类别	内容
关键词	ZSN603、ISO14443、ISO7816
摘要	本文档介绍了芯片的基本功能特性、芯片典型应用框图、通信协议及各命令详解，可指导用户正确使用芯片

修订历史

版本	日期	原因
1.0.00	2019/08/30	创建文档
1.0.01	2019/10/14	修改部分描述
1.0.02	2020/3/14	修改文档归类编码
1.0.03	2020/4/12	修改文档模板
1.0.04	2020/12/12	修改文档模板

目 录

1. 产品简介

1.1 产品概述

ZSN603 读卡专用芯片是广州致远微电子有限公司开发的一款集成了卡操作指令的芯片，用户不需要进行编程，只需要发送简单的命令，即可完成对卡片的读写。外部电路设计简单，可以快捷、高效地开发出产品。

ZSN603 读卡专用芯片采用 LGA 封装形式，厚度 1.05mm，引脚间距 0.8mm。可以帮助客户绕过繁琐的 RFID 硬件设计、开发与生产，加快产品上市。完善的软件开发平台可满足快速开发需求，减少软件投入，缩短研发周期。

1.2 功能特点

- 符合 ISO14443A、ISO14443B、ISO7816-3 标准；
- 集成 TypeB、Mifare UltraLight、Mifare S50/S70、PLUS CPU、SAM 卡的操作指令；
- 提供 ISO14443-4 的半双工块传输协议接口，可支持符合 ISO14443-4A 的 CPU 卡及符合 ISO14443-4B 的 TypeB 卡片；
- 支持串口、I^2C 两种通信接口，支持多种串口工作波特率；
- 可主动检测卡进入，检测到卡时可产生中断并且通过串口、I^2C 输出数据；
- 支持配合通道芯片拓展多路天线的应用，最多可拓展八路天线。

1.3 技术参数

表 1.1 ZSN603 技术参数表

产品型号	ZSN603
功率消耗	平均电流：3.3V 直流供电/73mA 峰值电流：小于 150mA
工作频率	13.56MHz
读卡距离	标准大小的 TypeA 卡：7cm （天线尺寸为 5 cm×5cm） 标准大小的 TypeB 卡：3cm ~4cm （增大天线大小，理论上读卡距离还能得到提升；同类型卡片中，卡片越小，读写距离会越短）
对外接口	I^2C、UART
数据传输速率	I^2C：300K UART：2400～9600bit/s
支持卡类型	接触式：SAM 卡 非接触式：Mifare 1 S50、Mifare 1 S70、Mifare UltraLight、Mifare Desfire、符合 ISO14443A 的逻辑加密卡和 CPU 卡、符合 ISO14443B 的卡片
物理特性	尺寸：9mm×9mm 封装：LGA 封装
环境	工作温度： -40～85 摄氏度

1.4 芯片尺寸

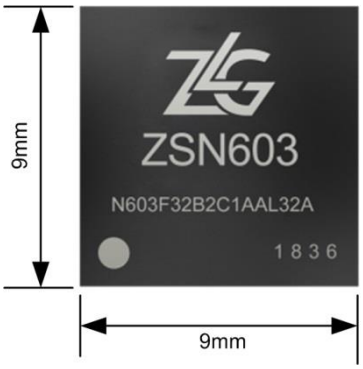

图 1.1 ZSN603 外形尺寸

1.5 引脚分布

ZSN603 芯片的引脚定义如图 1.2 所示。

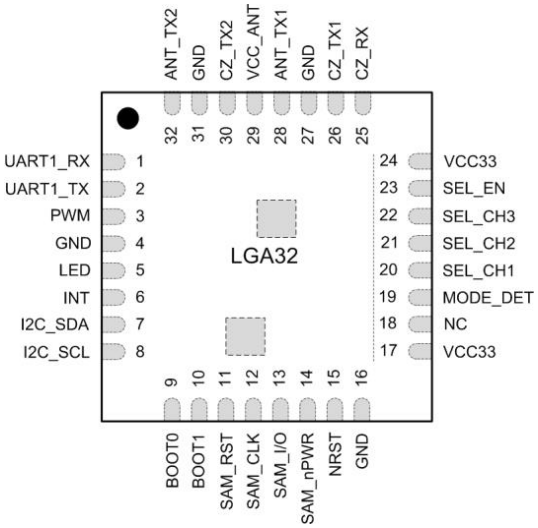

图 1.2 引脚分布图

1.6 典型应用

I^2C 工作模式下，ZSN603 芯片的典型应用如图 1.3 所示，MODE_DET 引脚必须设置为低电平，ZSN603 芯片才能在复位后自动进入 I^2C 工作模式。主机至少需要使用 4 个引脚与 ZSN603 相连，I^2C 接口和 INT 用于完成命令通信，nRST 用于实现 ZNS603 的复位控制。使用复位引脚能使 ZSN603 芯片更好的适应各种强干扰场合的应用，保证整机设备的稳定运行。

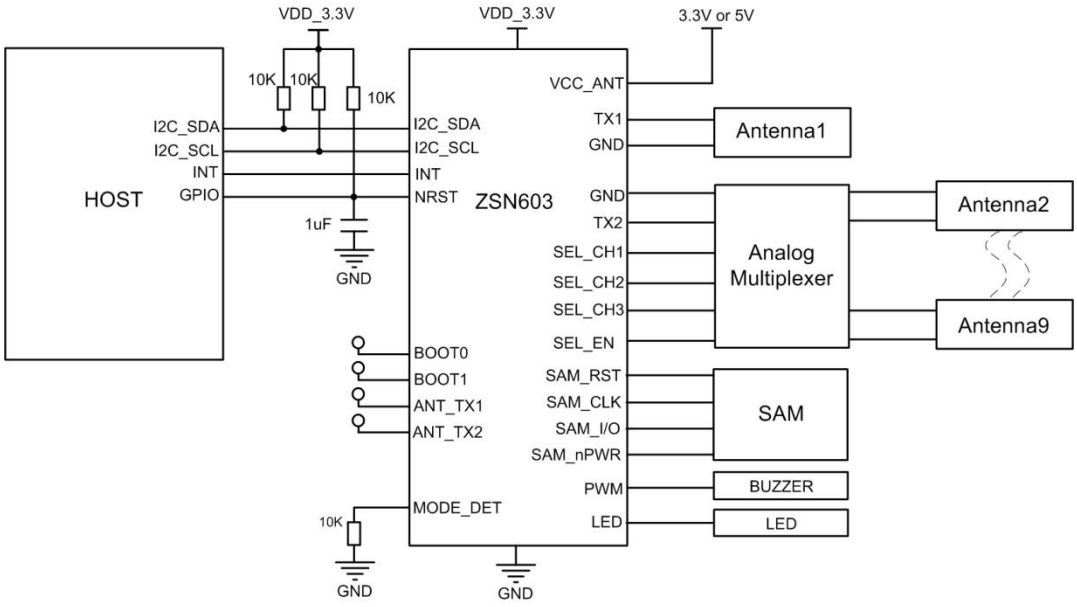

图 1.3　I²C 模式下的典型应用框图

UART 工作模式下，ZSN603 的典型应用如图 1.4 所示，MODE_DET 引脚需要设置为高电平，ZSN603 芯片才能在复位后自动进入 UART 工作模式，出厂芯片默认的通信波特率为 9600。

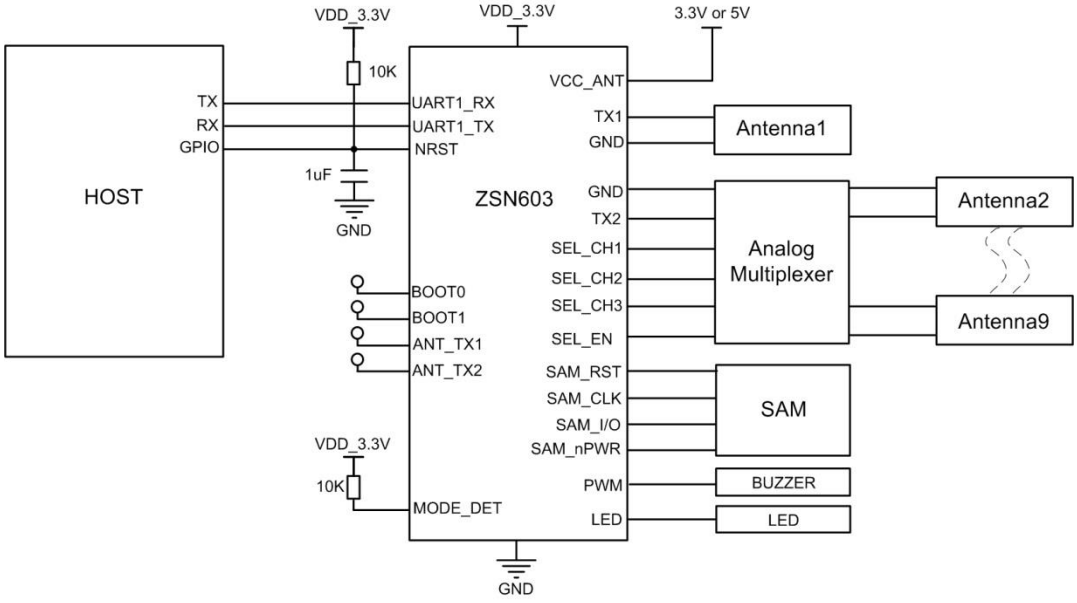

图 1.4　UART 模式下的典型应用框图

无论 ZSN603 工作在哪种模式，在芯片硬件设置时都需要注意以下两点：

- ZSN603 的 BOOT0、BOOT1、ANT_TX1、ANT_TX2 四个引脚需要在 PCB 布线时预留圆形测试点；
- 通常 VCC_ANT 引脚的供电电压为 3.3V，但如果实际应用当中有读取二代身份证的需求，建议采用 5V 供电并使用我司配套的天线板，以达到更好的读卡效果。

2. 通讯协议

本芯片有两种不可同时使用的通信接口：UART 和 I²C 接口。外部主机与芯片通过这两种接口通信，必需按照规定的协议进行。本芯片以命令——响应方式工作，在系统中芯片属于从属地位，不会主动发送数据（响应自动检测卡命令除外），通常首先由主机发出命令，然后等待芯片响应。

2.1 各通信模式介绍

2.1.1 UART 模式

当芯片上电时检测到 MODE_DET 引脚为高电平时，芯片进入 UART 通信模式，芯片出厂默认的通信波特率为 9600。UART 接口的数据格式为：1 个起始位、8 个数据位、无奇偶校验位、1 个停止位。ZSN603 可以设置的波特率有 2400、4800、9600。主机与 ZSN603 建立有效通信后，便可对 ZSN603 进行波特率设置。待主机收到设置波特率成功的回应帧后，主机便可以用新设置的波特率发送命令。

UART 通信模式下，主机向芯片发送命令，芯片收到命令后解析并执行，执行完毕后主动将数据发送给主机。若命令错误，则芯片直接丢弃接收到的数据，且不做任何回应。

2.1.2 I²C 模式

当芯片上电时检测到 MODE_DET 引脚为低电平时，芯片进入 I²C 通信模式，支持最高 300KHz 的硬件 I²C 接口，从机地址可设为：0xB0、0xB2、0xB4、0xB6 等，芯片出厂默认地址为 0xB2。只要从机地址正确，速率合适，则芯片可有效地收到主机命令，待芯片执行命令完成，会输出中断信号（/INT 脚变低），通知主机读取响应。

通信过程中，ZSN603 芯片是充当 I²C 通信中的 Slave 角色，而外部 MCU 则是 Master，具体数据格式如图 2.1 和图 2.2 所示：

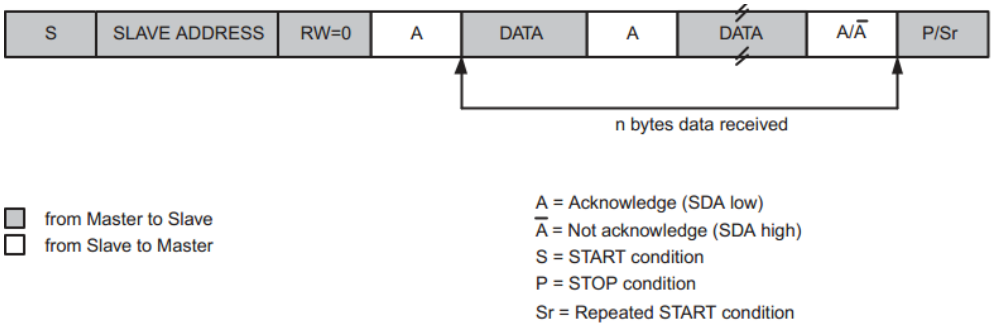

图 2.1　数据流向 Master to Slave

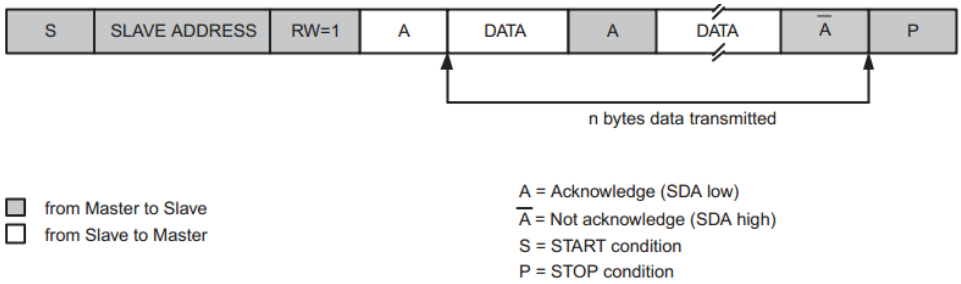

图 2.2　数据流向 Slave to Master

2.2 通信超时

串口通信过程中如果 ZSN603 在 4 毫秒内未接收到下一个字节，则本次通信接收完毕，进入数据处理阶段，处理完毕后，恢复正常通信。

I^2C 在通信过程中由于干扰，误操作等情况，会出现死锁的现象，导致主机无法正常与芯片通信，针对这类情况，I^2C 在通信过程中添加了超时机制，字节之间时间超过 4ms 会导致超时发生。当超时发生时，接收方会终止当前 I^2C 通信过程，返回 NACK，复位内部硬件 I^2C。对于主机而言，需要再发起一次 I^2C 通信，重复发送上一次的命令。

2.3 新帧格式

新帧格式根据 I^2C、UART 两种不同的通信接口，在使用上稍有不同，新帧格式的通信协议分为 2 层，分别如下。

- 物理链路层
- 协议层

其中，I^2C 通信接口必需符合这两层定义，而 UART 通信接口忽略物理链路层，只需按照协议层即可。

2.3.1 新帧格式物理链路层

物理链路层是基于 I^2C 的有器件子地址模式，器件地址固定为 0xB2，器件子地址为 2 字节。存储/数据交互空间为 542 字节，其中前 256 字节为保留使用，后 286 字节为命令帧/回应帧使用。详细描述见表 2.1 所示。

表 2.1 芯片存储空间分配

子地址	意义	备注
0x0000~0x00FF	保留使用	—
0x0100	保留对齐使用	无特殊意义，任意读写
0x0101	主机控制/芯片状态	写入‘STATUS_EXECUTING’（0x8D） 将启动芯片执行地址 0x0104~0x021D 中的命令（命令在写入结束后才开始执行），写入其他值芯片无动作 读出是芯片当前的状态： STATUS_EXECUTING（0x8D） —— 命令还未执行 STATUS_BUSY（0x8C） —— 命令正在执行 STATUS_IDLE （0x8A） —— 芯片空闲 其他值 —— 执行结果
0x0102~0x0103	命令/回应帧长度	命令/回应帧的长度（小端模式）
0x0104~0x021D	命令/回应帧	命令/回应帧，见表 2.2 和表 2.3

