡不正确，卡轨道数据为错误信息

0x4F 该轨道不读，卡轨道数据为 0xE0；

错误信息： 0xE1 读该轨数据错误，没有起始位 STX


0xE2 读该轨数据错误，没有结束位 ETX

0xE3 读该轨数据错误，位校验错误 VRC

0xE4 读该轨数据错误，字节校验位错误 LRC

0xE5 读该轨数据错误，该轨是空白信息磁道

当设置以 ASCII 码读卡时将卡每一轨信息的别换成一个字节 ASCII 码上传达卡数据。

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	40/46

如：一轨数据第一字节为： 0x03 (HEX)

上传数据时卡轨道数据包为： 0x33 (ASCII)

当设置成二进制读卡时将卡每一轨信息的每一字节数据按每 4 位转成一个字节以 ASCII 码形式上传数据。

如：一轨数据第一字节为： 0x03 (HEX)

上传数据时卡轨道数据包为： 0x30 0x33

9.10.2 按指定方式重新读指字轨道磁卡数据

只适用于读卡器的磁头位置是在后端的机型，可将卡进行重新走卡进行读磁卡操作后再上传磁卡数据，适用于第一次进卡读磁卡有错时，执行此命令可进行重新走卡读磁卡来完成。

HOST 发送：

0x02	0x00	0x04	0x45	0x31	读卡模式	指定轨道号	0x03	BCC
------	------	------	------	------	------	-------	------	-----

读卡模式： 0x30 以 ASCII 码读卡数据

0x31 以二进制码读卡数据

指定轨道号： 0x30 磁卡三轨都不读

0x31 读磁卡一轨

0x32 读磁卡二轨

0x33 读磁卡三轨

0x34 读磁卡一二轨

0x35 读磁卡二三轨

0x36 读磁卡一三轨

0x37 读磁卡一二三轨

操作成功返回：

0x02	通讯长度 N byte	0x45	0x31	读卡模式	指定轨道号	一轨数据包 n byte + 二轨数据包 n byte + 三轨数据包 n byte	0x03	BCC
------	-------------	------	------	------	-------	---	------	-----

通讯长度： N = 4 + 三轨数据长度

读卡模式： =0x30 卡机已设置成 ASCII 码读卡，上传卡数据为 ASCII 码编码

=0x31 卡机已设置成二进制码读卡，上传卡数据为二进制编码形式

注意：二进制读卡传送的数据格式是：

一轨： b0,b1,b2,b3,b4, P

二轨,三轨： b0,b1,b2 b3,P

其中每轨数据包格式如下：

轨道数据起始字+读卡状态字+卡轨道数据


轨道数据起始字： 0x1F

读卡状态字： 0x59 读该轨数据读正确，卡轨道数据为该轨信息数据

0x4E 读卡不正确，卡轨道数据为错误信息

0x4F 该轨道不读，卡轨道数据为 0xE0；

错误信息： 0xE1 读该轨数据错误，没有起始位 STX

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	41/46

- 0xE2 读该轨数据错误，没有结束位 ETX
- 0xE3 读该轨数据错误，位校验错误 VRC
- 0xE4 读该轨数据错误，字节校验位错误 LRC
- 0xE5 读该轨数据错误，该轨是空白信息磁道

当设置以 ASCII 码读卡时将卡每一轨信息的别换成一个字节 ASCII 码上传达卡数据。

如：一轨数据第一字节为： 0x03 (HEX)

上传数据时卡轨道数据包为： 0x33 (ASCII)

当设置成二进制读卡时将卡每一轨信息的每一字节数据按每 4 位转成一个字节以 ASCII 码形式上传数据。

如：一轨数据第一字节为： 0x03 (HEX)

上传数据时卡轨道数据包为： 0x30 0x33


操作失败返回：

0x02	0x00	0x05	0x45	0x31	读卡模式	指定轨道号	错误状态信息字 P	0x03	BCC
------	------	------	------	------	------	-------	-----------	------	-----

错误状态信息字 P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上

P= 'N' (0x4E) 操作失败

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	42/46

9.11. AT88SC1608 卡操作(仅 V3.0)

9.11.1 复位

HOST 发送:

0x02	0x00	0x02	0x3E	0x30	0x03	BCC
------	------	------	------	------	------	-----

Reader 操作返回:

0x02	0x00	0x03	0x3E	0x30	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

操作状态字 P= 'Y' (0x59) 复位成功
P= 'N' (0x4E) 复位不成功
P= 'E' (0x45) 卡机无卡
P='W' (0x57) 卡不在允许操作的位置上。

