校园一卡通系统

CPU卡结构定义规范

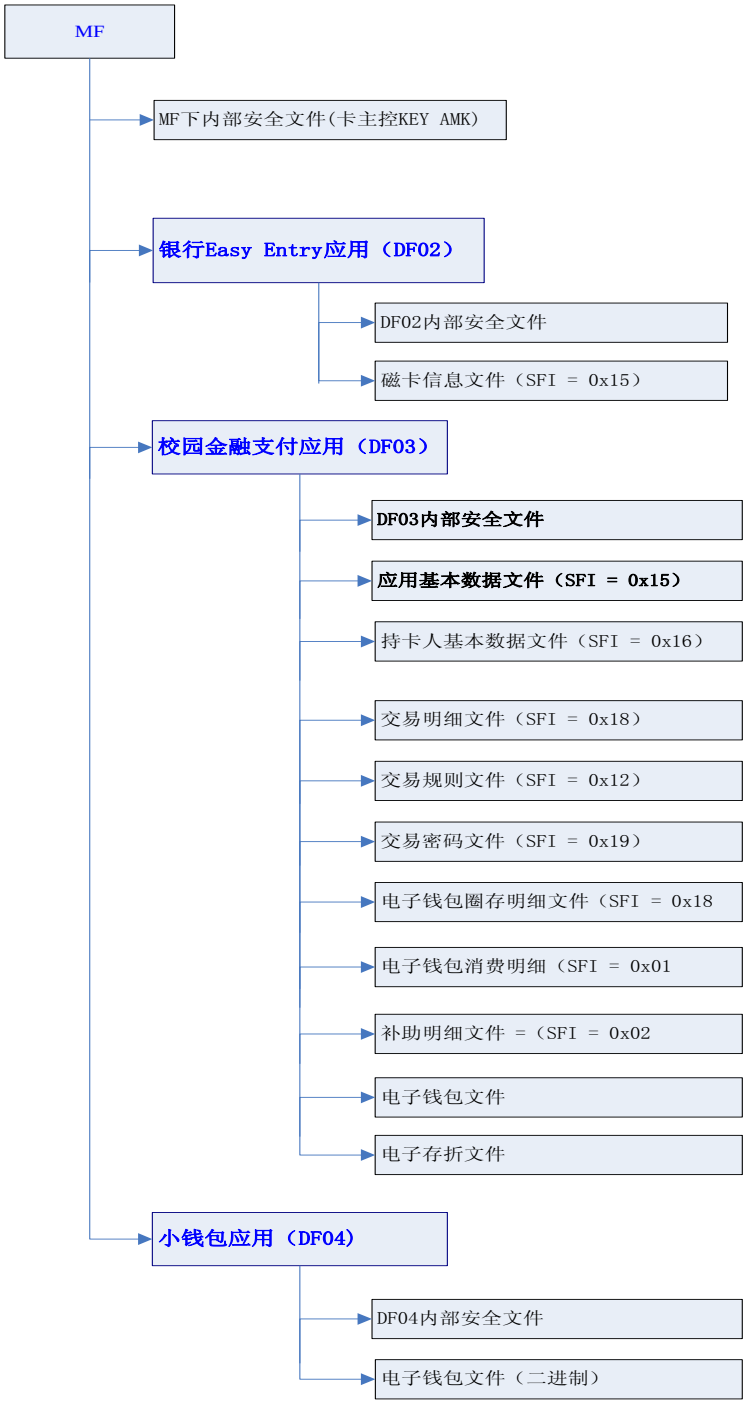
版本号 1.7

胜科金仕达数据系统有限公司

2010-1-15

目　录

1. 用户卡文件结构示意图



2.用户卡文件结构详细信息

2.1 MF 目录文件

MF 下密钥说明

文件类型	ISF 文件		文件大小	39bytes
文件权限	读取	禁止		
	更新	禁止		
文件说明				
KID	名称	长度	说明	
00	CCK	16bytes	卡片主控密钥	

文件名称	交易密钥文件		文件类型	定长记录文件
文件标识	EF-ID = 0000, SFI = 0x00		文件大小	1 * 18 bytes
文件权限	读取	禁止		
	更新	禁止		
密钥说明				
密钥用途 PURPOSE	密钥索引 INDEX	密钥		
01	00	应用维护密钥		

PSE 下文件说明

文件名称	目录文件		文件类型	定长记录文件
文件标识	EF-ID = 0001, SFI = 0x01		文件大小	4 * 16 bytes
文件权限	读取	自由		
	更新	安全报文		
文件说明				
记录号	说明			
01	Easy Entry 应用目录信息			
02	校园支付应用目录信息			
03	小额钱包应用目录信息			

