?????

本手册仅包含非接触式智能卡

- AID 索引
- 交通卡
  - 数字城市一卡通（City Union）
  - 北京市政公交一卡通（BMAC）
  - 交通联合卡（T-Union）
  - 深圳通（Shenzhen Tong）
  - 八达通
  - EZ-Link
  - 悠游卡
  - Oyster
  - 岭南通（Lingnan Pass）
- 金融卡
  - EMV
  - PBOC 2.0
- 区域性一卡通
  - 新开普一卡通
- 身份文件
  - 电子护照
  - 二代居民身份证
- 其他
  - YubiKey
  - FIDO U2F
  - NXP JCOP Javacard

- Canokey
- MIFARE Classic

- [illegible]

AID ??

AID	□□□□□
325041592E5359532E4444463031	EMV□□□□□□□
A00000000386980701	□□□□□□□□□□□□□
5041592E535A54	□□□
4150312E5748435443...	□□□
5041592E41505059, 5041592E5449434C	□□□
A000000333010101	□□□□□
A000000333010102	□□□□□□□□□□
A000000333010103	□□□□□□
A000000632010105	□□□□□□□□□
A000000632010106	□□□□□□□□□
A000000003...	VISA
A000000004...	MasterCard
A000000025...	American Express
A000000065...	JCB
A000000098...	VISA USA
A000000152...	Discover
A0000006472F0001	FIDO U2F
A00000030800001000	PIV
A0000005272101	OATH Applet
D27600012401...	OpenPGP Card
4A43416C6754657374	JcAlgTest

???

交通卡

????????City Union?

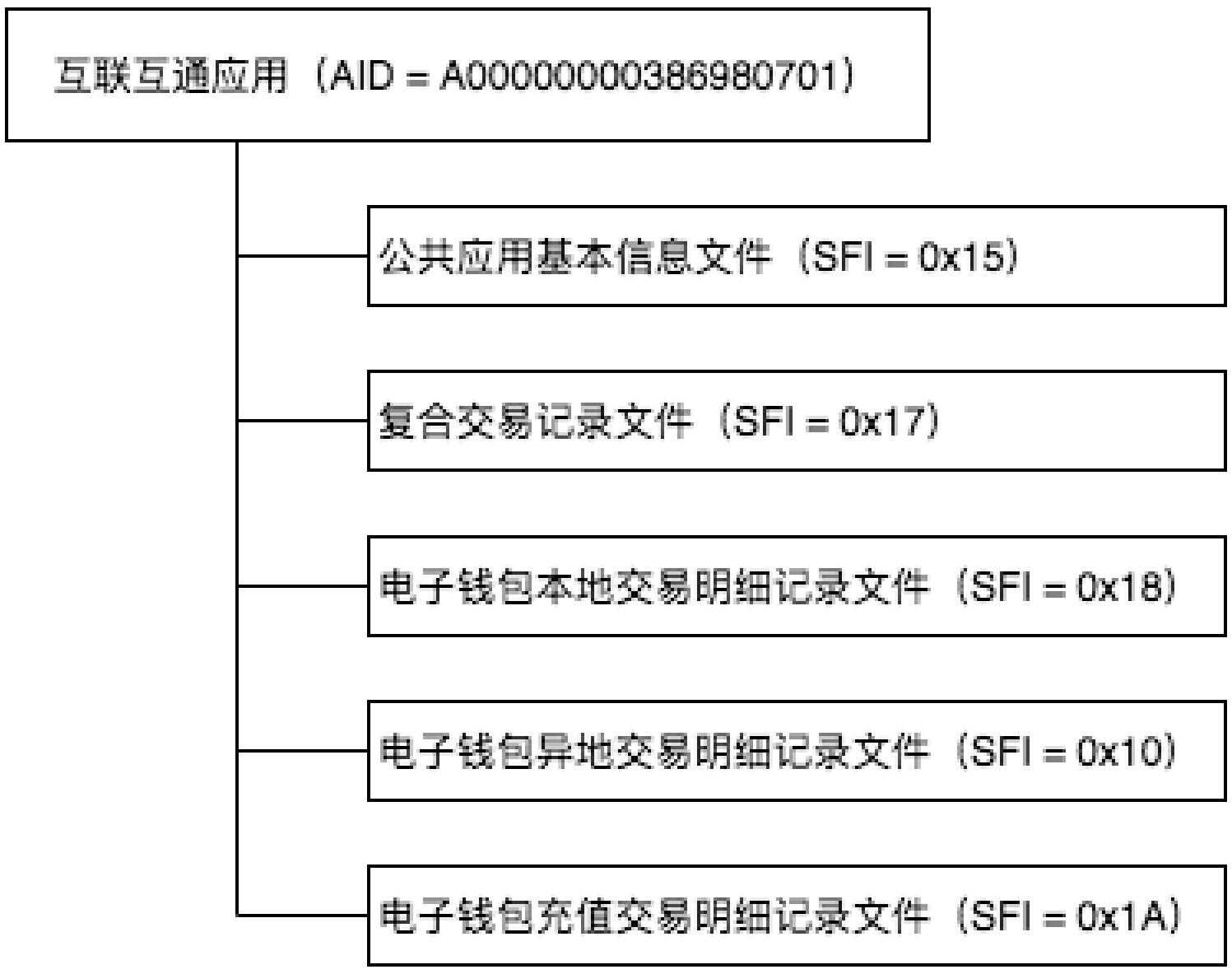
????

