辽阳公交一卡通系统
POS 机代理充值
报文规范

（V1.5）

北京瑞华通科技有限公司

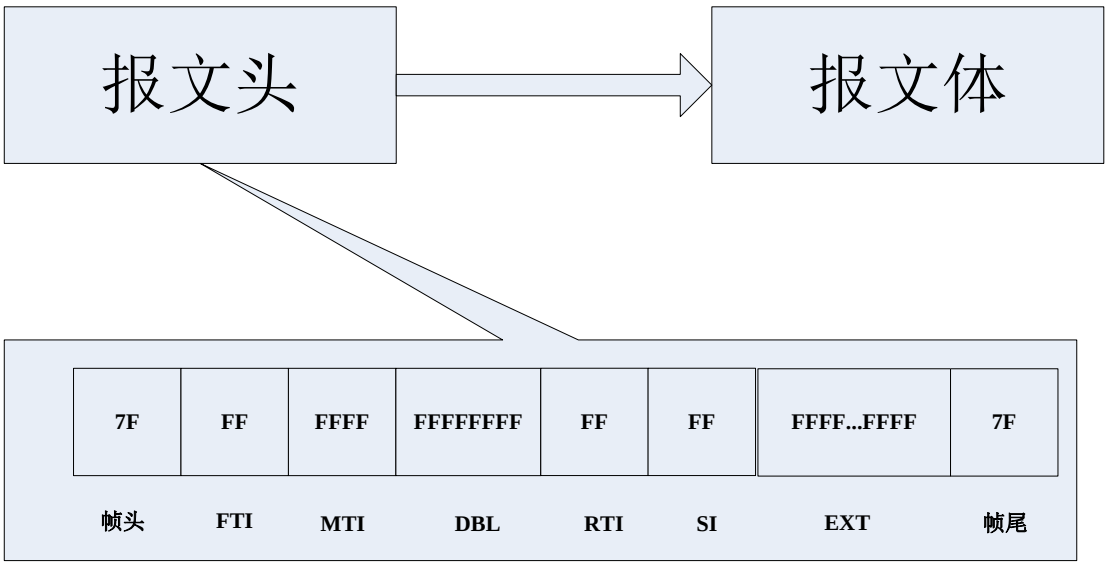
2017 年 9 月

目 录

1. 通讯报文格式要求

本通讯报文规范是基于 TCP/IP 通讯协议而设计，支持二进制字节流。采用统一的报文头识别方式进行处理。

完整的报文一般如下图所示：



报文由报文头和报文体组成。报文头由帧头（7F），帧尾（7F），FTI，MTI，DBL，RTI，SI,EXT 组成。长度固定是 17+N 个字节。

对于帧头和帧尾之间的字节在编码和解码的时候需要转义，转义规则如下：

编码：做 0x7E+value^0x20 即 0x7E –> 0x7E + 0x5E ,0x7F -> 0x7E + 0x5F,一个字节变两个字节

解码：将 0x7E 紧跟的后一字节做：value^0x20 还原，0x7E 丢弃，两个字节变一个字节

报文头帧内说明如下：

域	名称	字节数	说明
FTI	格式类型标识 (Format Type Identifier)	1	‘B’（0x42）：Binary 报文，
MTI	消息类型标识 (Message Type Identifier)	2	二进制报文自定义 MTI，范围：[0x1000 – 0xEFFF]
DBL	报文体长度 (Datagram Body Length)	4	无符号整数 INT32，二进制报文固定为 0
RTI	请求类型标识 (Request Type Identifier)	1	‘R’（0x52）：请求（Request） ‘A’（0x41）：回应（Answer）
SI	状态标识 (State Identifier)	1	0x00：正常处理， 0x01：捕获未处理异常， 0x02：未能支持的报文 0x03：CRC 校验错误
EXT	扩展	8 +N	默认，全 0，用于二进制报文扩展应用

