1. 通讯字符格式

波特率（BPS）： 9600/192000/38400/57600BPS（卡机自动识别）
通信类型： 异步通信
传输类型： 半双工,支持多机通讯，最大可支持 16 台分机。
数据帧结构：

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

起始位：1 位
数据位：8 位
校验位：无
停止位：1 位
编码方式： ASCII 8 位编码

2. 通讯控制方法和控制字符

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。

相关控制字符

ACK (06H)	确认字符
NAK (15H)	否认字符
EOT (04H)	取消清除字符

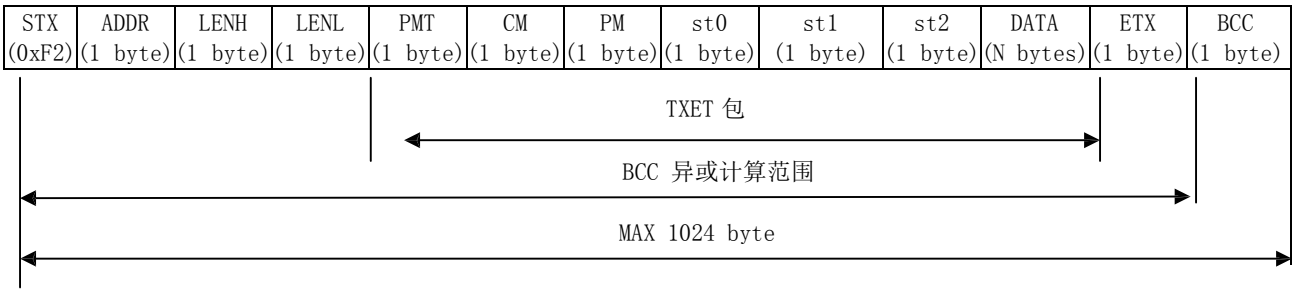
3. 通讯格式和相关字符

3.1 发送命令包(Command)格式

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

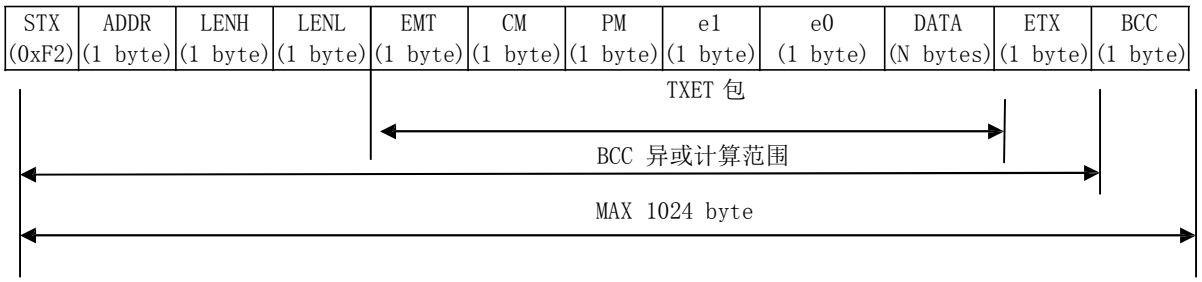
STX (F2H)	起始字符
ADDR	卡机地址字
LENH(1 byte)	发送 TXET 包数据长度高字节
LENL(1 byte)	发送 TXET 包数据长度低字节
CMT	发送命令头(‘C’,43H)
CM	发送命令字
PM	发送命令参数
DATA	发送命令数据(N byte,N=0~512)
ETX (03H)	结束字符
BCC(1 bytes)	异或校验值

3.2 卡机操作成功返回命令包(Response)格式



STX (F2H)	起始字符
ADDR	卡机地址字
LENH(1 byte)	返回 TXET 包长度高字节
LENL(1 byte)	返回 TXET 包长度低字节
PMT	返回命令头(‘P’,50H)
CM	返回命令字
PM	返回命令参数
st1,st0,st2	返回卡机状态码
DATA	返回命令数据(N byte,N=0~512)
ETX (03H)	结束字符
BCC(1 bytes)	异或校验值

3.3 卡机操作失败返回命令包(Response)格式



STX (F2H)	起始字符
ADDR	卡机地址字
LENH(1 byte)	返回 TXET 包长度高字节
LENL(1 byte)	返回 TXET 包长度低字节
EMT	返回命令头(‘N’,45H)
CM	返回命令字
PM	返回命令参数
e1,e0	返回卡机错误码
DATA	返回命令数据(N byte,N=0~512)
ETX (03H)	结束字符
BCC(1 bytes)	异或校验值

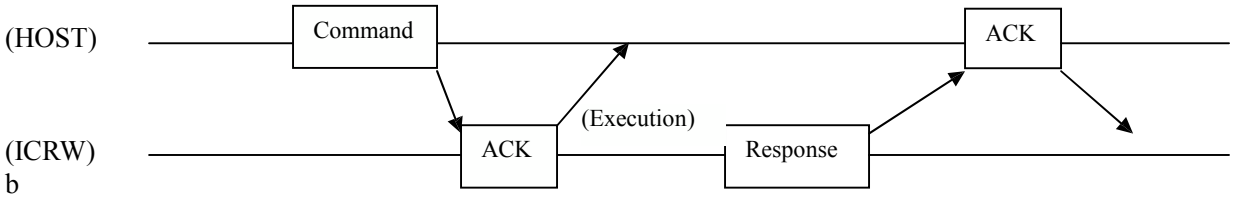
4. 多机通讯卡机地址 ADDR：卡机多机通讯时对其中一台卡机操作时对应地址字，具体定义如下:

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

卡机出厂前，默认卡机地址为 15#；进行多机通讯时，应将每一台卡机设为唯一地址，通过通讯包中对应地址字来选择每一台分机进行控制。

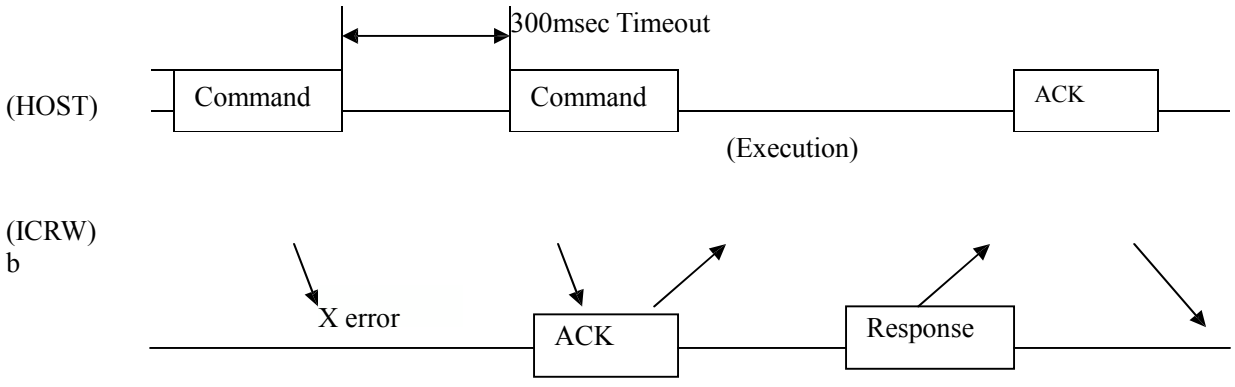
5. 卡机通讯描述:

5.1 正常通讯过程:(命令和反应)

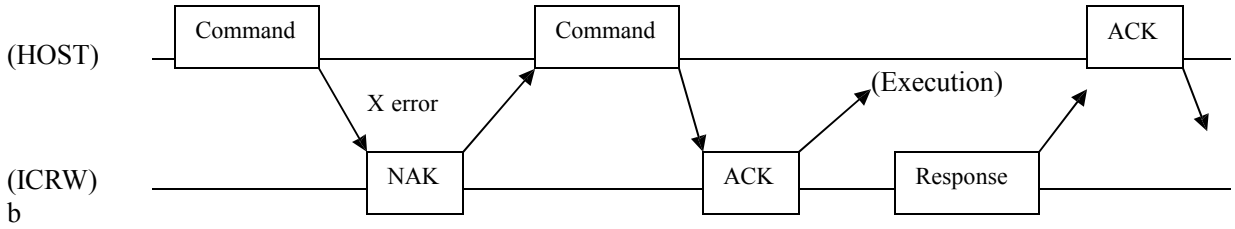


5.2 非正常通讯过程:(命令和反应)