根据 GB/T 31778-2015《数字城市一卡通互联互通通用技术要求》的表述，数字城市一卡通适用于互联互通城市间综合交通（公共汽车、地铁、轻轨、轮渡、出租车、公共自行车）、公用事业缴费、风景园林、社区/园区应用、停车场管理等领域应用。

目前，该标准覆盖的城市和项目为：

> 上海
> 天津
> 澳门（特别行政区）
> 浙江：宁波、绍兴、湖州、台州、舟山、长兴、金华、温州、义乌、嘉兴
> 江苏：常熟、昆山、淮安、江阴、无锡、南通、泰州、宜兴、太仓、盐城
> 甘肃：兰州、白银、华亭
> 江西：南昌、九江、鹰潭、赣州、上饶
> 湖南：永州、株洲、湘潭、望城
> 辽宁：葫芦岛、锦州、抚顺、沈阳、营口、兴城、铁岭、本溪
> 四川：江油、自贡、西昌、阆中
> 福建：福州、龙岩、泉州、莆田、晋江
> 海南：三亚
> 广东：湛江、珠海
> 吉林：辽源、松原
> 新疆：克拉玛依
> 陕西：榆林、渭南、咸阳、杨凌
> 河南：驻马店、郑州、南阳、漯河、荥阳、新郑、平顶山
> 贵州：凯里、遵义、都匀
> 云南：昆明、大理
> 湖北：十堰、潜江
> 安徽：淮南、阜阳
> 山东：临沂
> 河北：邯郸
>
> 互联互通项目：招商通、全国景区一卡通、无锡灵山、社区有我、北京未来科学城、天津海河游轮

需要指出的是，以上列出的城市/项目，仅表示该城市/项目使用了由中华人民共和国住房和城乡建设部生成的密钥，并不意味着所发行的卡片可以互通。例如，上海发行的紫色卡，虽然采用了该标准，但仅与江苏、浙江的部分城市互通。



????

互联互通应用的基本文件目录应至少包括下图中所有文件：

互联互通应用（AID = A000000000386980701）
公共应用基本信息文件（SFI = 0x15）
复合交易记录文件（SFI = 0x17）
电子钱包本地交易明细记录文件（SFI = 0x18）
电子钱包异地交易明细记录文件（SFI = 0x10）
电子钱包充值交易明细记录文件（SFI = 0x1A）

注意：由于标准发布于 2015 年，对于早期参与到该标准的城市，卡内数据可能不遵守这个规范，但可以保证的是，0x15和 0x18文件总是存在，其中 0x18里包含了所有类型的交易记录。

????

密钥名称	密钥代码	密钥标识	分散级别	密钥作用
应用主控子密钥	DACK	00	1	控制应用区内结构添加和删除
应用锁定子密钥	-	-	2	应用锁定
应用解锁子密钥	-	-	1	应用解锁
文件更新子密钥	-	-	1	应用区内有关信息文件的更新保护
复合消费维护密钥	DCPK	01	1	复合消费文件维护
PIN解锁密钥	DPUK	00	2	解锁 PIN
PIN重装密钥	DPLK	00	2	重装 PIN
消费子密钥	DPK	01~ 0A	2	共 10组密钥
圈存子密钥	DLK	01~ 02	1	共 2组密钥
TAC子密钥	DTK	00	2	消费交易验证

其中，应用锁定子密钥、消费子密钥、TAC子密钥是互通的；其他密钥均由发卡方自行管理。

????

??????????

SFI	0x15			
文件类型	二进制文件			
文件大小	0x1E			
权限	读 =自由		写 =SM	
字节	数据元	长度	格式	说明
01~ 02	发卡方代码	2	BCD	
03~ 04	城市/项目代码	2	HEX	
05	多算法支持	1	BCD	
06	行业代码	1	BCD	
07~ 08	预留	2	HEX	
09	互联互通启用标识	1	HEX	0x00为未启用，非0x00为启用
10	应用版本	1	HEX	
11~ 12	互联互通标识	2	HEX	同城市/项目代码
13~ 20	用户卡应用序列号	8	HEX	
21~ 24	应用生效日期（YYYYMMDD)	4	BCD	
25~ 28	应用失效日期（YYYYMMDD)	4	BCD	
29~ 30	预留	2	HEX	

????????

SFI		0x17			
文件类型		变长记录文件			
文件大小		0xA0			
权限		读 =自由		写 =SM/复合交易	
记录标识	字节	数据元	长度	格式	说明
0x09	01	0x09	1	HEX	
	02	复合消费数据长度	1	HEX	
	03	复合消费锁定标识	1	HEX	0x00表示允许，非0x00表示禁止
	04~48	应用方自定义	45	自定义	

????????????????

SFI	0x18

文件类型	循环记录文件			
记录长度	0x17			
权限	读 =自由		写 =N/A	
字节	数据元	长度	格式	说明
01~ 02	电子钱包消费交易序号	2	HEX	
03~ 05	预留	3	HEX	
06~ 09	交易金额	4	HEX	
10	交易类型	1	HEX	0x06表示消费，0x09表示复合消费
11~ 16	交易终端编号	6	BCD	
17~ 20	交易日期（YYYYMMDD）	4	BCD	
21~ 23	交易时间（HHMMSS）	3	BCD	

????????????????