二进制报文 EXT 扩展域定义如下：

扩展域	名称	字节数	说明
LEN	数据域长度	2	二进制报文的长度
SW	是否校验	1	0：表示不校验，1：表示校验
CRC	CRC16 校验	4	二进制数据域的 CRC 校验，默认：0
RESERVE	保留	1	默认：0
DATA	数据域	N	

2. POS 机代理充值报文定义

2.1 报文定义

2.1.1 初始化 POS(B000)

域编号	格式	字节	存放内容	说明
MTI	HEX	2	报文标识	B000
Request				
1	BCD	4	操作员编号	操作员的唯一编号，通过设置
2	HEX	16	验证码	
3	BCD	6	终端机编号	后台系统分配，设置到 POS 机
合计		26		
Response				
1	BCD	7	后台时间	格式：yyyyMMddHHmmss，POS 时钟同步
2	HEX	2	响应结果	采用统一结果编码，请看响应结果编码表
合计		9		

2.1.2 会话连接(B001)

域编号	格式	字节	存放内容	说明
MTI	HEX	2	报文标识	B001
Request				
1	BCD	4	操作员编号	操作员的唯一编号，通过设置
2	HEX	16	验证码	访问密码 (MD5 加密)
3	BCD	6	终端机编号	
合计		26		
Response				
1	BCD	7	后台时间	格式：yyyyMMddHHmmss，POS 时钟同步
2	BCD	4	最新黑名单	无符合整数，后台最新黑名单版本号
3	BCD	4	会话码	本次连接的唯一标识
4	HEX	2	响应结果	采用统一结果编码，请看响应结果编码表
合计		17		

此会话请求是请求其他功能的前提，请求成功后需要保持连接，断开后需要重新发送此报文，后台才会接受下面的报文请求处理。

2.1.3 检查用户卡状态(B002)

域编号	格式	字节	存放内容	说明
MTI	HEX	2	报文标识	B002
Request				
1	BCD	4	会话码	
2	BCD	4	操作员编号	操作员的唯一编号，通过设置
3	BCD	6	终端机编号	
4	BCD	5	卡物理号	
5	BCD	4	卡应用序列号	发行流水号
合计		**23**		
Response				
1	BCD	1	卡账户状态	0：未启用，1：启用　2：黑卡，　3 .无卡销卡，　4.有卡销卡
2	HEX	2	响应结果	采用统一结果编码，请看响应结果编码表
合计		**3**		

2.1.4 M1 卡充值(B003)

域编号	格式	字节	存放内容	说明
MTI	HEX	2	报文标识	B003
Request				
1	BCD	4	会话码	
2	BCD	4	操作员编号	操作员的唯一编号，通过设置
3	BCD	2	城市代码	用户卡中的城市代码
4	BCD	5	用户卡号	
5	BCD	4	卡应用序列号	发行流水号
6	BCD	1	卡应用类型	
7	HEX	4	交易金额	单位为“分”，1.00 元表示为：00000064
8	BCD	2	充值交易计数器	
9	BCD	1	交易类型	02：充值
10	BCD	6	终端机编号	
11	BCD	7	交易日期时间	格式：yyyyMMddHHmmss
12	HEX	4	卡片交易前余额	单位为“分”，1.00 元表示为：00000064
合计		**44**		
Response				
1	HEX	2	响应结果	采用统一结果编码，请看响应结果编码表
合计		**2**		

2.1.5 获取代理充值总笔数和总金额(B006)

域编号	格式	字节	存放内容	说明
MTI	HEX	2	报文标识	B006
Request				
1	BCD	4	会话码	
2	BCD	4	操作员编号	
3	BCD	6	终端机编号	
4	BCD	4	开始日期	格式：yyyyMMdd
5	BCD	4	结束日期	格式：yyyyMMdd
合计		22		
Response				
1	HEX	4	总笔数	单位为“分”，1.00 元表示为：00000064
2	HEX	4	总金额	单位为“分”，1.00 元表示为：00000064
3	HEX	2	响应结果	采用统一结果编码，请看响应结果编码表
合计		10		