注意：

1. 若一次性向包含‘0x0101’地址的连续存储空间写入数据，只有写入结束后，写入‘0x0101’地址的数据才起效。
2. ‘0x0101’地址的值为‘STATUS_EXECUTING’（0x8D）和‘STATUS_BUSY’（0x8C）时请勿向‘0x0101~0x021D’地址写入任何数据，因为此时‘0x0101~0x021D’地址空间是被芯片内部使用。向其写数据会造成不可估计的错误或异常情况。

3. ‘STATUS_IDLE’（0x8A）只有上电时才会自动出现。执行命令后亦不会自动恢复成‘STATUS_IDLE’状态，只会保持命令执行后的状态。若有需要，请在执行命令结束后将‘0x0101’地址的值改为‘STATUS_IDLE’。
4. 为了减少从机处理通信中断的次数，在命令执行期间，请勿频繁访问芯片的存储空间，即使是查询命令执行的状态。在命令执行期间，建议根据实际情况，2~10ms 查询一次，或者使用芯片中断输出脚（芯片命令执行完毕，中断脚会输出一个低电平，该电平持续到接收到本芯片的 SLA+W 或 SLA+R 为止）。
5. 只有命令帧格式有效的情况下，芯片才执行命令，命令帧格式无效的情况下只会产生状态，而不会产生中断。
6. 该层不适合于 UART 通信接口，UART 通信接口忽略该层。

芯片 I^2C 支持的最大速率为 300Kbps，命令执行完毕中断输出脚会产生一个低电平，该电平持续到芯片收到本芯片的 SLA+W 或 SLA+R 为止。可以通过检查该中断来判断命令是否执行完毕；也可以查询‘0x0101’地址的值来判断芯片执行的情况。命令执行完毕后可以读取‘0x0102~0x0103’的值来获取回应帧的长度，以便于确定读取回应帧的字节数。

2.3.2 新帧格式协议层

表 2.2 新命令帧数据结构

地址 LocalAddr	卡槽索引 SlotIndex	安全报文/包号 SMCSeq	命令类型 CmdClass	命令代码 CmdCode	信息长度 InfoLength
1 字节	1 字节	1 字节	1 字节	2 字节	2 字节
信息 Info					校验和 CheckSum
n 字节					2 字节

表 2.3 新回应帧数据结构

地址 LocalAddr	卡槽索引 SlotIndex	安全报文/包号 SMCSeq	命令类型 CmdClass	执行状态 Status	信息长度 InfoLength
1 字节	1 字节	1 字节	1 字节	2 字节	2 字节
信息 Info					校验和 CheckSum
n 字节					2 字节

特别注意事项：“命令码”、“信息长度”和“校验和”均以小端模式存放，即低字节在前。信息长度可以为 0，即没有信息。

表 2.4 新命令帧数据结构说明

字段	长度 （字节）	说明	备注
LocalAddr	1	同 I^2C 地址模式相同，高 7 位为本机地址，低位为方向。其中‘0x00’为通用地址	—
SlotIndex	1	IC 卡卡槽的索引编号（本芯片保留该字节，帧里面该字节填入 0x00 即可）。	—
SMCSeq	1	高 4 位为安全报文控制位（本芯片不支持安全报文模式，即高 4 位无效）；低 4 位为该命令帧的序号。可以用来作为通	可以为任意值

		信间的错误检查，从机接收到主机发来的信息，在应答信息中发出一个同样的“包号”信息，主机可以通过此信息检查是否发生的“包丢失”的错误。	
CmdClass	1	0x01： 设备控制类命令 0x02： Mifare S50/S70 卡类命令(包括 USI14443-3A) 0x05： ISO7816-3 类命令 0x06： ISO14443（PICC）类命令 0x07： PLUS CPU 卡类命令 0x08： ISO15693（VICC）类命令 0x09： ISO18000-6C 0x0A： ISO18092(NFCIP-1) 0x0B： 二代身份证类命令	不同的芯片，支持的命令类型是不一致的
CmdCode	2	命令代码	—
InfoLength	2	该帧所带信息的字节数	—
Info	InfoLength	数据信息	—
CheckSum	2	校验和，从地址字节开始到信息的最后字节的累加和取反	—

ZSN603 芯片收到命令帧后，检测帧格式是否正确，若不正确，则丢弃当前数据，也不做任何回应；若正确则进一步进行处理。处理完毕后将处理的结果组成回应帧返回。

表 2.5 新回应帧数据结构说明

字段	长度（字节）	说明	备注
LocalAddr	1	高 7 位同命令帧，低位为方向	—
SlotIndex	1	同命令帧	—
SMCSeq	1	同命令帧	—
CmdClass	1	同命令帧	—
Status	2	执行状态 0x00：命令执行成功 0x15：命令帧类型未找到错误 0x16：命令指令内容错误 0x17：命令参数无效 0x18：命令执行错误	—
InfoLength	2	该帧所带信息的字节数	—
Info	InfoLength	数据信息	—
CheckSum	2	校验和，从地址字节开始到信息的最后字节的累加和取反	—

注：“命令码”、“信息长度”和“校验和”均以小端模式存放，即低字节在前。信息长度可以为 0，即没有信息。

命令帧和回应帧的格式基本一致，只有“命令码”和“执行状态”之分。帧的最小长度为 10 字节（没有信息的情况），最长理论上可以到 65545 字节。实际上没有必需。ZSN603 芯片帧的最大长度为 282 字节，信息的最大长度为 272 字节，完全满足短 APDU 的处理。命令/回应帧的详细定义如程序清单 2.1 所示。

程序清单 2.1 命令帧/回应帧结构体定义

```
#define CMD_PROTOCOL_LENGTH          10          //!< 通讯帧协议字节数
#define CMD_INFO_MAX_LENGTH          272         //!< 通讯帧最大字节数。
                                                 //!  短 APDU 的字节数为 255 + 6 字节；
                                                 //!  T=CL 协议长度为 5 字节；
                                                 //!  ExchangeBlock()函数的头为 4 字节。
                                                 //!  升级数据包的最大长度为 16 + 256 字节
#define CMD_PACKET_MIN_SIZE          (CMD_PROTOCOL_LENGTH)      //!< 通讯帧信息最小字节数
#define CMD_PACKET_MAX_SIZE          (CMD_PROTOCOL_LENGTH + CMD_INFO_MAX_LENGTH)
//! @struct CommandFrame  命令帧结构体
typedef struct CommandFrame
{
    uint8_t         LocalAddr;                   //!< 本机地址(最低位为方向位，同 I2C 地址相同)
    uint8_t         SlotIndex;                   //!< 卡槽索引
    uint8_t         SMCSeq;                      //!< 安全报文/包号
    uint8_t         CmdClass;                    //!< 命令类
    union
    {
        uint16_t    CmdCode;                     //!< 命令码
        uint16_t    Status;                      //!< 命令执行状态
    };
    uint16_t        InfoLength;                  //!< 信息长度
    uint8_t         Info[CMD_INFO_MAX_LENGTH + 2];      //!< 信息和 2 字节的累加和取反校验
} CommandFrame;
```

“校验和”为从地址字节开始到信息的最后字节（若信息长度为 0，则不计算信息）的累加和取反（只取低 16 位，高 16 位丢弃），具体实现方式见程序清单 2.2。

程序清单 2.2　计算字节累加和

```
// ================================================================================
//! @brief              计算字节累加和
//! @param[in]          *p          -- 计算的数据
//! @param[in]          nBytes      -- 字节数
//! @return             字节累加和
// ================================================================================
uint32_t GetByteSum(const void *p, uint32_t nBytes)
{
    const uint8_t   *pBuf = (const uint8_t *)p;
    uint32_t        sum   = 0;
```

```
    while (nBytes--) {
        sum + = *pBuf++;
    }
    return sum;
}
```

3. 新帧格式应用命令详述

ZSN603 芯片的应用命令共分为以下几类。

- 设备控制类命令；
- Mifare S50/S70 卡类命令；
- ISO7816-3 类命令；
- ISO14443（PICC）卡类命令；
- PLUS CPU 卡类命令；

3.1 设备控制类命令（CmdClass = 0x01）

设备控制类命令汇总如表 3.1 所示。

表 3.1 设备控制类命令一览表

命令码	意义
‘A’	读设备信息
‘B’	配置 IC 卡接口
‘C’	关闭 IC 卡接口
‘D’	设置 IC 卡接口协议（工作模式）
‘E’	装载 IC 卡密钥
‘F’	设置 IC 卡接口的寄存器值
‘G’	获取 IC 卡接口的寄存器值
‘H’	设置波特率
‘I’	设置天线驱动模式
‘K’	切换天线通道
‘L’	设置设备从机地址
‘M’	LED 灯控制
‘N’	蜂鸣器控制
‘b’	读 E^2PROM
‘c’	写 E^2PROM

3.1.1 读设备信息（Cmd = A）

该命令能够获取芯片的型号所用版本信息。

声明：*uint8_t zsn603_get_device_info(zsn603_handle_t handle,*
*uint8_t *p_rx_data,*
*uint32_t *p_rx_data_count);*

主机命令

命令类型（CmdClass）： 0x01
命令代码（CmdCode）： ‘A’
信息长度（InfoLength）： 0
信　　息（Info）： none
例　　如： 获取芯片的版本号

表 3.2 读设备信息命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	01	0041	0000
Info					CheckSum
none					FF0B

1. 从机应答

状　　态（Status）： 0——成功，其它——失败

信息长度（InfoLength）：　0x14

信　　息（Info）：　‘ZSN603 V1.00’

例　　如：　获取芯片信息成功后，返回芯片的版本信息

表 3.3　读设备信息回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	01	0000	000D
Info					CheckSum
5A 53 4E 36 30 33 20 56 31 2E 30 30 00					FC75

3.1.2 配置 IC 卡接口（Cmd = B）

该命令配置 IC 卡的接口形式，这个命令执行后，默认为 ISO14443A 形式。

声明：*uint8_t　zsn603_config_icc_interface(zsn603_handle_t handle);*

1.　主机命令

命令类型（CmdClass）：　0x01

命令代码（CmdCode）：　‘B’

信息长度（InfoLength）：　0

信　　息（Info）：　none

例　　如：　配置 IC 卡的接口形式

表 3.4　配置 IC 卡接口命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	01	0042	0000
Info					CheckSum
none					FF0A

2.　从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　none

例　　如：　配置 IC 卡接口成功后的回应

表 3.5　配置 IC 卡接口成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	01	0000	0000
Info					CheckSum
none					FF4B

3.1.3 关闭 IC 卡接口（Cmd = C）

该命令关闭 IC 卡接口，执行该命令后，IC 卡相关命令将不能工作，如果还需要执行读/写卡相关操作，必需先执行“配置 IC 卡接口”命令。

声明：*uint8_t　zsn603_close_icc_interface(zsn603_handle_t　handle)*

1. 主机命令

命令类型（CmdClass）：　0x01

命令代码（CmdCode）：　‘C’

信息长度（InfoLength）：　0

信　　息（Info）：　none

例　　如：　关闭 IC 卡的接口

表 3.6　关闭 IC 卡接口命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	01	0043	0000
Info					CheckSum
none					FF09

2. 从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　none

例　　如：　关闭 IC 卡接口成功后的回应

表 3.7　关闭 IC 卡接口成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	01	0000	0000
Info					CheckSum
none					FF4B

3.1.4 设置 IC 卡接口协议（工作模式）（Cmd = D）

该命令设置 IC 卡接口协议，与“配置 IC 卡接口”命令不同之处在于该命令即可以配置 IC 卡接口为 ISO14443-3A 形式，也可以配置成 ISO14443-3B 形式。配置只对当前上电期间有效，掉电后，又恢复至默认的 ISO14443-3A 形式。

声明：*uint8_t　zsn603_set_ios_type(zsn603_handle_t　handle,*

uint8_t　isotype);

1. 主机命令

命令类型（CmdClass）：　0x01

命令代码（CmdCode）：　‘D’

信息长度（InfoLength）：　0x01

信　　息（Info）：　IC 卡接口协议（1 字节）：　0x00——ISO14443-3A 形式

0x04——ISO14443-3B 形式

例　　如：　配置 IC 卡的接口为 ISO14443-3B 形式

表 3.8　设置 IC 卡接口为 ISO14443-3B 命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength

B2	00	00	01	0044	0001
Info					CheckSum
04					FF03

2. 从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　none

例　　如：　配置 IC 卡接口为 ISO14443-3B 成功后的回应

表 3.9　设置 IC 卡接口为 ISO14443-3B 成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	01	0000	0000
Info					CheckSum
none					FF4B

3.1.5 装载 IC 卡密钥（Cmd = E）

该命令是将输入的密钥保存在芯片内部，芯片掉电后该密钥不丢失，ZSN603 芯片共能保存 A 密钥 16 组、B 密钥 16 组。

声明：*uint8_t　zsn603_load_icc_key(zsn603_handle_t　handle,*

uint8_t　key_type,

uint8_t　key_block,

*uint8_t　*p_key,*

uint32_t　key_length);

1. 主机命令

命令类型（CmdClass）：　0x01

命令代码（CmdCode）：　'E'

信息长度（InfoLength）：　若是 6 字节密钥，则为 8

若是 16 字节密钥，则为 18

信　　息（Info）：　密钥类型（1 字节）：　0x60——密钥 A

0x61——密钥 B

密钥区号（1 字节）：　取值范围 0～15

密钥（6 字节或 16 字节）

例　　如：　向密钥 01 区装载密钥 A：0xFF 0xFF 0xFF 0xFF 0xFF 0xFF

表 3.10　向密钥 01 区装载密钥命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	01	0045	0008
Info					CheckSum
60 01 FF FF FF FF FF FF					F8A4

2. 从机应答

状　　态（Status）：　　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　　none

例　　如：　　装载密钥成功芯片的回应

表 3.11　装载密钥成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	01	0000	0000
Info					CheckSum
none					FF4B

3.　说明

此命令是向芯片内装载密码，并非改变 Mifare1 卡内扇区的密码。芯片内有 16 个密码区（区号 0～15）可供装载，每个区分密钥 A（0x60）和密钥 B（0x61）两个，总共 32 个密码。装载成功后，可用该密钥对 Mifare1 卡或 PLUS CPU 卡进行验证。装载时若输入的密钥为 6 字节，则芯片自动将 6 字节密钥采用复制拼接的方式扩展为 16 字节的密钥。例如密钥为：0xA0 0xA1 0xA2 0xA3 0xA4 0xA5,经扩展后为：0xA0 0xA1 0xA2 0xA3 0xA4 0xA5 0xA0 0xA1 0xA2 0xA3 0xA4 0xA5 0xA0 0xA1 0xA2 0xA3，扩展后的密钥用于 PLUS CPU 卡的 AES 验证，若需要提高安全性，则直接输入 16 字节的密钥。

若要改变 Mifare1 卡内的密钥，可在用原密码验证通过后，直接用写块数据指令，将密码块改写。

3.1.6 设置 IC 卡接口的寄存器值（Cmd = F）

该命令用于设置芯片上读写卡芯片内部的寄存器值，通过该命令，我们可以实现很多现有命令不能完成的工作。

声明：*uint8_t　zsn603_set_icc_reg(zsn603_handle_t　handle,*

uint8_t　reg_addr,

uint8_t　reg_val);

