全国城市公共交通IC卡互联互通
SAM卡文件结构
（试行）

SAM 卡用于公交、地铁受理终端、网点终端、直联终端等端末设备上，负责机具的安全控管。SAM 卡具有一定的通用性。经过个人化处理的 SAM 卡能在不同的机具上使用。

SAM 卡支持多级发卡的机制，各级发卡方在卡片主控密钥和应用主控密钥的控制下创建文件和装载密钥。

1. SAM 卡结构

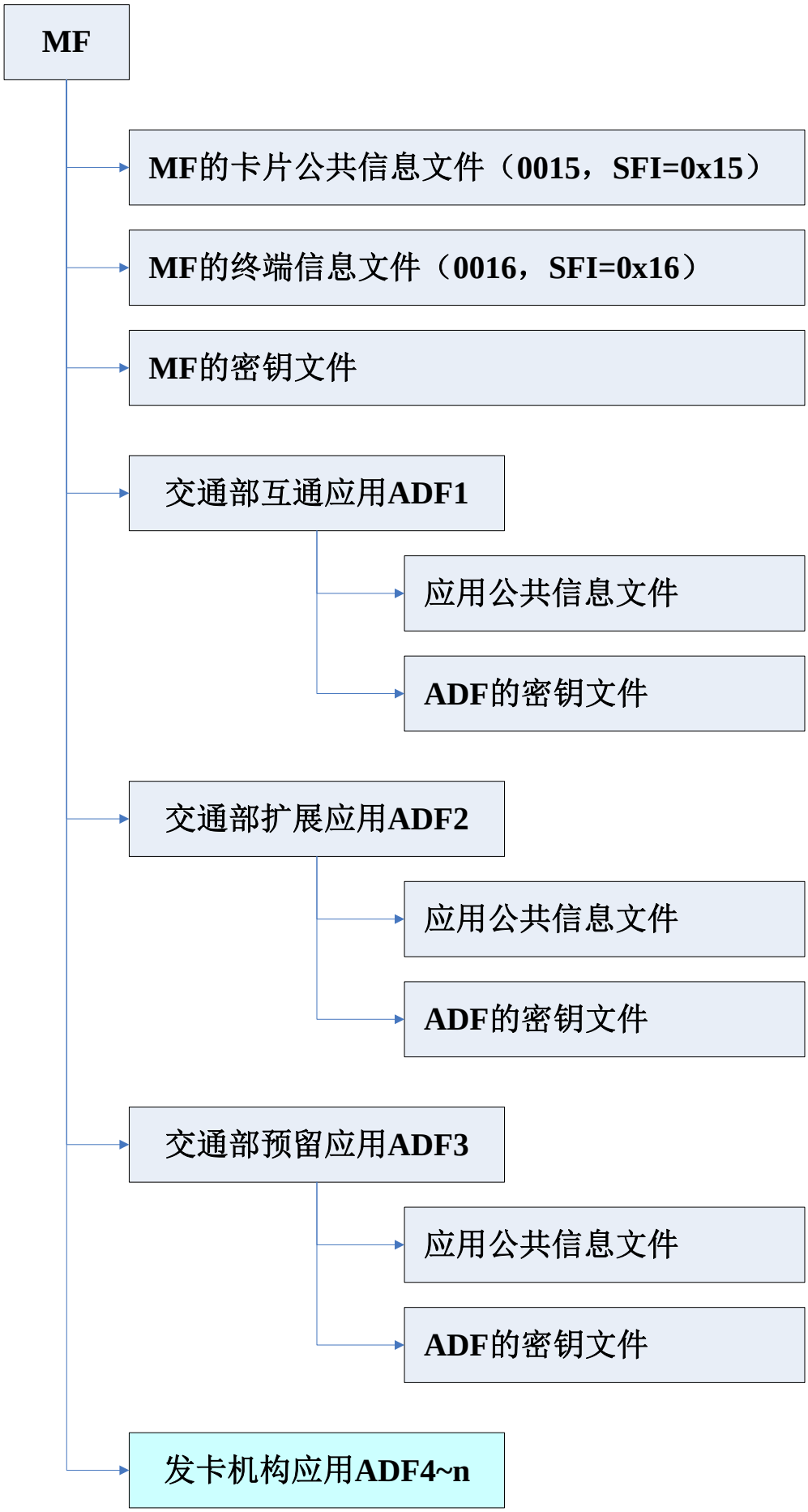
SAM 卡文件结构符合 ISO/IEC7816－4。

本条款描述了符合本规范的应用文件结构，这些应用被定义为支付系统应用（PSA）。符合 ISO/IEC7816－4，但不符合本规范的其他应用也可出现在 PSA 上，并可以使用本规范中定义的命令进行操作。

SAM 卡中 PSA 的路径可以通过明确选择支付系统环境（PSE）来激活。

SAM 卡文件结构如下图所示：

⑴ 卡片结构


MF
MF的卡片公共信息文件（0015，SFI=0x15）
MF的终端信息文件（0016，SFI=0x16）
MF的密钥文件
交通部互通应用ADF1
应用公共信息文件
ADF的密钥文件
交通部扩展应用ADF2
应用公共信息文件
ADF的密钥文件
交通部预留应用ADF3
应用公共信息文件
ADF的密钥文件
发卡机构应用ADF4~n