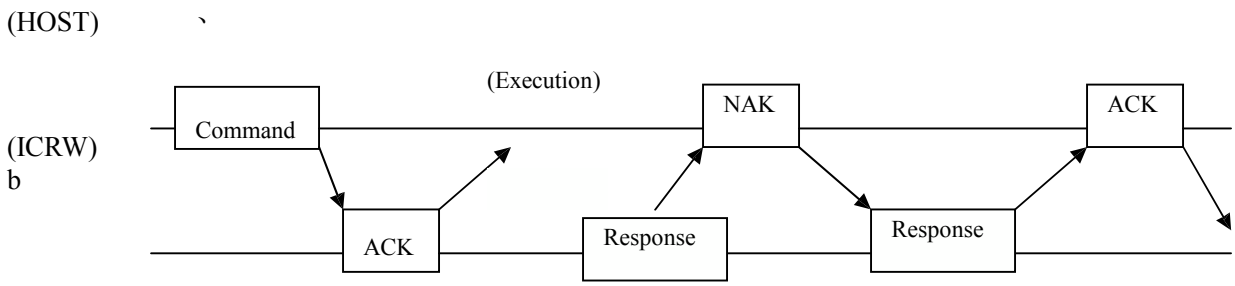
Case 1



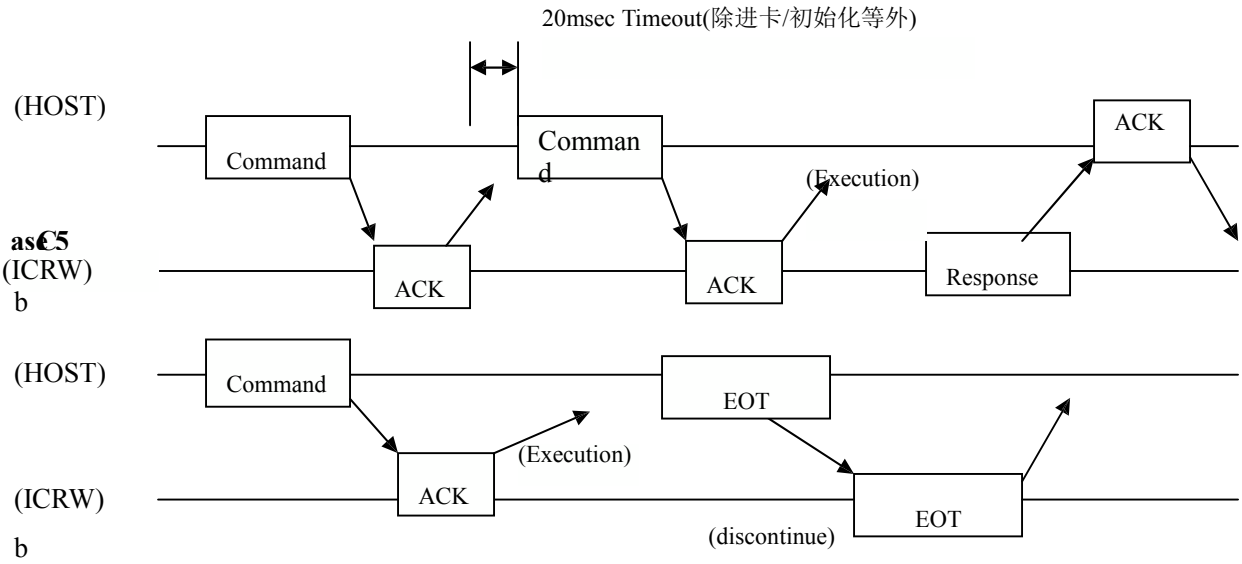
Case 2



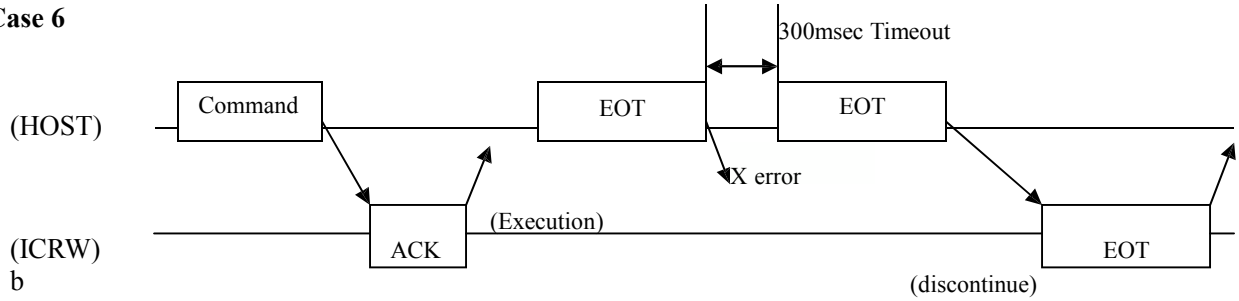
Case 3



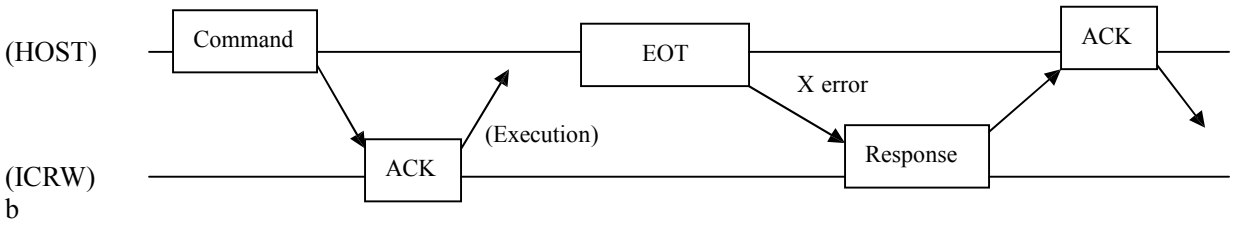
Case 4



Case 6



Case 7



6. 卡机操作命令列表：

章节	命令	功能	**Cm**	**Pm**	描述
9.1	卡机复位	初始化操作，如有卡，把卡移动到相应位置，如无卡，做检测微动，而后返回软件版本	30H	30H	复位并将卡移动到卡口（持卡位）
				31H	复位并将卡回收到回收盒中
				33H	复位但不移动卡
				34H	同30H并启动回收卡计数功能
				35H	同31H并启动回收卡计数功能
				37H	同 33H 并启动回收卡计数功能
9.2	查状态	查询卡机当前状态	31H	30H	查询卡机当前基本状态
				31H	查询卡机当前基本状态(Se状态)
9.3	移动卡	将卡机内的卡进行移动	32H	30H	将卡移动到出卡口(持卡位)
				31H	将卡移动到IC卡位
				32H	将卡移动到RF卡位
				33H	将卡回收到回收盒中
				39H	将卡移动到出卡口(不持卡位)
9.4	设置出卡口进卡		33H	30H	设置允许出卡口进卡
				31H	设置禁止出卡口进卡
9.5	IC卡/RF卡类型检测		50H	30H	自动检测IC卡类型
				31H	自动检测RF卡类型
9.6	CPU卡操作	CPU卡应用操作	51H	30H	CPU卡冷复位
				31H	CPU卡下电
				32H	CPU卡状态查询
				33H	T=0协议CPU卡APDU数据交换
				34H	T=1协议CPU卡APDU数据交换
				38H	CPU卡热复位
				39H	自动区分T=0/T=1协议CPU卡APDU数据交换
9.7	SAM卡操作	SAM卡应用操作	52H	30H	SAM卡冷复位
				31H	SAM卡下电
				32H	SAM卡状态查询
				33H	T=0协议SAM卡APDU数据交换
				34H	T=1协议SAM卡APDU数据交换
				38H	SAM卡热复位
				39H	自动区分T=0/T=1协议SAM卡APDU数据交换
				40H	选择SAM卡座
9.8	SLE4442/4428卡操作		53H	30H	SLE4442/4428卡复位(激活)
				31H	SLE4442/4428卡下电(释放)
				32H	查SLE4442/4428卡状态
				33H	操作SLE4442卡
				34H	操作SLE4428卡
9.9	IIC 存贮卡操作	24C01—24C256卡操作	54H	30H	IIC卡复位(激活)
				31H	IIC卡下电(释放)
				32H	查IIC卡状态
				33H	读IIC卡
				34H	写IIC卡

9.10	RF卡操作 (13.56 MHZ)	Mafare 标准卡 Type A & B T=CL协议操作	60H	30H 31H 32H 33H 34H 35H 39H	RF 卡激活 RF 卡下电释放 RF 卡操作状态查询 Mafare 标准卡读写 Type A 标准T=CL卡APDU数据交换 Type B 标准T=CL卡APDU数据交换 RF 卡唤醒/睡眠
9.11	卡机序列号		A2H	30H	读卡机序列号
9.12	读卡机配置信息		A3H	30H	读取卡机机型配置信息
9.13	版本信息读取		A4H	30H	卡机软件版本信息
9.14	回收卡计数		A5H	30H 31H	读取回收卡计数的数值 设置回收卡计数初始值

7.卡机状态码（st0,st1,st2）及其含义:

st0	含义
“**0**”	卡机通道内无卡
“**1**”	卡机通道出卡口处有一张卡
“**2**”	卡机通道 **RF/IC** 卡位有卡

st1	含义
“**0**”	发卡箱无卡
“**1**”	发卡箱卡少
“**2**”	发卡箱卡足

st2	含义
“**0**”	回收箱未满
“**1**”	回收箱卡满

8. e1,e0 错误字代码表**:**

e1,e0	含义
“00”	未定义的命令
“01”	命令参数有错误
“02”	命令执行顺序错误
“03”	硬件不支持命令
“04”	命令数据错误（通讯包中 DATA 有错误）
“05”	IC 卡接触未释放
“06”--“09”	
“10”	卡堵塞
“11”	
“12”	传感器错误
“13”	长卡错误
“14”	短卡错误
“15”--“39”	
“40”	回收卡时卡片被拔走
“41”	IC 卡电磁铁错误
“42”	
“43”	卡片不能移动卡 IC 卡位
“44”	
“45”	卡片被人为移动
“46”	
“47”	
“48”	
“49”	
“50”	收卡计数器溢出
“51”	马达错误
“52”--“59”	
“60”	IC 卡供电电源短路
“61”	IC 卡激活失败
“62”	IC 卡不支持当前命令
“63”	
“64”	
“65”	IC 卡未激活
“66”	当前 IC 卡不支持命令
“67”	传输 IC 卡数据错误
“68”	传输 IC 卡数据超时
“69”	CPU/SAM 卡不符合 EMV 标准
“A0”	发卡卡栈(箱)空,卡栈中无卡
“A1”	收卡箱满
“A2”--“A9”	
“B0”	卡机未复位