1.　主机命令

命令类型（CmdClass）：　0x01

命令代码（CmdCode）：　‘F’

信息长度（InfoLength）：　0x02

信　　息（Info）：　　寄存器地址（1 字节）：　取值范围 0x00～0x3F

寄存器值（1 字节）

例　　如：　　设置 TX1、TX2 天线驱动管脚的阻抗（0x12 寄存器）

表 3.12　设置寄存器值命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	01	0046	0002
Info					CheckSum
12 3F					FEB3

2.　从机应答

状　　态（Status）：　　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　　none

例　　如：　　设置寄存器值成功的回应

表 3.13　设置寄存器值成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	01	0000	0000
Info					CheckSum
none					FF4B

3.1.7 获取 IC 卡接口的寄存器值（Cmd = G）

该命令用于设置芯片上读写卡芯片内部的寄存器值，通过该命令，我们可以实现很多现有命令不能完成的工作。

声明：*uint8_t　zsn603_get_icc_reg(zsn603_handle_t　handle,*

uint8_t　reg_addr,

*uint8_t　*p_val);*

1.　主机命令

命令类型（CmdClass）：　0x01

命令代码（CmdCode）：　‘G’

信息长度（InfoLength）：　0x01

信　　息（Info）：　　寄存器地址（1 字节）：　　取值范围 0x00～0x3F

例　　如：　　读取 TX1、TX2 天线驱动管脚的阻抗（0x12 寄存器）

表 3.14　读取寄存器值命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	01	0047	0001
Info					CheckSum
12					FEF2

2.　从机应答

状　　态（Status）：　　0——成功，其它——失败

信息长度（InfoLength）：　0x01

信　　息（Info）：　　寄存器值

例　　如：　　读 0x12 寄存器返回的值

表 3.15　读取寄存器值成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	01	0000	0001
Info					CheckSum
3F					FF0B

3.1.8 设置波特率（Cmd = H）

该命令用于在 UART 通信过程中改变通信的波特率，该命令执行完毕，等到返回成功信息以后才会使新设置的通信波特率生效，掉电后该设置值保留。

声明：*uint8_t zsn603 _set_baud_rate(zsn603_handle_t handle,*

uint8_t baudrate_flag);

1. 主机命令

命令类型（CmdClass）： 0x01

命令代码（CmdCode）： ‘H’

信息长度（InfoLength）： 0x01

信　　息（Info）： 波特率编号（1 字节）： 可选取值如表 3.16 所示

表 3.16 波特率编号对应表

编号	8	9	0
波特率	2400	4800	9600

例　　如： 设置 UART 通信波特率为 2400

表 3.17 设置 UART 通信波特率为 2400 命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	01	0048	0001
Info					CheckSum
08					FBFE

2. 从机应答

状　　态（Status）： 0——成功，其它——失败

信息长度（InfoLength）： 0

信　　息（Info）： none

例　　如： 设置波特率成功的返回

表 3.18 设置 UART 波特率成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	01	0000	0000
Info					CheckSum
none					FF4B

3.1.9 设置天线驱动模式（Cmd = I）

该命令用于设置天线驱动模式，可以打开或关闭 TX1、TX2 中的任意一个管脚，特别适用于双天线应用的设置。

声明：*uint8_t zsn603_set_ant_mode(zsn603_handle_t handle,*

uint8_t antmode_flag);

1. 主机命令

命令类型（CmdClass）： 0x01

命令代码（CmdCode）：　‘I’

信息长度（InfoLength）：　0x01

信　　息（Info）：　　天线驱动模式（1 字节）：　0x01——仅 TX1 驱动天线

0x02——仅 TX2 驱动天线

0x03——TX1、TX2 同时驱动天线

例　　如：　　将芯片的天线驱动模式改为仅 TX2 输出

表 3.19　设置仅 TX2 驱动命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	01	0049	0001
Info					CheckSum
02					FF00

2.　从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　none

例　　如：　更改天线驱动模式成功的回应

表 3.20　更改天线驱动模式成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	01	0000	0000
Info					CheckSum
none					FF4B

3.1.10　切换天线通道（Cmd = K）

该命令用于在 ZSN603 中切换天线使用的通道。

声明：*uint8_t　zsn603_set_ant_channel(zsn603_handle_t　handle,*

uint8_t　ant_channel);

1.　主机命令

命令类型（CmdClass）：　0x01

命令代码（CmdCode）：　‘K’

信息长度（InfoLength）：　0x01

信　　息（Info）：　天线编号（0~7）

例　　如：　切换到天线通道 0

表 3.21　切换天线通道的命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	01	004B	0001
Info					CheckSum

00	FF00

2. 从机应答

状　　态（Status）：　　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　　none

例　　如：　　切换天线成功的返回

表 3.22　切换天线成功的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	01	0000	0000
Info					CheckSum
none					FF4B

3.1.11　设置设备从机地址（Cmd = L）

该命令用于设置芯片上电时的从机地址，在一主多从的应用中，应通过该命令先设置好芯片的从机地址。

声明：*uint8_t　zsn603_set_local_addr(zsn603_handle_t　handle,*

uint8_t　slv_addr);

1. 主机命令

命令类型（CmdClass）：　0x01

命令代码（CmdCode）：　‘L’

信息长度（InfoLength）：　0x01

从机地址（1 字节）：该字节保存从机的地址，从机地址采用 I^2C 地址的格式，最低位是读写位，所以从机地址最多只有 127 种。

例　　如：　　设置芯片的从机地址为 0x02

表 3.23　设置设备从机地址的命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	01	004C	0001
Info					CheckSum
02					FEFD

2. 从机应答

状　　态（Status）：　　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　　none

例　　如：　　设置芯片工作模式成功的回应

表 3.24　设置设备从机地址成功的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength

B3	00	00	01	0000	0000
Info					CheckSum
none					FF4B

3. 说明

经过从机地址设置为 0x02 并返回设置成功后，下一命令帧的地址应为 0x02，如果地址保持原来的 0xB2，芯片将不能响应。I^2C 通信方式下，必须使用旧地址读出完整的回应帧，芯片才会更新为新地址。

3.1.12 LED 灯控制（Cmd = M）

该命令用于控制 LED 专用引脚，可实现 LED 灯的亮灭控制，LED 点亮时，引脚电平为低。

声明：*uint8_t zsn603_control_led(zsn603_handle_t handle,*
uint8_t control_led);

1. 主机命令

命令类型（CmdClass）：0x01
命令代码（CmdCode）：‘M’
信息长度（InfoLength）：0x01
信　　息（Info）：LED 灯控制（1 字节）：0x01——点亮 LED
0x00——熄灭 LED
例　　如：点亮 LED。

表 3.25　点亮 LED 的命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	01	004D	0001
Info					CheckSum
01					FEFD

2. 从机应答

状　　态（Status）：0——成功，其它——失败
信息长度（InfoLength）：0
信　　息（Info）：none
例　　如：成功点亮 LED 的回应

表 3.26　成功点亮 LED 的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	01	0000	0000
Info					CheckSum
none					FF4B

3.1.13 蜂鸣器控制（Cmd = N）

该命令用于控制蜂鸣器专用引脚，蜂鸣器类型应为无源蜂鸣器。

声明：*uint8_t zsn603_control_buzzer(zsn603_handle_t handle,*

uint8_t control_byte);

1. 主机命令

命令类型（CmdClass）： 0x01

命令代码（CmdCode）： ‘N’

信息长度（InfoLength）： 0x01

信　　息（Info）： 控制字节（1 字节）内容定义如表 3.27 所示

表 3.27　蜂鸣器控制字节

B7～B4	B3～B0
蜂鸣器定时鸣叫控制 0000：RFU 0001~1111： 定时时间 = 位编码值 * 100 毫秒	蜂鸣器鸣叫次数控制 0000：RFU 0001~0111：鸣叫次数 1~7 次 蜂鸣器多次鸣叫时，停顿时间是固定 200 毫秒

用户应根据实际需求来设置控制字节的内容。

例　　如： 设置蜂鸣器连续鸣叫 3 次，每次鸣叫 100 毫秒

表 3.28　设置蜂鸣器连续鸣叫三次的命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	01	004E	0001
Info					CheckSum
13					FEEA

2. 从机应答

状　　态（Status）： 0——成功，其它——失败

信息长度（InfoLength）： 0

信　　息（Info）： none

例　　如： 设置蜂鸣器连续鸣叫成功后的回应

表 3.29　设置蜂鸣器连续鸣叫成功的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	01	0000	0000
Info					CheckSum
none					FF4B

3.1.14　读 E²PROM（Cmd = b）

芯片内部拥有一个 256Byte 的 E²PROM，该存储空间掉电不丢失，通过“读 E²PROM”、“写 E²PROM”命令可以对该存储器的数据进行读写。

声明：*uint8_t zsn603_read_eeprom(zsn603_handle_t handle,*

uint8_t eeprom_addr,

uint8_t nbytes,

*uint8_t *p_buf);*

1. 主机命令

命令类型（CmdClass）： 0x01

命令代码（CmdCode）： ‘b’

信息长度（InfoLength）： 0x02

信　　息（Info）： E^2PROM 址址（1 字节）：范围 0 ～255

读取数据的长度（1 字节）

例　　如： 读取 E^2PROM 从 0x08 开始 8 字节的数据

表 3.30　读 E^2PROM 的命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	01	0062	0002
Info					CheckSum
08 08					FED8

2. 从机应答

状　　态（Status）： 0——成功，其它——失败

信息长度（InfoLength）： 0x08

信　　息（Info）： none

例　　如： 读取 E^2PROM 里面从 0x08 地址开始 8 字节的数据的返回

表 3.31　读 E^2PROM 成功的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	01	0000	0008
Info					CheckSum
00 00 00 00 00 00 00 00					FF43

3.1.15　写 E^2PROM（Cmd = c）

该命令是往 E^2PROM 里面写数据。

声明：*uint8_t　zsn603_write_eeprom(zsn603_handle_t　handle,*

uint8_t　eeprom_addr,

uint8_t　nbytes,

*uint8_t　*p_buf);*

1. 主机命令

命令类型（CmdClass）： 0x01

命令代码（CmdCode）： ‘c’

信息长度（InfoLength）： 要写的数据长度+2

信　　息（Info）： E^2PROM 址址（1 字节）：范围 0 ～255

写数据的长度（1 字节）

要写入的数据信息（n 字节）

例　　如： 往 E^2PRPM 里面 0x02 地址开始写入 4 字节的数据

表 3.32　写 E^2PROM 的命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	01	0063	0006
Info					CheckSum
02 04 FF FF FF FF					FAE1

2. 从机应答

状　　态（Status）：　　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　　none

例　　如：　　往 E^2PROM 里面 0x02 地址开始写入 4 字节数据成功的返回

表 3.33　写 E^2PROM 成功的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	01	0000	0000
Info					CheckSum
none					FF4B

3.2 Mifare S50/S70 卡类命令（CmdClass = 0x02）

Mifare S50/S70 卡类命令总汇如表 3.34 所示。

表 3.34 Mifare S50/S70 卡类命令一览表

命令码	意义
‘A’	请求
‘B’	防碰撞
‘C’	卡选择
‘D’	卡挂起
‘E’	E^2 密钥验证
‘F’	直接密钥验证
‘G’	Mifare 卡读
‘H’	Mifare 卡写
‘I’	UltraLight 卡写
‘J’	Mifare 值操作
‘L’	卡复位
‘M’	卡激活
‘N’	自动检测
‘O’	读自动检测数据
‘P’	设置值块的值
‘Q’	获取值块的值
‘S’	命令传输
‘X’	数据交互命令

前 4 条命令（命令 A～D）是 ISO14443A 标准定义的命令，只要符合该标准的卡都应能发出响应；中间 6 条命令（命令 E～J）为 Mifare1 卡的专用命令，只有先进行验证（命令 E、F）成功之后才能进行；后四条命令（L、M、N、O）为实用的扩展命令；X 命令为读写器与卡交换数据块，该命令用于 ISO14443-4 标准。

注意：

命令 C 和 M 命令都做了 Mifare 卡和 PLUS CPU 卡自动辨别功能，并根据卡的类型不同自动调用相应的命令，该功能使用户的卡片由 M1 卡升级到 PLUS CPU 卡不必修改，若要执行其它符合 CPU 卡操作，建议使用 PLUS CPU 卡类命令。

3.2.1 请求（Cmd = A）

该命令用于 Mifare 卡的请求操作。

声明：*uint8_t zsn603_mifare_request(zsn603_handle_t handle,*
uint8_t req_mode,
*uint16_t *p_atq);*

1. 主机命令

命令类型（CmdClass）： 0x02

命令代码（CmdCode）： ‘A’

信息长度（InfoLength）：　0x01

信　　息（Info）：　　请求模式（1 字节）：　0x26——IDLE 模式

0x52——ALL 模式

例　　如：　　请求天线范围内所有的卡

表 3.35　请求卡命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	0041	0001
Info					CheckSum
52					FEB7

2.　从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0x02

信　　息（Info）：　　请求应答 ATQ（2 字节，低位在前）

表 3.36　ATQ 字节描述

b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0
RFU								UID 大小 00:4bytes 01:7bytes 10:10bytes		RFU	如果有任何位为 1，则为比特帧防冲突方式				

表 3.37 列举了各种类型的卡返回的 ATQ。

表 3.37　返回 ATQ 一览表

卡类型	Mifare1 S50	Mifare1 S70	Mifare1 Light	Mifare0 UltraLight	Mifare3 DESFire	SHC1101	SHC1102	11RF32
ATQ	0x0004	0x0002	0x0010	0x0044	0x0344	0x0004	0x3300	0x0004

例　　如：　　S50 卡返回的 ATQ

表 3.38　请求成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0002
Info					CheckSum
04 00					FF44

3.　说明

卡进入天线后，从射频场中获取能量，从而得电复位，复位后卡处于 IDLE 模式，用两种请求模式的任一种请求时，此时的卡均能响应；若对某一张卡成功进行了挂起操作（Halt 命令或 DeSelect 命令），则进入了 Halt 模式，此时的卡只响应 ALL（0x52）模式的请求，除非将卡离开天线感应区后再进入。

注：DeSelect 为 ISO14443-4 命令。另外，对 Mifare1 卡连续进行请求操作，总是一次成功，一次失败，循环往复。

3.2.2 防碰撞（Cmd = B）

该命令用于 Mifare 卡的防碰撞操作，需要执行成功一次请求命令，并返回请求成功，才能进行防碰撞操作，否则返回错误。

声明：*uint8_t zsn603_mifare_anticoll(zsn603_handle_t handle,*
uint8_t anticoll_level,
*uint8_t *p_know_uid,*
uint8_t nbit_cnt,
*uint8_t *p_uid,*
*uint32_t *p_uid_cnt);*

1. 主机命令

命令类型（CmdClass）：0x02

命令代码（CmdCode）：‘B’

信息长度（InfoLength）：若位计数=0，则长度=2

若位计数≠0，则长度=6

信　　息（Info）：选择代码（1 字节）：0x93——第一级防碰撞

0x95——第二级防碰撞

0x97——第三级防碰撞

位计数（1 字节）：已知的序列号的长度

序列号（4 字节）（若位计数≠0）

例　　如：第一级防碰撞

表 3.39　防碰撞命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	0042	0002
Info					CheckSum
93 00					FE74