1.1 约束

城市公共交通 IC 卡互连互通 SAM 中，MF 的创建和互通应用 ADF1 的创建需在全国认证中心处理进行个人化；全国认证中心下发 SAM 卡二次发行母卡和控制卡，用于配合各地方一卡通发卡机构 SAM 卡信息的更新和其它 ADF 的创建。

2. MF 下文件说明

文件名称	卡片公共信息文件		文件类型	二进制
文件标识	EF-ID = 0015，SFI = 0x15		文件大小	14 bytes
文件权限	读取	自由		
	更新	安全报文；可在 PSAM 发卡母卡和控制卡的前提下进行更新		

文件说明			
字节	数据元	长度（bytes）	数据类型
1-10	PSAM 序列号	10	cn
11	PSAM 版本号	1	b
12	密钥卡类型	1	b
13-14	发卡方自定义 FCI 数据	2	b

文件名称	终端信息文件		文件类型	二进制
文件标识	EF-ID = 0016，SFI = 0x16		文件大小	6 bytes
文件权限	读取	自由		
	更新	安全报文；可在 PSAM 发卡母卡和控制卡的前提下进行更新		

文件说明			
字节	数据元	长度（bytes）	数据类型
1-6	终端机编号	6	cn

MF 的密钥说明

密钥头			名称	说明
密钥用途	密钥标识	算法标识		
00	00	00	卡片主控密钥	
01	00	00	卡片维护密钥	

3. 应用（ADF1）说明

应用标识 AID	A0000006324D4F542E435053414D3031
文件标识 DF-ID	8011

文件名称	应用公共信息文件		文件类型	二进制
文件标识	EF-ID = 0017，SFI = 0x17		文件大小	25 bytes
文件权限	读取	自由		
	更新	安全报文		

文件说明			
字节	数据元	长度（bytes）	数据类型
1	城市公共交通 IC 卡消费密钥索引号	1	b
2-9	应用发行者标识	8	cn
10-17	应用接收者标识	8	cn
18-21	应用启用日期	4	cn
22-25	应用有效日期	4	cn

3.1 ADF1 的密钥说明

密钥头			名称	说明
密钥用途	密钥标识	算法标识		
00	00	00	应用主控密钥	
01	00	00	应用维护密钥	同 MF 下卡片维护密钥
42	01	00	公共钱包消费密钥。锁卡限制为 3 次。	城市公共交通 IC 卡的根密钥（DES）
45	01	00	预留	
45	02	00	用户卡应用维护密钥（应用锁定）	
45	03	00	预留	
45	04	00	预留	
45	05	00	互通记录保护密钥-电子现金	
45	06	00	互通记录保护密钥-电子钱包	
45	07	00	互通记录保护密钥（备用）	
42	01	01	公共钱包消费密钥	城市公共交通 IC 卡-国密预留，视情况发行
45	01	01	用户卡应用维护密钥	
45	02	01	用户卡应用维护密钥（应用锁定）	
45	03	01	用户卡应用解锁密钥	
45	04	01	用户卡文件更新密钥	
45	05	01	互通记录保护密钥-电子现金	
45	06	01	互通记录保护密钥（备用）	
45	07	01	互通记录保护密钥（备用）	
42	01	04	公共钱包消费密钥	城市公共交通 IC 卡根密钥--国密预留，视情况发行
45	01	04	用户卡应用维护密钥	
45	02	04	用户卡应用维护密钥（应用锁定）	
45	03	04	用户卡应用解锁密钥	
45	04	04	用户卡文件更新密钥	

45	05	04	互通记录保护密钥-电子现金	
45	06	04	互通记录保护密钥（备用）	
45	07	04	互通记录保护密钥（备用）	

4. 应用（ADF2）说明

应用标识 AID	A0000006324D4F542E435053414D3032
文件标识 DF-ID	8012

文件名称	应用公共信息文件		**文件类型**	二进制
文件标识	EF-ID = 0017，SFI = 0x17		**文件大小**	25 bytes
文件权限	读取	自由		
	更新	安全报文		

文件说明			
字节	**数据元**	**长度（bytes）**	**数据类型**
1	城市公共交通 IC 卡消费密钥索引号	1	b
2-9	应用发行者标识	8	cn
10-17	应用接收者标识	8	cn
18-21	应用启用日期	4	cn
22-25	应用有效日期	4	cn

4.1 ADF2 的密钥说明

密钥头			**名称**	**说明**
密钥用途	**密钥标识**	**算法标识**		
00	00	00	应用主控密钥	
01	00	00	应用维护密钥	同 MF 下卡片维护密钥

5. 应用（ADF3）说明

应用标识 AID	A0000006324D4F542E435053414D3033
文件标识 DF-ID	8013

文件名称	应用公共信息文件		**文件类型**	二进制
文件标识	EF-ID = 0017，SFI = 0x17		**文件大小**	25 bytes
文件权限	读取	自由		
	更新	安全报文		

文件说明			
字节	**数据元**	**长度（bytes）**	**数据类型**
1	城市公共交通 IC 卡消费密钥索引号	1	b

2-9	应用发行者标识	8	cn
10-17	应用接收者标识	8	cn
18-21	应用启用日期	4	cn
22-25	应用有效日期	4	cn

5.1 ADF3 的密钥说明

密钥头			名称	说明
密钥用途	密钥标识	算法标识		
00	00	00	应用主控密钥	
01	00	00	应用维护密钥	同 MF 下卡片维护密钥