SFI	0x10			
文件类型	循环记录文件			
记录长度	0x17			
权限	读 =自由		写 =N/A	
字节	数据元	长度	格式	说明
01~ 02	电子钱包消费交易序号	2	HEX	
03~ 05	预留	3	HEX	
06~ 09	交易金额	4	HEX	
10	交易类型	1	HEX	0x06表示消费，0x09表示复合消费
11~ 16	交易终端编号	6	BCD	
17~ 20	交易日期（YYYYMMDD）	4	BCD	
21~ 23	交易时间（HHMMSS）	3	BCD	

????????????????

SFI	0x1A	
文件类型	循环记录文件	
记录长度	0x17	
权限	读 =自由	写 =N/A

字节	数据元	长度	格式	说明
01~ 02	电子钱包充值交易序号	2	HEX	
03~ 05	预留	3	HEX	
06~ 09	交易金额	4	HEX	
10	交易类型	1	HEX	0x02
11~ 16	交易终端编号	6	BCD	
17~ 20	交易日期（YYYYMMDD）	4	BCD	
21~ 23	交易时间（HHMMSS）	3	BCD	

????

城市/项目代码表（城市邮编前4位）

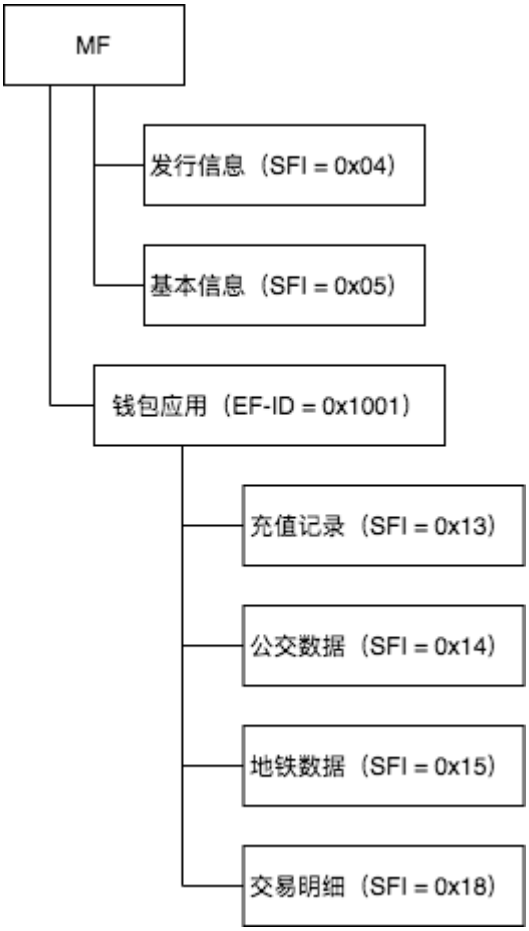
城市/项目	代码
上海	2000
天津	3000
招商通	
全国景区一卡通	
无锡灵山	
社区有我	
北京未来科学城	0001
天津海河游轮	

□□□

??????????BMAC?

□□□□ DB11/T 159.2-2015

????



????

???????MF?

SFI	0x04			
□□□□	□□□□□			
□□□□	0x3C			
□□	□ =□□		□ =SM	
□□	□□□	□□	□□	□□
01□ 08	□□	8	BCD	

09~ 24	不详	15	N/A	
25~ 28	应用生效日期（YYYYMMDD)	4	BCD	
29~ 32	应用失效日期（YYYYMMDD)	4	BCD	
23~ 60	不详	28	N/A	

???????MF?

SFI	0x05			
文件类型	二进制文件			
文件大小	0x20			
权限	读 =自由		写 =SM	
字节	数据元	长度	格式	说明
01~ 03	透支金额	3	HEX	
04~ 05	累计交易次数	2	HEX	
06~ 32	不详	27	N/A	

???????DF-ID=1001?

SFI	0x13			
文件类型	循环记录			
记录长度	0x17			
记录数量	3			
权限	读 =自由		写 =SM	
字节	数据元	长度	格式	说明
01~ 03	充值前金额	3	HEX	
04~ 06	充值后金额	3	HEX	
07~ 08	不详	2	N/A	
09~ 11	充值日期	3	BCD	YYMMDD
12~ 17	终端编号	6	HEX	
18~ 23	不详	6	N/A	

?????????DF-ID=1001?

SFI	0x14
文件类型	二进制

文件长度	0x18			
权限	读 =自由		写 =SM	
字节	数据元	长度	格式	说明
01~ 06	上车时间	6	BCD	YYMMDDhhmmss
07	方向?	1	HEX	AB或 BA
08~ 09	不详	2	N/A	
10~ 11	线路	2	HEX	小端序
12~ 24	不详	13	N/A	

??????

交易终端以 300开头的，表示地铁的终端设备。
十六进制表示的第 4、5位为地铁线路编号，例如 300040000570 的 04 表示编号。

编号	线路
01	一号线
02	二号线
04	四号线
05	五号线
06	六号线
07	七号线
08	八号线
09	九号线
10	十号线
13	十三号线
14	十四号线
15	十五号线
18	西郊线
88	大兴机场线
93	大兴线
94	昌平线
95	房山线
96	亦庄线
97	八通线

98	□□□□□

交通卡

??????T-Union?

??