2. 从机应答

状　　态（Status）：0——成功，其它——失败

信息长度（InfoLength）：0x04

信　　息（Info）：UID（4 字节，低字节在先），若 UID 不完整，则最低字节为级联标志 0x88，需要进行更高一级的防碰撞。

例　　如：返回防碰撞的卡序列号 0xEB1C1814

表 3.40　防碰撞回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0004
Info					CheckSum
14 18 1C EB					FE13

3. 说明

符合 ISO14443A 标准卡的序列号都是全球唯一的，正是这种唯一性，才能实现防碰撞的算法逻辑，若有若干张卡同时在天线感应区内则这个函数能够找到一张序列号较大的卡来操作。实际上由于天线辐射的磁场能量有限，同时在天线感应区内的所有卡都要从辐射场中吸收，因此同时在天线感应区内的卡不能太多，否则辐射场能量被平分，没有一张卡能获得足够的能量来正常工作。

位计数为已知的序列号的位数，若位计数=0，则序列号的所有位都要从本函数获得；若位计数≠0，则序列号中有已知的序列号的值，表示要获得序列号的前位计数位为序列号中所示的卡的其余位的值。位计数必须小于 32，若位计数等于 32，则可直接用选择命令，选择一张已知序列号的卡。

3.2.3 卡选择（Cmd = C）

该命令用于 Mifare 卡的选择操作。

声明：*uint8_t zsn603_mifare_select(zsn603_handle_t handle,*
uint8_t anticoll_level,
*uint8_t *p_uid,*
*uint8_t *p_sak);*

1. 主机命令

命令类型（CmdClass）：0x02
命令代码（CmdCode）：‘C’
信息长度（InfoLength）：0x05
信　　息（Info）：选择代码（1 字节）：0x93——第一级防碰撞
0x95——第二级防碰撞
0x97——第三级防碰撞
UID（4 字节）：前一个防碰撞命令返回的 UID
例　　如：第一级选择，UID 为 0xEB1C1814

表 3.41　卡选择命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	0043	0005
Info					CheckSum
93 14 18 1C EB					FD3D

2. 从机应答

状　　态（Status）：0——成功，其它——失败
信息长度（InfoLength）：0x01
信　　息（Info）：选择应答 SAK，如表 3.42 所示，其中 Bit 2 位是 Cascade 位，表示 UID 是否完整。若 Bit 2 = 0，表示 UID 完整
若 Bit 2 = 1，表示 UID 不完整，还有部分 UID 未读出

表 3.42　返回 SAK 一览表

卡类型	Mifare1	Mifare1	Mifare1	Mifare0	Mifare3	SHC1101	SHC1102	11RF32

	S50	S70	Light	UltraLight	DESFire			
SAK	0x08	0x18	0x01	0x04	0x24	0x22	—	0x08

例　　如：　　返回 S50 卡应答

表 3.43　卡选择成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0001
Info					CheckSum
08					FF41

3.　说明

卡的序列号长度有三种：4 字节、7 字节和 10 字节。4 字节的只要用一级选择即可得到完整的序列号，如 Mifare1 S50/S70 等；7 字节的要用二级选择才能得到完整的序列号，前一级所得到的序列号的最低字节为级联标志 0x88，在序列号内只有后 3 字节可用，后一级选择能得到 4 字节序列号，两者按顺序连接即为 7 字节序列号，如 UltraLight 和 DesFire 等；10 字节的以此类推，但至今还未发现此类卡。

在程序中可用 SAK.2 位来判断是还有序列号未读出，如 if(SAK & 0x04){…}。

3.2.4 卡挂起（Cmd = D）

该命令用于 Mifare 卡的挂起操作，使所选择的卡进入 HALT 状态，在 HALT 状态下，卡将不响应读卡器发出的 IDLE 模式的请求，除非将卡复位或离开天线感应区后再进入。但它会响应读卡器发出的 ALL 请求。

声明：*uint8_t　zsn603_mifare_halt(zsn603_handle_t　　handle);*

1.　主机命令

命令类型（CmdClass）：　0x02

命令代码（CmdCode）：　‘D’

信息长度（InfoLength）：　0

信　　息（Info）：　none

例　　如：　将已激活的卡挂起，使之不响应请求空闲卡命令

表 3.44　卡挂起命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	0044	0000
Info					CheckSum
none					FF07

2.　从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　none

例　　如：　挂起命令执行成功的回应

表 3.45　卡挂起成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0000
Info					CheckSum
none					FF4A

3.2.5 E^2 密钥验证（Cmd = E）

该命令用芯片内部已存入的密钥与卡的密钥进行验证，所以使用该命令前，应事先用“装载 IC 卡密钥”命令把密钥成功载入芯片内，另外，需要验证的卡的扇区号不必与芯片内密钥区号相等。

声明：*uint8_t zsn603_eeprom_auth(zsn603_handle_t handle,*
uint8_t key_type,
*uint8_t *p_uid,*
uint8_t key_sec,
uint8_t nblock);

1. 主机命令

命令类型（CmdClass）：0x02
命令代码（CmdCode）：‘E’
信息长度（InfoLength）：0x07
信　　息（Info）：密钥类型（1 字节）：0x60——密钥 A
0x61——密钥 B
卡序列号（4 字节）
密钥区号（1 字节）：取值范围 0～15
卡块号（1 字节）：S50（0～63）
S70（0～255）
PLUS CPU 2K（0～127）
PLUS CPU 4K（0～255）
例　　如：用密钥 1 区的密钥 A 证实序列号为 0xEB1C1814 卡的块 4

注：PLUS CPU 系列的卡的卡号有 4 字节和 7 字节之分，对于 7 字节卡号的卡，只需要将卡号的高 4 字节（等级 2 防碰撞得到的卡号）作为验证的卡号即可。

表 3.46　E^2 密钥验证命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	0045	0007
Info					CheckSum
60 14 18 1C EB 01 04					FD67

2. 从机应答

状　　态（Status）：0——成功，其它——失败
信息长度（InfoLength）：0
信　　息（Info）：none

例　　如：　　验证成功返回的信息

表 3.47　E2 密钥验证成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0000
Info					CheckSum
none					FF4A

3.2.6 直接密钥验证（Cmd = F）

该命令将密码作为参数传递，因此在此之前不需用“装载 IC 卡密钥”命令。若当前卡为 PLUS CPU 卡的等级 2 或等级 3，且输入的密码只有 6 字节，则芯片自动将输入的密码复制 2 次，取前 16 字节作为当前验证密钥。

声明：*uint8_t　zsn603_key_auth(zsn603_handle_t　handle,*
uint8_t　key_type,
*uint8_t　*p_uid,*
*uint8_t　*p_key,*
uint8_t　key_len,
uint8_t　nblock);

1.　主机命令

命令类型（CmdClass）：　0x02
命令代码（CmdCode）：　‘F’
信息长度（InfoLength）：　密钥为 6 字节，则为 12
密钥为 16 字节，则为 22
信　　息（Info）：　密钥类型（1 字节）：　0x60——密钥 A
0x61——密钥 B
卡序列号（4 字节）
密钥（6 字节或 16 字节）
卡块号（1 字节）：　S50（0～63）
S70（0～255）
PLUS CPU 2K（0～127）
PLUS CPU 4K（0～255）

例　　如：　　用密钥“0xFF 0xFF 0xFF 0xFF 0xFF 0xFF”验证序列号为 0xEB1C1814 的卡的块 4

注：PLUS CPU 系列的卡的卡号有 4 字节和 7 字节之分，对于 7 字节卡号的卡，只需要将卡号的高 4 字节（等级 2 防碰撞得到的卡号）作为验证的卡号即可。

表 3.48　直接密钥验证命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	0046	000C
Info					CheckSum

60 14 18 1C EB FF FF FF FF FF FF 04	F768

2. 从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　none

例　　如：　验证成功返回的信息

表 3.49　直接密钥验证成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0000
Info					CheckSum
none					FF4A

3.2.7 Mifare 卡读（Cmd = G）

该命令对 Mifare 卡进行读操作，读之前必需成功进行密钥验证。

声明：*uint8_t　zsn603_mifare_read(zsn603_handle_t　handle,*

uint8_t　nblock,

*uint8_t　*p_buf);*

1. 主机命令

命令类型（CmdClass）：　0x02

命令代码（CmdCode）：　‘G’

信息长度（InfoLength）：　0x01

信　　息（Info）：　卡块号（1 字节）：　S50（0～63）

S70（0～255）

PLUS CPU 2K（0～127）

PLUS CPU 4K（0～255）

例　　如：　读块 4 的数据

表 3.50　Mifare 卡读命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	0047	0001
Info					CheckSum
04					FEFF

2. 从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0x10

信　　息（Info）：　块数据（16 字节）

例　　如：　从卡的块 4 读出数据为：“0x7F 0x4B 0xD8 0x37 0xAA 0x99 0xF3 0xE0 0xA5 0xD9 0x93 0x70 0x8F 0x89 0xE2 0x64”

表 3.51　Mifare 读成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0010
Info					CheckSum
7F 4B D8 37　AA 99 F3 E0　A5 D9 93 70　8F 89 E2 64					F56C

1.　说明

在验证成功之后，才能读相应的块数据，所验证的块号与读块号必须在同一个扇区内，Mifare1 卡从块号 0 开始按顺序每 4 个块 1 个扇区，若要对一张卡中的多个扇区进行操作，在对某一扇区操作完毕后，必须进行一条读命令才能对另一个扇区直接进行验证命令，否则必须从请求开始操作。

对于 PLUS CPU 卡，若下一个读扇区的密钥和当前扇区的密钥相同，则不需要再次验证密钥，直接读即可。

3.2.8 Mifare 卡写（Cmd = H）

该命令对 Mifare 卡进行写操作，写之前必需成功进行密钥验证。

声明：*uint8_t　zsn603_mifare_write(zsn603_handle_t　handle,*
uint8_t　nblock,
*uint8_t　*p_buf);*

1.　主机命令

命令类型（CmdClass）：　0x02
命令代码（CmdCode）：　‘H’
信息长度（InfoLength）：　0x11
信　　息（Info）：　卡块号（1 字节）：　S50（0～63）
S70（0～255）
PLUS CPU 2K（0～127）
PLUS CPU 4K（0～255）
数据（16 字节）
例　　如：　向块 4 写入 16 字节数据“0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x0A 0x0B 0x0C 0x0D 0x0E 0x0F”

表 3.52　Mifare 卡写命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	0048	0011
Info					CheckSum
04　00 01 02 03　04 05 06 07　08 09 0A 0B　0C 0D 0E 0F					FE76

2.　从机应答

状　　态（Status）：　0——成功，其它——失败
信息长度（InfoLength）：　0
信　　息（Info）：　none

例　　如：　　数据成功写入卡片芯片的回应

表 3.53　Mifare 写成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0000
Info					CheckSum
none					FF4A

3.　说明

对卡内某一块进行验证成功后，即可对同一扇区的各个进行写操作（只要访问条件允许），其中包括位于扇区尾的密码块，这是更改密码的唯一方法。对于 PLUS CPU 卡等级 2、3 的 AES 密钥则是在其他位置修改密钥。

3.2.9 UltraLight 卡写（Cmd = I）

该命令对 UltraLight 卡进行写操作。

声明：*uint8_t　zsn603_ultralight_write(zsn603_handle_t　handle,*
uint8_t　nblock,
*uint8_t　*p_buf);*

1.　主机命令

命令类型（CmdClass）：　0x02
命令代码（CmdCode）：　‘I’
信息长度（InfoLength）：　0x05
信　　息（Info）：　卡块号（1 字节）：1～15
数据（4 字节）
例　　如：　写块 4 数据

表 3.54　UltraLight 卡写命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	0049	0005
Info					CheckSum
04　05 05 05 05					FEE5

2.　从机应答

状　　态（Status）：　0——成功，其它——失败
信息长度（InfoLength）：　0
信　　息（Info）：　none
例　　如：　数据成功写入卡片芯片的回应

表 3.55　UltraLight 卡写成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0000
Info					CheckSum
none					FF4A

3. 说明

此命令只对 UltraLight 卡有效，对 UltraLight 卡进行读操作与 Mifare1 卡一样。

3.2.10 Mifare 值操作（Cmd = J）

该命令对 Mifare 卡的值块进行加减操作。

声明：*uint8_t zsn603_mifare_value(zsn603_handle_t handle,*
uint8_t mode,
uint8_t nblock,
uint8_t ntransblk,
uint32_t value);

1. 主机命令

命令类型（CmdClass）：0x02
命令代码（CmdCode）：‘J’
信息长度（InfoLength）：0x07
信　　息（Info）：模式（1 字节）：0xC0～减
0xC1～加
卡块号（1 字节）：S50（0～63）
S70（0～255）
PLUS CPU 2K（0～127）
PLUS CPU 4K（0～255）
值（4 字节有符号数，低字节在先）
传输块号（1 字节）
例　　如：将块 4 的值减 1，其结果保存到块 5

表 3.56 Mifare 值操作命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	004A	0007
Info					CheckSum
C0 04 01 00 00 00 05					FE30

2. 从机应答

状　　态（Status）：0——成功，其它——失败
信息长度（InfoLength）：0
信　　息（Info）：none
例　　如：值块操作成功后芯片的回应

表 3.57 Mifare 值操作成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0000
Info					CheckSum

none	FF4A

3. 说明

要进行此类操作，块数据必须要有值块的格式，可参考 NXP 的相关文档。若卡块号与传输块号相同，则将操作后的结果写入原来的块内；若卡块号与传输块号不相同，则将操作后的结果写入传输块内，结果传输块内的数据被覆盖，原块内的值不变。处于等级 2 的 PLUS CPU 卡不支持值块操作，等级 1、3 支持。

3.2.11 卡复位（Cmd = L）

该命令是通过将载波信号关闭指定的时间，再开启来实现卡片复位。

声明：*uint8_t zsn603_card_reset(zsn603_handle_t handle,*
uint8_t time_ms);

1. 主机命令

命令类型（CmdClass）： 0x02
命令代码（CmdCode）： ‘L’
信息长度（InfoLength）： 0x01
信　　息（Info）： 时间（1 字节），以毫秒为单位，0 为一直关闭
例　　如： 将载波信号关闭 1ms

表 3.58 卡复位命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	004C	0001
Info					CheckSum
01					FEFD

2. 从机应答

状　　态（Status）： 0——成功，其它——失败
信息长度（InfoLength）： 0
信　　息（Info）： none
例　　如： 执行卡复位成功芯片的回应

表 3.59 卡复位成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0000
Info					CheckSum
none					FF4A

3. 说明

该命令将天线信号关闭数毫秒，若一直关闭，则等到执行一个请求命令时打开。

3.2.12 卡激活（Cmd = M）

该命令用于激活卡片，是请求、防碰撞和选择三条命令的组合。

声明：*uint8_t zsn603_mifare_card_active(zsn603_handle_t handle,*

1. 主机命令

命令类型（CmdClass）：　0x02
命令代码（CmdCode）：　‘M’
信息长度（InfoLength）：　0x02
信　　息（Info）：　保留（1 字节），设置为 0
请求代码（1 字节）：　0x26～IDLE
0x52～ALL
例　　如：　以 IDLE 方式激活卡

表 3.60　卡激活命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	004D	0002
Info					CheckSum
00 26					FED6

