乌鲁木齐市轨道交通

清分中心系统设备采购项目

乌鲁木齐轨道交通 AFC 技术标准

（加密机应用报文）

20180109v00.03

文档历史

版本号	日期	编写者	审核者	描述
20171109v00.01	20171109	铭鸿数据		编写初版
20171110v00.02	20171110	铭鸿数据		增加密钥计算信息
20180109v00.03	20180109	铭鸿数据		增加 PSAM 激活计算信息

1. 目的

结合应用，对加密机使用的报文进行使用描述。使项目的需求方、系统集成商对项目实现及用户卡应用有一致的理解。

2. 参考

下列文件中的条款通过在本标准的引用而成为本标准的条款。凡是注日期的相关引用文件，其随后所有的修改单（不包括堪误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

《CJ/T 0025.1 中国金融集成电路（IC）卡规范》

——第 1 部分：电子钱包 / 电子存折应用卡片规范

——第 2 部分：电子钱包 / 电子存折应用规范

——第 9 部分：电子钱包 / 电子存折扩展应用指南

3. 说明

数据存储的基本格式有如下定义。

标识	说明
A	字母数字（包括任何非控制类型）字符
H	16进制字符
N	数字域
B	二进制数据
n	不定数据

举例说明：

2A，表示 2字节字符，符合要求数据如：x0Dx0A或“AB”

4H，表示 4位16进制数据字符串，符合要求数据如：“03E8”

3N，表示 3位10进制数据字符串，符合要求数据如：“ 123 ”

8B，表示 8字节二进制数据，符合要求数据如： x12x34x56x78x9AxBCxDExF0

1A+3H ，符合要求数据如： x12 “ ABC ”或“K23F”

4. 指令说明

电子钱包应用使用到的相关加密机指令包括以下。

4.1. 分散密钥数据加解密计算

数据域		长度	说明
命令消息			
消息长度		2B	后续所有数据长度
消息头	区域编码	2B	待计算数据使用区域编码（x88x10）
	密钥索引	2B	待计算数据使用加密机内指定密钥的索引
	报文序号	4B	
	预留	4B	
消息内容	命令代码	2A	“U1”
	算法标识	1A	“X”=DES计算（缺省为“X”） “S”=SM4
	加密模式标识	1N	“0”=离散密钥3DES/SM4/SM1/AES加密 “1”=离散密钥3DES/SM4/SM1/AES解密 “4”=离散密钥DES加密 “5”=离散密钥DES解密 “6”=过程密钥DES加密 “7”=过程密钥DES解密 “8”=过程密钥3DES/SM4/SM1/AES加密 “9”=过程密钥3DES/SM4/SM1/AES解密
	方案ID	1N	加解密算法模式： “01”=ECB “02”=CBC
	根密钥类型	3H	产生卡片密钥的发卡行密钥类型： “109”=MK-AC “209”=MK-SMI “309”=MK-SMC “509”=MK-DN “00A”=ZEK
	根密钥	1A+3H	表示“K”+3位待计算数据使用加密机内指定密钥的索引
	离散次数	1N	对指定密钥分散次数（“0”～“5”）
	离散数据	n * 16H	n为离散次数
	过程数据	16H	用于产生过程密钥的数据，仅当加密模式标识为6，7，8，9时有此域,当模式为8,9时此域为（00||00||00||00||00||00||ATC）的形式，ATC为4H。
	MAC数据填充标识	2N	“01”=不强制填充80 00... “02”=强制填充80 00...
	IV-CBC	16H	初始向量。加密算法为CBC时，该域存在
	数据长度	3N	数据长度/2（DES实际长度应为8的倍数，其它算法为16的倍数）
	数据	n * 2H	数据明文/密文

数据域		长度	说明
响应消息			
消息长度		2B	后续所有数据长度
消息头	区域编码	2B	待计算数据使用区域编码
	密钥索引	2B	待计算数据使用加密机内指定密钥的索引
	报文序号	4B	
	预留	4B	
消息内容	响应代码	2A	“U2”
	错误代码	2N	“00” = 无错误 “04” = 模式标志错 “05” = 未定义的方案ID “06” = 非法的偏移量 “10” = 根密钥奇偶校验错 “11” = 保护密钥奇偶校验错 “12” = 用户存储区没有装载密钥 “13” = LMK错误 “15” = 输入数据错。 “34” = 离散次数错 “28” = 密钥类型错 “50” = 保护密钥类型错 “80” = MAC填充长度错
	数据长度	3N	数据长度/2
	数据	n * 2H	数据明文/密文