2.3 银行 Easy Entry 应用

应用标识 AID：D1 56 00 00 01 45 41 53 59 45 4E 54 52 59 00 00

DF 文件标识 DF-ID：DF02

DF02 下密钥说明

文件类型	ISF 文件		文件大小	62bytes
文件权限	读取	禁止		
	更新	禁止		
文件说明				
KID	名称	长度	说明	
00	CCK	16bytes	Dummy CCK	

文件名称	交易密钥文件		文件类型	定长记录文件
文件标识	EF-ID = 0000，SFI = 0x00		文件大小	1 * 18 bytes
文件权限	读取	禁止		
	更新	禁止		
密钥说明				
密钥用途 PURPOSE	密钥索引 INDEX	密钥		
36	00	应用维护密钥		

DF02 下文件说明

文件名称	银行信息		文件类型	二进制
文件标识	EF-ID = 0015，SFI = 0x15		文件大小	60bytes
文件权限	读取	自由		
	更新	安全报文(明文＋MAC)		
文件说明				
字节	数据元		长度（bytes）	数据类型
1-20	银行卡号		20	an
21-60	预留(没有特征定义时为 FF)		40	

2.4 校园支付应用

应用标识 AID：D1 56 00 00 01 BD F0 CA CB B4 EF D6 A7 B8 B6

DF 文件标识 DF-ID：DF03

DF03 下密钥说明

文件名称	密钥文件		文件类型	
文件标识	EF-ID = 0000，SFI = 0x00		文件大小	
文件权限	读取	禁止		

	更新	禁止
密钥说明		
密钥类型 TYPE	**密钥索引 INDEX**	**密钥**
3E	01-02	消费密钥
3F	01-02	圈存密钥
34	00	TAC 密钥
37	00	PIN 解锁密钥
38	00	重装 PIN 密钥
36	01	应用维护密钥
39	01-03	外部认证密钥

DF03 下文件说明

文件名称	交易密码文件		**文件类型**	定长记录文件
文件标识	EF-ID = 0019, SFI = 0x19		**文件大小**	1 * 16 bytes
文件权限	读取	外部认证+安全报文(明文+MAC)		
	更新	安全报文(明文＋MAC)		
文件说明				
字节	**数据元**		**长度（bytes）**	**数据类型**
1-16	交易密码		16	cn

文件名称	应用基本数据文件		**文件类型**	二进制
文件标识	EF-ID = 0015, SFI = 0x15		**文件大小**	56bytes
文件权限	读取	自由		
	更新	安全报文(明文＋MAC)		
文件说明				
字节	**数据元**		**长度（bytes）**	**数据类型**
1-10	应用序列号		10	cn
11-20	显示卡号		10	an
21-21	卡状态 (0-正常 1—锁卡 2 冻结 3 挂失 4 注销 5 过期)		1	b
22-28	黑名单版本(YYYYMMDD+6 位流水号)		7	cn
29-34	设备 ID 号		6	cn
35-35	卡收费类别		1	b

36-36	卡结构版本	1	b
37-40	启用日期(YYYYMMDD)	4	cn
41-44	有效日期(YYYYMMDD)	4	cn
45-48	补助批次号	4	b
49-50	发行方标识	2	B
51	卡类别	1	B
52-55	发行日期（YYYYMMDD）	4	cn
56	预留(没有特征定义时为 FF)	1	b

文件名称	持卡人基本数据文件		**文件类型**	二进制
文件标识	EF-ID = 0016，SFI = 0x16		**文件大小**	112 字节
文件权限	读取	自由		
	更新	安全报文(明文＋MAC)		
文件说明				

字节	**数据元**	**长度（bytes）**	**数据类型**
1-32	姓名	32	an
33-64	证件号码	32	an
65-65	证件类型	1	b
66-66	性别	1	b
67-86	学工号	20	an
87-106	部门代码	20	an
107-107	客户类型	1	b
108-111	客户号	4	b
112-112	预留(没有特征定义时为 FF)	1	b

文件名称	交易规则文件		**文件类型**	二进制
文件标识	EF-ID = 0012，SFI = 0x12		**文件大小**	16 字节
文件权限	读取	自由		
	更新	安全报文(明文＋MAC)		
文件说明				

字节	**数据元**	**长度（bytes）**	**数据类型**
1-3	单次消费限额	3	b
4-6	日累计消费限额	3	b
7-8	卡消费次数	2	b
9-12	消费时间(DDHHMMSS)	4	cn
13-16	设备 ID	4	b

文件名称	存折交易明细文件		文件类型	循环记录文件
文件标识	EF-ID = 0018，SFI = 0x18		文件大小	10 * 23 bytes
文件权限	读取	校验 PIN		
	更新	禁止		