9.11.2 验证密码

HOST 发送:

0x02	0x00	0x06	0x3E	0x31	密码区号	密码数据 3 byte	0x03	BCC
------	------	------	------	------	------	-------------	------	-----


Reader 操作返回:

0x02	0x00	0x04	0x3B	0x31	密码区号	操作状态字 P	0x03	BCC
------	------	------	------	------	------	---------	------	-----

操作状态字 P= 'Y' (0x59) 验证密码成功
P= 'N' (0x4E) 验证密码失败
P= 'F' (0x46) 卡已报废或应用块报废
P= 'E' (0x45) 卡机无卡
P= 'W' (0x57) 卡不在允许操作的位置上

其中密码类型号: = 0x30 验证应用一 区读密码
= 0x31 验证应用二 区读密码
= 0x32 验证应用三 区读密码
= 0x33 验证应用四 区读密码
= 0x34 验证应用五 区读密码
= 0x35 验证应用六 区读密码
= 0x36 验证应用七 区读密码
= 0x37 验证应用八 区读密码

= 0x38 验证应用一 区写密码
= 0x39 验证应用二 区写密码
= 0x3A 验证应用三 区写密码
= 0x3B 验证应用四 区写密码
= 0x3C 验证应用五 区写密码
= 0x3D 验证应用六 区写密码
= 0x3E 验证应用七 区写密码/验证主密码
= 0x3F 验证应用八 区写密码

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	43/46

每一个区密码只有允许验证 8 次，8 次校验错误后卡锁死，就表明卡这个区块不能读或写。

9.11.3 读数据

HOST 发送:

0x02	0x00	0x06	0x3E	0x32	区号	操作首地址	操作长度	0x03	BCC
					1 byte	1 byte	1 byte		

Reader 操作成功返回: P= 'Y' (0x59)

0x02	通讯长度 L	0x3E	0x32	区号	操作状	操作首地址	操作长度	数据	0x03	BCC
	2 byte			1 byte	态字 P	1 byte	1 byte	n byte		

通讯长度: L= 7 + n byte

Reader 操作失败返回:

0x02	0x00	0x06	0x3E	0x32	区号	操作状	操作首地址	操作长度	0x03	BCC
					1 byte	态字 P	1 byte	1 byte		

操作状态字 P= 'E' (0x45) 读卡失败
 P= 'E' (0x45) 卡机无卡
 P= 'W' (0x57) 卡不在允许操作的位置上。

操作地址范围:

应用区: 0x00----0xFF

设置区: 0x00----0x80

操作长度范围: 0x01----0x80


区号: = 0x30 应用一区 (len=0x01—0x80)
 = 0x31 应用二区 (len=0x01—0x80)
 = 0x32 应用三区 (len=0x01—0x80)
 = 0x33 应用四区 (len=0x01—0x80)
 = 0x34 应用五区 (len=0x01—0x80)
 = 0x35 应用六区 (len=0x01—0x80)
 = 0x36 应用七区 (len=0x01—0x80)
 = 0x37 应用八区 (len=0x01—0x80)
 = 0x38 设置区 (len=0x01—0x80)

要对应用区进行读时请校验该区读密码正确后才能进行读，否则读的数据无效，设置区数据只有密码区域 (0x40---0x7F) 是受密码保护，只能校验正确后才能正确读出

9.11.4 写数据

HOST 发送:

0x02	通讯长度 2 byte	0x3E	0x33	区号 1 byte	操作首地址 1 byte	操作长度 len1 byte	数据 n byte	0x03	BCC
------	-------------	------	------	-----------	--------------	----------------	-----------	------	-----

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	44/46

Reader 操作返回:

0x02	0x00	0x06	0x3E	0x33	区号	操作状态字 P	操作首地址 1 byte	操作长度 len 1 byte	0x03	BCC
------	------	------	------	------	----	---------	--------------	-----------------	------	-----

P= 'Y' (0x59) 写卡成功
P= 'E' (0x45) 写卡失败
P= 'E' (0x45) 卡机无卡
P= 'W' (0x57) 卡不在允许操作的位置上。

操作地址范围:

应用区: 0x00----0xFF

设置区: 0x00----0x80

操作长度范围: 0x01----0x80

区号: = 0x30 应用一区 (len=0x01—0x80)
= 0x31 应用二区 (len=0x01—0x80)
= 0x32 应用三区 (len=0x01—0x80)
= 0x33 应用四区 (len=0x01—0x80)
= 0x34 应用五区 (len=0x01—0x80)
= 0x35 应用六区 (len=0x01—0x80)
= 0x36 应用七区 (len=0x01—0x80)
= 0x37 应用八区 (len=0x01—0x80)
= 0x38 设置区 (len=0x01—0x80)