4.2. 计算及校验 MAC/TAC

数据域		长度	说明
命令消息			
消息长度		2B	后续所有数据长度
消息头	区域编码	2B	待计算数据使用区域编码（x88x10）
	密钥索引	2B	待计算数据使用加密机内指定密钥的索引
	报文序号	4B	
	预留	4B	
消息内容	命令代码	2A	“UB”
	算法标识	1A	“X”=DES计算（缺省为“X”） “S”=SM4
	模式标识	1H	“1”=计算MAC “2”=校验MAC
	方案ID	1N	计算MAC模式： “0”=使用子密钥进行3DES “1”=使用过程密钥进行DESMAC “2”=使用子密钥进行DESMAC “3”=使用过程密钥进行3DES
	根密钥类型	3H	产生卡片密钥的发卡行密钥类型： “109”= MK-AC “209”= MK-SMI “309”= MK-SMC “509”= MK-DN “003”= TAK “008”= ZAK
	根密钥	1A+3H	表示“K”+3位待计算数据使用加密机内指定密钥的索引
	离散次数	1N	对指定密钥分散次数（“0”～“5”）
	离散数据	n * 16H	n为离散次数
	过程数据	16H	用于产生过程密钥的数据，仅当方案ID为1、3时有此项
	MAC数据填充标识	1N	“1”=强制填充80 00... “0”=不强制填充80 00...
	IV-MAC	16H	MAC 计算初始值
	MAC计算数据长度	3N	
	MAC计算数据	n * 2H	n为MAC计算数据长度
	MAC长度	2N	
	待校验MAC值	n * 2H	n为MAC长度 仅当模式标识 = “2”时有此域

数据域		长度	说明
响应消息			
消息长度		2B	后续所有数据长度
消息头	区域编码	2B	待计算数据使用区域编码
	密钥索引	2B	待计算数据使用加密机内指定密钥的索引
	报文序号	4B	
	预留	4B	
消息内容	响应代码	2A	“UC”
	错误代码	2N	“00” = 无错误 “01” = MAC校验错 “04” = 模式标志错 “05” = 未定义的方案ID “06” = 非法的偏移量 “10” = 根密钥奇偶校验错 “11” = 保护密钥奇偶校验错 “12” = 用户存储区没有装载密钥 “13” = LMK错误 “15” = 输入数据错 “34” = 离散次数错 “28” = 密钥类型错 “50” = 保护密钥类型错 “80” = MAC填充长度错
	待校验MAC值	n * 2H	n为MAC长度 仅当模式标识 = “1”时有此域

5. 业务使用

5.1. 卡密钥计算

使用指令：分散密钥数据加解密计算（指令代码“U1”）。
关键数据填充如下描述。

算法标识	1A	“X”=DES计算
加密模式标识	1N	“0”
方案ID	2N	“01”
根密钥类型	3H	“109”
离散次数	1N	“2”
离散数据	32H	轨道交通离散数据（16H）||地区代码（16H）
MAC数据填充标识	2N	“01”
数据长度	3N	“016”
数据	32H	待计算密钥卡逻辑卡号（16H）||逻辑卡号的反（16H）

5.2. 文件修改

使用指令：计算及校验 MAC/TAC （指令代码“UB”）。
关键数据填充如下描述。

算法标识	1A	“X”=DES计算
模式标识	1H	“1”=计算MAC
方案ID	1N	“0”=使用子密钥进行3DES
根密钥类型	3H	“109”
离散次数	1N	“3”
离散数据	48H	轨道交通离散数据（16H）||地区代码（16H）||用户卡卡号右16位
MAC数据填充标识	1N	“1”=强制填充80 00...
IV-MAC	16H	用户卡获取的 8位随机数 + “00000000”
MAC计算数据长度	3N	用户卡文件修改实际命令（不包括 MAC）长度
MAC计算数据	n * 2H	用户卡文件修改实际命令（不包括 MAC）
MAC长度	2N	“04”

5.3. 充值MAC1计算

使用指令：计算及校验 MAC/TAC （指令代码“UB”）。
关键数据填充如下描述。

算法标识	1A	“X”=DES计算
模式标识	1H	“1”=计算MAC
方案ID	1N	“1”=使用过程密钥进行DESMAC
根密钥类型	3H	“109”
离散次数	1N	“3”
离散数据	48H	轨道交通离散数据（16H）||地区代码（16H）||用户卡卡号右16位
过程数据	16H	伪随机数+ 钱包联机交易序号+ 8000
MAC数据填充标识	1N	“1”=强制填充80 00...
IV-MAC	16H	“0000000000000000”
MAC计算数据长度	3N	“015”
MAC计算数据	30H	钱包余额+ 交易金额+ 交易类型标识(02)+ 终端机编号
MAC长度	2N	“04”

5.4. 充值MAC2计算

使用指令：计算及校验 MAC/TAC （指令代码“UB”）。
关键数据填充如下描述。

算法标识	1A	“X”=DES计算
模式标识	1H	“1”=计算MAC
方案ID	1N	“1”=使用过程密钥进行DESMAC
根密钥类型	3H	“109”
离散次数	1N	“3”
离散数据	48H	轨道交通离散数据（16H）||地区代码（16H）||用户卡卡号右16位
过程数据	16H	伪随机数+ 钱包联机交易序号+ 8000
MAC数据填充标识	1N	“1”=强制填充80 00...
IV-MAC	16H	“0000000000000000”
MAC计算数据长度	3N	“018”
MAC计算数据	36H	交易金额+ 交易类型标识(02)+ 终端机编号+ 日期时间
MAC长度	2N	“04”

