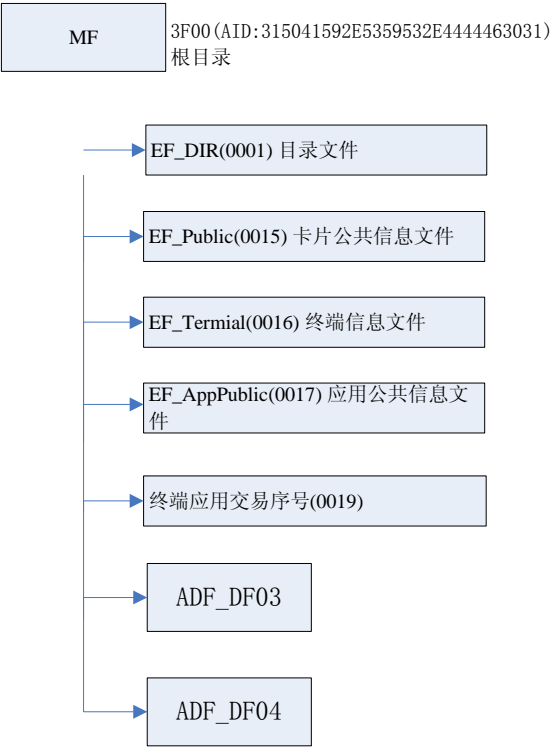


目录

1.1.	.PSAM 卡片结构一览.....	2
1.2.	PSAM 卡片文件详细说明.....	2
1.2.1.	MF 目录文件.....	2
1.2.1.1.	EF_DIR.....	3
1.2.1.2.	EF_Public.....	3
1.2.1.3.	EF_Terminal.....	3
1.2.2.	ADF_DF02 金融应用目录.....	错误！未定义书签。
1.2.2.1.	EF_APublic.....	3
1.2.2.2.	终端应用交易序号数据文件.....	4
1.3.	附录(测试密钥).....	5

1.1. .PSAM 卡片结构一览



1.2. PSAM 卡片文件详细说明

1.2.1. MF 目录文件

卡片根目录文件

文件类型	卡片根目录文件
FID	3F00
AID	31 50 41 59 2E 53 59 53 2E 44 44 46 30 31(1PAY.SYS.DDF01)
DIR 文件 SFI	01

文件存取控制	读 =AMK	写 =AMK	创建= MCK (外部认证)
--------	--------	--------	----------------

1.2.1.1. EF_DIR

该文件记录了 MF 下的应用目录信息

文件类型	变长记录文件	
FID	0001	
记录长度	变长	
文件记录条数	3	
文件存取控制	读 = 自由	改写 = AMK
记录号	记录内容	
1	D1 56 00 00 01 BD F0 CA CB B4 EF D6 A7 B8 B6	
2	保留	
3	保留	

1.2.1.2. EF_Public

卡片公共信息

文件类型	二进制			
FID	0015			
文件大小	14			
文件存取控制	读 = 自由		改写 = AMK	
序号	数据元	类型	长度(Dec)	
文件内容	1	PSAM 序列号	BCD	10
	2	PSAM 版本号	BINARY	1
	3	密钥卡类型	BINARY	1
	4	指令集版本	BINARY	1
	8	发卡方自定义 FCI 数据	BINARY	1

1.2.1.3. EF_Terminal

终端信息

文件类型	二进制			
FID	0016			
文件大小	6			
文件存取控制	读 = 自由		改写 = AMK	
序号	数据元	类型	长度(Dec)	
文件内容	1	终端机编号	BCD	6

1.2.1.4. EF_APublic

应用公共信息

文件类型	二进制			
FID	0017			
文件大小	25			
文件存取控制	读 = 自由		改写 = AMK	
序号	数据元	类型	长度(Dec)	
文	1	消费密钥索引号	BINARY	1

件 内 容	2	应用发行者标识	BCD	8
	3	应用接收者标识	BCD	8
	4	应用启用日期	BCD(YYYYMMDD)	4
	5	应用有效日期	BCD(YYYYMMDD)	4

1.2.1.5. 终端应用交易序号数据文件

DF 终端应用交易序号数据元

文件类型		二进制		
FID		0019		
文件大小		4		
文件存取控制		读 = 自由	改写=禁止, 由 COS 自动改写	
序号		数据元	类型	长度(Dec)
文件内容	1	终端应用交易序号	BINARY	4

1.2.2. ADF_DF03 金融应用目录

金融应用目录文件

文件类型		子目录文件		
AID		D156000001BDF0CACBB4EFD6A7B8B6FF		
FCI 文件 SFI		DF03		
文件存取控制		读= AMK	写= AMK	创建 = MCK (外部认证)

1.2.2.1. EF_APublic

应用公共信息

文件类型		二进制		
FID		0017		
文件大小		25		
文件存取控制		读 = 自由	改写 = AMK	
序号		数据元	类型	长度(Dec)
文 件 内 容	1	消费密钥索引号	BINARY	1
	2	应用发行者标识	BCD	8
	3	应用接收者标识	BCD	8
	4	应用启用日期	BCD(YYYYMMDD)	4
	5	应用有效日期	BCD(YYYYMMDD)	4

1.2.2.2. 终端应用交易序号数据文件

DF 终端应用交易序号数据元

文件类型		二进制		
FID		0019		
文件大小		4		
文件存取控制		读 = 自由	改写=禁止, 由 COS 自动改写	
序号		数据元	类型	长度(Dec)
文件内容	1	终端应用交易序号	BINARY	4

1.2.3. ADF_DF04 门禁应用目录

金融应用目录文件

文件类型	子目录文件		
AID	D156000004BDF0CACBB4EFD6A7B8B6FF		
FCI 文件 SFI	DF04		
文件存取控制	读= AMK	写= AMK	创建 = MCK (外部认证)

1.3. 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

注：红色不用