2.　从机应答

状　　态（Status）：　0——成功，其它——失败
信息长度（InfoLength）：　Mifare1 S50、S70、Light 卡：8 字节
Mifare0 UltraLight 卡：11 字节
Mifare3 Desfire 卡：11 字节
Plus CPU 卡：8 字节或 11 字节
信　　息（Info）：　请求应答 ATQA（2 字节）
最后一级选择应答 SAK（1 字节）
序列号长度（1 字节）
序列号（N 字节，由序列号长度决定）
例　　如：　一张序列号为 0xEB1C1814 的 Mifare1 S50 卡返回的数据

表 3.61　卡激活成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0008
Info					CheckSum
04 00 08 04 14 18 1C EB					FDFF

3.2.13　自动检测（Cmd = N）

该命令用于卡片的自动检测，执行该命令成功后，在 UART 模式下，芯片将主动发送读取到卡片的数据。

声明：*uint8_t　zsn603_auto_detect(zsn603_handle_t　handle,*
uint8_t　admode,
uint8_t　txmode,
uint8_t　reqcode,
uint8_t　authmode,
uint8_t　key_type,

uint8_t **p_key,*
uint8_t *key_lenght,*
uint8_t *block);*

1. 主机命令

命令类型（CmdClass）： 0x02

命令代码（CmdCode）： ‘N’

信息长度（InfoLength）： 若验证模式 = “E”，则为 7

若验证模式 = “F”，则为 12 或 22

若验证模式 = 0，则为 4

信　　息（Info）： 自动检测模式 *ADMode*（1 字节）：该字节内容如表 3.62 所示

表 3.62　ADMode 字节位描述

B7～B4	B3	B2	B1	B0
RFU 0000	执行完一次自动检测后的动作 0:无动作 1:最后执行 Halt 命令	数据输出后 0:不继续检测 1:继续检测	当 UART 接口，检测到有卡时 0:不产生中断 1:产生中断，当串口发送数据完毕后，中断消失；当 I²C 接口时此位无效，应设置为 0，因肯定产生中断	当 UART 接口，检测到有卡时 0:串口不发送 1:串口主动发送，发送的数据格式见“检测卡回应格式”。当 I²C 接口时此位无效，应设置为 0，因为是从模式

天线驱动方式 *TxMode*（1 字节）：字节描述如表 3.63 所示

表 3.63　TxMode 字节位描述

B7～B2	B1	B0
RFU 000000	00：TX1、TX2 交替驱动 01：仅 TX1 驱动 10：仅 TX2 驱动 11：TX1、TX2 同时驱动	

请求代码 *ReqCode*（1 字节）： 0x26～IDLE

0x52～ALL

验证模式 *AuthMode*（1 字节）： ‘E’～用 E2 密钥验证

‘F’～用直接密钥验证

0 ～不验证

密钥 AB *KeyType*（1 字节）： 0x60～密钥 A

0x61～密钥 B

密钥 *Key*： 若验证模式为‘E’，则为密钥区号（1 字节）

若验证模式为‘F’，则为密钥（6 或 16 字节）

卡块号 *Block*（1 字节）： S50（0～63）

S70（0～255）

PLUS CPU 2K（0～127）

PLUS CPU 4K（0～255）

例　　如：　设置芯片检测到有卡时产生中断，串口输出，以 IDLE 方式激活卡，用直接密码验证密钥 A（密码为 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF），读出第 1 块数据内容

表 3.64　自动检测命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	004E	000C
Info					CheckSum
03 03 26 46 60 FF FF FF FF FF FF 01					F824

2.　从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　none

例　　如：　芯片设置自动检测成功的回应

表 3.65　设置自动检测成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0000
Info					CheckSum
none					FF4A

3.　检测卡回应格式

“从机应答”只是说明芯片设置成自动检测成功，在串口通信方式下，自动检测模式使能后，若允许串口主动发送（即 *ADMode*.0=1），有卡靠近芯片，芯片将自动把检测到卡的相应信息按如下的格式发送。

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　若验证命令不为 0，则为：21+序列号长度

若验证命令为 0，则为：5+序列号长度

信　　息（Info）：　天线驱动 *TxDrv*（1 字节）：如表 3.66 所示

表 3.66　TxDrv 字节位描述

B7～B2	B1	B0
RFU 000000	00：TX1、TX2 交替驱动 01：仅 TX1 驱动 10：仅 TX2 驱动 11：TX1、TX2 同时驱动	

请求应答 *ATQ*（2 字节）

选择应答 *SAK*（1 字节）

序列号长度 *UIDLen*（1 字节）

序列号 UID（长度为各种卡序列号的实际长度）

块数据：若验证命令不为 0，则块数据为 16 字节
若验证命令为 0，则块数据为 0 字节

例　　如：　　检测到序列号为 0xEB1C1814 的 S50 卡，并读出块 1 数据

表 3.67　检测卡成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0019
Info					CheckSum
03 04 00 08　04 14 18 1C　EB 14 18 1C　EB FB 88 04　00 47 C1 24　37 E1 00 11　06					F8D6

4.　说明

执行自动检测命令成功后，并且读取卡片信息成功返回，整个过程相当于以下命令的组合：请求——防碰撞——选择——验证（若 *AuthMode*!=0）——读取（若 *AuthMode*!=0）——挂起（若 *AuthMode*.3=1）。当输入的密钥为 6 字节时，芯片内部将按 Key[0:15]=pKey[0:5]pKey[0:5]pKey[0:3]模式扩展。

串口主动发送之后，芯片状态由 *ADMode*.2 位来决定，若 *ADMode*.2=1，则自动进入自动检测模式；否则结束自动检测模式，主机可以发送其它任何命令。若 *ADMode*.1=1，则芯片检测到卡后产生中断信号，可以通过读取自动检测数据命令（Cmd = O）读取。

当为 I^2C 接口通信时，因芯片为从模式，所以不主动发送数据，但肯定输出中断信号，应使 *ADMode*.1=0，产生中断后，主机可以通过以下两种方式读回数据。

- 一是直接读取，这样读取之后的芯片状态由 *ADMode*.2 位来决定：若 *ADMode*.2=1，则继续进入自动检测模式；否则结束自动检测模式，主机可以发送其它任何命令。
- 二是通过读取自动检测数据命令（Cmd=O）读取数据之后的芯片状态由该函数的参数来决定：在自动检测模式期间，主机可以随时发出读取自动检测数据命令，读取自动检测数据、查询自动检测状态、取消或继续自动检测；验证和读命令只对 Mifare1 卡和 PLUS CPU 卡有效。

注：在自动检测期间，若主机发送任何除读自动检测数据外的，且数据长度小于 3（帧长小于 9）的命令，将退出自动检测模式，如请求 *PiccA_Request()*命令，在此期间，芯片将不接收数据长度大于 2（帧长大于 8）的命令。

3.2.14　读自动检测数据（Cmd = O）

该命令用于读取自动检测的数据，特别适合于 I^2C 通信模式下使用。通过该读取自动检测数据命令，可以决定读取数据后是否继续检测。

声明：*uint8_t　zsn603_get_auto_detect(zsn603_handle_t　handle,*
uint8_t　ctrl_mode,
*uint8_t　*p_data,*
*uint32_t　*p_data_count);*

1.　主机命令

命令类型（CmdClass）：　0x02
命令代码（CmdCode）：　‘O’
信息长度（InfoLength）：　0x01
信　　息（Info）：　读模式（1 字节），该字节内容如表 3.68 所示

表 3.68　读模式字节描述

B7～B1	B0
RFU 000000	数据发回之后： 00：取消检测 01：继续检测

例　　如：　　读取自动检测数据之后取消自动检测

表 3.69　读自动检测数据命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	004F	0001
Info					CheckSum
00					FEFB

2.　从机应答

状　　态（Status）：　　0——成功，其它——失败

信息长度（InfoLength）：　0x19

信　　息（Info）：　　自动检测读取成功保存的信息

例　　如：　　读自动检测数据成功的回应

表 3.70　读自动检测数据成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0019
Info					CheckSum
03 04 00 08　04 14 18 1C　EB 14 18 1C　EB FB 88 04　00 47 C1 24　37 E1 00 11　06					F8D6

3.2.15　设置值块的值（Cmd = P）

该命令用于设置值块的值。

声明：*uint8_t　zsn603_mifare_set_value(zsn603_handle_t　handle,*
uint8_t　block,
int　data);

1.　主机命令

命令类型（CmdClass）：　0x02

命令代码（CmdCode）：　‘P’

信息长度（InfoLength）：　0x05

信　　息（Info）：　　块地址（1 字节）：将要写入数值的块地址

块值（4 字节）：有符号的 32 位数据，低字节在前

例　　如：　　将 0x05 值块地址的值设置为 0x03

表 3.71　设置值块的值命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	0050	0005
Info					CheckSum

05 03 00 00 00	FEEE

2. 从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　none

例　　如：　将 0x05 值块地址的值设置为 0x03 成功后的返回

表 3.72　设置值块的值成功的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0000
Info					CheckSum
none					FF4A

3.2.16　获取值块的值（Cmd = Q）

该命令用于获取值块的值，值块里面的数据只有是按照值格式存储时，才能通过该命令读取成功，否则返回失败。

声明：*uint8_t　zsn603_mifare_get_value(zsn603_handle_t　handle,*

uint8_t　block,

*int　*p_value);*

1. 主机命令

命令类型（CmdClass）：　0x02

命令代码（CmdCode）：　‘Q’

信息长度（InfoLength）：　0x01

信　　息（Info）：　块地址（1 字节）：将要读取数值的块地址

例　　如：　读 0x06 值块地址的值

表 3.73　获取值块的值命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	0051	0001
Info					CheckSum
06					FEF3

2. 从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　4

信　　息（Info）：　块值（4 字节）：有符号的 32 位数据，低字节在前

例　　如：　读 0x06 值块地址的值成功后的返回

表 3.74　获取值块的值成功的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0004

Info	CheckSum
01 00 00 00	FF45

3.2.17 命令传输（Cmd = S）

该命令属于芯片扩展功能，用于芯片向卡片发送任意长度组合的数据串，例如针对 NXP 新推出的 NTAG213F 是属于 Ultralight C 系列卡片，但是该卡片又新添加了扇区数据读写密钥保护功能。而这个密钥验证命令即可利用此命名传输命令来实现。

声明：*uint8_t zsn603_mifare_cmd_trans(zsn603_handle_t handle,*

*uint8_t *p_tx_buf,*

uint8_t tx_nbytes,

*uint8_t *p_rx_buf,*

*uint32_t *p_rx_nbytes);*

1. 主机命令

命令类型（CmdClass）： 0x02

命令代码（CmdCode）： ‘S’

信息长度（InfoLength）： n

信　　息（Info）： 数据长度（1 字节）：实际数据长度

数据（n-1 字节）：实际传输的命令数据串

例　　如： 验证 NTAG213F 的密钥，默认密钥 4 个 FF

表 3.75　获取值块的值命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	0053	0006
Info					CheckSum
06 1B FF FF FF FF					FAD5

2. 从机应答

状　　态（Status）： 0——成功，其它——失败

信息长度（InfoLength）： n

信　　息（Info）： 数据（n 字节）：卡片返回信息

例　　如： 验证 NTAG213F 密钥命令返回（返回 2byte 的 PACK）

表 3.76　获取值块的值成功的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0002
Info					CheckSum
00 00					FF48

3.2.18 数据交互命令（Cmd = X）

该命令用读写器与卡片的数据交互，通过该命令可以实现读写卡器的所有功能。

声明：*uint8_t zsn603_mifare_exchange_block(zsn603_handle_t handle,*

*uint8_t *p_data_buf,*

```
uint8_t     len,
uint8_t     wtxm_crc,
uint8_t     fwi,
uint8_t     *p_rx_buf,
uint32_t    *p_len);
```

1. 主机命令

命令类型（CmdClass）：　0x02

命令代码（CmdCode）：　‘X’

信息长度（InfoLength）：　交互数据块长度+2

信　　息（Info）：　交互数据块（其内容与实际使用的 CPU 卡有关）

WTXM_CRC（1 字节），该字节内容如表 3.77 所示

表 3.77　WTXM_CRC 字节描述

B7～B2	B1	B0
WTXM	RFU 0	0　CRC 禁能 1　CRC 使能

FWI（1 字节）：　超时等待时间编码，FWI 应小于 0x10

超时时间=（（0x01<<FWI）*302us）

例　　如：　向一张已被激活的 Mifare DESFire 卡发送“请求应答以选择（RATS）”命令，交互的数据块为该命令的命令帧（0xE0,0x50），帧长 2 字节（不包括 CRC 校验，其中 0xE0 是 RATS 的命令编码，0x50 的高半字节为 FSDI，低半字节为 CID，FSDI=5 表示最大交互帧为 64 字节）

表 3.78　数据交互命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	02	0058	0004
Info					CheckSum
E0 50 01 04					FDBA

2. 从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0x06

信　　息（Info）：　ATS

例　　如：　RATS 命令执行成功的回应

表 3.79　数据交互成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	02	0000	0006
Info					CheckSum
06 77 81 02 80 00					FDC4

3.3 ISO7816-3 类命令（CmdClass = 0x05）

ISO7816-3 类命令汇总表如表 3.80 所示。

表 3.80 ISO7816-3 类命令一览表

命令码	意义
‘B’	接触式 IC 卡传输协议
‘C’	接触式 IC 卡冷复位
‘D’	接触式 IC 卡热复位
‘E’	接触式 IC 卡停活（关闭电源和时钟）
‘G’	接触式 IC 卡 T=0 传输协议

其中‘B’命令是组合命令，根据卡片的实际情况自动调整通信协议；‘C’、‘D’、‘E’~‘E’命令需要使用者自己根据卡片的情况来调用不同的命令；‘E’命令是停活命令，执行该命令后，IC 卡处于掉电状态。实际上对用户来说，只需要使用‘B’、‘C’ 、 ‘D’命令即可。

注意：与接触式卡通信，采用的是 9600 固定波特率进行通信。‘D’命令没有控制电源，执行该命令前必须保证该 IC 卡没有处于停活状态。

3.3.1 接触式 IC 卡传输协议（自动处理 T = 0）

该命令根据接触式 IC 卡的复位信息，自动选择 T = 0 或 T = 1 传输协议，整个过程不需要使用者干预。该命令用于传输 APDU 数据流。

声明：*uint8_t zsn603_cicc_tpdu(zsn603_handle_t handle,*
*uint8_t *p_tx_buf,*
uint32_t tx_bufsize,
*uint8_t *p_rx_buf,*
*uint32_t *p_rx_len);*

1. 主机命令

命令类型(CmdClass)： 0x05

命令代码(CmdCode)： ‘B’

信息长度(InfoLength)： 1~272

信　　息(Info)： 发送到 IC 卡的数据

例　　如： 通过 FID（文件标识符）选择 MF（FID 为：3F00）。选择文件的 APDU 如表 3.81 所示，将其转换为数据流为：00 A4 00 00 02 3F 00 00（不需要区分 APDU 的 4 种情况，‘3F00’在数据流中是以大端模式存放，即高字节在前），该命令能自动处理，其命令帧如表 3.82 所示

表 3.81 某 CPU 卡选择文件的 APDU

代码	长度 (字节)	值 (Hex)	说明
CLA	1	00	—

INS	1	A4	—
P1	1	00/04	P1=00，表示按文件标识符选择（P2 必须等于 0），可选择： • 当前目录（DF）下基本文件或子目录文件 • 同级目录文件（DF） P1=04，表示用 DF 名称选择，分如下两种情况： • P2=00，表示第一个或仅有一个 • P2=02，表示下一个
P2	1	00/02	—
Lc	1	xx	—
Data	xx	xx…xx	文件标识符或 DF 名称
Le	1	00	对于 DF 而言为卡片自动返回的 FCI 的最大长度

