CUT100-A 用户手册

版本：2019-06-14

广州盛炬智能科技有限公司
GUANGZHOU SHENGJU INTELLIGENT TECHNOLOGY CO .,LTD.

客户服务

广州盛炬智能科技有限公司

地址：广州天河区东圃二马路 61 号车陂十三社东湖工业区 A 栋 320

电话：020-85671661

网址：www.sj-rfid.com

淘宝：https://shop106253114.taobao.com

阿里巴巴：https://shop1383789519286.1688.com

微信公众号：

销售服务

门禁控制器

电话：020-85761661
邮箱：2885383778@qq.com
QQ： 2885383778

发卡器、读卡器、读卡模块

电话：020-85761661
邮箱：2885531693@qq.com
QQ： 2885531693

技术支持

门禁控制器

电话：020-85761661
邮箱：38946844@qq.com
QQ： 38946844

发卡器、读卡器、读卡模块

电话：15902094500
邮箱：2522281179@qq.com
QQ： 2522281179

管理软件

电话：020-85761661
邮箱：2645192632@qq.com
QQ： 2645192632

售后服务

售后客服

电话：020-85761661
邮箱：2885509613@qq.com
QQ： 2885509613

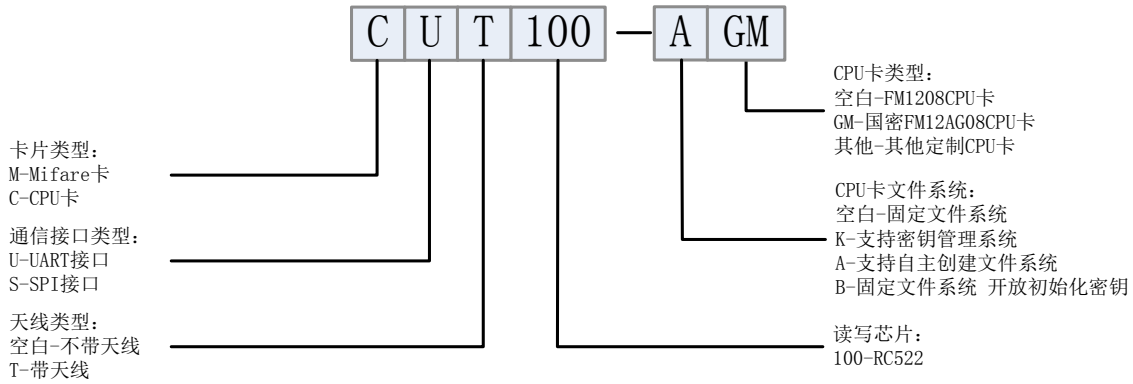
目 录

第1章 CUT100-A读卡模块数据手册

1.1 模块选型表

产品型号	卡片类型	读卡类型	接口类型	机械尺寸
MUT100	Mifare	读写数据	UART	55.5mm×35.5mm
CUT100	FM1208	固定文件系统	UART	55.5mm×35.5mm
CUT100-GM	FM12AG08	固定文件系统	UART	55.5mm×35.5mm
CUT100-A	FM1208	用户可自定义文件结构 支持接触和非接触式 CPU 卡透传命令	UART	55.5mm×35.5mm
CUT100-DES	Desfire	固定文件系统	UART	55.5mm×35.5mm
CUT100-PLUS	Mifare PLUS	支持等级 1 和等级 3	UART	55.5mm×35.5mm
CU200	B 型卡	读 B 型卡卡号	UART	55.5mm×35.5mm
CUT200-ID	二代证	二代证物理序列号	UART	55.5mm×35.5mm
CUT200-FELICA	索尼 Felica 卡	只读卡号	UART	55.5mm×35.5mm
CU300	ICODE	读卡号、读数据	UART	41mm×28mm
MU100-10ANT	Mifare	10 天线 分时读写数据	UART	56mm×41mm

1.2 型号命名规则



1.3 通信协议数据帧结构

读卡模块与控制器的通信采用数据帧方式。

数据帧格式分为两种：控制器（主机）数据帧，模块（从机）应答数据帧。

● **控制器发送命令数据帧结构**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	命令后的数据	校验字（累加和取反）
0-32	1-256	0x11-0xFF	0xXX ……	累加和取反

● **模块返回数据帧结构**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC

数据长度	模块地址	命令代码	返回操作状态	模块返回的数据	校验字（累加和取反）
0-32	1-256	0x11-0xFF	0x00	0xXX ……	累加和取反

注意：CPU 卡读卡模块操作错误时数据域会返回 CPU 卡内部的操作状态，操作状态为两个字节数据，例如：返回 0x6982 表示密钥验证失败，权限不足。

- **帧数据含义**

LEN 整个数据帧的长度，包含 LEN 本身及帧最后的校验值
ID 读卡模块的地址，485 通信会校验此地址，地址错误模块不响应命令
FC 命令代码，具体含义参考命令列表
DATA 命令代码的参数
BCC 除了 BCC 以外的所有数据累加和取反后取最低字节
SW 模块执行命令后返回的操作状态 0x00-操作成功 其他值为错误代码

- **数据帧实例**

例：（Mifare 卡读卡模块）读卡片第 0 块数据发送的命令：

第 1 步：查看读数据的命令说明，确认需要输入参数：数据块和密钥值

第 2 步：确认数据区数据长度，数据块参数长 1 字节 密钥值参数长 6 字节

第 3 步：计算数据帧长度 LEN 本身 1 字节+模块地址 1 字节+命令代码 1 字节+数据块参数 1 字节+密钥值参数 6 字节+校验码 1 字节，因此 LEN=11 字节=0x0B

