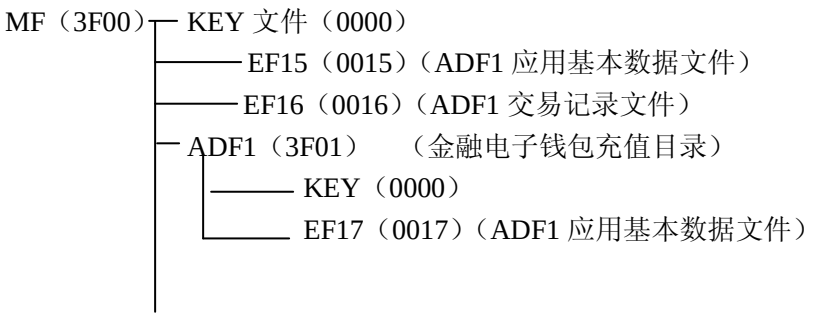
九、充值 SAM 卡



文件名称	文件类型	文件标识符	文件大小	读权	写权
MF	78	3F00	FFFF	AA	AA
KEY 文件	62	6F3F	17H		AA
DIR 文件	54	2F01	50H	F0	F0
卡片公共信息文件	41	2F15	0EH	F0	F0
终端信息文件	41	2F16	06H	F0	F0
ADF1	78	3F01		EF	EF
KEY 文件	62	6F3F			EF
应用公共信息	41	2F17	19H	F0	F0
ADF2	78	7F02		EF	EF
KEY 文件	62	6F3F			EF
应用公共信息	41	2F17	19H	F0	F0

MF 下 KEY 文件内容：

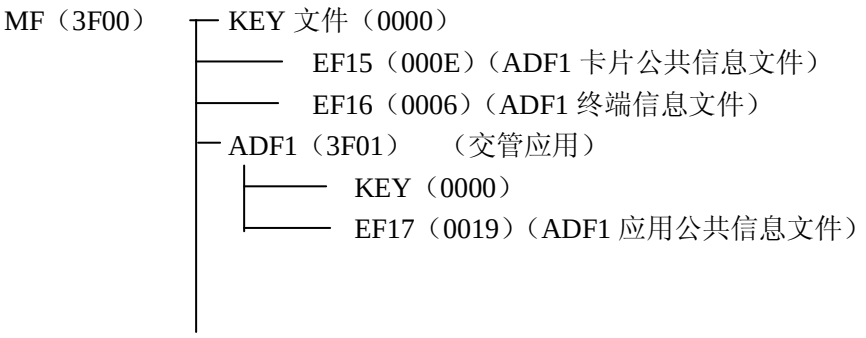
密钥名称	密钥类型	密钥标识	密钥大小	使用权	更改权	后续状态	错误计数器
主控密钥 Kictlr	00	00	10H	F0	AA	AA	33
卡片维护密钥	01	00	10H				

ADF1 下 KEY 文件内容：

密钥名称	密钥类型	密钥标识	密钥大小	使用权	更改权	后续状态	错误计数器
应用主控密钥	00	00	10H				
应用维护密钥	01	00	10H				
公共钱包充值主密钥	22	01-05	10H				

公共消费密钥	27	01-05	10H				
TAC 密钥	28	01	10H	……	……	……	……
用户卡应用维护密钥	28	02	10H				
内部认证密钥	28	03	10H				
复合消费记录更新密钥	28	04	10H				
行业应用维护密钥	28	05	10H				
MAC 密钥	28	06	10H				

十、PSAM 卡



文件名称	文件类型	文件标识符	文件大小	建立权	擦除权
MF	78	3F00	FFFF	AA	AA
KEY 文件	62	6F3F	17H		AA
DIR 文件	54	2F01	50H	F0	F0
卡片公共信息文件	41	2F15	0EH	F0	F0
终端信息文件	41	2F16	06H	F0	F0
ADF1	78	3F01		EF	EF
KEY 文件	62	6F3F			EF
应用公共信息	41	2F17	19H	F0	F0
ADF2	78	7F02		EF	EF
KEY 文件	62	6F3F			EF

应用公共信息	41	2F17	19H	F0	F0
ADF3	78	7F02		EF	EF
KEY 文件	62	6F3F			EF
应用公共信息	41	2F17	19H	F0	F0

各 ADF 下的大小为：密钥组数*3*23+2*23+5+50；

各 ADF 下的 KEY 文件大小为：密钥组数*3*23+2*23+5；

MF 下 KEY 文件内容：

密钥名称	密钥类型	密钥标识	密钥大小	使用权	更改权	后续状态	错误计数器
卡片主控	00	00	10H	F0	F0	AA	33
卡片维护密钥	01	00	10H	F0	EF	00	00

维护密钥内容为 PSAM 卡传输卡的二进制文件解密后的内容。

主密钥传输卡的加密密钥对待发卡复位信息后 8 字节分散得到各 ADF 下的应用主控密钥；

各 ADF 下的应用维护密钥与 MF 维护密钥内容相同；

ADF1 下 KEY 文件内容：

密钥名称	密钥类型	密钥版本号	算法标识	密钥大小
应用主控	00	00	00	10H
应用维护密钥	01	00	00	10H
公共消费密钥	27	01-05	10H	
TAC 密钥	28	01	10H	……
用户卡应用维护密钥	28	02	10H	
内部认证密钥	28	03	10H	
复合消费记录更新密钥	28	04	10H	
行业应用维护密钥	28	05	10H	
MAC 密钥	28	06	10H	

业务密钥从 PSAM 卡母卡导出公用业务密钥组，可安装 1~2 组。