注意：在任何情况下均可通过标识符‘3F00’或目录名称 1PAY.SYS.DDF01 选择 MF。

表 3.82 通过 FID 选择 MF（FID 为‘3F00’）的命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	05	0042	0008
Info					CheckSum
00 A4 00 00 02 3F 00 00					FE19

2. 从机回应

执行状态（Status）： 0 — 执行成功； 其他 — 警告或失败

信息长度(InfoLength)： 不同的卡回应的字节数不同

信 息(Info)： IC 卡回复的数据

例 如： 选择 MF 操作执行成功的回应帧如表 3.83 所示

表 3.83 选择 MF 操作执行成功的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	05	0000	0019
Info					CheckSum
6F 15 84 0E 31 50 41 59 2E 53 59 53 2E 44 44 46 30 31 A5 03 88 01 01 90 00					F8B1

表 3.83 中的前 23 字节为 MF 的 FCI，最后 2 字节‘90 00’表示卡片处理成功。需要注意的是 Info 域的最后 2 字节表示卡片执行结果与回应帧中的‘Sataus’字段表示的不是同一状态，‘Sataus’字段表示是通信链路层的状态；而 Info 域的最后 2 字节表示卡片执行结果。

3.3.2 接触式 IC 卡冷复位

该命令是冷复位，执行了接触式 IC 卡上电时序，执行成功后会自动根据 IC 卡的复位信息来选择‘B’命令使用的传输协议（T = 0），并使用 9600 波特率进行通信。

声明：*uint8_t zsn603_cicc_cold_reset(zsn603_handle_t handle,*
*uint8_t *p_rx_buf,*
*uint32_t *p_rx_len);*

1. 主机命令

命令类型(CmdClass)： 0x05

命令代码(CmdCode)： ‘C’

信息长度(InfoLength)： 0x00

例　　如： 接触式 IC 卡冷复位命令帧，如表 3.84 所示

表 3.84　接触式 IC 卡冷复位命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	05	0043	0000
Info					CheckSum
none					FE05

2. 从机回应

执行状态（Status）： 0 — 执行成功； 其他 — 警告或失败

信息长度(InfoLength)： 16 + （不同的卡回应的字节数不同）

信　　息(Info)： 保留信息（16 字节，该信息为任意值）

接触式 IC 卡复位信息（不同的卡复位信息长度不同）

例　　如： 接触式 IC 卡复位操作执行成功的回应帧如表 3.85 所示。

表 3.85　接触式 IC 卡冷复位操作执行成功的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	05	0000	001D
Info					CheckSum
13 50 41 59　2E 53 59 53　2E 44 44 46　30 31 A5 03　3B 69 00 00　57 44 37 51 BA CB 18 18　35					F985

注意：表 3.85 中信息字段中的前 16 字节是无效字节，没有任何意义，保留为将来使用，用户不用理会；后 13 字节才是接触式 IC 卡的复位信息。

3.3.3 接触式 IC 卡热复位

该命令是热复位，没有执行接触式 IC 卡上电时序，执行成功后会自动根据 IC 卡的复位信息来选择‘B’命令使用的传输协议（T = 0），该命令和 3.3.2 比较只是没有执行 IC 卡上电操作。

声明：*uint8_t　zsn603_cicc_warm_reset(zsn603_handle_t　handle,*

*uint8_t　　*p_rx_buf,*

*uint32_t　　*p_rx_len);*

1. 主机命令

命令类型(CmdClass)： 0x05

命令代码(CmdCode)： ‘D’

信息长度(InfoLength)： 0x00

例　　如： 接触式 IC 卡热复位命令帧，如表 3.86 所示

表 3.86　接触式 IC 卡热复位命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	05	0044	0000
Info					CheckSum

none	FF04

2. 从机回应

执行状态（Status）：　0 — 执行成功；　其他 — 警告或失败

信息长度(InfoLength)：　16 +　（不同的卡回应的字节数不同）

信　　息(Info)：　保留信息（16 字节，该信息为任意值）

接触式 IC 卡复位信息（不同的卡复位信息长度不同）

例　　如：　接触式 IC 卡复位操作执行成功的回应帧如表 3.87 所示。

表 3.87　接触式 IC 卡热复位操作执行成功的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	05	0000	001D
Info					CheckSum
13 53 59 53　2E 44 44 46　30 31 A5 03　3B 69 00 00　3B 69 00 00　57 44 37 51 BA CB 18 18　35					F7BE

注意：表 3.88 中信息字段中的前 16 字节是无效字节，没有任何意义，保留为将来使用，用户不用理会；后 13 字节才是接触式 IC 卡的复位信息。

3.3.4 接触式 IC 卡停活

该命令是关闭接触式 IC 卡的电源和时钟。

声明：*uint8_t　zsn603_cicc_deactivation(zsn603_handle_t　handle);*

1. 主机命令

命令类型(CmdClass)：　0x05

命令代码(CmdCode)：　'E'

信息长度(InfoLength)：　0

信　　息(Info)：　none

例　　如：　关闭接触式 IC 卡电源和时钟的命令帧如表 3.88 所示

表 3.88　接触式 IC 卡停活命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	05	0045	0000
Info					CheckSum
none					FF03

2. 从机回应

执行状态（Status）：　0 — 执行成功；　其他 — 警告或失败

信息长度(InfoLength)：　0

信　　息(Info)：　none

例　　如：　接触式 IC 卡停活操作执行成功的回应帧如表 3.89 所示

表 3.89　接触式 IC 卡停活操作执行成功的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength

B3	00	00	05	0000	0000
Info					CheckSum
none					FF47

3.3.5 接触式 IC 卡传输协议（T = 0）

该命令用于 T = 0 传输协议。若接触式 IC 卡的传输协议为 T = 0，该命令等同于 Cicc_TPDU()。

声明：*uint8_t zsn603_cicc_tp0(zsn603_handle_t handle,*
*uint8_t *p_tx_buf,*
uint32_t tx_bufsize,
*uint8_t *p_rx_buf,*
*uint32_t *p_rx_len);*

1. 主机命令

命令类型(CmdClass)： 0x05

命令代码(CmdCode)： ‘G’

信息长度(InfoLength)： 1~272

信　　息(Info)： 发送到 IC 卡的数据

例　　如： 通过 FID（文件标识符）选择 MF（FID 为：3F00）。选择文件的 APDU 如表 3.81 所示，将其转换为数据流为：00 A4 00 00 02 3F 00 00（不需要区分 APDU 的 4 种情况，‘3F00’在数据流中是以大端模式存放，即高字节在前），该命令能自动处理，其命令帧如表 3.90 所示

表 3.90　通过 FID 选择 MF（FID 为‘3F00’，T=0）的命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	05	0047	0008
Info					CheckSum
00 A4 00 00 02 3F 00 00					FE14

2. 从机回应

执行状态（Status）： 0 — 执行成功；　其他 — 警告或失败

信息长度(InfoLength)： 不同的卡回应的字节数不同

信　　息(Info)： IC 卡回复的数据

例　　如： 选择 MF 操作执行成功的回应帧如表 3.91 所示

表 3.91　选择 MF（T=0）操作执行成功的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	05	0000	0019
Info					CheckSum
6F 15 84 0E　31 50 41 59　2E 53 59 53　2E 44 44 46　30 31 A5 03　88 01 01 90　00					F8B1

表 3.91 中的前 23 字节为 MF 的 FCI，最后 2 字节‘90 00’表示卡片处理成功。需要注意的是 Info 域的最后 2 字节表示卡片执行结果与回应帧中的‘Sataus’字段表示的不是同一

状态，‘Sataus’字段表示是通信链路层的状态；而 Info 域的最后 2 字节表示卡片执行结果。

3.4 ISO14443（PICC）卡类命令（CmdClass = 0x06）

ISO14443（PICC）卡类命令总汇如表 3.92 所示。

表 3.92 ISO14443（PICC）卡类命令一览表

命令码	意义
‘A’	A 型卡请求
‘B’	A 型卡防碰撞
‘C’	A 型卡选择
‘D’	A 型卡挂起
‘E’	A 型卡 RATS
‘F’	A 型卡 PPS
‘G’	A 型卡解除激活
‘H’	T=CL
‘J’	数据交换
‘L’	A 型卡复位
‘M’	A 型卡激活
‘N’	B 型卡激活
‘O’	B 型卡复位
‘P’	B 型卡请求
‘R’	B 型卡修改传输属性
‘S’	B 型卡挂起
‘T’	读二代身份证 ID

前 4 条命令（命令 A～D）是 ISO14443-3A 标准定义的命令，只要符合该标准的卡都应能发出响应；中间 4 条命令（命令 E～H）为是 ISO14443-4 标准定义的命令。其中 A～D 命令和 Mifare S50/S70 卡类命令的 A～D 命令完全相同

3.4.1 A 型卡请求（Cmd = A）

该命令用于 A 型卡的请求操作，该命令的操作与 Mifare S50/S70 卡类的请求命令一样。

例　　如：请求天线范围内所有的 A 型卡。

主机命令：B2 00 00 06 41 00 01 00 52 B3 FE。

3.4.2 A 型卡防碰撞（Cmd = B）

该命令用于 A 型卡的防碰撞，该命令的操作与 Mifare S50/S70 卡类的防碰撞命令一样。

例　　如：第一级防碰撞。

主机命令：B2 00 00 06 42 00 02 00 93 00 70 FE。

3.4.3 A 型卡选择（Cmd = C）

该命令用于 A 型卡的选择，该命令的操作与 Mifare S50/S70 卡类的卡选择命令一样。

例　　如：第一级选择，UID 为 0xEB1C1814。

主机命令：B2 00 00 06 43 00 05 00 93 14 18 1C EB 39 FD。

3.4.4 A 型卡挂起（Cmd = D）

该命令用于 A 型卡的挂起，该命令的操作与 Mifare S50/S70 卡类的卡挂起命令一样。

例　　如：将已激活的卡挂起，使之不响应请求空闲卡命令。

主机命令：B2 00 00 06 44 00 00 00 03 FF。

3.4.5 A 型卡 RATS（Cmd = E）

RATS（request for answer to select）是 ISO14443-4 协议的命令，芯片发送 RATS，卡片发出 ATS（answer to select）作为 RATS 的应答，在执行该命令前，必需先进行一次卡选择操作，且执行过一次 RATS 命令后，想再次执行 RATS 命令，必需先解除激活。

声明：*uint8_t　zsn603_picca_rats(zsn603_handle_t　handle,*

uint8_t　cid,

*uint8_t　*p_ats_buf,*

*uint32_t　*p_rx_len);*

1.　主机命令

命令类型（CmdClass）：　0x06

命令代码（CmdCode）：　'E'

信息长度（InfoLength）：　0x01

信　　息（Info）：　CID（1 字节）：　卡标识符（card IDentifier，取值范围 0x00～0x0E）

例　　如：　向 PLUS CPU 卡发送 RATS 命令，CID 设备为 0x0A

表 3.93　A 型卡 RATS 命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	06	0045	0001
Info					CheckSum
0A					FEF7

2.　从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0x0C（不同的卡，ATS 的字节数不同）

信　　息（Info）：　ATS

例　　如：　一张 SL3 的 PLUS CPU 卡会回应的 ATS

表 3.94　A 型卡响应 RATS 的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	06	0000	000C
Info					CheckSum
0C 75 77 80　02 C1 05 2F　2F 01 BC D6					FB09

3.4.6 A 型卡 PPS（Cmd = F）

PPS（protocal and parameter selection）是 ISO14443-4 协议的命令，用于改变有关的专用协议参数，该命令不是必需的，命令只支持默认参数，即该命令的参数设置为 0 即可。在执行该命令前，必需先成功执行一次 RATS 命令。

声明：*uint8_t zsn603_picca_pps(zsn603_handle_t handle,*
uint8_t dsi_dri);

1. 主机命令

命令类型（CmdClass）：0x06
命令代码（CmdCode）：‘F’
信息长度（InfoLength）：0x01
信　　息（Info）：DSI_DRI（1 字节）：芯片与卡通信波特率，设置为 0（106Kb/s）
例　　如：将 PLUS CPU 卡与芯片间的通信波特率设置为 106Kb/s

表 3.95　A 型卡 PPS 命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	06	0046	0001
Info					CheckSum
00					FF00

2. 从机应答

状　　态（Status）：0——成功，其它——失败
信息长度（InfoLength）：0
信　　息（Info）：none
例　　如：PLUS CPU 卡执行 PPS 成功后的回应

表 3.96　A 型卡响应 PPS 的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	06	0000	0000
Info					CheckSum
none					FF46

3.4.7 A 型卡解除激活（Cmd = G）

该命令是 ISO14443-4 协议的命令，用于将卡片置为挂起（HALT）状态，处于挂起（HALT）状态的卡可以用“请求”命令（请求代码为 ALL）来重新激活卡，只有执行“RATS”命令的卡才用该命令。

声明：*uint8_t zsn603_picca_deselect(zsn603_handle_t handle);*

1. 主机命令

命令类型（CmdClass）：0x06
命令代码（CmdCode）：‘G’
信息长度（InfoLength）：0
信　　息（Info）：none
例　　如：将激活的卡置为挂起状态

表 3.97　A 型卡解除激活命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	06	0047	0000
Info					CheckSum
none					FF00

2. 从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　none

例　　如：　PLUS CPU 卡执行 PPS 成功后的回应

表 3.98　A 型卡响应解除激活的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	06	0000	0000
Info					CheckSum
none					FF46

3.4.8 T=CL（Cmd = H）

T=CL 是半双工分组传输协议，ISO14443-4 协议命令，用于读写器与卡片之间的数据交互，一般符合 ISO14443 协议的 CPU 卡均用该协议与读写器通信。调用该命令时只需要将 CPU 卡 COS 命令的数据作为输入即可，其他的如分组类型、卡标识符 CID、帧等待时间 FWT、等待时间扩展倍增因子 WTXM（waiting time extensionmultiplier），等等由该命令自动完成。

声明：*uint8_t　zsn603_picca_tpcl(zsn603_handle_t　handle,*

*uint8_t　　*p_cos_buf,*

uint8_t　　cos_bufsize,

*uint8_t　　*p_res_buf,*

*uint32_t　　*p_rx_len);*

1. 主机命令

命令类型（CmdClass）：　0x06

命令代码（CmdCode）：　‘H’

信息长度（InfoLength）：　COS 命令的长度

信　　息（Info）：　COS 命令

例　　如：　选择 FM1208 的 MF 标识符为 3F00，选择 COS 命令如下

表 3.99　FM1208 选择 MF 的命令编码

代码	CLA	INS	P1	P2	Lc	Data	Le
值	00	A4	00	00	02	3F 00	—

表 3.100　A 型卡 T=CL 命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	06	0048	0007
Info					CheckSum

00 A4 00 00 02 3F 00	FE13

2. 从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　COS 命令回应数据长度

信　　息（Info）：　COS 命令回应数据

例　　如：　FM1208 选择 MF 时响应的数据为嵌套的 TLV 格式的变长记录，其意义请参考《FMCOS 用户手册》

表 3.101　A 型卡响应 T=CL 的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	06	0000	0016
Info					CheckSum
6F 15 84 0E　31 50 41 59　53 2E 44 44　46 30 31 A5　03 88 01 01　90 00					F98D