9. 命令详细说明

9.1 复位(初始化):

HOST 命令(TXET):

“C”	30H	Pm

正常返回(TXET):

“P”	30H	Pm	st0	st1	st2	Rev_type

错误返回(TEXT):

“N”	30H	Pm	e1	e0

该条指令是上电后必须执行的第一条指令，否则其他指令不能执行，而后可以多次执行该指令； 在该指令第一次执行时，ICRW 自动检测和判定HOST 的通讯波特率（BAUD），并按该波特率通讯； 一旦执行该命令，会清除之前所有的错误代码，卡机处于禁止进卡状态,并返回卡机软件版本信息。

Pm: 卡机复位处理参数 如果卡机内无卡，卡机会轻微转动电机(整理卡栈中卡片)。 若卡机内有卡，将按下列情况处理。

=30H 移动卡片到卡口
=31H 回收卡片到回收箱中
=33H 不移动卡
=34H 同 Pm=30H，启动回收卡计数
=35H 同 Pm=31H，启动回收卡计数
=37H 同 Pm=33H，启动回收卡计数

Rev_type: 卡机软件版本信息,“CRT-571-V1.00” 。

9.2 查状态

HOST 命令:

“C”	31H	Pm

正常返回:

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

错误返回:

“N”	31H	Pm	e1	e0

Pm=30H 返回卡机当前卡机有无卡状态 **st0,st1,st2** (具体含义见 7.说明)

Pm=31H 返回卡机当前有无卡状态,并返回卡机所有传感器(10 字节)状态信息,见下表:

Sensor	status
S1	30H 无卡
	31H 有卡
S2	30H 无卡
	31H 有卡
S3	30H 无卡
	31H 有卡
S4	30H 无卡
	31H 有卡
S5（系统保留）	
S6	30H 无卡
	31H 有卡
S7	30H 无卡
	31H 有卡
S8	30H 无卡
	31H 有卡
S9	30H 无卡
	31H 有卡
S10	30H 无卡
	31H 有卡

KS1 30H 无卡
31H 有卡

KS2 30H 无卡
31H 有卡

9.3 移动卡:

HOST 命令:

“C”	32H	Pm

正常返回:

“P”	32H	Pm	st0	st1	st2

错误返回:

“N”	32H	Pm	e1	e0

Pm=30H 将卡移动到出卡口(持卡位)
Pm=31H 将卡移动到 IC 卡位(仅针对卡栈出卡)
Pm=32H 将卡移动到 RF 卡位
Pm=33H 将卡回收到回收盒中
Pm=39H 将卡移动到出卡口(不持卡位)

当进行移动卡过程中不能将卡移动到指定位置，卡机将返回卡堵塞错误。 注：当执行回收卡时，收卡箱回收卡满时，将返回“收卡箱满错误”,此时应及时清理回收卡箱中卡。

9.4 出卡口进卡使能:

HOST 命令:

“C”	33H	Pm

正常返回:

“P”	33H	Pm	st0	st1	st2

错误返回:

“N”	33H	Pm	e1	e0

设定出卡口进卡工作使能/禁能. 使能出卡口进卡后，一旦有卡从出卡口插入，卡机将卡移动到卡机内 RF 卡操作位. 也可通过查状态命令获取进卡结束。

Pm=30H 允许出卡口进卡
Pm=31H 禁止出卡口进卡

当执行复位(初始化)命令后，卡机自动禁止出卡口进卡.

9.5 自动测 IC 卡/RF 卡类型:

9.5.1 自动测 IC 卡类型:

HOST 命令:

“C”	50H	30H

正常返回:

“P”	50H	30H	st0	st1	st2	Card_type

错误返回:

“N”	50H	30H	e1	e0

自动测试当前 IC 卡的类型，将卡机内的卡走卡到 IC 卡位，自动测试当前 IC 卡类型, 测试完成返回 Card_type 信息。

Cart_type(2 byte)		说明
‘0’	‘0’	未知 IC 卡类型
‘1’	‘0’	T=0 CPU 卡
	‘1’	T=1 CPU 卡
‘2’	‘0’	SLE4442 卡
	‘1’	SLE4428 卡
‘3’	‘0’	AT24C01 卡
	‘1’	AT24C02 卡
	‘2’	AT24C04 卡
	‘3’	AT24C08 卡
	‘4’	AT24C16 卡
	‘5’	AT24C32 卡
	‘6’	AT24C64 卡
	‘7’	AT24C128 卡
	‘8’	AT24C256 卡

9.5.2 自动测 RF 卡类型:

HOST 命令:

“C”	50H	31H

正常返回:

“P”	50H	31H	st0	st1	st2	Card_type

错误返回:

“N”	50H	31H	e1	e0

自动测试当前 RF 卡的类型，将停在卡机内的卡走卡到 RF 卡位，自动测试当前 RF 卡类型,测试完成返回 Card_type 信息。

Cart_type(2 byte)		说明
‘0’	‘0’	未知 RF 卡类型
‘1’	‘0’	Mifare one S50 卡
	‘1’	Mifare one S70 卡
	‘2’	Mifare one UL 卡
‘2’	‘0’	Type A CPU 卡
‘3’	‘0’	Type B CPU 卡

9.6 CPU 卡操作:

9.6.1 CPU 卡复位(激活):

HOST 命令:

“C”	51H	30H	Vcc

正常返回:

“P”	51H	30H	st0	st1	st2	Type	ATR

错误返回:

“N”	51H	30H	e1	e0	ATR

卡机提供电源(VCC)，时钟信号(CLK)，和复位信号(RST) 给卡， 卡被激活，并返回 ATR.
Vcc=30H 对 CPU 卡以 5V 电源，EMV 方式对 CPU 卡进行复位(激活).
Vcc=33H 对 CPU 卡以 5V 电源，ISO7816 方式对 CPU 卡进行复位(激活).
Vcc=35H 对 CPU 卡以 3V 电源，ISO7816 方式对 CPU 卡进行复位(激活).
Vcc 是可选参数，若命令中无 Vcc 参数，等同于 Vcc=30H.

在复位过程中，CPU 卡片 ATR 信息不符合 EMV 方式，将返回 e1,e0=“69”错误.
在复位过程中，检测 IC 卡电源失败，返回 e1,e0=“60”错误.
Type: CPU 卡协议类型
=30H T=0 协议 CPU 卡
=31H T=1 协议 CPU 卡

ATR：复位应答信息格式如下：

TS	TO	TA1	TB1	…	TCK

9.6.2 CPU 卡下电:

HOST 命令:

“C”	51H	31H

正常返回:

“P”	51H	31H	st0	st1	st2

错误返回:

“N”	51H	31H	e1	e0

对 CPU 卡下电操作。

对已上电激活 CPU 卡下电操作。

9.6.3 CPU 卡查状态:

HOST 命令:

“C”	51H	32H

正常返回:

“P”	51H	32H	st0	st1	st2	Sti

错误返回:

“N”	51H	32H	e1	e0

检查当前操作 CPU 卡的状态,返回 Sti 状态:

Sti=30H 卡片未激活

=31H 卡片已激活，当前 CPU 卡工作时钟频率为 3.57 MHZ

=32H 卡片已激活，当前 CPU 卡工作时钟频率为 7.16 MHZ

检查到 IC 卡电源电路失败，将返回 e1,e0=“60”错误.

9.6.4 T=0 协议 CPU 卡 APDU 操作

HOST 命令:

“C”	51H	33H	C-APDU

正常返回:

“P”	51H	33H	st0	st1	st2	R-APDU

错误返回:

“N”	51H	33H	e1	e0

对已复位(激活)成功的 T=0 协议 CPU 卡进行数据交换操作。

C-APDU HOST 发送给 T=0 CPU 卡数据包，最小为 4 byte,最大为 261 byte。格式如下：

CLA	INS	P1	P2	LC	Data1	。。。。	Le

R-APDU CPU 卡返回给 HOST 数据包,最小为 2 byte,最大为 258 byte.格式如下：

Data1	…..	Data(n)	Sw1	Sw0

如在操作过程中检测 IC 卡电源失败，卡机返回 e1,e0-=“60”错误；
如协议当前 CPU 卡不是 T=0 协议，卡机返回错误代码 e1,e0=“62”错误； 如 CPU 卡超时，卡机先对 CPU 卡下电，而后返回 e1,e0=“63”错误； 如其它协议错误出现，卡机先对 CPU 卡下电，而后返回错误代码 e1,e0=“64”错误； 如 HOST 在 CPU 未执行复位激活操作，卡机返回 e1,e0=“65”错误

T=0 APDU 格式请参照 ISO/IEC7816-3 相关内容，具体 C-APDU 命令操作以卡的 COS 指令为准。

9.6.5 T=1 协议 CPU 卡 APDU 操作

HOST 命令:

“C”	51H	34H	C-APDU

正常返回:

“P”	51H	34H	st0	st1	st2	R-APDU

错误返回:

“N”	51H	34H	e1	e0

对已复位(激活)成功的 T=1 协议 CPU 卡进行数据交换操作。

读卡器执行 T=1 协议 C-APDU 操作，将按 T=1 协议规范，将 HOST 发送的 C-APDU 组合成一个 I-bolck，发送给 CPU 卡，再将 CPU 卡返回的 I-block 提取 R-ADPU 包返回给 HOST。过程如下：

A. 发送 C-APDU(增加块头，块尾，将发送 C-APDU 作块信息，组合成 I-block 发给 CPU 卡)。

C-APDU

CLA	INS	P1	P2	Lc	Data1	…	Data(Lc)	Le

I-block

NAD	PCB	LEN	CLA	INS	P1	P2	Lc	Data1	…	Data(Lc)	Le	EDC
块头			块信息									块尾

B. 接收 R-APDU(从 CPU 卡返回的 I-block,将块信息返回 R-ADPU)

I-block

块头			块信息									块尾
NAD	PCB	LEN	CLA	INS	P1	P2	Lc	Data1	…	Data(Lc)	Le	EDC

R-APDU

CLA	INS	P1	P2	Lc	Data1	…	Data(Lc)	Le

如在操作过程中检测 IC 卡电源失败，卡机返回 e1,e0-=“60”错误；
如协议当前 CPU 卡不是 T=1 协议，卡机返回错误代码 e1,e0=“62”错误； 如 CPU 卡超时，卡机先对 CPU 卡下电，而后返回 e1,e0=“63”错误； 如其它协议错误出现，卡机先对 CPU 卡下电，而后返回错误代码 e1,e0=“64”错误； 如 HOST 在 CPU 末执行复位激活操作，卡机返回 e1,e0=“65”错误

T=1 APDU 格式请参照 ISO/IEC7816-3 相关内容，具体 C-APDU 命令操作以卡的 COS 指令为准。

9.6.6 CPU 卡热复位

HOST 命令:

“C”	51H	38H

正常返回:

“P”	51H	38H	st0	st1	st2	Type	ATR

错误返回:

“N”	51H	38H	e1	e0

该命令是在 IC 卡激活状态下，卡机做复位操作，重新得到 ATR。

Type: CPU 卡协议类型

=30H T=0 协议 CPU 卡

=31H T=1 协议 CPU 卡

9.6.7 自动选择 T=0/T=1 协议 CPU 卡 APDU 操作

HOST 命令:

“C”	51H	39H	C-APDU

正常返回:

“P”	51H	39H	st0	st1	st2	R-APDU

错误返回:

“N”	51H	39H	e1	e0

卡机自动判断当前 CPU 卡 T=0/T=1 协议，自动选择相应协议的 C-APDU 操作, 返回 R-APDU。

在操作过程中检测 IC 卡电源失败，卡机返回 e1,e0-=“60”错误；

如协议当前 CPU 卡不是 T=0/T=1 协议，卡机返回错误代码 e1,e0=“62”错误； 如 CPU 卡超时，卡机先对 CPU 卡下电，而后返回 e1,e0=“63”错误； 如其它协议错误出现，卡机先对 CPU 卡下电，而后返回错误代码 e1,e0=“64”错误； 如 HOST 在 CPU 未执行复位激活操作，卡机返回 e1,e0=“65”错误

9.7 SAM 卡复位(激活):

9.7.1 SAM 卡复位(激活):

HOST 命令:

“C”	52H	30H	Vcc

正常返回:

“P”	52H	30H	st0	st1	st2	Type	ATR

错误返回:

“N”	52H	30H	e1	e0	ATR

卡机提供电源(VCC)，时钟信号(CLK)，和复位信号(RST) 给卡， 卡被激活，并返回 ATR.

Type: SAM 卡协议类型

=30H T=0 协议 SAM 卡

=31H T=1 协议 SAM 卡

ATR：复位应答信息格式如下：

TS	TO	TA1	TB1	…	TCK

Vcc=30H 对 SAM 卡以 5V 电源，EMV 方式对 SAM 卡进行复位(激活).
Vcc=33H 对 SAM 卡以 5V 电源，ISO7816 方式对 SAM 卡进行复位(激活).
Vcc=35H 对 SAM 卡以 3V 电源，ISO7816 方式对 SAM 卡进行复位(激活).

Vcc 是可选参数，若命令中无 Vcc 参数，等同于 Vcc=30H.

在复位过程中，SAM 卡片 ATR 信息不符合 EMV 方式，将返回 e1,e0=“69”错误.

在复位过程中，检测 IC 卡电源失败，返回 e1,e0=“60”错误.

9.7.2 SAM 卡下电:

HOST 命令:

“C”	52H	31H

正常返回:

“P”	52H	31H	st0	st1	st2

错误返回:

“N”	52H	31H	e1	e0

对 SAM 卡下电操作。

对已上电激活 SAM 卡下电操作。

9.7.3 SAM 卡查状态:

HOST 命令:

“C”	52H	32H

正常返回:

“P”	52H	32H	st0	st1	st2	Sti	Stj

错误返回:

“N”	52H	32H	e1	e0

检查当前操作 SAM 卡的状态,返回 Sti,Stj 状态:

Sti =30H 当前 SAM 卡未激活
Sti =31H 当前 SAM 卡已激活,工作频率为 3.57 MHZ
Sti =32H 当前 SAM 卡已激活,工作频率为 7.16 MHZ

Stj =30H 当前 SAM 卡卡座为 1 号卡座
Stj =31H 当前 SAM 卡卡座为 2 号卡座(可选)
Stj =32H 当前 SAM 卡卡座为 3 号卡座(可选)
Stj =33H 当前 SAM 卡卡座为 4 号卡座(可选)
Stj =34H 当前 SAM 卡卡座为 5 号卡座(可选)

检查到 SAM 卡电源电路失败，将返回 e1,e0=“60”错误.

9.7.4 T=0 协议 SAM 卡 APDU 操作

HOST 命令:

“C”	52H	33H	C-APDU

正常返回:

“P”	52H	33H	st0	st1	st2	R-APDU

错误返回:

“N”	52H	33H	e1	e0

对已复位(激活)成功的 T=0 协议 SAM 卡进行数据交换操作。

如在操作过程中检测 IC 卡电源失败，卡机返回 e1,e0-=“60”错误； 如协议当前 SAM 卡不是 T=0 协议，卡机返回错误代码 e1,e0=“62”错误； 如 SAM 卡超时，卡机先对 SAM 卡下电，而后返回 e1,e0=“63”错误；
如其它协议错误出现，卡机先对 SAM 卡下电，而后返回错误代码 e1,e0=“64”错误；
如 HOST 在 SAM 末执行复位激活操作，卡机返回 e1,e0=“65”错误

T=0 APDU 格式请参照 ISO/IEC7816-3 相关内容，具体 C-APDU 命令操作以卡的 COS 指令为准。

9.7.5 T=1 协议 SAM 卡 APDU 操作

HOST 命令:

“C”	52H	34H	C-APDU

正常返回:

“P”	52H	34H	st0	st1	st2	R-APDU

错误返回:

“N”	52H	44H	e1	e0

对已复位(激活)成功的 T=1 协议 SAM 卡进行数据交换操作。 如在操

作过程中检测 IC 卡电源失败，卡机返回 e1,e0-=“60”错误；
如协议当前 SAM 卡不是 T=1 协议，卡机返回错误代码 e1,e0=“62”错误； 如 SAM 卡超时，卡机先对 SAM 卡下电，而后返回 e1,e0=“63”错误； 如其它协议错误出现，卡机先对 SAM 卡下电，而后返回错误代码 e1,e0=“64”错误； 如 HOST 在 SAM 未执行复位激活操作，卡机返回 e1,e0=“65”错误

T=1 APDU 格式请参照 ISO/IEC7816-3 相关内容，具体 C-APDU 命令操作以卡的 COS 指令为准。

9.7.6 SAM 卡热复位

HOST 命令:

“C”	52H	38H

正常返回:

“P”	52H	38H	st0	st1	st2	Type	ATR

错误返回:

“N”	52H	38H	e1	e0

该命令是在 IC 卡激活状态下，卡机做复位操作，重新得到 ATR。

Type：SAM 卡协议类型

=30H T=0 协议 SAM 卡

=31H T=1 协议 SAM 卡

9.7.7 自动选择 T=0/T=1 协议 SAM 卡 APDU 操作

HOST 命令:

“C”	52H	39H	C-APDU

正常返回:

“P”	52H	39H	st0	st1	st2	R-APDU

错误返回:

“N”	52H	39H	e1	e0

卡机自动判断当前 SAM 卡 T=0/T=1 协议，自动选择相应协议的 C-APDU 操作,返回 R-APDU。
在操作过程中检测 IC 卡电源失败，卡机返回 e1,e0-=“60”错误；
如协议当前 SAM 卡不是 T=0/T=1 协议，卡机返回错误代码 e1,e0=“62”错误； 如 SAM 卡超时，卡机先对 SAM 卡下电，而后返回 e1,e0=“63”错误； 如其它协议错误出现，卡机先对 SAM 卡下电，而后返回错误代码 e1,e0=“64”错误； 如 HOST 在 SAM 末执行复位激活操作，卡机返回 e1,e0=“65”错误

9.7.8 选择 SAM 卡座

HOST 命令:

“C”	52H	40H	SAMn

正常返回:

“P”	52H	40H	st0	st1	st2

错误返回:

“N”	52H	40H	e1	e0

对 SAM 卡板上的 SAM 卡进行选择。

SAMn =30H 选择 SAM1
=31H 选择 SAM2(可选)
=32H 选择 SAM3(可选)
=33H 选择 SAM4(可选)
=34H 选择 SAM5(可选)

该命令只能针对有 PSAM 卡板的型号的卡机有效，并每次只能针对一个 SAM 卡来操作，卡机初始化时 SAM1 自动被选择。

9.8 SLE4442/4428 卡操作

9.8.1 SLE4442/4428 卡复位(激活):

HOST 命令:

“C”	53H	30H

正常返回:

“P”	53H	30H	st0	st1	st2	ATR(4 byte)

错误返回:

“N”	54H	30H	e1	e0

卡机提供电源(VCC)，时钟信号(CLK)，和复位信号(RST) 给卡， 卡被激活，并返回 ATR.