组合后的数据值为：0b 01 21 00 ff ff ff ff ff ff

第 4 部：计算校验值，校验值=校验值前面的所有数据依次累加后取最低字节的值再取反。

累加和 = 0b+01+21+00+ff+ff+ff+ff+ff+ff = 0x0627

最低字节值 = 0x27 校验值 = 0x27 取反 = 0xd8

1.4 命令代码分段说明

命令段	命令用途	备注
0x11……0x1F	MU100 CU100 系列模块	通用命令 包含透传 LED 控制等
0x21……0x2F	MU100	Mifare 卡系统
0x31……0x3F	CU100	标准 CPU 卡固定文件结构
0x41……0x4F	CU100-GM	国密 CPU 卡固定文件结构
0x51……0x5F	CU100-KGM	支持国密密钥管理系统
0x61……0x7F	CU100-AGM	国密 CPU 卡自定义文件系统
0x81……0x8F	CU100-AGM	国密 PSAM 卡自定义文件系统
0x90……0xAF	CU100-PBOC	电子钱包消费系统
0xB0……0xBF	CU100-DES	DES Fire EV1 系统
0xC0……0xCF	CU100-A	标准 CPU 卡自定义文件结构 支持 SAM 透传
0xD0……0xDF	保留	
0xE0……0xEF	保留	
0xF0……0xFF	保留	

1.5 命令列表

命令字节长度为 1 字节，高半字节表示命令类型，低半字节表示命令编号。

命令字	命令类型	命令含义	备注
0x14	通用命令	控制 LED 闪烁	通过 INI 引脚可以输出高低电平信号，

0x15	通用命令	读取模块信息	返回模块名称和版本的 ASCII 码信息
0x16	通用命令	A 型卡激活	此命令可以读取 A 型卡卡号-
0x17	通用命令-RC523	B 型卡激活	此命令可以读取 B 型卡卡号(特定模块支持)
0x18	通用命令	CPU 卡激活卡片	将卡片激活到 ISO14443-4，然后才能对 CPU 卡进行文件操作
0x19	通用命令	CPU 卡数据透传	数据透传命令，支持自定义开发 CPU 卡
0x1A	通用命令	SAM 卡复位指令	复位 SAM 卡获取复位信息
0x1B	通用命令	SAM 卡透传指令	数据透传命令，支持 SAM 卡自由操作
……			
0xC0	FM1208 命令	外部认证	外部认证获取 CPU 卡操作权限
0xC1	FM1208 命令	内部认证	数据加解密
0xC2	FM1208 命令	创建目录	在当前目录下创建应用目录和密钥文件，并写入主控密钥
0xC3	FM1208 命令	选择目录或文件	选择要操作的目录或者文件
0xC4	FM1208 命令	创建二进制文件	在当前目录下创建二进制数据文件
0xC5	FM1208 命令	擦除目录	外部认证获取操作权限后擦除当前目录
0xC6	FM1208 命令	创建密钥文件	创建密钥文件 并写入一个密钥
0xC7	FM1208 命令	增加或修改密钥	在密钥文件中增加或修改密钥
0xC8	FM1208 命令	写二进制文件	更新二进制文件数据
0xC9	FM1208 命令	读二进制文件	读取二进制文件数据
0xCA	密钥操作命令	更新 EEPROM 密钥	更新模块内部 EEPROM 存储的 4 组密钥
0xCB	密钥操作命令	加载密钥	将指定编号的密钥加载到密钥缓冲区
0xCC	FM1208 命令	EEPROM 密钥外部认证	用加载的 EEPROM 密钥对卡做外部认证
0xCD	FM1208 命令	取随机数	从用户卡取随机数
0xCE	FM1208 命令	外部输入密文的外部认证	利用外部输入的密文数据完成对用户卡的数据认证
0xCF			
……			
0xE0	PSAM 卡命令		
0xE1	PSAM 卡命令		
0xE2	PSAM 卡命令		
0xE3	PSAM 卡命令	选择目录或文件	选择 PSAM 卡内的目录或者文件
0xE4	PSAM 卡命令		
0xE5	PSAM 卡命令		
0xE6	PSAM 卡命令		
0xE7	PSAM 卡命令		
0xE8	PSAM 卡命令		
0xE9	PSAM 卡命令		
0xEA	PSAM 卡命令	通用加密计算初始化	PSAM 卡用分散代码计算过程密钥
0xEB	PSAM 卡命令	通用加密计算	利用过程密钥计算动态密文
0xEC			
0xED			

0xEE			
0xEF			
……			

1.6 模块返回状态码定义

0x00 // 命令执行成功
0x01 // RS485 地址错误
0x02 // 激活卡片错误
0x03 // 激活卡片失败或者没有卡片存在
0x04 // 验证密码失败
0x05 // 读数据失败
0x06 // 写数据失败
0x07 // CPU 卡执行 RATS 失败
0x08 // 读 CPU 卡文件失败
0x09 // 写 CPU 卡文件失败
0x0A // 初始化 CPU 卡文件系统失败
0x0B // 回收 CPU 卡失败
0x0C // 修改密钥失
0x0D // 创建应用目录失败
0x0E // SAM 卡复位失败
0x0F // SAM 卡透传命令错误
0x10 // 修改密钥失
0x11 // 创建应用目录失败
0x12 // SAM 卡复位失败

0xFE // APDU 命令错误
0xFF // 不支持的命令

1.7 CPU卡片返回操作代码定义

9000 // 正确执行
61xx // 还有 xx 字节可读.
6281 // 回送的数据可能错误
6283 // 选择文件无效，文件或密钥校验错误
6300 // 认证识别码出错
63Cx // x 表示还可再试次数
6400 // 状态标志未改变
6581 // 写 EEPROM 不成功
6700 // 错误的长度
6900 // CLA 与线路保护要求不匹配
6901 // 无效的状态
6981 // 命令与文件结构不相容
6982 // 权限不满足
6983 // 密钥被锁死
6985 // 使用条件不满足
6987 // 无安全报文

6988 // 安全报文数据项不正确
6A80 // 数据域参数错误
6A81 // 功能不支持或卡中无 MF 或卡片已锁定
6A82 // 文件未找到
6A83 // 记录未找到
6A84 // 文件无足够空间
6A86 // 参数 P1P2 错误
6A88 // 密钥未找到
6B00 // 在达到 Le/Lc 字节之前文件结束，偏移量错误
6Cxx // Le 错误,记录实际长度为 xx 字节
6D00 // INS 错误或不支持
6E00 // 无效的 CLA
6F00 // 数据无效
9302 // MAC 错误
9303 // 应用已被锁定
9401 // 金额不足
9403 // 密钥未找到
9406 // 所需的 MAC 不可用