3.4.9 数据交换（Cmd = J）

该命令用读写器与卡片的数据交互，通过该命令可以实现读写卡器的所有功能。

声明：*uint8_t　zsn603_picca_exchange_block(zsn603_handle_t　handle,*

*uint8_t　*p_data_buf,*

uint8_t　len,

uint8_t　wtxm_crc,

uint8_t　fwi,

*uint8_t　*p_rx_buf,*

*uint32_t　*p_rx_len);*

1. 主机命令

命令类型（CmdClass）：　0x06

命令代码（CmdCode）：　'J'

信息长度（InfoLength）：　交互数据块长度+2

信　　息（Info）：　交互数据块（其内容与实际使用的 CPU 卡有关）

WTXM_CRC（1 字节），该字节内容如表 3.102 所示

表 3.102　WTXM_CRC 字节描述

B7～B2	B1	B0
WTXM	RFU 0	0　CRC 禁能 1　CRC 使能

FWI（1 字节）：　超时等待时间编码，FWI 应小于 0x10

超时时间=（(0x01<<FWI）*302us）

例　　如：　向一张已被激活的 Mifare DESFire 卡发送"请求应答以选择（RATS）"命令，交互的数据块为该命令的命令帧（0xE0,0x50），帧长 2 字节（不包括 CRC 校验，其中 0xE0 是 RATS 的命令编码，0x50 的高半字节为 FSDI，低半字节为 CID，FSDI=5 表示最大交互帧为 64 字节）

表 3.103　数据交互命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	06	004A	0004
Info					CheckSum
E0 50 01 04					FDC4

2.　从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0x06

信　　息（Info）：　ATS

例　　如：　RATS 命令执行成功的回应

表 3.104　数据交互成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	06	0000	0006
Info					CheckSum
06 77 81 02 80 00					FDC0

3.4.10　A 型卡复位（Cmd = L）

该命令是通过将载波信号关闭指定的时间，再开启来实现卡片复位。

声明：*uint8_t　zsn603_picca_reset(zsn603_handle_t　handle,*

uint8_t　time_ms);

1.　主机命令

命令类型（CmdClass）：　0x06

命令代码（CmdCode）：　‘L’

信息长度（InfoLength）：　0x01

信　　息（Info）：　时间（1 字节），以毫秒为单位，0 为一直关闭

例　　如：　将载波信号关闭 1ms

表 3.105　卡复位命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	06	004C	0001
Info					CheckSum
01					FEF9

2.　从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　none

例　　如：　执行卡复位成功芯片的回应

表 3.106　卡复位成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	06	0000	0000
Info					CheckSum
none					FF46

3. 说明

该命令将天线信号关闭数毫秒，若一直关闭，则等到执行一个请求命令时打开。

3.4.11 A 型卡激活（Cmd = M）

该命令用于激活卡片，是请求、防碰撞和选择三条命令的组合。

声明：*uint8_t zsn603_picca_active(zsn603_handle_t handle,*
uint8_t req_mode,
*uint16_t *p_atq,*
*uint8_t *p_saq,*
*uint32_t *p_len,*
*uint8_t *p_uid);*

1. 主机命令

命令类型（CmdClass）：0x06
命令代码（CmdCode）：‘M’
信息长度（InfoLength）：0x02
信　　息（Info）：保留（1 字节），设置为 0
请求代码（1 字节）：0x26～IDLE
0x52～ALL
例　　如：以 IDLE 方式激活卡

表 3.107 卡激活命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	06	004D	0002
Info					CheckSum
00 26					FED2

2. 从机应答

状　　态（Status）：0——成功，其它——失败
信息长度（InfoLength）：Mifare1 S50、S70、Light 卡：8 字节
Mifare0 UltraLight 卡：11 字节
Mifare3 Desfire 卡：11 字节
Plus CPU 卡：8 字节或 11 字节
信　　息（Info）：请求应答 ATQ（2 字节）
最后一级选择应答 SAK（1 字节）
序列号长度（1 字节）
序列号（N 字节，由序列号长度决定）

例　　如：　　一张序列号为 0xEB1C1814 的 Mifare1 S50 卡返回的数据

表 3.108　卡激活成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	06	0000	0008
Info					CheckSum
04 00 08 04 14 18 1C EB					FDFB

3.4.12　B 型卡激活（Cmd = N）

该命令用于激活 B 型卡片，在调用该命令前，需要先执行设备控制类的“设置 IC 卡接口协议（工作模式）（Cmd = D）”，把芯片先配置成 TypeB 模式。

声明：*uint8_t　zsn603_piccb_active(zsn603_handle_t　handle,*

uint8_t　　req_mode,

*uint8_t　　*p_info);*

1.　主机命令

命令类型（CmdClass）：　0x06

命令代码（CmdCode）：　‘N’

信息长度（InfoLength）：　0x02

信　　息（Info）：　请求代码（1 字节）：　0x00～IDLE

0x08～ALL

应用标识（1 字节）：　默认为 0x00

例　　如：　以 IDLE 方式激活卡

表 3.109　卡激活命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	06	004E	0002
Info					CheckSum
00 00					FEF7

2.　从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0x0C

信　　息（Info）：　UID 相关信息

例　　如：　一张 TypeB 卡激活后返回的数据

表 3.110　卡激活成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	06	0000	000C
Info					CheckSum
70 05 34 07 00 00 00 00 00 81 C1 00					FD48

3.4.13　B 型卡复位（Cmd = O）

该命令是通过将载波信号关闭指定的时间，再开启来实现卡片复位，其实现方式与 A 型卡复位一样。

声明：*uint8_t zsn603_piccb_reset(zsn603_handle_t handle,*
uint8_t time_ms);

1. 主机命令

命令类型（CmdClass）：0x06
命令代码（CmdCode）：‘O’
信息长度（InfoLength）：0x01
信　　息（Info）：时间（1 字节），以毫秒为单位，0 为一直关闭
例　　如：将载波信号关闭 1ms

表 3.111　卡复位命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	06	004F	0001
Info					CheckSum
01					FEF6

2. 从机应答

状　　态（Status）：0——成功，其它——失败
信息长度（InfoLength）：0
信　　息（Info）：none
例　　如：执行卡复位成功芯片的回应

表 3.112　卡复位成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	06	0000	0000
Info					CheckSum
none					FF46

3.4.14　B 型卡请求（Cmd = P）

该命令用于 B 型卡请求。

声明：*uint8_t zsn603_piccb_request(zsn603_handle_t handle,*
uint8_t req_mode,
uint8_t slot_time,
*uint8_t *p_uid);*

1. 主机命令

命令类型（CmdClass）：0x06
命令代码（CmdCode）：‘P’
信息长度（InfoLength）：0x03
信　　息（Info）：请求代码（1 字节）：0x00～IDLE
0x08～ALL

应用标识（1 字节）： 默认为 0x00

时隙总数（1 字节）： 范围 0～4

例　　如： 以 IDLE 方式请求卡片

表 3.113　卡请求命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	06	0050	0003
Info					CheckSum
00 00 00					FEF4

2. 从机应答

状　　态（Status）： 0——成功，其它——失败

信息长度（InfoLength）： 0x0C

信　　息（Info）： UID 相关信息

例　　如： 一张 TypeB 卡请求成功后返回的数据

表 3.114　卡请求成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	06	0000	000C
Info					CheckSum
70 05 34 07　00 00 00 00　00 81 C1 00					FD48

3.4.15　B 型卡修改传输属性（Cmd = R）

该命令用于 B 型卡修改传输属性（卡选择）。

声明：*uint8_t　zsn603_piccb_attrib(zsn603_handle_t　handle,*

*uint8_t　　*p_pupi,*

uint8_t　　cid,

uint8_t　　protype);

1. 主机命令

命令类型（CmdClass）： 0x06

命令代码（CmdCode）： ‘R’

信息长度（InfoLength）： 0x06

信　　息（Info）： PUPI（4 字节）： 卡片标识符

CID（1 字节）： 取值范围为 0 - 14，若不支持 CID，则设置为 0

proType（1 字节）：支持的协议，由请求回应中的 ProtocolType 指定

proType.3：PCD 与 PICC 是否继续通信

1～PCD 中止与 PICC 继续通信

0～PCD 与 PICC 继续通信

proType.2:1：PICC EOF 和 PCD SOF 间的最小延迟

11～10 etu + 512 / fs

10～10 etu + 256 / fs

01～10 etu + 128 / fs

00～10 etu + 32 / fs

proType.0：是否遵循 ISO14443-4

1～遵循 ISO14443-4;

0～不遵循 ISO14443-4. (二代证必须为 1)

例　　如：　　选择 PUPI 为 0x07340570

表 3.115　卡选择命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	06	0052	0006
Info					CheckSum
70 05 34 07 00 01					FE3E

2.　从机应答

状　　态（Status）：　　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　　none

例　　如：　　卡选择成功的回应

表 3.116　卡选择成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	06	0000	0000
Info					CheckSum
none					FF46

3.4.16　B 型卡挂起（Cmd = S）

该命令用于 B 型卡挂起，在执行挂起命令前，必需先执行成功过一次请求命令。执行挂起命令成功后，卡片处于挂起状态，芯片必需通过 ALL 方式请求卡片，而不能用 IDLE 方式请求。

声明：*uint8_t　zsn603_piccb_halt(zsn603_handle_t　handle,*

*uint8_t　*p_pupi);*

1.　主机命令

命令类型（CmdClass）：　0x06

命令代码（CmdCode）：　‘S’

信息长度（InfoLength）：　0x04

信　　息（Info）：　　PUPI（4 字节）：　4 字节标识符

例　　如：　　挂起 PUPI 为：0x38492295 的卡片

表 3.117　卡挂起命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength

B2	00	00	06	0053	0004
Info					CheckSum
95 22 49 38					FDB8

2. 从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　none

例　　如：　卡挂起成功的回应

表 3.118　卡挂起成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	06	0000	0000
Info					CheckSum
none					FF46

3.4.17　读二代身份证 ID（CMD = T）

该命令用于获取身份证的物理 ID，在调用该命令前，需要先执行设备控制类的“设置 IC 卡接口协议（工作模式）（Cmd = D）”，把芯片先配置成 TypeB 模式。

声明：*uint8_t　zsn603_piccb_getid(zsn603_handle_t　handle,*

uint8_t　req_mode,

*uint8_t　*p_uid);*

1. 主机命令

命令类型（CmdClass）：　0x06

命令代码（CmdCode）：　‘T’

信息长度（InfoLength）：　0x02

信　　息（Info）：　请求代码（1 字节）：　0x00～IDLE

0x08～ALL

应用标识（1 字节）：　默认为 0x00

例　　如：　读取身份证 ID 号

表 3.119　读二代身份证命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	06	0054	0002
Info					CheckSum
00 00					FEF1

2. 从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　8

信　　息（Info）：　none

例　　如：　读二代身份证 ID 成功的回应

表 3.120　读 ID 成功的回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	06	0000	0008
Info					CheckSum
22 03 F4 80 A0 81 69 69					FBB

3.5 PLUS CPU 卡类命令（CmdClass = 0x07）

PLUS CPU 卡类命令总汇如表 3.121 所示，该命令集包括了 PLUS CPU 卡 SL0（Security Level 0）、SL3 的命令，其中等级 1 的命令与 Mifare S50/S70 卡（M1）相同，所以不在本命令集中。

表 3.121 PLUS CPU 卡类命令一览表

命令码	意义
‘B’	SL0 个人化更新数据
‘C’	SL0 提交个人化
‘J’	SL3 首次验证（直接密钥验证）
‘K’	SL3 首次验证（E^2 密钥验证）
‘L’	SL3 跟随验证（直接密钥验证）
‘M’	SL3 跟随验证（E^2 密钥验证）
‘N’	SL3 复位验证
‘O’	SL3 读数据块
‘P’	SL3 写数据块
‘S’	SL3 值块操作

卡片激活后，只有通过“首次验证”之后才能使用“跟随验证”，卡片激活后，则只需要第一次验证命令使用“首次验证”命令，之后的验证命令都可以使用“跟随验证”，当然也可以都是用“首次验证”；若执行“复位验证”，则“复位验证”之后的第一次验证，也必须使用“首次验证”命令。两种验证的区别在于使用的时机不同，“首次验证”所需要的时间比“跟随验证”的时间要长些。

PLUS CPU 卡的密钥 A/B 是通过地址的奇偶数来区分，AES 的密钥地址与数据块的扇区关系对应如下。

- 密钥 A 地址=0x4000 + 扇区 × 2
- 密钥 B 地址=0x4000 + 扇区 × 2 + 1

除扇区密钥外，其它密钥不分密钥 A/B，详细的 PLUS CPU 卡地址分配请参阅 PLUS CPU 卡的数据手册。

PLUS CPU 卡的基本操作流程为：

SL0 卡：卡片激活→RATS 命令→更新个人化数据→提交个人化（此时等级卡片为 SL1 或 SL3，支持 SL1 的卡先会变成 SL1）。

SL1 卡（升级操作）：卡片激活→ RATS 命令→首次密钥认证（采用 SL3 的地址、密钥，操作完后，卡片重新上电，等级变为 SL3）。

SL1 卡：普通操作，操作内容完全兼容 M1 卡。

SL3 卡：卡片激活→ RATS 命令→首次密钥认证→跟随认证→读写块操作。

3.5.1 SL0 个人化更新数据（Cmd = B）

该命令用于 SL0（Security Level 0，安全等级 0）的 PLUS CPU 卡个人化，PLUS CPU 卡出厂时的安全等级为 SL0，该等级下，不需要任何验证就可以向卡里写数据，写入的数据是作为其它安全等级的初始值，例如：

向 SL0 的 0x0003 块写入 0xA0 0xA1 0xA2 0xA3 0xA4 0xA5 0xFF 0x07 0x80 0x69 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF，当卡片升级到 SL1 后，扇区 0 的 A 密钥为 0xA0 0xA1 0xA2 0xA3 0xA4 0xA5，而不是默认的 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF，即可以在 SL0 修改卡片的默认数据和密钥。

注意：PLUS CPU 卡在 SL0 的存储器地址均为 2 字节，其中地址 0x0000～0x00FF 为用户数据块，与 Mifare S50/S70 卡的数据/密钥块一一对应，该命令是 ISO14443-4 的命令。

声明：*uint8_t zsn603_plus_cpu_write_perso(zsn603_handle_t handle,*
uint16_t addr,
*uint8_t *p_data);*

1. 主机命令

命令类型（CmdClass）： 0x07
命令代码（CmdCode）： ‘B’
信息长度（InfoLength）： 0x12
信　　息（Info）： BNr（2 字节）： PLUS CPU 卡存储器地址
Data（16 字节）： 数据/AES 密钥/配置字
例　　如： 更改 PLUS CPU 卡的主控密钥（地址为 0x9000）

表 3.122　SL0 个人化更新数据命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	07	0042	0012
Info					CheckSum
00 90 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF					EE72

2. 从机应答

状　　态（Status）： 0——成功，其它——失败
信息长度（InfoLength）： 0
信　　息（Info）： none
例　　如： 更改主控密钥成功的回应

表 3.123　SL0 个人化更新数据成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	07	0000	0000
Info					CheckSum
none					FF45