交通联合卡是由交通部主导的标准，采取电子现金、电子钱包双应用模式。截止 2018年 7月，已有 210 个城市市区全部公交线路实现互联互通， 13个城市轨道线路实现互联互通， 35 个城市开通了试运行公交线路，总计覆盖全国 2.2万条公交线路、 52条轨道线路。

市区全部公交线路可使用“交通联合”卡城市列表（210 个城市）

省（直辖市）	城市
北京市（1，全部）	北京市公交和轨道
天津市（1，全部）	天津市公交和轨道
河北省（11，全部）	石家庄市公交和轨道；承德市、张家口市、秦皇岛市、唐山市、廊坊市、保定市、沧州市、衡水市、邢台市、邯郸市公交
山西省（10）	大同市、阳泉市、长治市、晋城市、朔州市、晋中市、忻州市、临汾市 、运城市、吕梁市公交
内蒙古自治区（1）	包头市公交
辽宁省（14，全部）	沈阳市、营口市、锦州市、朝阳市、本溪市、鞍山市 、盘锦市、铁岭市、葫芦岛市、大连市、抚顺市、辽阳市、丹东市、阜新市公交
吉林省（10，全部）	长春市公交和轨道；吉林市、四平市、辽源市、通化市、白山市、松原市、白城市、延边朝鲜族自治州、长白山管委会及全省区县内公交
江苏省（13，全部）	南京市、苏州市、无锡市公交和轨道；徐州市、常州市、南通市、连云港市、淮安市、盐城市、扬州市、镇江市、泰州市、宿迁市及全省区县公交
浙江省（5）	宁波市、温州市、嘉兴市、台州市 、绍兴市公交
安徽省（4）	蚌埠市、滁州市、马鞍山市、阜阳市公交
福建省（10，全部）	福州市、厦门市、漳州市、泉州市、三明市、莆田市、南平市、龙岩市、宁德市、平潭综合实验区公交
江西省（10）	南昌市、赣州市 、吉安市、九江市、萍乡市、新余市、上饶市、鹰潭市、宜春市、抚州市公交
山东省（6）	青岛市公交和轨道；威海市、临沂市、德州市、滨州市、菏泽市公交
河南省（18，全部）	郑州市公交和轨道;洛阳市、平顶山市、安阳市、新乡市、焦作市、许昌市、商丘市、信阳市、驻马店市、濮阳市、开封市、济源市、南阳市、漯河市、三门峡、鹤壁市、周口市公交
湖北省（10）	黄石市、咸宁市、随州市、潜江市、襄阳市、宜昌市、鄂州市、十堰市、荆门市、黄冈市公交
湖南省（9）	张家界市、邵阳市、永州市、岳阳市、湘潭市、衡阳市、常德市、益阳市、怀化市公交
广东省（7）	广州市、深圳市、中山市、韶关市、河源市、江门市、潮州市公交
广西壮族自治区（11）	南宁市全部公交和轨道线路；柳州市、钦州市、百色市、贺州市、来宾市、桂林市、北海市、防城港市、贵港市、玉林市公交
海南省（4）	海口市、三亚市、儋州市、文昌市公交
四川省（12）	自贡市、德阳市、广元市、遂宁市、乐山市、宜宾市、达州市、阿坝州、甘孜州、凉山州、广安市、巴中市公交
贵州省(8)	贵阳市全部公交和轨道线路；黔南州、毕节市、遵义市、六盘水市、铜仁市、黔东南州、黔西南州公交
云南省(13)	昆明市公交和轨道；楚雄市 、玉溪市、昭通市、保山市、文山州、红河州、丽江市、迪庆州、西双版纳、普洱市、怒江州、临沧市公交
西藏自治区(1)	拉萨市公交
陕西省（11）	西安市公交和轨道；宝鸡市、咸阳市、铜川市、渭南市、延安市 、汉中市、安康市、韩城市、商洛市、杨凌示范区公交
甘肃省（4）	武威市、张掖市、酒泉市、金昌市公交
青海省（4）	西宁市、海东市、海西州、玉树州公交
宁夏回族自治区（2）	银川市、固原市公交

备注：上海市、重庆市、哈尔滨市、乌鲁木齐市、长沙市、鄂尔多斯市、丽水市、枣庄市、株洲市、娄底市、郴州市、成都市、南充市、攀枝花市、雅安市、绵阳市、泸州市、眉山市、内江市、阿坝州、珠海市、湛江市、肇庆市、惠州市、汕尾市、东莞市、揭阳市、云浮市、梧州市、崇左市、曲靖市、大理市、德宏州、平凉市和新疆生产建设兵团均开通部分试运行线路

来源: https://www.cttic.cn/info/3171

????

文件可以通过 AID 或 SFI 引用， SFI 的范围如下:

数值	说明
0x1A, 0x1E	发卡基本信息，按标准使用
0x15~0x19	电子现金应用中由机构自定义



0x05~0x08, 0x19	电子钱包应用中由机构自定义
其他	预留

文件结构

变长记录文件（0x1A）的记录见下表：

记录号	记录描述
1	城市轨道应用信息记录
2	公共汽电车应用信息记录
3	城市水上客运应用信息记录
4	出租汽车应用信息记录
5	租赁汽车应用信息记录
6	公共自行车应用信息记录
7	停车收费应用信息记录
8	长途客运应用信息记录
9	轮渡应用信息记录
10	城际铁路应用信息记录
11	民航应用信息记录
12	高速公路收费应用信息记录
13	优惠信息记录
14~ 18	预留

????

终端通过选择DF名称2PAY.SYS.DDF01，然后根据卡片返回的应用信息和AID选择电子现金或电子钱包应用。

??????

????????

SFI	0x15
文件类型	二进制文件
文件大小	0x1E

权限	读 =自由		写 =SM	
字节	数据元	长度	格式	说明
01~ 08	发卡机构标识	8	HEX	
09	应用类型标识	1	HEX	
10	发卡机构应用版本	1	HEX	
11~ 20	应用序列号	10	HEX	
21~ 24	应用生效日期（YYYYMMDD)	4	BCD	
25~ 28	应用失效日期（YYYYMMDD)	4	BCD	
29~ 30	发卡机构自定义 FCI 数据	2	HEX	

?????????