1.8 命令响应时间

UART 接口

测试条件：波特率 19200 UART 接口 电源电压 5V

激活 A 型卡 40ms
读 A 型卡数据 50ms
写 A 型卡数据 50ms

1.9 通用命令详解

1.9.1 0x14 IO 口电平控制

● 主机发送

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	变化次数 高电平时间 低电平时间	校验字（累加和取反）
0x07	0x01	0x14	0x02 0x14 0x14	0XB9
命令功能：控制 INT 引脚电平变化 **数据说明**：[0] 高低电平的交替次数 [1] 高电平时间 10ms 为基准单位 例如 0x14 = 20*10ms 亮 200ms [2] 低电平时间 10ms 为基准单位 例如 0x14 = 20*10ms 灭 200ms 注意：亮的时间和灭的时间值 加起来不能大于 250				

● 模块返回

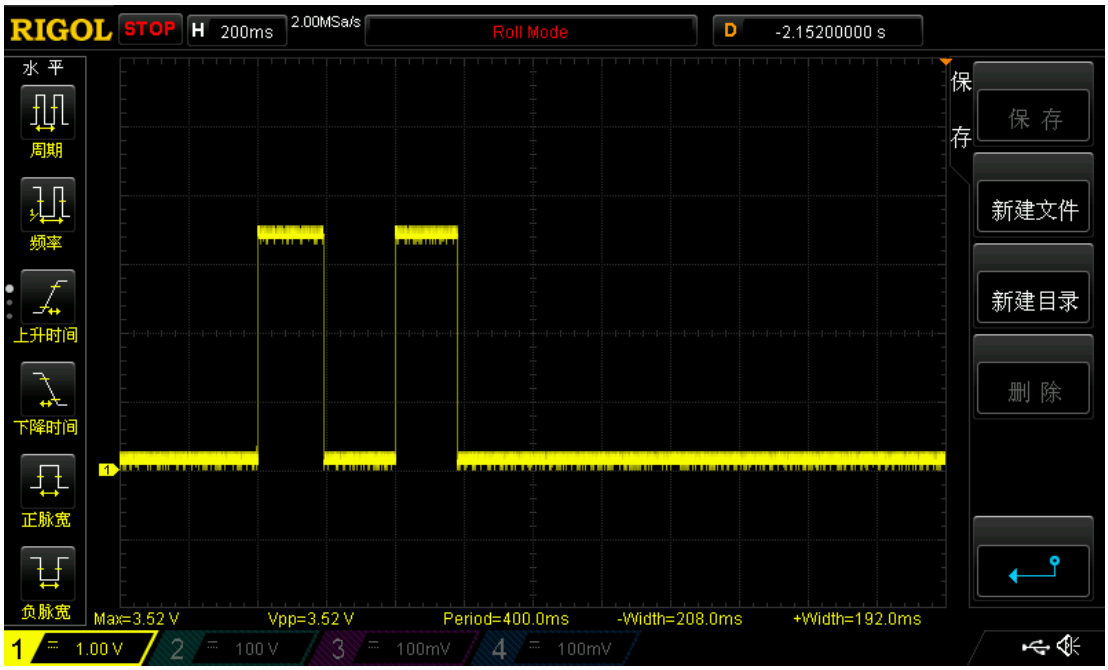
帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	无	校验字（累加和取反）

0x05	0x01	0x14	0x00	无	0xE5
数据说明：无					

● **通信实例**

主机发送：07 01 14 02 14 14 B9 // 控制 LED 闪烁 2 次 亮 200ms 灭 200ms 模块返回：05 01 14 00 E5 // 命令执行成功

● **辅助输出 I0 口输出波形图**



1.9.2 0x15 读取模块信息

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	无	校验字（累加和取反）
0x04	0x01	0x15	-	0xE5
命令功能：读取模块的型号、版本等信息 **数据说明：**无				

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	模块返回的数据	校验字（累加和取反）
0xXX	0x01	0x15	0x00	0xXX……	0xXX
数据说明：[0] 命令执行成功的状态码 0x00 [1-n] 后续 n 个数据为模块信息 数据位 ASCII 码					

● **通信实例**

主机发送：04 01 15 E5 // 读取模块型号、版本号等信息

模块返回：1F 01 15 00 43 55 54 31 30 30 2D 41 20 56 31 2E 30 32 20 32 30 31 33 2D 31 32 2D 31 32 00 A2 // 返回 ASCII 码 = CUT100-A V1.02 2013-12-12

1.9.3 0x16 A 型卡激活

● 主机发送

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	无	校验字（累加和取反）
0x04	0x01	0x16	-	0xE4
命令功能：激活 A 型卡，返回卡片 UID **数据说明**：无				

● 模块返回

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	UID	校验字（累加和取反）
0xXX	0x01	0x16	0x00	卡号数据	0xXX
数据说明：数据区返回卡片的 UID 数据					

● 通信实例

主机发送：04 01 16 E4 // 激活 A 型卡片
模块返回：09 01 16 00 **CC 06 81 5F** 2D // 激活成功，返回卡片 UID **CC 06 81 5F**
// UID 为小端模式 16 进制应为 **0x5F8106CC**

1.9.4 0x18 CPU 卡激活 ISO14443-4

● 主机发送

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	无	校验字（累加和取反）
0x04	0x01	0x18	-	0xE2
命令功能：激活 A 型 CPU 卡到 ISO14443-4 **数据说明**：无				

● 模块返回

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	ATS	校验字（累加和取反）
0xXX	0x01	0x16	0x00	返回 CPU 卡的 ATS 信息	0xXX
数据说明：数据区返回 CPU 卡片的 ATS 信息 包含 TS T0 TA1 TB1 TC1 历史字符等信息 [0] ATS 信息长度，长度值包含了长度字节本身，因此有效的 ATS 数据长度为此字节数据减 1 [1] TS [2] T0					