5.5. 充值 TAC 计算

使用指令：计算及校验 MAC/TAC （指令代码“UB”）。
关键数据填充如下描述。

算法标识	1A	“X”=DES计算
模式标识	1H	“1”=计算MAC
方案ID	1N	“2”=使用子密钥进行DESMAC
根密钥类型	3H	“109”
离散次数	1N	“3”
离散数据	48H	轨道交通离散数据（16H）||地区代码（16H）||用户卡卡号右16位
MAC数据填充标识	1N	“1”=强制填充80 00...
IV-MAC	16H	“0000000000000000”
MAC计算数据长度	3N	“024”
MAC计算数据	48H	钱包余额(交易后)+ 钱包联机交易序号(加一前)+ 交易金额+ 交易类型标识(02)+ 终端机编号+ 交易时间
MAC长度	2N	“04”

5.6. 消费MAC1计算

使用指令：计算及校验 MAC/TAC （指令代码“UB”）。
关键数据填充如下描述。

算法标识	1A	“X”=DES计算
模式标识	1H	“1”=计算MAC
方案ID	1N	“1”=使用过程密钥进行DESMAC
根密钥类型	3H	“109”
离散次数	1N	“3”
离散数据	48H	轨道交通离散数据（16H）||地区代码（16H）||用户卡卡号右16位
过程数据	16H	伪随机数+ 钱包脱机交易序号+ 终端交易序号的右两字节
MAC数据填充标识	1N	“1”=强制填充80 00...
IV-MAC	16H	“0000000000000000”
MAC计算数据长度	3N	“018”
MAC计算数据	36H	交易金额+ 交易类型标识(06)+ 终端机编号+ 交易时间
MAC长度	2N	“04”

5.7. 消费MAC2计算

使用指令：计算及校验 MAC/TAC （指令代码“UB”）。
关键数据填充如下描述。

算法标识	1A	“X”=DES计算
模式标识	1H	“1”=计算MAC
方案ID	1N	“1”=使用过程密钥进行DESMAC
根密钥类型	3H	“109”
离散次数	1N	“3”
离散数据	48H	轨道交通离散数据（16H）||地区代码（16H）||用户卡卡号右16位
过程数据	16H	伪随机数+ 钱包脱机交易序号+ 终端交易序号的右两字节
MAC数据填充标识	1N	“1”=强制填充80 00...
IV-MAC	16H	“0000000000000000”
MAC计算数据长度	3N	“004”
MAC计算数据	8H	交易金额
MAC长度	2N	“04”

5.8. 消费 TAC 计算

使用指令：计算及校验 MAC/TAC （指令代码“UB”）。
关键数据填充如下描述。

算法标识	1A	“X”=DES计算
模式标识	1H	“1”=计算MAC
方案ID	1N	“2”=使用子密钥进行DESMAC
根密钥类型	3H	“109”
离散次数	1N	“3”
离散数据	48H	轨道交通离散数据（16H）||地区代码（16H）||用户卡卡号右16位
MAC数据填充标识	1N	“1”=强制填充80 00...
IV-MAC	16H	“0000000000000000”
MAC计算数据长度	3N	“022”
MAC计算数据	44H	交易金额+ 交易类型标识(06)+ 终端机编号+ 终端机交易序号+ 交易时间
MAC长度	2N	“04”

5.9. 应用锁定 MAC 计算

使用指令：计算及校验 MAC/TAC （指令代码“UB”）。
关键数据填充如下描述。

算法标识	1A	“X”=DES计算
模式标识	1H	“1”=计算MAC
方案ID	1N	“0”=使用子密钥进行3DES
根密钥类型	3H	“109”
离散次数	1N	“3”
离散数据	48H	轨道交通离散数据（16H）||地区代码（16H）||用户卡卡号右16位
MAC数据填充标识	1N	“1”=强制填充80 00...
IV-MAC	16H	用户卡获取的 8位随机数 + “00000000”
MAC计算数据长度	3N	“005”
MAC计算数据	n * 2H	应用锁定实际命令（不包括 MAC）
MAC长度	2N	“04”

5.10. PSAM激活计算

使用指令：分散密钥数据加解密计算（指令代码“U1”）。
关键数据填充如下描述。

算法标识	1A	“X”=DES计算
加密模式标识	1N	“0”
方案ID	2N	“01”
根密钥类型	3H	“109”
离散次数	1N	“3”
离散数据	48H	轨道交通离散数据（16H）||地区代码（16H）||PSAM逻辑卡号（16H）
MAC数据填充标识	2N	“01”
数据长度	3N	“008”
数据	16H	从PSAM获得的随机数（16H）