SFI	0x16			
文件类型	二进制文件			
文件大小	0x37			
权限	读 =自由		写 =SM	
字节	数据元	长度	格式	说明
01	卡类型标识	1	HEX	
02	本行职工标识	1	HEX	
03~ 22	持卡人姓名	22	HEX	
23~ 54	持卡人证件号码	32	HEX	
55	持卡人证件类型	1	HEX	

??????

SFI	0x17			
文件类型	二进制文件			
文件大小	0x3C			
权限	读 =自由		写 =SM	
字节	数据元	长度	格式	说明
01~ 04	国际代码	4	HEX	
05~ 06	省级代码	2	HEX	
07~ 08	城市代码	2	HEX	银联地区码

09~ 10	互通卡种	2	HEX	
11	卡种类型	1	HEX	
12~ 60	预留	49	HEX	

????????

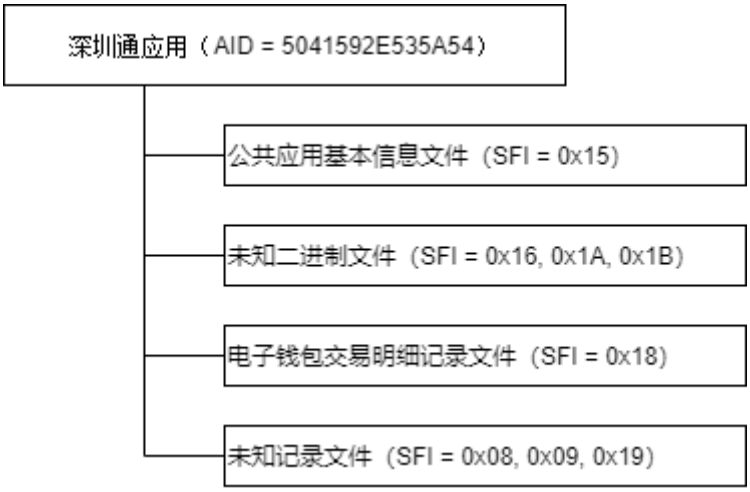
SFI	0x18			
文件类型	循环记录文件			
记录长度	0x17			
权限	读 =自由		写 =N/A	
字节	数据元	长度	格式	说明
01~ 02	电子钱包消费交易序号	2	HEX	
03~ 05	透支限额	3	HEX	
06~ 09	交易金额	4	HEX	
10	交易类型	1	HEX	0x06 表示消费, 0x09 表示复合消费
11~ 16	交易终端编号	6	BCD	
17~ 20	交易日期（YYYYMMDD）	4	BCD	
21~ 23	交易时间（HHMMSS）	3	BCD	

□□□

????Shenzhen Tong?

????

AID: 5041592E535A54



????

??????????

SFI	0x15			
□□□□	□□□□□			
□□□□	0x20			
□□	□ =□□		□ =SM	
□□	□□□	□□	□□	□□
01□ 16	□□	16	N/A	
17□ 20	□□	4	HEX	□□□
21□ 24	□□□□□□□ YYYYMMDD□	4	BCD	
25□ 28	□□□□□□□ YYYYMMDD□	4	BCD	

29~ 32	预留	4	HEX	

电子钱包交易明细记录文件

SFI	0x18			
文件类型	循环记录文件			
记录长度	0x17			
权限	读 =自由		写 =N/A	
字节	数据元	长度	格式	说明
01~ 02	电子钱包交易序号	2	HEX	
03~ 05	预留	3	HEX	
06~ 09	交易金额	4	HEX	
10	交易类型	1	HEX	0x09表示消费，0x02表示充值
11~ 16	交易终端编号	6	BCD	
17~ 20	交易日期（YYYYMMDD）	4	BCD	
21~ 23	交易时间（HHMMSS）	3	BCD	

□□□

???