…… 后续数据与 T0 的值有关 非固定值

● **通信实例**

主机发送：04 01 18 E2 // 激活 A 型 CPU 片到 ISO14443-4
模块返回：25 01 18 00 10 78 80 90 02 20 90 00 00 00 00 00 CC 06 81 5F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 C5 // 激活成功，返回卡片 ATS 信息
// ATS = 10 78 80 90 02 20 90 00 00 00 00 00 CC 06 81 5F

1.9.5 0x19 APDU 透传命令

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	Case CLA INS P1 P2 Data Le	校验字（累加和取反）
0xXX	0x01	0x19	-	0xXX

命令功能：CPU 卡 APDU 透传命令 **注意：需要输入命令与应答结构的 CASE 参数**
数据说明：APDU 命令参数 Case CLA INS P1 P2 Data Le

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	SW+DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	CPU 操作代码+数据	校验字（累加和取反）
0xXX	0x01	0x19	0x00	90 00 +Data	0xXX

数据说明：[0-1] CPU 卡操作结果 0x9000 表示操作成功
[2-n] CPU 卡返回数据
注意：这里的 CPU 卡返回代码是卡片直接返回，固定为大端模式，其他命令为小端模式

● **通信实例**

主机发送：0A 01 19 02 00 84 00 00 08 4D // 取 8 字节随机数
模块返回：0F 01 19 00 90 00 48 86 A2 23 57 26 63 61 72 // APDU 取随机数命令成功
// 00 APDU 命令执行成功
// 90 00 CPU 卡操作成功
// 48 86 A2 23 57 26 63 61 8 字节随机数

1.9.6 0x1A SAM 卡复位

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	Case CLA INS P1 P2 Data Le	校验字（累加和取反）
0x04	0x01	0x1A	-	0xE0

命令功能：复位 SAM 卡，并返回 SAM 卡的复位应答信息
数据说明：复位应答信息包含 CPU 卡的操作状态码 2 字节 90 00 表示 CPU 卡操作成功

● **模块返回**

帧头	返回状态	数据区	校验值

LEN	ID	FC	SW	SW+DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	CPU 操作代码+数据	校验字（累加和取反）
0xXX	0x01	0x1A	0x00	Data	0xXX

数据说明：[0-n] CPU 卡返回数据

注意：这里的 CPU 卡返回代码是卡片直接返回，固定为大端模式，其他命令为小端模式

● **通信实例**

主机发送：04 01 1A E0 // 复位 SAM 卡

模块返回：15 01 1A 00 3B 7B 18 00 00 20 90 00 04 FB FF FF 76 35 B2 50 A7

//复位 SAM 卡成功

// 00 APDU 命令执行成功

// 3B 7B 18 00 00 20 90 00 04 FB FF FF 76 35 B2 50 16 字节 SAM 卡应答信息

1.9.7 0x1B SAM 卡 CPDU 透传命令

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	Case CLA INS P1 P2 Data Le	校验字（累加和取反）
0xXX	0x01	0x1B	-	0xXX

命令功能：CPU 卡 APDU 透传命令 **注意：需要输入命令与应答结构的 CASE 参数**

数据说明：APDU 命令参数 Case CLA INS P1 P2 Data Le

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	SW+DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	CPU 操作代码+数据	校验字（累加和取反）
0xXX	0x01	0x1B	0x00	Data + 90 00	0xXX

数据说明：

注意：这里的 CPU 卡返回代码是卡片直接返回，固定为大端模式，其他命令为小端模式

● **通信实例**

主机发送：0A 01 1B 02 00 84 00 00 08 4B // 取 8 字节随机数

模块返回：0F 01 1B 00 A7 1E 4C E9 1A 5F 67 B3 90 00 B7 // CPDU 取随机数命令成功

// 00 CPDU 命令执行成功

// 90 00 CPU 卡操作成功

// A7 1E 4C E9 1A 5F 67 B3 8 字节随机数

1.10 非接触CPU卡命令详解

1.10.1 0xC0 外部认证

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	密钥编号 密钥值	校验字（累加和取反）
0x15	0x01	0xC0	00 FF……FF	0x7B

命令功能：外部认证获取 CPU 卡操作权限 **注意：连续外部认证错误会导致密钥锁死**
数据说明：[0] 密钥编号
[1-16] 16 字节密钥值

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	认证结果	校验字（累加和取反）
0x07	0x01	0xC0	0x00	00 90	0xXX

数据说明：返回 0x9000=认证成功 0x6983=密钥锁死 0x63CX=密钥错误

● **通信实例**

主机发送：15 01 C0 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 39
// 验证 00 号密钥 密钥值 16 字节 FF
模块返回：07 01 C0 00 00 90 A7 // 验证密钥成功

1.10.2 0xC1 内部认证

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	密钥编号 被加密数据长度 被加密数据	校验字（累加和取反）
0xXX	0x01	0xC1		0xXX

命令功能：写 CPU 卡应用目录内的文件 **注意：数据长度必须是 8 字节或 16 字节**
数据说明：[0] 密钥编号
[2] 被加密数据长度（固定为 8 字节或者 16 字节）
[3…] 被加密数据

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	操作结果	CPU 卡操作代码 被加密数据	校验字（累加和取反）
0xXX	0x01	0xC1	0x00	00 90 XX……XX	0xXX

数据说明：[0-1] CPU 卡操作结果
[2-n] CPU 卡返回数据

● **通信实例**

主机发送：0E 01 C1 00 08 01 02 03 04 05 06 07 08 03 // 用 00 号密钥加密 8 字节数据 01 02 03 04 05 06 07 08
模块返回：0F 01 C1 00 00 90 EC D0 70 AC C7 1A 8C 5B FE // 加密成功

1.10.3 0xC2 创建目录

● 主机发送

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	外部认证密钥 目录 ID 目录大小 建立权限 擦除权限 目录名称 目录内的传输密钥	校验字（累加和取反）
0x32	0x01	0xC2	FF……FF F1 AD 00 04 F0 F1 31 C3 D3 A6 D3 00 00 00 FF……FF	0x67