其中： SLE4442 Card ATR=“A2H，13H，10H，91H”

SLE4442 Card ATR=“92H，23H，10H，91H”

9.8.2 SLE4442/4428 卡下电(释放):

HOST 命令:

“C”	53H	31H

正常返回:

“P”	53H	31H	st0	st1	st2

错误返回:

“N”	53H	31H	e1	e0

卡机停止电源(VCC)，时钟信号(CLK)，和复位信号(RST) 给卡,卡被下电释放.

9.8.3 SLE4442/4428 卡查状态:

HOST 命令:

“C”	53H	32H

正常返回:

“P”	53H	32H	st0	st1	st2	Sti

错误返回:

“N”	54H	32H	e1	e0

该命令用于查询卡的状态，正确执行后，返回的 Sti 中显示状态

Sti= 30H SLE4442/4428 卡未激活

Sti= 31H SLE4442 卡已激活

Sti= 32H SLE4428 卡已激活

9.8.4 SLE4442 卡操作：

在对 SLE4442(读写等)操作，所使用的命令数据是通过类似于 ISO/IEC 7816 T=0 标准数据交换命令(C-APDU)形式进行操作。

因此，卡机收到指定含义的命令数据后再执行对卡片相应操作。当命令执行成功，在正常返回数据包中增加 9000H；命令执行中出现错误，在正常返回中只返回类似于 ISO/IEC 7816-3 T=0 标准规范中“sw1+sw2”两个错误响应码。

Sw1	Sw2	说　明
90H	00H	操作成功
6FH	00H	操作失败
6FH	01H	密码校验失败
6FH	02H	密码校验失败，卡锁死
67H	00H	操作地址溢出
6BH	00H	操作长度溢出

9.8.4.1. 读 SLE4442 主存贮区：

HOST 命令:

“C”	53H	33H	00H	B0H	00H	abH	cdH

正常返回:

“P”	53H	33H	st0	st1	st2	data

错误返回:

“N”	53H	33H	e1	e0

其中：　ab:　读主存贮区起始地址

　　cd:　读数据操作长度

卡机通过指定的 abH 和 cdH 参数对 SLE4442 卡主存贮区进行读取。SLE4442 卡主存贮区容量为 256 byte.

通过下列命令读取 SLE4442 卡全部存贮数据。

Ex). “CR3”+00B0000000

9.8.4.2. 读 SLE4442 保护位数据：

HOST 命令:

“C”	53H	33H	00H	B0H	01H	abH	cdH

正常返回:

“P”	53H	33H	st0	st1	st2	data

错误返回:

“N”	53H	33H	e1	e0

其中：　ab:　读保护位起始地址

　　cd:　读数据操作长度

SLE4442 卡 32 bit(位)保护位状态通过 4 byte 数据来表示.对应保护位地址为 00H—1FH。

通过下列命令读取 SLE4442 卡所有保护位数据。

Ex). “CR3”+00B0010004

9.8.4.3 读 SLE4442 卡安全区数据

HOST 命令:

“C”	53H	33H	00H	B0H	02H	abH	cdH	efH…

正常返回:

“P”	53H	33H	st0	st1	st2	data

错误返回:

“N”	53H	33H	e1	e0

其中： ab: 读安全区起始地址

cd: 读安全区数据操作长度

读取 SLE4442 卡安全区数据。

SLE4442 卡安全区有 4 byte，分别为 1 byte 密码错误计数数据 + 3 byte 密码数据值(密码数据在正确校验密码后才可读)

通过下列命令读取 SLE4442 卡安全区所有数据.

Ex). “CR3”+00B0020004

9.8.4.4 写 SLE4442 卡主存贮区:

HOST 命令:

“C”	53H	33H	00H	D0H	00H	abH	cdH	efH…

正常返回:

“P”	53H	33H	st0	st1	st2	data

错误返回:

“N”	53H	33H	e1	e0

其中： ab: 写主存贮区起始地址

cd: 写数据操作长度

ef: 要写数据(cdH byte)

对 SLE4442 卡主存贮区进行写数据，将指定的数据写入主存贮区，卡机写完数据进行校验后返回操作结果。

在进行写数据之前，必须正确校验 SLE4442 卡密码.

SLE4442 卡存贮容量为 256 byte. 当 cd=00H 时可对全部主存贮区进行写操作。

下列命令写主存贮区全部区域:

Ex). “CR3”+00D000000+Write data(256 byte)

当命令执行后，返回 9000H(操作成功)或 sw1,sw2(操作失败)结果。 当指定要写入数据是在写保护区且处于写保护状态，数据将不能被写入。

9.8.4.5 SLE4442 卡带保护位写数据

HOST 命令:

“C”	53H	33H	00H	D0H	01H	abH	cdH	efH…

正常返回:

“P”	53H	33H	st0	st1	st2	data

错误返回:

“N”	53H	33H	e1	e0

其中： ab: 写操作起始地址
cd: 写数据操作长度
ef: 要写保护数据(cdH byte)

对主存贮区带写护的存贮单元进行写保护。在执行此命令前，必须正确校验 SLE442 卡密码。
SLE4442 卡写保护区位于主存贮区 00H—1FH。00H—1FH 这些存贮单元受约束于 32 bit 写保护位状态，例如，读到保护数据 byte0 的 bit0=1 ，则说明地址为 00H 存贮单元是写保护的 。
一亘被设置写保护后，写保护状态再不能被改变.
例如：对址址 10H 单元写入 20H 后立即进入写保护
Ex). “CR3”+00D001100120
当命令执行后，返回 9000H(操作成功)或 sw1,sw2(操作失败)结果。
卡机首先读保护区的数据与接收到命令中要写保护数据进行比较，如果不同，卡机将不执行写保护。
写保护操作只能在主存贮区操作一次。

9.8.4.5 SLE4442 卡写安全区(修改密码):

HOST 命令:

“C”	53H	33H	00H	D0H	02H	abH	cdH	efH…

正常返回:

“P”	53H	33H	st0	st1	st2	data

错误返回:

“N”	53H	33H	e1	e0

其中： ab: 写安全区起始地址
cd: 写数据操作长度
ef: 要写数据(cdH byte)

当正确校验密码后，安全区中 3 byte 密码将允许更改。 例如：
更改密码可通过下列命令来完成(将密码更改成 123456H)
Ex). “CR3”+00D0020103123456
当命令执行后，返回 9000H(操作成功)或 sw1,sw2(操作失败)结果。
注意：因为安全区中密码错误计数器允许写，所以写密码错误计数器要小心，如果可能，最好不写。密码错误计数器受控于校验密码操作。

9.8.4.6 校验 SLE4442 卡密码:

HOST 命令:

“C”	53H	33H	00H	20H	03H	01H	03H	efH…

正常返回:

“P”	53H	33H	st0	st1	st2	data

错误返回:

“N”	53H	33H	e1	e0

其中： ef: 密码数据(3 byte)

要更改 SLE4442 卡数据，必须先校验卡密码。因为这是卡片功能要求，是下一个发行操作命令必须操作。

Ex). “CR3”+0020030103xxxxxx (xxxxxx 3 byte 密码数据)

卡片将它本身存贮的密码数据与命令中数据进行比较。

用户要改写 SLE4442 卡数据必须知道卡的密码，密码错误计数器值会从 2 或小于 2 的值直至复位成零，当错误计数值为零时，卡片锁死报废。

9.8.5 SLE4428 卡操作：

在对 SLE4428(读写等)操作，所使用的命令数据是通过类似于 ISO/IEC 7816 T=0 标准数据交换命令(C-APDU)形式进行操作。

因此，卡机收到指定含义的命令数据后再执行对卡片相应操作。当命令执行成功，在正常返回数据包中增加 9000H；命令执行中出现错误，在正常返回中只返回类似于 ISO/IEC 7816-3 T=0 标准规范中“sw1+sw2”两个错误响应码。

Sw1	Sw2	说　明
90H	00H	操作成功
6FH	00H	操作失败
6FH	01H	密码校验失败
6FH	02H	密码校验失败，卡锁死
6BH	00H	操作地址溢出
67H	00H	操作长度溢出

9.8.5.1. 读 SLE4428 主存贮区：

HOST 命令:

“C”	53H	34H	00H	B0H	0aH	bcH	deH

正常返回:

“P”	53H	34H	st0	st1	st2	data

错误返回:

“N”	53H	34H	e1	e0

其中： abc: 读主存贮区起始地址

de: 读数据操作长度

卡机通过指定的 abcH 和 deH 参数对 SLE4428 卡主存贮区进行读取。

SLE4428 卡主存贮区容量为 1024 byte.