2.1.6 POS 充值申请（B040）

本报文适用代理充值 POS，适用交通部互联互通卡充值

域编号	格式	字节	存放内容	说明
MTI	HEX	2	报文标识	B040
Request				
1	INT	4	会话码	
2	BCD	2	城市代码	用户卡 17H 文件中的城市代码
3	HEX	10	卡应用序列号	用户卡 15H 文件读取，后 8 字节参与密钥分散
4	HEX	1	卡类型	用户卡 17H 文件中的卡类型
5	INT	4	交易金额	单位为“分”，1.00 元表示为：00000064
6	HEX	1	交易类型	02：充值
7	HEX	6	终端机编号	PSAM 卡 16H 文件中读取或后台指定终端机编号
8	INT	2	卡交易序号	CPU 卡产生
9	BCD	7	交易日期时间	格式：yyyyMMddHHmmss
10	INT	4	卡片交易前余额	单位为“分”
11	INT	4	卡随机数	CPU 卡内产生
12	HEX	4	MAC1	
合计		49		
Response				
1	HEX	4	MAC2	
2	INT	4	终端交易序号	

域编号	格式	字节	存放内容	说明
3	HEX	2	响应结果	采用统一结果编码，请看响应结果编码表
合计		**10**		

2.1.7 POS 充值提交（B041）

本报文适用代理充值 POS，适用交通部互联互通卡充值

域编号	格式	字节	存放内容	说明
MTI	HEX	2	报文标识	B041
Request				
1	INT	4	会话码	
2	HEX	10	卡应用序列号	用户卡 15H 文件读取，后 8 字节参与密钥分散
3	HEX	6	终端机编号	PSAM 卡 16H 文件中读取或后台指定终端机编号
4	INT	4	终端交易序号	POS 充值申请报文返回
5	INT	2	卡交易序号	CPU 卡产生
6	BCD	7	交易日期时间	格式：yyyyMMddHHmmss
7	INT	4	交易金额	单位为“分”，1.00 元表示为：00000064
8	HEX	1	写卡状态	00：成功，01 表示失败
9	HEX	4	交易验证码	交易 TAC
合计		**42**		
Response				
1	HEX	2	响应结果	采用统一结果编码，请看响应结果编码表
合计		**2**		

3. 统一结果响应编码

正常：

E000: 正确，正常，有效

异常 ：

E001：操作员不存在
E002：操作员未启用
E003：验证码错误
E004：终端机编号不存在
E005：终端机编号未注册
E006：终端机编号已使用
E007：会话码错误
E008：访问拒绝（未登录验证）
E009：充值信誉额度不足

E010：充值额度超过上限
E011：操作员没有充值权限
E012：卡状态异常
E013：M1 卡充值失败
E014：不存在最后一笔充值记录
E015：M1 卡取消充值失败
E016：POS 机充值请求失败
E017：POS 机充值提交失败
E018：POS 机充值写卡失败，删除灰记录失败
E020：密钥索引不存在
E021：计算 MAC1 失败
E022：计算 MAC2 失败
E0FF：系统未知异常