命令功能：在当前目录下创建新的应用目录 并且自动创建好密钥文件（可以存放 14 个密钥）密钥增加权限 FA

数据说明：[0-15] 当前目录的外部认证密钥
[16- 17] 应用目录 ID 低字节在前 ID=0xADF1
[18 - 19] 目录大小 低字节再点 0x0400=1024 字节
[20] 在应用目录内创建文件的权限 0xF0 任意创建
[21] 擦除当前目录内文件的权限 0xF1 需要外部认证权限大于 1 的密钥才能擦除
[22-29] 8 字节目录名称 不足 16 字节则补 0
[30-45]16 字节应用目录传输密钥 此密钥的密钥标志或者密钥编号是 0x00

● 模块返回

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	操作结果	校验字（累加和取反）
0x07	0x01	0xC2	0x00	00 90	0xA5

数据说明：返回 CPU 卡操作结果

● 通信实例

主机发送：32 01 C2 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF F1 AD 00 04 F0 F1 31 C3 D3 A6 D3 00 00 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 67
// 创建应用目录
模块返回：07 01 C2 00 00 90 A5 // 创建应用成功

1.10.4 0xC3 选择目录或文件

● 主机发送

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	目录 ID 或者文件 ID	校验字（累加和取反）
0x06	0x01	0xC3	F1 AD	0x97

命令功能：选择目录或者文件

数据说明：目录或者文件 ID 低字节在前

● 模块返回

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	操作结果 文件信息	校验字（累加和取反）
0xXX	0x01	0xC3	0x00	-	0xXX
数据说明：[0-1] CPU 卡操作结果 [2-n] 应用目录返回的文件信息					

● **通信实例**

主机发送：06 01 C3 F1 AD 97 // 选择应用目录 0xADF1
模块返回：1F 01 C3 00 00 90 6F 16 84 10 31 C3 D3 A6 D3 00 00 00 FF FF FF FF FF FF FF FF A5 04 9F 08 EB // 选择应用目录成功

1.10.5 0xC4 创建二进制数据文件

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	文件 ID 文件大小 读权限 写权限	校验字（累加和取反）
0x0A	0x01	0xC4	17 00 40 00 F1 F2	0xF6
命令功能：创建二进制数据文件 **数据说明：**[0-1] 文件 ID [2-3] 文件大小 低字节在前 [4] 读权限 [5] 写权限				

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	CPU 卡操作结果	校验字（累加和取反）
0x07	0x01	0xC4	0x00	00 90	0xA3
数据说明：返回 CPU 卡操作结果					

● **通信实例**

主机发送：0A 01 C4 17 00 40 00 F1 F2 F6 // 创建二进制数据文件
模块返回：07 01 C4 00 00 90 A3 // 创建二进制数据文件成功

1.10.6 0xC5 擦除目录

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	无	校验字（累加和取反）
0x04	0x01	0xC5	-	0x35
命令功能：擦除当前目录下的所有文件（不包括目录本身）				

特殊说明：擦除目录后可以任意在该 DF 下创建文件而不受创建权限的控制，当重新创建 KEY 文件后下次再进入该目录操作时将受到目录创建权限的控制，因此创建密钥文件后必须要同时写入一个高于创建权限的密钥，否则创建 KEY 文件后又没有写入密钥或者没有高于当前目录创建权限的密钥，那么操作者将失去该目录的创建权限。

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	CPU 卡操作结果	校验字（累加和取反）
0x07	0x01	0xC5	0x00	00 90	0xA2
数据说明：返回 CPU 卡操作结果					

● **通信实例**

主机发送：04 01 C5 35 // 擦除当前目录下的所有文件
模块返回：07 01 C5 00 00 90 A2 // 擦除目录成功

1.10.7 0xC6 创建密钥文件

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	文件空间 增加权限 密钥编号 密钥权限值 密钥值	校验字（累加和取反）
0x19	0x01	0xC6	00 01 F0 00 0F FF……FF	0x6F
命令功能：在当前目录创建密钥文件 并写入一个外部认证密钥 **数据说明：**[0-1] 文件空间 低字节在前 [2] 密钥增加权限 [3] 密钥编号 [4] 当前密钥权限值 [5--20] 密钥值 16 字节				

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	CPU 卡操作结果	校验字（累加和取反）
0x07	0x01	0xC6	0x00	00 90	0xA1
数据说明：返回 CPU 卡操作结果					

● **通信实例**

主机发送：19 01 C6 00 01 F0 00 0F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 2F
// 创建密钥文件
模块返回：07 01 C6 00 00 90 A1 // 创建密钥文件成功

1.10.8 0xC7 增加或修改密钥

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC

数据长度	模块地址	命令代码	操作类型 密钥编号 密钥控制信息	校验字（累加和取反）
0x1B	0x01	0xC7	01 00 30 F0 F1 00 00 FF……FF	0x1A

命令功能： 修改现有应用目录的主控密钥

数据说明： [0] 密钥操作类型 01 增加密钥 00 修改密钥

[2] 密钥编号

[4] 密钥控制信息

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	CPU 卡操作结果	校验字（累加和取反）
0x07	0x01	0xC7	0x00	00 90	0xA0

数据说明： CPU 卡操作结果

● **通信实例**

主机发送：1B 01 C7 01 00 30 F0 F1 00 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 1A // 增加内部认证密钥

模块返回：07 01 C7 00 00 90 A0 // 增加内部认证密钥成功

主机发送：1B 01 C7 01 01 39 F0 F1 0E FF 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 C3 // 增加 01 号外部认证密钥 使用权限 F0 修改权限 F1 后续状态 0E 错误计数器 16 次

模块返回：07 01 C7 00 00 90 A0 // 增加外部认证密钥成功

● **命令报文数据说明**

DATA 区域						
命令信息	**密钥控制信息**					
操作类型	内部认证密钥、TAC 密钥、消费、圈提、圈存、修改透支限额					
01 增加密钥 00 修改密钥	30/34/3C/3D/3E/3F	使用权	修改权	密钥版本号	算法标志	16 字节密钥
	外部认证密钥					
	39	使用权	修改权	后续状态	错误计数器	16 字节密钥
	增加口令密钥					
密钥编号	3A	使用权	EF	后续状态	错误计数器	8 字节口令
从 00 开始 不能为 FF	增加解锁口令密钥					
	37	使用权	更改全	FF	错误计数器	16 字节密钥
	线路保护密钥、重装口令密钥的密钥					
	36/38	使用权	更改权	FF	错误计数器	16 字节密钥