当 de=00H 时读取 256 byte 数据 通过

下列命令读取 SLE4428 卡数据。

Ex). “CR3”+00B0000000

9.8.5.2. 读 SLE4428 保护位数据：

HOST 命令:

“C”	53H	34H	00H	B0H	10H	abH	cdH

正常返回:

“P”	53H	34H	st0	st1	st2	data

错误返回:

“N”	53H	34H	e1	e0

其中： ab: 读保护区起始地址

cd: 读数据操作长度

SLE4428 卡在主存贮区有写保护功能的单元有 1024 byte.对应写保护位数据有 1024 bit. 在读保护位时等同于 128 byte (1024=128 x 8).

保护位数据从址地以 000H—007H 组成 1 byte 保护位数据。

下列命令读取全部保护位数据。

Ex). “CR4”+00B0100080

卡机根据 abH 参数指定起始地址读取 cdH 长度的保护位数据。

9.8.5.3 写主存贮区数据：

HOST 命令:

“C”	53H	34H	00H	D0H	0aH	bcH	deH	fgH…

正常返回:

“P”	53H	34H	st0	st1	st2	data

错误返回:

“N”	53H	34H	e1	e0

其中： abc: 写主存贮区起始地址
de: 写数据操作长度
fg: 要写数据

对 SLE4428 卡主存贮区进行写数据，将指定的数据写入主存贮区，卡机写完数据进行校验后返回操作结果。
在进行写数据之前，必须正确校验 SLE4428 卡密码.
SLE4428 卡存贮容量为 1024 byte.
下列命令写存贮区 256 byte：
Ex). “CR4”+00D000000+Write data(256 byte)

当命令执行后，返回 9000H(操作成功)或 sw1,sw2(操作失败)结果。 当指
定要写入数据是在写保护区且处于写保护状态，数据将不能被写入。

9.8.5.4 带校验写数据：

HOST 命令:

“C”	53H	34H	00H	D0H	1aH	bcH	deH	fgH…

正常返回:

“P”	53H	34H	st0	st1	st2	data

错误返回:

“N”	53H	34H	e1	e0

其中： abc: 写主存贮区起始地址
de: 写数据操作长度
fg: 要写数据(deH byte)

对 SLE4428 卡进行写数据，将指定的数据写入主存贮区，卡机写完数据进行校验后返回操作结果。
在进行写数据之前，必须正确校验 SLE4428 卡密码.

9.8.5.5 带保护位写数据：

HOST 命令:

“C”	53H	34H	00H	D0H	2aH	bcH	deH	fgH…

正常返回:

“P”	53H	34H	st0	st1	st2	data

错误返回:

“N”	53H	34H	e1	e0

其中： abc: 带写保护写操作起始地址
de: 写数据操作长度
fg: 要写数据(deH byte)

对主存贮区带写护的存贮单元进行写保护。在执行此命令前，必须正确校验 SLE428 卡密码。

当命令执行后，返回 9000H(操作成功)或 sw1,sw2(操作失败)结果。 卡机首先从主存贮区读出数据，与接收到要写入数据进行比较，当比较数据不相同时，停止带写保护操作。带写保护 功能只允许写入数据与卡中存贮数据相同时才能进行写保护。

9.8.5.6 校验 **4428** 卡密码**:**

HOST 命令:

“C”	53H	34H	00H	20H	00H	00H	02H	efH…

正常返回:

“P”	53H	34H	st0	st1	st2	data

错误返回:

“N”	53H	34H	e1	e0

其中： ef: 密码数据(2 byte)

要更改 SLE4442 卡数据，必须先校验卡密码。因为这是卡片功能要求，是下一个发行操作命令必须操作。

Ex). “CR3”+0020000002xxxx (xxxx 2 byte 密码数据)

卡片将它本身存贮的密码数据与命令中数据进行比较。

用户要改写 SLE4442 卡数据必须知道卡的密码，密码错误计数器值会从 7 或小于 7 的值直至复位成零，当错误计数值为零时，卡片锁死报废。

9.9 I2C Memory Card 操作：

9.9.1 I2C 卡上电复位(激活)：

HOST 命令:

“C”	54H	30H	Wrd	Vcc

正常返回:

“P”	54H	30H	st0	st1	st2

错误返回:

“N”	54H	30H	e1	e0

对 I2C(24C01,24C02,24C04,24C08,24C16,24C32,24C64,24C128,24C256)卡复位激活。
卡机提供电源(VCC)，时钟信号(CLK)，和复位信号(RST) 给卡.
其中：

Wrd 设定 I2C 卡类型
Wrd =30 H 对(24C01,24C02,24C04,24C08,24C16,24C32,24C64,24C128,24C256)卡自动激活
Wrd =31 H 对 24C01 卡激活
Wrd =32 H 对 24C02 卡激活
Wrd =33 H 对 24C04 卡激活
Wrd =34 H 对 24C08 卡激活
Wrd =35 H 对 24C16 卡激活
Wrd =36 H 对 24C32 卡激活
Wrd =37 H 对 24C64 卡激活
Wrd =38 H 对 24C128 卡激活
Wrd =39 H 对 24C256 卡激活

Vcc 选择对卡片供给的电压
Vcc=30H 卡机提供 5V 电压来复位激活卡片
Vcc=31H 卡机提供 3V 电压来复位激活卡片
Vcc 是可选参数，命令中无 Set 参数，等效同 Set=30H

9.9.2 I2C 卡下电(释放)：

HOST 命令:

“C”	54H	31H

正常返回:

“P”	54H	31H	st0	st1	st2

错误返回:

“N”	54H	31H	e1	e0

卡机停止电源(VCC)，时钟信号(CLK)，和复位信号(RST) 给卡,卡被下电释放.

9.9.3 I2C 卡查状态：

HOST 命令:

“C”	54H	32H

正常返回:

“P”	54H	32H	st0	st1	st2	Sti

错误返回:

“N”	54H	32H	e1	e0

该命令用于查询卡的状态，正确执行后，返回的 Sti 中显示状态

Sti 状态含义：

Sti=30 H 无 I2C 卡激活
Sti=31 H 24C01 卡激活
Sti=32 H 24C02 卡激活
Sti=33 H 24C04 卡激活
Sti=34 H 24C08 卡激活
Sti=35 H 24C16 卡激活
Sti=36 H 24C32 卡激活
Sti=37 H 24C64 卡激活
Sti=38 H 24C128 卡激活
Sti=39 H 24C256 卡激活

9.9.4 I2C 卡读写操作：

在对 I2C 卡(读写等)操作，所使用的命令数据是通过类似于 ISO/IEC 7816 T=0 标准数据交换命令(C-APDU)形式进行操作。

因此，卡机收到指定含义的命令数据后再执行对卡片相应操作。当命令执行成功，在正常返回数据包中增加 9000H；命令执行中出现错误，在正常返回中只返回类似于 ISO/IEC 7816-3 T=0 标准规范中“sw1+sw2”两个错误响应码。

Sw1	Sw2	说 明
90H	00H	操作成功
6FH	00H	操作失败
6BH	00H	操作地址溢出
67H	00H	操作长度溢出

读写 I2C 卡时应注意相应读写操作地址范围,见下表

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

9.9.4.1 读 I2C 卡数据:

HOST 命令:

“C”	54H	33H	00H	B0H	abH	cdH	efH

正常返回:

“P”	54H	33H	st0	st1	st2	Data

错误返回:

“N”	54H	33H	e1	e0

其中： ab: 读操作高字节地址
cd： 读操作低字节地址
ef: 读操作长度

卡机根据 abH,cdH 指定起始地址,读取 efH 指定长度 I2C 卡数据返回给 HOST。efH 指定操作长度不能超过 I2C 卡地址范围上限。

下列命令从 I2C 卡中读取数据：(从卡中读取 8 byte 数据)

Ex). “CU3”+00B0000008

9.9.4.2 写 I2C 卡数据:

HOST 命令:

“C”	54H	34H	00H	D0H	abH	cdH	efH	ghH…

正常返回:

“P”	54H	34H	st0	st1	st2	Data

错误返回:

“N”	54H	34H	e1	e0

其中： ab: 写操作高字节地址
cd： 写操作低字节地址
ef: 写操作长度
gh: 写数据(efH byte)

卡机根据 abH,cdH 指定起始地址,写 efH 指定长度数据写到 I2C 卡。efH 指定操作长度不能超过 I2C 卡地址范围上限。

下列命令写 8 byte 数据到 I2C 卡:

Ex). “CU3”+00B0000008+ write data(8 byte)

当命令执行后，返回 9000H(操作成功)或 sw1,sw2(操作失败)结果。

9.10 射频卡(Contactless IC card)操作：

9.10.1 射频卡复位激活：

HOST 命令:

“C”	60H	30H	Set1	Set2

(1) Mafare one 卡正常返回：

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

Mafare one 卡错误返回:

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

(2) 14443 type A 卡正常返回：

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

14443 type A 卡错误返回:

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

(3) 14443 type B 卡正常返回:

“P”	60H	30H	st0	st1	st2	Rtype	ATQB

14443 type b 卡错误返回:

“N”	60H	30H	e1	e0	Rtype	ATQB

对射频卡进行复位激活。
卡机支持对 IEC/ISO14443 Type A 和 IEC/ISO 14443 Type B 卡进行复位激活。
卡机对射频卡执行复位激活处理过程如下：

1).Mifare one card:
1. Request A(REQ A) / Answer Request A (ATQ A).
2. Anticollision
3. Select(SEL) / Unique Identifier(UID) & Select Acknowledge(SAK)

当 Mifare card 被成功激活时，卡机返回:
请求应答 ATQA(2 byte),卡片序列号 UID_data (4—10 byte) 和 选卡应答 SAK(1 byte).