System Code: 0x8008

□□□

EZ-Link

□□□

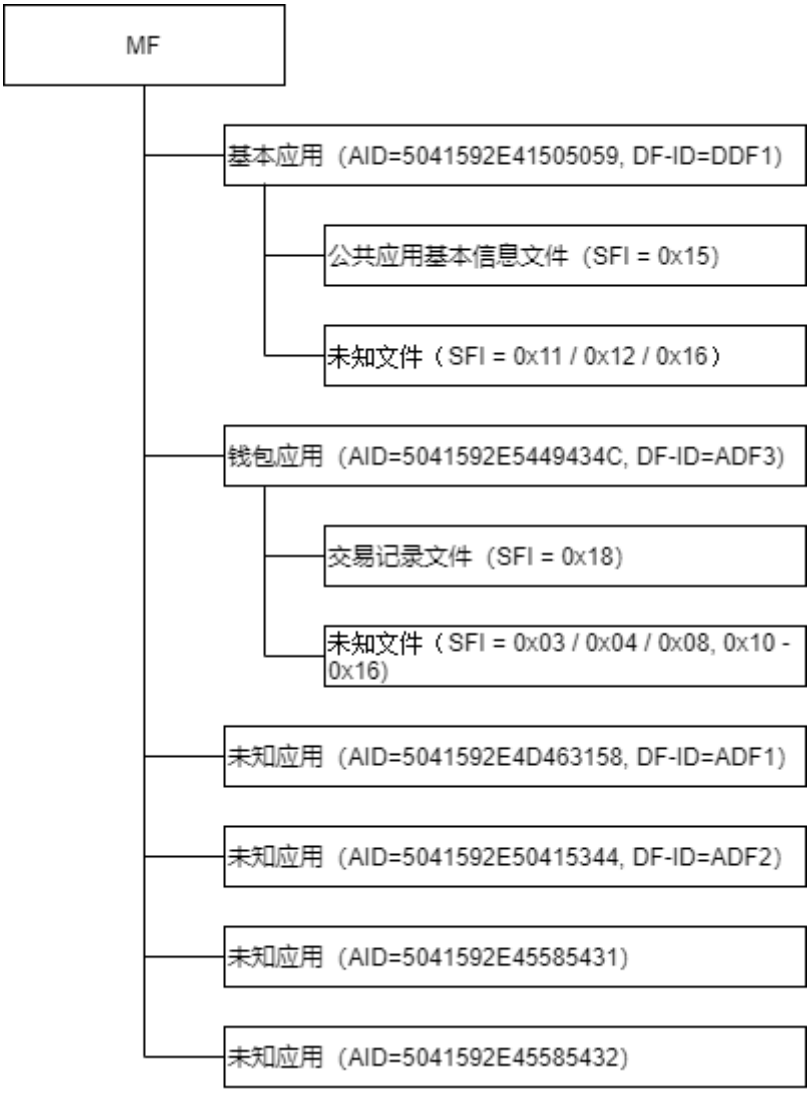
???

□□□

Oyster

□□□

????Lingnan Pass?



????

???????????DF-ID=DDF1?

SFI	0x15			
□□□□	□□□□□			
□□□□	0x58			
□□	□ =□□		□ =SM	
□□	□□□	□□	□□	□□

01～ 11	□□	11	N/A	
12～ 16	□□	5	BCD	
17～ 88	□□	62	N/A	

???

□□□

EMV

□□□

PBOC 2.0

??????

□□□□□□

??????

????

□□□□

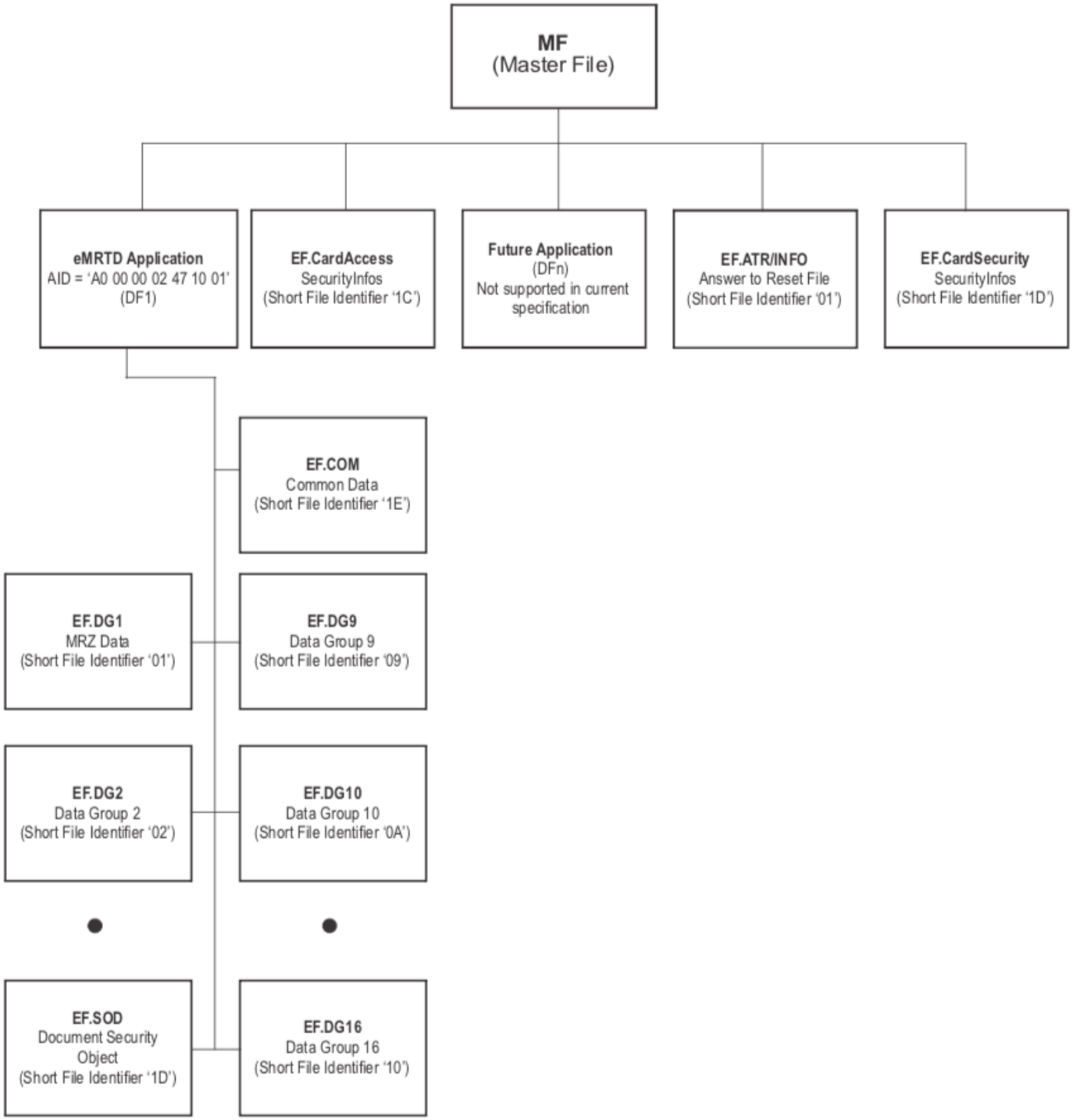
????