● **密钥类型及含义**

密钥类型	意义
30	内部认证密钥（加密密钥）
34	TAC 密钥
36	文件线路保护密钥
37	解锁口令密钥
38	重装口令密钥的密钥
39	外部认证密钥
3A	口令密钥

3C	修改透支限额
3D	圈提密钥
3E	消费密钥
3F	圈存密钥

1.10.9 0xC8 写二进制文件

● 主机发送

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	文件 ID 地址偏移 写数据长度 数据	校验字（累加和取反）
0x19	0x01	0xC8	17 00 00 00 10 AA……AA	0x56
命令功能：写二进制数据文件 **数据说明**：[0-1] 文件 ID [2-3] 地址偏移 [4] 数据长度 [5-n] 数据				

● 模块返回

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	CPU 卡操作结果	校验字（累加和取反）
0x07	0x01	0xC8	0x00	00 90	0x9F
数据说明：CPU 卡操作结果					

● 通信实例

主机发送：19 01 C8 17 00 00 00 10 AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA 56 // 修改 2001 目录的主控密钥

模块返回：07 01 C8 00 00 90 9F // 修改应用目录主控密钥成功

1.10.10 0xC9 读二进制文件

● 主机发送

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	文件 ID 地址偏移 读数据长度	校验字（累加和取反）
0x09	0x01	0xC9	17 00 00 00 10	0x05
命令功能：读二进制数据文件 **数据说明**：[0-1] 文件 ID [2-3] 地址偏移 [4] 读数据长度				

● 模块返回

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	CPU 卡操作结果 数据	校验字（累加和取反）

0xXX	0x01	0xC9	0x00	XX	0xXX
数据说明：[0-1] CPU 卡操作结果 [2-n] 数据					

● **通信实例**

主机发送：09 01 C9 17 00 00 00 10 05 // 读取二进制数据文件
模块返回：17 01 C9 00 00 90 AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA EE // 读取数据成功

1.10.11 0xCA 更新 EEPROM 密钥

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	密钥 1 密钥 2 密钥 3 密钥 4	校验字（累加和取反）
0x44	0x01	0xCA	11……22……33……44……	0xXX
命令功能：更新 EEPROM 密钥 密钥固定为 4 组 每组 16 字节长 **数据说明**：[0-15] 密钥 1 [16-31] 密钥 2 [32-47] 读数 3 [48-63] 读数 4				

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	无	校验字（累加和取反）
0x05	0x01	0xCA	0x00	-	0x2F
数据说明：无					

● **通信实例**

主机发送：44 01 CA 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 44 44 44 44 44 44 44 44 44 44 44 44 44 44 44 44 44 44 50 // 更新 EEPROM 密钥
模块返回：05 01 CA 00 2F // 更新 EEPROM 密钥成功

1.10.12 0xCB 加载 EEPROM 密钥

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	EEPROM 编号	校验字（累加和取反）
0x05	0x01	0xCB	0xXX	0xXX
命令功能：加载 EEPROM 中存储的密钥 **数据说明**：[0] EEPROM 中的密钥编号 只能为 1、2、3、4				

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC

数据长度	模块地址	命令代码	返回操作状态	无	校验字（累加和取反）
0x05	0x01	0xCB	0x00	-	0x2E
数据说明：无					

● **通信实例**

主机发送：05 01 CB 01 2D // 加载 EEPROM 中的 1 号密钥
模块返回：05 01 CB 00 2E // 加载 EEPROM 密钥成功

1.10.13 0xCC EEPROM 密钥外部认证

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	CPU 卡外部认证密钥编号	校验字（累加和取反）
0x05	0x01	0xCC	0xXX	0xXX
命令功能：利用加载的 EEPROM 密钥对 CPU 卡中指定编号的外部认证密钥进行认证 **数据说明：**[0] CPU 卡外部认证密钥编号				

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	CPU 卡操作结果	校验字（累加和取反）
0x07	0x01	0xCC	0xXX	0xXX	0xXX
返回状态：0x00=验证命令执行成功 其他值验证命令执行失败 **数据说明：**[0-1] CPU 卡返回的密钥认证结果 【00 90】=验证成功 其他值请参考【1.7 节 CPU 卡片返回操作代码定义】					

● **通信实例**

主机发送：05 01 CC 01 2C // 用 EEPROM 加载的密钥对 CPU 卡内 01 号外部认证密钥认证
模块返回：07 01 CC 00 00 90 9B // 外部认证成功

1.10.14 0xCD 用户卡取随机数

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	取随机数的长度	校验字（累加和取反）
0x05	0x01	0xCD	0xXX	0xXX
命令功能：从非接触式用户卡中去随机数 **数据说明：**[0] 取随机数的长度				

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	CPU 卡操作结果	校验字（累加和取反）
0x07	0x01	0xCD	0xXX	0xXX	0xXX
返回状态：0x00=验证命令执行成功 其他值验证命令执行失败					

数据说明:[0-1] CPU 卡返回的密钥认证结果 【00 90】=验证成功 其他值请参考【1.7 节 CPU 卡片返回操作代码定义】
[2-X] CPU 卡返回的随机数

● **通信实例**

主机发送：05 01 CD 04 28 // 取 4 字节随机数
模块返回：0B 01 CD 00 00 90 81 1E 11 53 93 // 返回 4 字节随机数 81 1E 11 53

1.10.15 0xCE 外部输入密文的外部认证

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	CPU 卡外部认证密钥编号	校验字（累加和取反）
0x0D	0x01	0xCE	0xXX	0xXX

命令功能：利用加载的 EEPROM 密钥对 CPU 卡中编号的外部认证密钥进行认证
数据说明：[0] CPU 卡外部认证密钥编号

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	CPU 卡操作结果	校验字（累加和取反）
0x07	0x01	0xCE	0xXX	0xXX	0xXX