4. POS 机充值流程

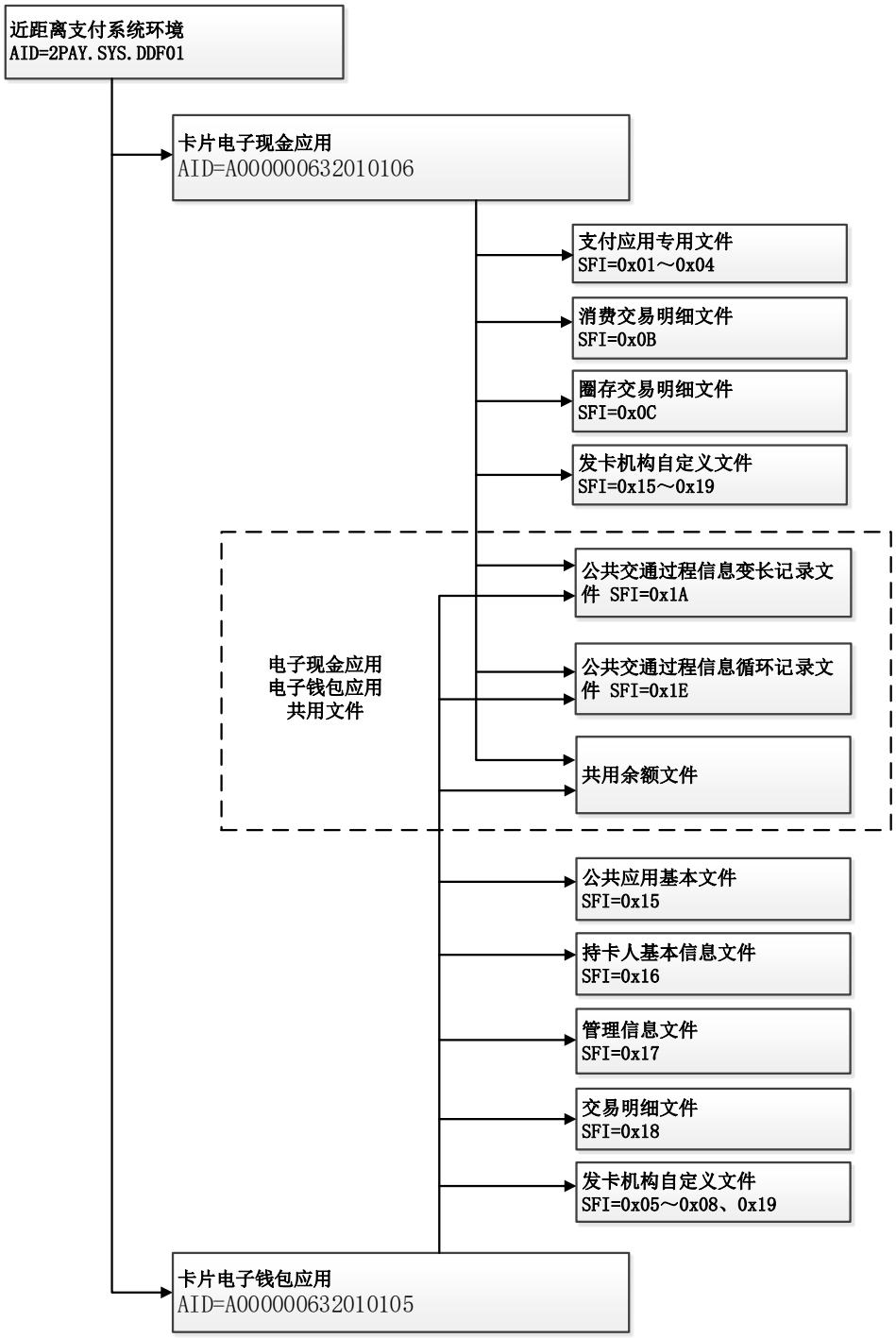
可充值卡类型：普通消费卡 00，学生优惠卡 02，学生卡 03，老人优惠卡 05

步骤	指令	备注
1	M1 卡寻卡	
2	读发行区块 4，获取城市代码+发行流水号+认证码+启用标志+卡类型	1 扇区认证需要读 CSN，keyA=CSN+CSN 前 4 位
3	读 5 块的发行日期+有效日期+启用日期+钱包启用标识	
4	ISAM 卡上电复位	
5	00A4000002 1002	选择 ISAM 卡目录
6	801A080000	ISAM 卡初始化
7	80FA000008 + csn + sn + mac 高字节 + secter Csn：卡物理号，SN：发行流水号，secter：扇区号	计算充值 KeyB

5. 卡片结构

2.1 用户卡

用户卡包括：普通卡、老年卡、员工卡等全部消费卡。



用户卡的基本文件结构图

(1) 公共应用信息文件

文件标识（SFI）	0x15			
文件类型	二进制文件			
文件大小	30			
文件存取控制	读 = 自由	改写 = 应用维护密钥计算MAC		
字节	数据元	长度（字节）	格式	值
01～08	发卡机构标识（中交金卡分	8	HEX	组成方式如下