2).ISO/IEC 14443 Type A:
1. Request A(REQ A) / Answer Request A (ATQ A).
2. Anticollision
3. Select(SEL) / Unique Identifier(UID) & Select Acknowledge(SAK)
4. Request for answer to select (RATS) / Answer to Select(ATS)
5. Protcol and parameter selection request(PPSR) / PPS start(PPSS)

当 ISO/IEC 14443 Type A card 被成功激活，卡机返回:
在 Mifare card 返回值增加请求应答 ATS(1-254 byte)和协议参数选择(1 byte)。

3).ISO/IEC 14443 Type B:
1. Request B(REQ B) / Answer Request B (ATQ B).
2. Attribute(A TTRIB) / Answer to ATTRIB

当 ISO/IEC 14443 Type B card 被成功激活，卡机返回 ATQB 12 byte (包含以下信息):
50H, PUPI(4 byte) , App.data(4 byte), Protoclol info(3 byte)

其中：

Set1,Set2 设定操作不同协议的射频卡复位激活操作顺序。

其有效值为：41H (‘A’= Type A)，42H(‘B’= Type B), 30H(‘0’= 不使用)

Ex1：Set1=‘A’，Set2 =‘B’ (默认)

指在复位激活操作顺序为： Type A 协议 为第一复位激活顺序，Type B 协议 为第二复位激活顺序

Ex2：Set1=‘B’，Set2 =‘A’

指在复位激活操作顺序为： Type B 协议 为第一复位激活顺序，Type A 协议 为第二复位激活顺序

Ex3：Set1=‘A’，Set2 =‘0’

指在复位激活操作顺序为： Type A 协议 为第一复位激活顺序，Type B 协议为不激活.

Ex4：Set1=‘B’，Set2 =‘0’，

指在复位激活操作顺序为： Type B 协议 为第一复位激活顺序，Type A 协议为不激活.

Rtype: 当前激活卡的协议。

= 41H (‘A’) 当前卡片符合 ISO/IEC 14443 Type A 协议.

= 42H (‘B’) 当前卡片符合 ISO/IEC 14443 Type B 协议.

= 4DH (‘M’) 当前卡片符合 Philps Mifare one card 协议.

当 Rtype=4DH(‘M’) 时:

ATQA= 0044H 卡片为 Mifare Ultralight Card

ATQA= 0004H 卡片为 Mifare S50 1K Card

ATQA= 0002H 卡片为 Mifare S70 4K Card

Mafare one, ISO/IEC 14443 Type A 卡返回的 UID_len 指定返回卡片序列号 UID_data 信息长度。

UID_len=4 表示返回卡片序列号 UID_data 信息长度为 4 byte

UID_len=7 表示返回卡片序列号 UID_data 信息长度为 7 byte

UID_len=10 表示返回卡片序列号 UID_data 信息长度为 10 byte

9.10.2 射频卡下电释放：

HOST 命令:

“C”	60H	31H

正常返回:

“P”	60H	31H	st0	st1	st2

错误返回:

“N”	60H	31H	e1	e0

对射频卡下电释放,RF 模块芯片对天线输出信号全部关闭。

9.10.3 射频卡查状态：

HOST 命令:

“C”	60H	32H

正常返回:

“P”	60H	32H	st0	st1	st2	sti	stj

错误返回:

“N”	60H	32H	e1	e0

查当前射频卡状态 sti,stj：

sti	stj	说　明
‘0’	‘0’	没有 RF 卡激活
‘1’	‘0’	Mifare one S50 卡
	‘1’	Mifare one S70 卡
	‘2’	Mifare one UL 卡
‘2’	‘0’	Type A CPU 卡
‘3’	‘0’	Type B CPU 卡

9.10.4 **Mifare 1 card** 卡操作：

在对 Mifare 1 卡(读写等)操作，所使用的命令数据是通过类似于 ISO/IEC 7816 T=0 标准数据交换命令(C-APDU)形式进行操作。

因此，卡机收到指定含义的命令数据后再执行对卡片相应操作。当命令执行成功，在正常返回数据包中增加 9000H；命令执行中出现错误，在正常返回中只返回类似于 ISO/IEC 7816-3 T=0 标准规范中“sw1+sw2”两个错误响应码。

Sw1	Sw2	说　明
90H	00H	操作成功
6FH	00H	操作失败
6BH	00H	操作地址溢出
67H	00H	操作长度溢出

9.10.4.1 校验密码**:**

HOST 命令:

“C”	60H	33H	00H	20H	ks	sn	lc	pdata

正常返回:

“P”	60H	33H	st0	st1	st2	rdata

错误返回:

“N”	60H	33H	e1	e0

下载密码到卡机中直接校验指定扇区的密码.

ks(1byte): key select 密码类型字选择 (Key A=00H，Key B=01H)

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

lc(1byte): 密码数据长度 lc=06H

pdata(6 byte): password data 密码数据

rdata(2 byte): return data 操作返回结果.操作成功返回 9000.操作失败仅返回 sw1+sw2(2 byte).

9.10.4.2 从 **EEPROM** 中加载密码校验**:**

HOST 命令:

“C”	60H	33H	00H	21H	ks	sn

正常返回:

“P”	60H	33H	st0	st1	st2	rdata

错误返回:

“N”	60H	33H	e1	e0

从卡机 RF 模块 EEPROM 读取已存贮的密码来校验指定扇区的密码.

通过 9.10.4.4 命令对密码预先下载到 EEPROM 中

卡机中的 RF 模块 EEPROM 能存储 32 组密码数据.

ks(1byte): key select 密码类型字选择 (Key A=00H，Key B=01H)

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

rdata(2 byte): return data 操作返回结果.操作成功返回 9000H

9.10.4.3 修改扇区密码(KEY A):

HOST 命令:

“C”	60H	33H	00H	D5H	00H	sn	lc	pdata

正常返回:

“P”	60H	33H	st0	st1	st2	rdata

错误返回:

“N”	60H	33H	e1	e0

对扇区密码 **KEY A** 进行修改。

执行该命令只能对 KEY A 的密码更改操作，并对 KEY B 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)。

需要对 KEY A ， KEY B ，控制字进行更改，使用块写命令来操作.

sn(1byte): sector number 扇区号 (S50 card sn=00H-0FH, S70 card sn=00H-27H)
lc(1byte): 密码数据长度 lc=06H

pdata ： password data 新密码数据 6 byte**.**
rdata(2 byte): return data 操作返回结果.操作成功返回 9000.操作失败仅返回 sw1+sw2(2 byte).

9.10.4.4 下载密码到 **EEPROM:**

HOST 命令:

“C”	60H	33H	00H	D0H	ks	sn	lc	pdata

正常返回:

“P”	60H	33H	st0	st1	st2	rdata

错误返回:

“N”	60H	33H	e1	e0

下载密码到卡机中 RF 模块 EEPROM 中.用于直接加载密码校验扇区密码
卡机中的 RF 模块 EEPROM 能存储 32 组密码数据.

ks(1byte):	key select 密码类型字选择	(Key A=00H， Key B=01H)
sn (1byte):	sector number 扇区号	(sn=00H-0FH)
lc(1byte):	密码数据长度 lc=06H	
pdata(6 byte):	password data 密码数据	
rdata(2 byte):	return data 操作返回数据. 操作	
	成功返回 sw1+sw2=9000H. 操作	
	失败返回 sw1+sw2=6F00H	

9.10.4.4 读扇区块数据**:**

HOST 命令:

“C”	60H	33H	00H	B0H	sn	bn	le

正常返回:

“P”	60H	33H	st0	st1	st2	rdata

错误返回:

“N”	60H	33H	e1	e0

从 RF 卡扇区读取一个块数据或连续读取多个块数据.

sn(1 byte): sector number 操作扇区号

bn(1 byte): block number 操作起始块号

le(1 byte): block number 操作块长度 (le=01H 读取扇区一个块数据，le=03H 读取扇区三个块数据)

rdata(2 byte): return data 操作返回结果.操作成功返回读到块数据+9000H. 操作失败仅返回 sw1+sw2(2 byte).

注：

1.Ultralight Card 每一个扇区仅有一个块，每块的仅有 4 byte 的数据.S50,S70 卡每个块有 16 byte 数据

2.Ultralight Card,Mifare 1k(S50), Mifare 1k (S70) card 操作扇区号，操作起始块号, 操作块长度的取值范围，不能超过卡片容量范围.

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

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

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

sn=21H-27H, bn=00H-0FH, le=01H-10H(S70 card 在最后 8 个扇区中是每一个扇区是 16 块)

9.10.4.5 写扇区块数据**:**

HOST 命令:

“C”	60H	33H	00H	D1H	sn	bn	lc	wdata

正常返回:

“P”	60H	33H	st0	st1	st2	rdata

错误返回:

“N”	60H	33H	e1	e0

对 RF 卡扇区写一个块数据或连续写多个块数据.

sn(1 byte): sector number 操作扇区号

bn(1 byte): block number 操作起始块号

le(1 byte): block number 操作块长度

wdata: 要写的块数据(n byte)

rdata(2 byte): return data 操作返回结果.操作成功返回读到块数据+9000H. 操作失败仅返回 sw1+sw2(2 byte).