返回状态：0x00=验证命令执行成功 其他值验证命令执行失败
数据说明:[0-1] CPU 卡返回的密钥认证结果 【00 90】=验证成功 其他值请参考【1.7 节 CPU 卡片返回操作代码定义】

● **通信实例**

主机发送:0D 01 CE 01 4F 8A AF 18 85 BB 9A 1C 8C // 外部输入密文对 CPU 卡内 01 号外部认证密钥认证
模块返回：07 01 CE 00 00 90 9B // 外部认证成功

1.11 PSAM卡命令详解

1.11.1 0xE3 选择命令（选择目录或者文件）

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	目录或者文件 ID	校验字（累加和取反）
0x06	0x01	0xE3	0xXX 0xXX	0xXX

命令功能：选择 PSAM 卡的目录或者文件
数据说明：[0-1] 目录或者文件 ID 2 字节 低字节在前

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	CPU 卡操作结果	校验字（累加和取反）
0xXX	0x01	0xE3	0xXX	0xXX	0xXX

返回状态：0x00=验证命令执行成功 其他值验证命令执行失败

数据说明：[0-1] CPU 卡返回的密钥认证结果 【00 90】=验证成功 其他值请参考【1.7 节 CPU 卡片返回操作代码定义】

[2-X] 选择目录后返回的文件信息 n 字节

● **通信实例**

主机发送：06 01 E3 04 DF 32 // 选择 PSAM 卡 0xDF04 目录

模块返回：20 01 E3 00 00 90 6F 17 84 10 D1 56 00 00 04 BD F0 CA CB B4 EF D6 A7 B8 B6 FF A5 03 88 01 01 25 // 选择成功 返回应答信息

1.11.2 0xEA 通用加密计算初始化

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	密钥类型、分散级数、分散代码	校验字（累加和取反）
0x08	0x01	0xEA	0xXX 0xXX 0xXX……0xXX	0xXX

命令功能：对 PSAM 卡中指定的密钥用分散代码进行分散生成过程密钥

数据说明：[0] 密钥类型 取密钥用途的低 5 位

[1] 密钥分散级数 取密钥用途的高 3 位

[2] 密钥版本

[3-10] 8 字节分散代码

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	CPU 卡操作结果	校验字（累加和取反）
0x07	0x01	0xEA	0xXX	0xXX	0xXX

返回状态：0x00=验证命令执行成功 其他值验证命令执行失败

数据说明：[0-1] CPU 卡返回的密钥认证结果 【00 90】=验证成功 其他值请参考【1.7 节 CPU 卡片返回操作代码定义】

● **通信实例**

主机发送：10 01 EA 07 01 01 08 32 0F 50 8D 80 00 00 00 55 // 通用加密计算初始化 密钥类型 07 分散级数 01 组成完整 1 字节密钥用途为 0x27

模块返回：07 01 EA 00 00 90 7D // 通用加密计算成功

1.11.3 0xEB 通用加密计算

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC

数据长度	模块地址	命令代码	计算类型、待加密数据长度	校验字（累加和取反）
0xXX	0x01	0xEB	0xXX、0xXX	0xXX

命令功能： 利用 EA 命令中计算的过程密钥对输入的密文进行加密计算

数据说明： [0] 加密计算的类型

[1] 待加密数据长度

加密计算类型说明（按 bit 位区分 X 位数据控制相应功能）								
B7	B6	B5	B4	B3	B2	B1	B0	该位数据的含义
							X	0=加密 1=MAC 计算
						X		0=无后续块 1=有后续块
					X			0=无初始值 1=有初始值

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	BCC
数据长度	模块地址	命令代码	返回操作状态	CPU 卡操作结果	校验字（累加和取反）
0xXX	0x01	0xEB	0xXX	0xXX	0xXX

返回状态：0x00=验证命令执行成功 其他值验证命令执行失败

数据说明：[0-1] CPU 卡返回的密钥认证结果 【00 90】=验证成功 其他值请参考【1.7 节 CPU 卡片返回操作代码定义】

[2-X] PSAM 卡返回的 n 字节没问数据

● **通信实例**

主机发送：0E 01 EB 00 08 48 7E 18 7A 00 00 00 00 A5

// 用 EA 命令计算的过程密钥对 48 7E 18 7A 00 00 00 00 这 8 字节数据进行加密

模块返回：0F 01 EB 00 00 90 4F 8A AF 18 85 BB 9A 1C DE

// PSAM 卡返回 8 字节密文 4F 8A AF 18 85 BB 9A 1C

第2章 CPU卡模块调试指南

2.1 文件结构

- FMCOS 文件系统由主文件 MF、目录文件 DF、基本文件 EF 组成，并且每张卡片只有唯一的 MF，MF 下面可以建立多级目录和基本文件。
- 默认出厂的 CPU 卡只包含 MF 主文件目录和一个密钥文件，密钥文件里面存储有外部认证的传输密钥，在创建、擦除、修改密钥时需要首先认证传输密钥。

2.2 密钥结构

- CPU 卡内的密钥文件可以写入多种不同类型的密钥，同类型密钥也可以写入多个密钥编号和密钥值不同的密钥。
- 密钥类型及含义

密钥类型	意义
30	内部认证密钥（加密密钥）
34	TAC 密钥
36	文件线路保护密钥
37	解锁口令密钥
38	重装口令密钥的密钥
39	外部认证密钥
3A	口令密钥
3C	修改透支限额密钥
3D	圈提密钥
3E	消费密钥
3F	圈存密钥

2.3 访问安全权限定义

- 安全状态是指当前卡片所处的一种安全级别，安全状态寄存器的值是 0~~F，卡片刚刚激活或者复位后安装状态寄存器的值复位为 0.
- 假定文件的访问权限为 XY
  当 X>Y 时：当前的安全状态寄存器的值大于等于 Y 且小于 X 才能访问文件
  当 X=Y 时：当前的安装状态寄存器的值等于 X 等于 Y 才能访问文件
  当 X<Y 时：表示不允许操作
- 例如：二进制数据文件的读权限 F1、写权限 F2，那么读文件要验证外部认证密钥或者口令密钥，使安全状态寄存器的值大于 1 小于 F 才可以读文件，写文件则要求验证安全状态寄存器的值大于 2 小于 F 的密钥才可以。如果某个文件的写权限是 EF 则表示该文件禁止写操作为只读文件。