要对应用区进行写时请校验该区读密码正确后才能进行写, 否则写的的数据无效, 设置区的密码, 厂家的固化的信息, 用卡商固化信息, 访问权限控制区, 认证区, 密钥区受相关条件才能进行写操作, 只有符合写操作才能进行写。请使用详细参阅相关资料。

9.11.5 读熔丝

HOST 发送:

0x02	0x00	0x06	0x3E	0x34	0x03	BCC
------	------	------	------	------	------	-----


Reader 操作成功返回: P= 'Y' (0x59)

0x02	0x00	0x06	0x3E	0x34	操作状态字 P	熔丝状态字 FAB	熔丝状态字 CMA	熔丝状态字 PER	0x03	BCC
------	------	------	------	------	---------	-----------	-----------	-----------	------	-----

Reader 操作失败返回:

0x02	0x00	0x06	0x3E	0x34	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

P= 'N' (0x4E) 读熔丝失败
P= 'E' (0x45) 卡机无卡
P= 'W' (0x57) 卡不在允许操作的位置上。
熔丝状态字 FAB: FAB =0X30 已熔断, FAB=0X31 未熔断
熔丝状态字 CMA: CMA =0X30 已熔断, CMA =0X31 未熔断

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	45/46

熔丝状态字 PER : PER =0X30 已熔断, PER =0X31 未熔断

FAB 为 ATMEL 的芯片出厂时的熔断标志。

CMA 为卡厂的卡片出厂时的熔断标志。

PER 为发行商熔丝, 在应用系统启动前个人化时的熔断标志。

9.11.6 写熔丝: (写熔丝是一级一级往下熔断, 由 FAB → CMA → PER, 熔丝熔断后不能再恢复)

HOST 发送:

0x02	0x00	0x03	0x3E	0x35	0x03	BCC
------	------	------	------	------	------	-----

Reader 操作返回:

0x02	0x00	0x03	0x3E	0x35	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

P= 'Y' (0x59) 写熔丝成功

P= 'N' (0x4E) 写熔丝失败, 卡所有熔丝已熔断

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

9.11.7 初始化认证区

HOST 发送:

0x02	0x00	0x0A	0x3E	0x36	8 byte 随机数 Q0、Q1、Q2、Q3、Q4、Q5、Q6、Q7	0x03	BCC
------	------	------	------	------	------------------------------------	------	-----

Reader 操作返回:

0x02	0x00	0x03	0x3E	0x36	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

P= 'Y' (0x59) 初始化成功

P= 'N' (0x4E) 初始化失败, 卡已初始化。

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

初始化认证区是先读取卡中的 Nc, Ci, 通过 F1 或 F2 算法, 计算出 $Gc=F1(Ks, Nc)$ 得到的随机数 Q0~Q7, 送入 AT88SC1608 卡中, 完成进行初始化认证区。

9.11.8 校验认证区

HOST 发送:

0x02	0x00	0x0A	0x3E	0x37	8 byte 随机数 Q0、Q1、Q2、Q3、Q4、Q5、Q6、Q7	0x03	BCC
------	------	------	------	------	------------------------------------	------	-----

Reader 操作返回:


0x02	0x00	0x03	0x3E	0x37	操作状态字 P	0x03	BCC
------	------	------	------	------	---------	------	-----

P= 'Y' (0x59) 验证成功

P= 'N' (0x4E) 验证失败

P= 'E' (0x45) 卡机无卡

P= 'W' (0x57) 卡不在允许操作的位置上。

	SPECIFICATION	Model No.	CRT-310 读卡器
		Date	2007/4/1
	通讯协议	Ver.	3.0
		Page	46/46

校验认证区是在进行初始化认证区操作后，按 F2 算法完成 $Q1 = F2(Gc, Ci, Q0)$ ，分别生成的 Q0, Q1, Q2, Q3, Q4, Q5, Q6, Q7 送入 AT88SC1608 卡中由卡中来完成校验认证区，进行此验证。

注：Nc：识别码，通常用作卡的唯一标识——卡号。个人化前定义。

Ci：密文，个人化前可写一随机数，认证卡时使用，每次认证会被自动改写。

Gc：密钥，64 位的保密种子，由 Nc 通过 F1 公式推算出来，在个人化前，写入卡中。个人化后不可访问，认证时作为该卡的 F2 公式的参数。(详细用法参见认证协议)

CREATOR