/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*接触卡SAM1操作\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

//IC卡复位3V

aabb 0500 0000 1106 51

//IC卡复位5V

aabb 0500 0000 1206 51

//IC卡收发数据

aabb 0A00 0000 1306 00A4040000 51 回：aa bb 08 00 00 00 13 06 00 67 00 72

aabb 0A00 0000 1306 00A4040012 51

//IC卡去活

aabb 0500 0000 1406 51

//IC卡热复位

aabb 0500 0000 1506 51

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*接触卡SAM2操作\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

//IC卡复位3V

aabb 0500 0000 2106 51

//IC卡复位5V

aabb 0500 0000 2206 51

//IC卡收发数据

aabb 0A00 0000 2306 00A4 0400 00 51

aabb 0A00 0000 2306 00A4 0400 12 51

//IC卡去活

aabb 0500 0000 2406 51

//IC卡热复位

aabb 0500 0000 2506 51

aabb 0A00 0000 2306 00A4040012 51 其中 00A4040012 表示 下发的APDU命令

一、读写卡器与上位机通讯规则

1．上位机命令格式

Aabb 0500 00 00 11 06 51

命令头 + 长度字 + 设备标识符 ＋ 命令码 + 命令内容 + 校验字

命令头 ：2BYTE，0xAABB

长度 字 ：2BYTE (word)（低字节在前）表示长度字后的字节数；

设备标识：2BYTE 在读卡器中以“00 00”表示

命令码 ：2BYTE (word)（低字节在前）

命令内容：命令报文（可以为空）

校验字(CHK) ：1BYTE、从设备标识到命令内容最后一字节的逐字节异或

注：如果从长度字到校验字中有一个字节=AA，则后跟一字节00以区分命令头,长度字不变

2．读写卡器应答格式

命令头 + 长度字 + 设备标识符＋命令码 + 状态字 + 数据 + 校验字

命令头 ：2BYTE，0xAABB

长度字 ：2BYTE (word)（低字节在前）

设备标识：2BYTE 在没有指定设备标识时，此数为随机数。

命令码 ：2BYTE (word)（低字节在前）

状态字 ：1BYTE 、00=成功；

数据 ：返回的数据, （可以为空）

校验字(CHK) ：1BYTE、从长度字的第二字节到命令内容最后一字节的逐字节异或



选文件

*00 a4 00 00 02 3f 00 住建部的卡*

*getResponse len为要读取的长度*

0x00, 0xc0, 0x00, 0x00, len

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*SLE4442卡操作\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

//卡上电

aabb05000000310651

//卡下电

aabb05000000320651

//读卡（偏移地址1字节、读字节数2字节）

aabb08000000330600010051

//写卡（需核对密码后执行，偏移地址1字节、写字节数2字节、要写入的数据）

aabb0A0000003406400002000151

//读取密码

aabb05000000360651

//核对密码

aabb080000003706FFFFFF51

//修改密码（需核对密码后执行）

aabb08000000380601020351