注：

1.Ultralight Card 每一个扇区仅有一个块，每块的仅有 4 byte 的数据;S50,S70 卡每个块有 16 byte 数据

2.Ultralight Card,Mifare 1k(S50), Mifare 1k (S70) card 操作扇区号，操作起始块号, 操作块长度的取值范围，不能超过卡片容量的范围.

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

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

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

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

(S70 card 在最后 8 个扇区中是每一个扇区是 16 块)

3.S50,S70 card 每一个扇区的最后一块是该扇区的控制块，存贮 Key A 密码，读写控制字，Key B 密码。

在多个块写时应注意不要误写这个块,卡机也禁止在连续写多个块数据时操作扇区最后一个块。

9.10.4.6 值初始化操作:

HOST 命令:

“C”	60H	33H	00H	D2H	sn	bn	lc	wdata

正常返回:

“P”	60H	33H	st0	st1	st2	rdata

错误返回:

“N”	60H	33H	e1	e0

对 RF 卡扇区的块进行初始化值操作.

sn(1 byte): sector number 操作扇区号

bn(1 byte): block number 操作起始块号

lc(1byte): 值初始化数据长度 lc=04H

wdata: 值初始化数据(4 byte)

rdata(2 byte): return data 操作返回结果.操作成功返回 9000H. 操作失败仅返回 sw1+sw2(2 byte).

注：Mifare 1k(S50), Mifare 1k (S70) card 操作扇区号，操作起始块号,不能超过卡片容量的范围.且每一扇区的最后一块是不能进行值操作.

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

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

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

(S70 card 在最后 8 个扇区中是每一个扇区是 16 块)

9.10.4.7 读值:

HOST 命令:

“C”	60H	33H	00H	B1H	sn	bn

正常返回:

“P”	60H	33H	st0	st1	st2	rdata

错误返回:

“N”	60H	33H	e1	e0

对 RF 卡扇区的块进行读值操作.

sn(1 byte): sector number 操作扇区号

bn(1 byte): block number 操作起始块号

rdata: return data 操作返回结果.操作成功返回读到值数据(4 byte)+9000H.

操作失败仅返回 sw1+sw2(2 byte).

注：Mifare 1k(S50), Mifare 1k (S70) card 操作扇区号，操作起始块号,不能超过卡片容量的范围.且每一扇区的最后一块是不能进行值操作.

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

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

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

(S70 card 在最后 8 个扇区中是每一个扇区是 16 块)

9.10.4.8 增值:

HOST 命令:

“C”	60H	33H	00H	D3H	sn	bn	lc	wdata

正常返回:

“P”	60H	33H	st0	st1	st2	rdata

错误返回:

“N”	60H	33H	e1	e0

对 RF 卡扇区的块进行增值操作.

sn(1 byte): sector number 操作扇区号
bn(1 byte): block number 操作起始块号
lc(1byte): 增值数据长度 lc=04H
wdata: 增值数据(4 byte)
rdata: return data 操作返回结果.操作成功返回 9000H.
操作失败仅返回 sw1+sw2(2 byte).

注：Mifare 1k(S50), Mifare 1k (S70) card 操作扇区号，操作起始块号,不能超过卡片容量的范围.且每一扇区的最后一块是不能进行值操作.

Mifare 1k(S50): sn=00H-0FH, bn=00H-03H,
Mifare 1k(S70): sn=00H-20H, bn=00H-03H,
sn=20H-27H, bn=00H-0EH,
(S70 card 在最后 8 个扇区中是每一个扇区是 16 块)

9.10.4.9 减值:

HOST 命令:

“C”	60H	33H	00H	D4H	sn	bn	lc	wdata

正常返回:

“P”	60H	33H	st0	st1	st2	rdata

错误返回:

“N”	60H	33H	e1	e0

对 RF 卡扇区的块进行减值操作.

sn(1 byte): sector number 操作扇区号
bn(1 byte): block number 操作起始块号
lc(1byte): 减值数据长度 lc=04H
wdata: 减值数据(4 byte)
rdata: return data 操作返回结果.操作成功返回 9000H.
操作失败仅返回 sw1+sw2(2 byte).

注：Mifare 1k(S50), Mifare 1k (S70) card 操作扇区号，操作起始块号,不能超过卡片容量的范围.且每一扇区的最后一块是不能进行值操作.

Mifare 1k(S50): sn=00H-0FH, bn=00H-03H,
Mifare 1k(S70): sn=00H-20H, bn=00H-03H,
sn=20H-27H, bn=00H-0EH,
(S70 card 在最后 8 个扇区中是每一个扇区是 16 块)

9.10.5 Type A RF card 通讯:

HOST 命令:

“C”	60H	34H	C-APDU

正常返回:

“P”	60H	34H	st0	st1	st2	R-APDU

错误返回:

“N”	60H	34H	e1	e0

该命令是按 ISO/IEC 14443-4 规范,执行对 RF Type A T=CL 协议的卡进行数据交换操作.

注： C-APDU 包最大长度为 261 byte; R-APDU 包最大长度为 258 byte.

9.10.6 Type B RFcard 通讯:

HOST 命令:

“C”	60H	35H	C-APDU

正常返回:

“P”	60H	35H	st0	st1	st2	R-APDU

错误返回:

“N”	60H	35H	e1	e0

该命令是按 ISO/IEC 14443-4 规范,执行对 RF Type B T=CL 协议的卡进行数据交换操作.

注： C-APDU 包最大长度为 261 byte; R-APDU 包最大长度为 258 byte.

9.11 读写卡机序列号**:**

9.11.1 读卡机序列号**:**

HOST 命令:

“C”	A2H	30H

正常返回:

“P”	A2H	30H	st0	st1	st2	len	ICRW_SN

错误返回:

“N”	A2H	30H	e1	e0

对 RF 卡进行睡眠/唤醒操作

Set=30H 对 RF 卡进行睡眠操作

Set=31H 对 RF 卡进行唤醒操作

len: 读出卡机序列号数据长度(最小为 0 字节，最大为 18 字节)

ICRW_SN: 卡机序列号

9.11.2 写卡机序列号**:**

略

9.12 读卡机配置信息**:**

HOST 命令:

“C”	A3H	30H

正常返回:

“P”	A3H	30H	st0	st1	st2	ICRW_Config

错误返回:

“N”	A3H	30H	e1	e0

读取卡机配置信息说明： ICRW_Config: 读取卡机配置信息(S1-S10 总共 10 字节)。

Name	Value	Description	说明
S1		ACT Reader Type option	ACT 读卡器标识字
	“7”	S1 =“7”	ACT-571 标识字 S1=37H
S2/S3/S4 (3 Byte)		User Code option	客户软件代码
	“V10”	ACT version	ACT 标准程序
	“XXX”		客户定制版本
S5		Card r/w type option	读卡器支持卡操作类型
	“0”		有发卡功能无读写卡功能
	“I”	IC card r/w	仅支持接触式 IC 卡读写
	“C”	RF card r/w	仅支持 RF 卡读写
	“E”	IC + RF card r/w	支持 IC 卡+RF 卡读写操作
S6		Interface type option	通讯接口类型
	“R”	RS-232Interface type	RS-232 通讯接口
S7		IC card write type	IC 卡读写功能类型
	“0”		无 IC 卡读写
	“1”		有 IC 卡触点组件,供第三方模块使用
	“2”		ACT 标准 IC 卡读写
S8		RF card write type	RF 卡读写功能类型
	“0”		无 RF 卡读写
	“1”		有 RF 卡天线组件,供第三方模块使用
	“2”		ACT 标准 RF 卡读写
S9		SAM option	
	“0”	Not SAM	无 SAM 卡操作功能
	“1”	SAM 1	支持一个 SAM 卡操作
	“2”	SAM 2	支持二个 SAM 卡操作
	“3”	SAM 3	支持三个 SAM 卡操作
	“4”	SAM 4	支持四个 SAM 卡操作
	“5”	SAM 5	支持五个 SAM 卡操作
S10			发卡组件类型
	“0”		搓卡组件发卡
	“1”		拔卡组件发卡

9.13 卡机版本信息读取:

HOST 命令:

“C”	A4H	Pm

正常返回:

“P”	A4H	30H	st0	st1	st2	Rev

错误返回:

“N”	A4H	30H	e1	e0

读取卡机软件相关版本信息.

Pm=30H 读取卡机软件版本信息
Ex: Rev =“C571_V1.00_A_090910”

Pm=31H 读取 IC 卡软件版本信息
Ex: Rev =“ICCARD_V10_A_090910”

Pm=32H 读取 RF 卡软件版本信息
Ex: Rev =“RFCARD_V10_A_090910”

9.14 回收卡计数器操作:

9.14.1 读回收卡计数器值

HOST 命令:

“C”	A5H	30H

正常返回:

“P”	A5H	30H	st0	st1	st2	Count(3 byte)

错误返回:

“N”	A5H	30H	e1	e0

读取回收卡计数值，当在复位命令启动回收卡计数器工作后，每回收一张卡，计数值加一。

Count= “000” ~ “999”

回收卡计数值 最小为 0 张，最大为 999 张。回收卡计数值超过 999 次后报回收卡计数溢出错误(e1,e0=“50”)

9.14.2 设置回收卡计数器初值

HOST 命令:

“C”	A5H	31H	Count(3 byte)

正常返回:

“P”	A5H	31H	st0	st1	st2

错误返回:

“N”	A5H	31H	e1	e0

设置回收卡的计数初值.

Count= “000” ~ “999”

回收卡计数值 最小为 0 张，最大为 999 张。