□□□□□□□□□□□□□□ ICAO□ Doc9303□□□□□□□□□□□□

https://www.icao.int/publications/pages/publication.aspx?docnum=9303

□□□□□□□□□□ Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)

????



????

Data Group	EF Name	Short File Identifier	FID	Tag
Common	EF.COM	1E	01 1E	60
DG1	EF.DG1	01	01 01	61
DG2	EF.DG2	02	01 02	75
DG3	EF.DG3	03	01 03	63
DG4	EF.DG4	04	01 04	76

DG5	EF.DG5	05	01 05	65
DG6	EF.DG6	06	01 06	66
DG7	EF.DG7	07	01 07	67
DG8	EF.DG8	08	01 08	68
DG9	EF.DG9	09	01 09	69
DG10	EF.DG10	0A	01 0A	6A
DG11	EF.DG11	0B	01 0B	6B
DG12	EF.DG12	0C	01 0C	6C
DG13	EF.DG13	0D	01 0D	6D
DG14	EF.DG14	0E	01 0E	6E
DG15	EF.DG15	0F	01 0F	6F
DG16	EF.DG16	10	01 10	70
Document Security Object	EF.SOD	1D	01 1D	77
Common	EF.CARDACCESS	1C	01 1C	
Common	EF.ATR/INFO			
Common	EF.CardSecurity	1D	01 1D	

身份文件

???????

中华人民共和国居民身份证是由公安机关签发的用于证明大陆居民身份的证件。二代居民身份证中增加了射频芯片，里面存储了包括照片在内的个人信息，用于机器读取。

????

二代证中存储的机读信息由行业标准 GA/T 490 规定，数据加密后存储在卡片中，读取时需用 SAM 解密。所用加密算法包括 SM1[1]。

卡片包括如下文件：

?????????256???

序号	数据项名称	字节数	标识符	说明
1	姓名	30	xm	
2	性别代码	2	xbdm	符合 GB/T 2261.1 的规定
3	民族代码	4	mzdm	符合 GB/T 3304 的规定
4	出生日期	16	csrq	年月日 YYYYMMDD
5	住址	70	dzmc	
6	公民身份号码	36	gmsfhm	符合 GB 11643 的规定
7	签发机关	30	qfjgmc	
8	有效期起始日期	16	yxqqsrq	居民身份证的有效期截止日期符合 GA/T 2000.16 的规定
9	有效期截止日期	16	yxqjzrq	居民身份证的有效期截止日期符合 GA/T 2000.16 的规定
10	预留区域	36		

?????????1024???

序号	数据项名称	字节数	标识符	说明
1	机读相片	1024	jdxp	以二进制数存储的 WLT 格式图片（参考发明专利 CN1779717A）

????????

序号	数据项名称	字节数	标识符	说明
1	指纹一_指纹特征数据	512	zwy_zwtzsj	第一枚指纹的指纹特征数据，以二进制数存储
2	指纹二_指纹特征数据	512	zwe_zwtzsj	第二枚指纹的指纹特征数据，以二进制数存储

????????

序号	数据项名称	字节数	标识符
1	机读追加住址1	70	jdzjzz1
2	机读追加住址2	70	jdzjzz2
3	机读追加住址3	70	jdzjzz3
4	机读追加住址4	70	jdzjzz4

???????

序号	数据项名称	字节数	标识符
1	居民身份证专用集成电路序列号	8	jmsfzzyjcdlxlh
2	居民身份证证卡序列号	16	jmsfzzkxlh

????

卡内射频芯片按照ISO14443-3 Type-B制式与读卡器通信。与一般CPU卡不同，二代证直接在ISO14443-3层收发APDU，不支持ISO14443-4。

命令	**CLA**	**INS**	**P1**	**P2**	**Lc**	**Data**	**Le**	**Response**
选择文件	00	A4	00	00	02	EF-ID	无	状态码
读二进制文件	80	B0	偏移量高位	偏移量低位	无	无	读取长度	内容+状态码
内部（卡片）认证	00	88	00	42	0A	10字节认证数据	无	8字节认证响应+状态码
外部（读卡器）认证	00	82	00	42	0A	10字节认证数据	无	状态码
获取随机数	00	84	00	00	无	无	08	8字节随机数+状态码

□□	CLA	INS	P1	P2	Lc	Data	Le	Response
□□□□□ □	00	36	00	00	□	□	08	8 □□□□□ +□□□

- [1]http://www.gov.cn/jrzg/2011-09/08/content_1942943.htm

??