3.5.2 SL0 提交个人化（Cmd = C）

该命令用于 SL0（Security Level 0，安全等级 0）的 PLUS CPU 卡提交个人化数据，命令“SL0 个人化更新数据”只是更新卡中的数据，但该数据还未生效，用户还不能直接使用。“SL0 提交个人化”使更新的个人化数据生效。执行该命令后，PLUS CPU 卡的安全等级提高到 SL1 或者 SL3（若是支持 SL1 的卡，则执行该命令后卡片安全等级提高到 SL1；若是只支持 SL0 和 SL3 的卡，则执行该命令后卡片安全等级提高到 SL3）。

注意：在 SL0 的 PLUS CPU 卡，只有修改了以下地址才能执行“SL0 提交个人化”命令：

- 0x9000（主控密钥）
- 0x9001（配置块密钥）
- 0x9002（SL2 提升密钥，只有支持 SL2 的卡才有该密钥）
- 0x9003（SL3 主控密钥，只有支持 SL3 的卡才有该密钥）

该命令是 ISO14443-4 的命令

声明：*uint8_t zsn603_plus_cpu_commit_perso(zsn603_handle_t handle);*

1. 主机命令

命令类型（CmdClass）：0x07

命令代码（CmdCode）：‘C’

信息长度（InfoLength）：0

信　　息（Info）：none

例　　如：将已修改主控密钥、配置块密钥、SL2 提升密钥和 SL3 主控密钥卡的安全等级提高到 SL1

表 3.124　SL0 提交个人化命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	07	0043	0000
Info					CheckSum
none					FF 03

2. 从机应答

状　　态（Status）：0——成功，其它——失败

信息长度（InfoLength）：0

信　　息（Info）：none

例　　如：更改主控密钥成功的回应

表 3.125　SL0 提交个人化成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	07	0000	0000
Info					CheckSum
none					FF45

3.5.3 SL3 首次验证（直接密钥验证）（Cmd = J）

该命令用于 SL3 PLUS CPU 卡的密钥验证，验证的密钥通过该命令的参数输入。

声明：*uint8_t zsn603_plus_cpu_first_auth_e2(zsn603_handle_t handle,*
uint16_t addr,
uint8_t key_block);

1. 主机命令

命令类型（CmdClass）：0x07

命令代码（CmdCode）：‘J’

信息长度（InfoLength）：0x12

信　　息（Info）：　　AES 密钥地址（2 字节）

AES 密钥（16 字节）

例　　如：　　用密钥“FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF”验证 1 扇区的 AES 密钥 A（1 扇区的 AES 密钥 A 对应的密钥地址为 0x4002）

表 3.126　SL3 首次验证（直接密钥验证）命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	07	004A	0012
Info					CheckSum
02 40 FF FF　FF FF FF FF　FF FF FF FF　FF FF FF FF　FF FF					EEB8

2.　从机应答

状　　态（Status）：　　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　　none

例　　如：　　验证密钥成功的回应

表 3.127　SL3 首次验证（直接密钥验证）成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	07	0000	0000
Info					CheckSum
none					FF45

3.5.4 SL3 首次验证（E^2 密钥验证）（Cmd = K）

该命令也是用于 SL3 PLUS CPU 卡的密钥验证，验证的密钥来自芯片内部，掉电不丢失的数据。

声明：*uint8_t　zsn603_plus_cpu_follow_auth(zsn603_handle_t　handle,*

uint16_t　addr,

*uint8_t　*p_data);*

1.　主机命令

命令类型（CmdClass）：　0x07

命令代码（CmdCode）：　‘K’

信息长度（InfoLength）：　0x03

信　　息（Info）：　　AES 密钥地址（2 字节）

密钥区号（1 字节）

例　　如：　　用密钥 1 区的密钥验证 1 扇区的 AES 密钥 A（密钥地址为 0x4002）

表 3.128　SL3 首次验证（E^2 密钥验证）命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	07	004B	0003
Info					CheckSum

02 40 01	FEB5

2. 从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　none

例　　如：　验证密钥成功的回应

表 3.129　SL3 首次验证（E^2 密钥验证）成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	07	0000	0000
Info					CheckSum
none					FF45

3.5.5 SL3 跟随验证（直接密钥验证）（Cmd = L）

该命令用于 SL3 PLUS CPU 卡的跟随密钥验证，验证的密钥来自命令参数，只有执行过“首次验证”命令成功后才能使用该命令。

声明：*uint8_t　zsn603_plus_cpu_follow_auth_e2(zsn603_handle_t　handle,*
uint16_t　addr,
uint8_t　key_block);

1. 主机命令

命令类型（CmdClass）：　0x07

命令代码（CmdCode）：　‘L’

信息长度（InfoLength）：　0x12

信　　息（Info）：　AES 密钥地址（2 字节）

AES 密钥（16 字节）

例　　如：　用密钥“FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF”验证 1 扇区的 AES 密钥 A（1 扇区的 AES 密钥 A 对应的密钥地址为 0x4002）

表 3.130　SL3 跟随验证（直接密钥验证）命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	07	004C	0012
Info					CheckSum
02 40 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF					EEB6

2. 从机应答

状　　态（Status）：　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　none

例　　如：　验证密钥成功的回应

表 3.131　SL3 跟随验证（直接密钥验证）成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	07	0000	0000
Info					CheckSum
none					FF45

3.5.6 SL3 跟随验证（E² 密钥验证）（Cmd = M）

该命令用于 SL3 PLUS CPU 卡的跟随密钥验证，验证的密钥来自芯片内部掉电不丢失的数据，只有执行过“首次验证”命令成功后才能使用该命令。

声明：*uint8_t zsn603_plus_cpu_follow_auth_e2(zsn603_handle_t handle,*
uint16_t addr,
uint8_t key_block);

1. 主机命令

命令类型（CmdClass）：0x07
命令代码（CmdCode）：‘M’
信息长度（InfoLength）：0x03
信　　息（Info）：AES 密钥地址（2 字节）
密钥区号（1 字节）
例　　如：用密钥 1 区的密钥验证 1 扇区的 AES 密钥 A（密钥地址为 0x4002）

表 3.132　SL3 跟随验证（E² 密钥验证）命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	07	004D	0003
Info					CheckSum
02 40 01					FEB3

2. 从机应答

状　　态（Status）：0——成功，其它——失败
信息长度（InfoLength）：0
信　　息（Info）：none
例　　如：验证密钥成功的回应

表 3.133　SL3 跟随验证（E² 密钥验证）成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	07	0000	0000
Info					CheckSum
none					FF45

3.5.7 SL3 复位验证（Cmd = N）

该命令用于 PLUS CPU 卡通过首次验证后的使用过程中，复位读写计数器和验证等信息。

声明：*uint8_t zsn603_plus_cpu_sl3_reset_auth(zsn603_handle_t handle);*

1. 主机命令

命令类型（CmdClass）： 0x07

命令代码（CmdCode）： ‘N’

信息长度（InfoLength）： 0

信　　息（Info）： none

例　　如： 复位验证卡片的验证信息

表 3.134　SL3 复位验证命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	07	004E	0000
Info					CheckSum
none					FEF8

2. 从机应答

状　　态（Status）： 0——成功，其它——失败

信息长度（InfoLength）： 0

信　　息（Info）： none

例　　如： 验证密钥成功的回应

表 3.135　SL3 复位验证成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	07	0000	0000
Info					CheckSum
none					FF45

3. 说明

若执行“复位验证”命令，读写计数器和所有的认证信息都将清空，若还需要对卡片进行操作，则必需使用“首次验证”命令或者将卡片重新激活。

3.5.8 SL3 读数据块（Cmd = O）

该命令用于读取 SL3 的数据块，在读数据块之前必需成功执行一次密钥验证。

声明：*uint8_t　zsn603_plus_cpu_sl3_read(zsn603_handle_t　handle,*
uint8_t　read_mode,
uint16_t　start_addr,
uint8_t　block_num,
*uint8_t　*p_rx_data,*
*uint32_t　*p_rx_lenght);*

1. 主机命令

命令类型（CmdClass）： 0x07

命令代码（CmdCode）： ‘O’

信息长度（InfoLength）： 0x04

信　　息（Info）： 读模式（1 字节）：0x30～命令有 MAC；数据密文；回应无 MAC
0x31～命令有 MAC；数据密文；回应有 MAC
0x32～命令有 MAC；数据明文；回应无 MAC
0x33～命令有 MAC；数据明文；回应有 MAC
0x34～命令无 MAC；数据密文；回应无 MAC
0x35～命令无 MAC；数据密文；回应有 MAC
0x36～命令无 MAC；数据明文；回应无 MAC
0x37～命令无 MAC；数据明文；回应有 MAC
起始块号（2 字节）
读的块数（1 字节）： 范围 1～3

例　　如： 从块 4 开始以“命令有 MAC，数据明文，回应有 MAC”的方式读 1 块数据

表 3.136　SL3 读数据块命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	07	004F	0004
Info					CheckSum
33 04 00 01					FEBB

2. 从机应答

状　　态（Status）： 0——成功，其它——失败

信息长度（InfoLength）： 0x10

信　　息（Info）： 数据（16 字节）

例　　如： 从卡中读出的数据为“05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05”

表 3.137　SL3 读数据块成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	07	0000	0010
Info					CheckSum
05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05					FEE5

3. 说明

在验证成功之后，才能读相应的块数据，若不同扇区的密钥相同，则所验证的块号与读块号不必在同一个扇区内。当读的块数不为 1 时，且读的块包含了区尾块（密钥/配置块），则该读操作会自动跳过区尾块读到下一个扇区的数据，若需要对区尾块进行访问时，则需要将读的起始地址设为区尾块的地址，读的块数设置为 1 即可。

PLUS CPU 卡的数据块、区尾块和 Mifare S50/70 卡分配相同，只是将块地址扩展为 2 字节。读命令可以根据需要设置如下不同的安全模式。

- 0x30～命令有 MAC；数据密文；回应无 MAC
- 0x31～命令有 MAC；数据密文；回应有 MAC

- 0x32～命令有 MAC；数据明文；回应无 MAC
- 0x33～命令有 MAC；数据明文；回应有 MAC
- 0x34～命令无 MAC；数据密文；回应无 MAC
- 0x35～命令无 MAC；数据密文；回应有 MAC
- 0x36～命令无 MAC；数据明文；回应无 MAC
- 0x37～命令无 MAC；数据明文；回应有 MAC

注意：PLUS S 系列的卡只支持“命令有 MAC，数据明文，回应有 MAC”这一种模式，数据是否加密是指——读写芯片与卡之间的数据通信是否加密，而不是芯片与主控制器间的数据是否加密。

3.5.9 SL3 写数据块（Cmd = P）

该命令用于写 SL3 的数据块，在写数据块之前必需成功执行一次密钥验证。

声明：*uint8_t zsn603_plus_cpu_sl3_write(zsn603_handle_t handle,*
uint8_t write_mode,
uint16_t start_addr,
uint8_t block_num,
*uint8_t *p_tx_data,*
uint8_t tx_lenght);

1. 主机命令

命令类型（CmdClass）： 0x07

命令代码（CmdCode）： ‘P’

信息长度（InfoLength）： 写的块数×16+4

信　　息（Info）： 写模式（1 字节）：0xA0～命令有 MAC；数据密文；回应无 MAC
0xA1～命令有 MAC；数据密文；回应有 MAC
0xA2～命令有 MAC；数据明文；回应无 MAC
0xA3～命令有 MAC；数据明文；回应有 MAC
起始块号（2 字节）
写的块数（1 字节）： 范围 1～3
写入的数据（写的块数×16 字节）

例　　如： 将“05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05”用“命令有 MAC，数据明文，回应有 MAC”的方式写到第 0x0004 块。

表 3.138 SL3 写数据块命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	07	0050	0014
Info					CheckSum
A3 04 00 01 05 05 05 05 05 05 05 05 05 05 05 05 05 05					FDEA

2. 从机应答

状　　态（Status）： 0——成功，其它——失败

信息长度（InfoLength）： 16

信　　息（Info）：　　数据（16 字节）

例　　如：　　从卡中读出的数据为“05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05”

表 3.139　SL3 写数据块成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	07	0000	0000
Info					CheckSum
none					FF45

3.　说明

在验证成功之后，才能写相应的块数据，若不同扇区的密钥相同，则所验证的块号与写块号不必在同一个扇区内。当写的块数不为 1 时，且写的块包含了区尾块（密钥/配置块），则该写操作会自动跳过区尾块写到下一个扇区的数据，若需要对区尾块进行访问时，则需要将写的起始地址设为区尾块的地址，写的块数设置为 1 即可。

PLUS CPU 卡的数据块、区尾块和 Mifare S50/70 卡分配相同，只是将块地址扩展为 2 字节。写命令可以根据需要设置如下不同的安全模式。

- 0xA0～命令有 MAC；数据密文；回应无 MAC
- 0xA1～命令有 MAC；数据密文；回应有 MAC
- 0xA2～命令有 MAC；数据明文；回应无 MAC
- 0xA3～命令有 MAC；数据明文；回应有 MAC

注意：PLUS S 系列的卡只支持“命令有 MAC，数据明文，回应有 MAC”这一种模式，数据是否加密是指——读写芯片与卡之间的数据通信是否加密，而不是芯片与主控制器间的数据是否加密。

3.5.10　SL3 值块操作（Cmd = S）

该命令用于写 SL3 的数据块，在写数据块之前必需成功执行一次密钥验证。

声明：*uint8_t　zsn603_plus_cpu_sl3_value_opr(zsn603_handle_t　handle,*
uint8_t　write_mode,
uint16_t　src_addr,
uint16_t　dst_addr,
int　data);

1.　主机命令

命令类型（CmdClass）：　0x07

命令代码（CmdCode）：　‘S’

信息长度（InfoLength）：　0x09

信　　息（Info）：　值操作模式（1 字节）：　0xB7～加值
0xB9～减值
源块号（2 字节）
目的块号（2 字节）
值数据（4 字节）：　4 字节有符号数，低字节在前，高字节的符号位被忽略

例　　如：　　将 0x0004 块的值用“加值传输模式，回应有 MAC”方式加上 0x01234567 其结果存放到 0x0005。

表 3.140　SL3 值块操作命令帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	CmdCode	InfoLength
B2	00	00	07	0053	0009
Info					CheckSum
B7 04 00 05 00 67 45 23 01					FD5A

2.　从机应答

状　　态（Status）：　　0——成功，其它——失败

信息长度（InfoLength）：　0

信　　息（Info）：　　none

例　　如：　　加值成功芯片的回应

表 3.141　SL3 值块操作成功回应帧

LocalAddr	SlotIndex	SMCSeq	CmdClass	Status	InfoLength
B3	00	00	07	0000	0000
Info					CheckSum
none					FF45

注意：PLUS S 系列卡不支持该命令。

4. 免责声明

本着为用户提供更好服务的原则，广州致远微电子有限公司（下称“致远微电子”）在本手册中将尽可能地为用户呈现详实、准确的产品信息。但介于本手册的内容具有一定的时效性，致远微电子不能完全保证该文档在任何时段的时效性与适用性。致远微电子有权在没有通知的情况下对本手册上的内容进行更新，恕不另行通知。为了得到最新版本的信息，请尊敬的用户定时访问官方网站或者与致远微电子工作人员联系。感谢您的包容与支持！

专业 . 专注成就梦想

Dreams come true with professionalism and dedication.

广州致远微电子有限公司

更多详情请访问
ww.zlgmcu.com

欢迎拨打全国服务热线
400-888-2705