交易明细记录说明			
字节	数据元	长度 bytes	数据类型
0-1	ED 或 EP 联机或脱机交易序号	2	b
2-4	透支限额	3	b
5-8	交易金额	4	b
9	交易类型标识	1	b
10-15	终端机编号	6	cn
16-19	交易日期（终端）(YYYYMMDD)	4	cn
20-22	交易时间（终端）(HHMMSS)	3	cn

文件名称	电子钱包消费文件		文件类型	循环记录文件
文件标识	EF-ID = 0001，SFI = 0x01		文件大小	N * 40 bytes
文件权限	读取	自由		
	更新	安全报文(明文＋MAC)		

消费明细记录说明			
字节	数据元	长度 bytes	数据类型
1-4	交易日期(YYYYMMDD)	4	cn
5-7	交易时间(HHMMSS)	3	cn
8-8	交易类型	1	b
9-14	终端机编号(PSAM 卡中的终端号)	6	cn
15-18	终端交易序号(计算 TAC 用)	4	b
19-22	交易前余额	4	b
23-25	交易金额(包含搭伙费)	3	b
26-28	搭伙费	3	b
29-30	消费次数	2	b
31-34	补写金额(加钱为正减钱为负)	4	B
35-37	日累计消费金额	3	B
38-39	商户号	2	B
40	预留(没有特征定义时为 FF)	1	B

注：文件的记录数由交易规则文件中的消费明细文件创建最大记录数决定，最大为 255。

文件名称	补助明细文件		文件类型	循环记录文件
文件标识	EF-ID = 0002，SFI = 0x02		文件大小	10 * 40 bytes
文件权限	读取	自由		
	更新	安全报文(明文＋MAC)		

交易明细记录说明			
字节	数据元	长度 bytes	数据类型
1-4	交易日期(YYYYMMDD)	4	cn
5-7	交易时间(HHMMSS)	3	cn
8-8	交易类型(正补助、负补助)	1	b
9-14	终端机编号(PSAM 卡中的终端号)	6	cn
15-18	终端交易序号(计算 TAC 用)	4	b
19-22	交易前余额	4	b
23-25	补助金额	3	b
26-29	补助批次号	4	b
30-31	累计补助领取次数	2	b
32-35	TAC	4	b
36-40	预留 (没有特征定义时为 FF)	5	

A．两明细文件不合并理由：

1. 由于日消费累计跨天时需要清 0，则可以直接读钱包消费明细文件第 1 条记录，就知道是否需要清 0，若并在一起，则需要循环查找，影响性能。
2. 不合并其实没有任何影响，且清析直观。
3. 在消费明细中增加日累计消费金额栏，消费时，只读交易规则文件，不需要再改写交易规则文件，这样节省消费整个流程的时间。

B．若交易类型为正补则为充值，若为负补助，则直接消费就可以了。

2.6 小额钱包应用

应用标识 AID：D1 56 00 00 01 BD F0 CA CB B4 EF C7 AE B0 FC 32

DF 文件标识 DF-ID：DF04

DF04 下密钥说明

文件类型	ISF 文件		文件大小	62bytes
文件权限	读取	禁止		
	更新	禁止		

密钥说明			
密钥类型	密钥索引	密钥长度	说明
36	01	16	应用维护密钥
39	01	16	外部认证密钥

文件名称	小钱包文件		文件类型	二进制	
文件标识	EF-ID = 0001，SFI = 0x01		文件大小	7 字节	
文件权限	读取	外部认证+安全报文			
	更新	外部认证+安全报文			
1	钱包状态(0-可用 n-其它值不可用)			1	b
2-5	金额			4	b
6-7	备用			2	b

3. 附录(数据类型)

b: 是指二制读写。 如：3A 十制数为 58

cn: 是指含有 0~9 a~f A~F

an: 是指所有字符串，包括汉字

在卡片中保存的原则为：

cn 类型为压缩进行保存 如 12AB34 则卡中为\x12\xAB\x34

bin 类型为二进制数据保存 如：1223476 则在卡中为\x12\xAB\x34

an 类型为字符保存 如 1234 则在卡中为\x31\x32\x33\x34

4. 附录(测试密钥)

密钥名称	密钥数据
消费密钥	77777777777777777777777777777777
圈存密钥	66666666666666666666666666666666
TAC 密钥	55555555555555555555555555555555
PIN 解锁密	44444444444444444444444444444444
PIN 重装密钥	33333333333333333333333333333333
应用维护密钥	11111111111111111111111111111111
应用主控密钥	22222222222222222222222222222222
个人 PIN	123456