2.4 应用目录创建

- 创建应用目录时需要注意，刚刚创建完应用目录必须要马上创建一个密钥文件，并且写入一个权限较高的外部认证密钥，不然当目录具有创建权限和擦除权限时先创建了其他类型的文件后再次进入该目录时就会要求操作权限，而此时还没有创建密钥文件和写入密钥，因此就会失去对此目录的操作权限。

2.5 认证机制

- 卡片认证分为外部认证和内部认证，分别用来实现卡片对机具的认证和机具对卡片的认证，CPU 卡的操作可以单独使用某一种认证方式，也可以同时使用两种认证方式。

2.6 详细操作请参考卡片的COS手册

第3章 APDU透传指令应用说明

3.1 APDU的命令与应答分为四种不同的情形（Case参数）

1. 情形一 Case=0x01

命令	CLA	INS	P1	P2	00		
应答	SW1	SW2					

2. 情形二Case=0x02

命令	CLA	INS	P1	P2	Le		
应答	Le 字节数据			SW1	SW2		

3. 情形三Case=0x03

命令	CLA	INS	P1	P2	Lc	Data	
应答	SW1	SW2					

4. 情形四Case=0x04

命令	CLA	INS	P1	P2	Lc	Data	Le
应答	Le 字节数据			SW1	SW2		

3.2 SW状态字含义

SW1 SW2	含义
90 00	操作成功
62 81	回送的数据可能错误
62 83	选择文件无效，文件或密钥校验错误
63 Cx	X 表示可以再尝试的次数(一般是应用在密钥中表示可以再验证的次数)
64 00	状态标志未改变
65 81	写存储器失败
67 00	长度错误
69 00	CLA 与线路保护要求不匹配
69 01	无效的状态
69 81	命令与文件结构不符
69 82	不满足安装状态，操作权限不足
69 83	密钥被锁死
69 85	使用条件不满足
69 87	无安全报文
69 88	安全报文数据项不正确
6A 80	数据域参数错误
6A 81	功能不支持或者无 MF 或卡片已锁定
6A 82	文件未找到
6A 83	记录未找到

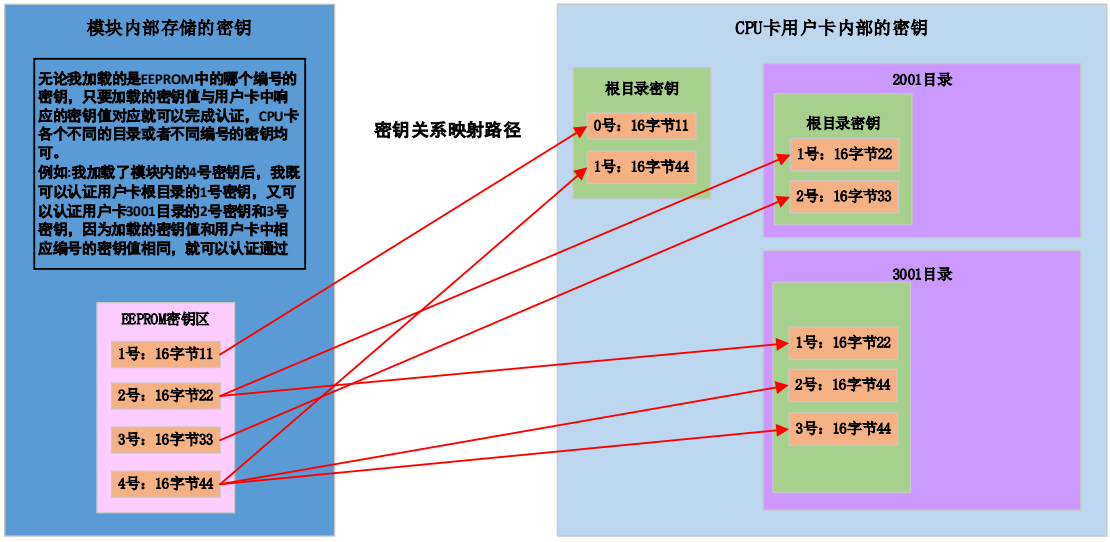
6A 84	空间不足
6A 86	参数 P1 P2 错误
6A 88	密钥为找到
6B 00	在达到 Le/Lc 字节之前文件结束，偏移量错误
6C xx	Le 错误
6E 00	无效的 CLA
6F 00	数据无效
93 02	MAC 错误
93 03	应用被锁定
94 01	余额不足
94 03	应用密钥未找到
94 06	所需的 MAC 不可用

注:更详细的错误代码可以参考《中国人民银行金融 IC 卡规范》

第4章 模块内部密钥与用户卡密钥对应关系及使用方法

4.1 读卡模块装载密钥功能说明

- 装载密钥功能的应用环境
  用户为了保障密钥安全不想密钥在模块与控制设备之间的通信数据中传输时可以体检对模块进行更新密钥操作，将未来需要使用的密钥装载到模块中，以后需要密钥验证时，只要加载模块内对应编号的密钥再用加载的密钥去对用户卡做外部认证即可，这样对用户卡进行密钥验证时不需要在通信线上传输密钥，保障了用户密钥的安全。
- 模块内存储的密钥与实际用户卡中外部认证密钥在使用过程中的对应关系说明



4.2 读卡模块内部EEPROM密钥使用流程

- EEPROM 密钥更新
  发送 0xCA 命令更新模块内部 EEPROM 存储的 4 组密钥
- 加载 EEPROM
  发送 0xCB 命令加载 4 组密钥中的一组
- 使用加载的 EEPROM 密钥进行外部认证
  发送 0xCC 命令使用已经加载的密钥对 CPU 卡进行外部密钥认证

第5章 文件更新记录

5.1 2019-06-14

- 增加模块内部 EEPROM 密钥使用流程描述
- 增加 xC2 命令中创建目录时增加的密钥编号的说明

5.2 2019-06-27

- 更新取随机数命令的描述