其他

YubiKey

YubiKey 是 Yubico, Inc. 发行的，具有 OTP、TOTP、FIDO 2FA、静态密码、Challenge-Response、PIV、OpenPGP Card 等功能的便携密码学硬件。本文主要描述其智能卡相关功能，即 PIV 与 OpenPGP Card。

YubiKey Neo, YubiKey 5 NFC 具有 NFC 功能，其余的 YubiKey 均通过 USB 与主机进行通信。

详细的访问方式如下表所示：

功能	接口	**AID**
OTP/静态密码（NDEF）	USB-HID/NFC	D2 76 00 00 85 01 01
U2F	USB-HID/NFC	A0 00 00 06 47 2F 00 01
OpenPGP	USB-CCID/NFC	D2 76 00 01 24 01 02 00 00 00 00 00 00 01 00 00
PIV	USB-CCID/NFC	A0 00 00 03 08 00 00 10 00 01 00
TOTP(OATH)	USB-CCID/NFC	A0 00 00 05 27 21 01 01

FIDO U2F

□□

NXP JCOP Javacard

NXP JCOP □□ NXP □□□□□ Javacard □□□□□ NXP □□□ Javacard □□□□□□□□□□□□□□

□□□□□□□□□

J3 A 080 G dd(d) / T 0B rr ff o

- J = NXP JCOP
  - J5=NFC(S2C)
  - J3=Dual IF,CD=PKI+DES
  - J2=CT,CD=PKI+DES
  - J1=CT,DES

- A = JCOP version
  - A=JCOP 2.4.1 R3(Java Card 2.2.2 GP 2.1.1)
  - C=JCOP 2.4.2 R1
  - D=JCOP 2.4.2 R2(Java Card 3.0.1 GP 2.2.1)
  - E=JCOP 2.4.2 R3(Java Card 3.0.1 GP 2.2.1)
  - G=JCOP 3.0
  - H=JCOP3 P60-2
  - O=JCOP 4.0
  - Q=JCOP 4.2

- 080 = EEPROM Size 80K
- G = JCOP type
  - G=Java Std-Generic
  - V=Java Std-VISA
  - C=Java Std-Customized
  - M=Java Std-MasterCard
  - C=Java Static-Generic
  - U=Java Static-VISA
  - T=Java Static-MasterCard

- dd(d) = Delivery type
  - UA=sawn wafer 150u FFC
  - X0=PDM module
  - A4=MOB4
  - A6=MOB6
  - HN1=HVQFN32 package

- T = FAB ID
- 0B = HW Version

- rr = ROM code ID
- ff = FAB key ID
- o = Option
  - 0=no Mifare
  - 1=1k Mifare
  - 4=4k Mifare
  - 7=7k DESFire
  - 8=8k DESFire

□□□□□□□□□□ IDENTIFY □□□ 00A4040009A000000167413000FF00

□□□□□□□□□

Offset	Size	Name	Base mask value
0	1	FABKEY ID	xxh (customer dependent)
1	1	PATCH ID	xxh (see Patch ID in Administrator Manual)
2	1	TARGET ID	00h
3	1	MASK ID	33h (mask51)
4	4	CUSTOM MASK ID	00h 00h 00h 00h [1]
8	6	MASK NAME	NX011C
14	1	FUSE STATE	00h (not fused) or 01h (fused)
15	1	ROM INFO LENGTH	03h
16	3	ROM INFO[2]	J3A080 and J2A080: EDh 10h 3Ch J3A040 and J2A040: 23h B7h 16h

□□

Canokey

Canokey□□□□□□□□ USB□□□□□ 4□□□□ U2F/FIDO2□ HID□□ OpenPGP Card□ CCID□□ PIV+OATH□ CCID□□ WebUSB□

其他

MIFARE Classic

MIFARE Classic 有 1K 和 4K 两种类型，1k 和 4k 代表存储空间的大小。

在 MIFARE Classic 中，有 Sector 和 Block 的概念，每个 Sector 有若干个 Block，其中最后一个 Block 是特殊的（称为 Sector Trailer），保存了这个 Sector 的一些信息：Key A、Access Bits、GPB 和 Key B。对于 Classic 4K，首先是 32 个有 4 blocks 的 sector，然后是 8 个有 16 blocks 的 sector，整体的内存布局大概是：

```
Sector 0:
□Block 0
□Block 1
□Block 2
□Block 3(Sector Trailer)
Sector 1:
□Block 4
□Block 5
□Block 6
□Block 7(Sector Trailer)
...
Sector 32:
□Block 128
□Block 129
□...
□Block 143(Sector Trailer)
...
Sector 39:
□...
```

每个 Block 有 16 字节，一共 256 个 block，所以是 4K 大小的存储空间。Block 0 比较特殊，保存的是生产商写入的信息，不可更改（特殊的卡除外）。

见 MIFARE Classic 配置 NDEF

?????

□□	□□□□	□□□□	□□□□	□□□□ 2	NFC Forum
MIFARE Classic	ISO 14443-2 Type A	ISO 14443-3 Type A			Type 2
MIFARE Plus EV1	ISO 14443-2 Type A	ISO 14443-3 Type A	ISO 14443-4 Type A	ISO 7816-4	Type 4
MIFARE Plus X/SE	ISO 14443-2 Type A	ISO 14443-3 Type A	ISO 14443-4 Type A		?
MIFARE Ultralight	ISO 14443-2 Type A	ISO 14443-3 Type A			Type 2
MIFARE DESFire	ISO 14443-2 Type A	ISO 14443-3 Type A	ISO 14443-4 Type A	ISO 7816-4	Type 4
FeliCa	ISO 18092	ISO 18092	ISO 18092	JIS X 6219-4	Type 3
NTAG 213/215/216	ISO 14443-2 Type A	ISO 14443-3 Type A			Type 2
ICODE SLIX	ISO 15693-2	ISO 15693-3			Type 5

Note:

1. MIFARE Classic 4k □□□□□□ MF1 S70

2. MIFARE □□□□□□□□□□

3. Type 2 tag spec