	配）			00010001+FFFFFFFF
09～09	应用类型标识 01：只有ED 02：只有EP 03：ED和EP都存在 说明：ED（电子存折），EP（电子钱包）	1	BCD	当前为02
10～10	发卡机构应用版本	1	BCD	00：初始值 01：已启用 与08的启用标识同步
11～20	应用序列号 规则：19位卡账号，左补0，后8字节参与密钥分散	10	HEX	0+6 位 IIN+2 位扩展+11 位自定义
21～24	应用启用日期（YYYYMMDD）	4	BCD	与电子现金08文件数据同步
25～28	应用有效日期（YYYYMMDD）	4	BCD	与电子现金08文件数据同步
29～30	发卡机构自定义FCI数据	2	HEX	

(2) 持卡人基本信息文件

文件标识（SFI）	0x16			
文件类型	二进制文件			
文件大小	55			
文件存取控制	读 = 自由	改写 = 应用维护密钥计算MAC		
字节	数据元	长度（字节）	格式	值
01～01	卡类型标识	1	BCD	00：个人卡 10：单位卡
02～02	本行职工标识	1	BCD	
03～22	持卡人姓名	20	GB2312，右补空格	
23～54	持卡人证件号码	32	ASCII，右补空格	
55～55	持卡人证件类型	1	HEX	00：身份证 01：军官证 02：护照 03：入境证 04：临时身份证 05：其他

(3) 管理信息文件

文件标识（SFI）	0x17			
文件类型	二进制文件			
文件大小	60			
文件存取控制	读 = 自由	改写 = 应用维护密钥计算MAC		
字节	数据元	长度	格式	值
01～04	国际代码	4	BCD	00000156

05～06	省级代码	2	HEX	《全国清算中心代码》(GB 13497-92)省级代码
07～08	城市代码	2	HEX	《全国清算中心代码》(GB 13497-92)城市代码
09～10	互通卡种	2	HEX	与电子现金 08 文件数据同步 0000：非互通卡 0001：互通卡
11～11	卡种类型	1	HEX	与电子现金 08 文件数据同步，包括且不限于如下类型： 01：普通卡 02：学生卡 03：老人卡 04：夕阳红卡 05：稽查证卡 06：成人卡 07：军人卡 08：伤残卡 09：退休干部卡 10：特殊卡 11：教师卡 21：员工卡 具体详见 3.4 附录一
12～60	预留	49	HEX	

(4) 交易明细文件

这个文件必须能够容纳至少十条消费、取款、圈存、圈提交易记录。

文件标识（SFI）	0x18		
文件类型	循环记录文件		
记录长度	10×23		
文件存取控制	读 = 自由	改写 = COS内部操作	
字节	数据元	长度	格式
01～02	EP联机或脱机交易序号	2	HEX
03～05	透支限额	3	HEX
06～09	交易金额	4	HEX
10～10	交易类型标识	1	BCD
11～16	终端机编号	6	HEX
17～20	交易日期（终端，格式：YYYYMMDD）	4	BCD
21～23	交易时间（终端，格式：HHMMSS）	3	BCD

注 1：交易类型为 06 表示消费，09 表示复合消费，02 表示充值。

注 2：此数据由 cos 内部维护。若 18 文件为空，在卡片首次充值交易后应在 18 文件中也

写入一条充值交易记录。

(5) 公共交通过程信息变长记录文件

文件标识（SFI）	0x1A		
文件类型	变长记录文件		
记录长度	2190		
文件存取控制	读 = 自由	改写 = 应用维护密钥计算MAC	
记录号	记录描述	长度(bytes)	备注
1	城市轨道应用信息记录	128	
2	公共汽电车应用信息记录	128	
3	城市水上客运应用信息记录	128	
4	出租汽车应用信息记录	128	
5	租赁汽车应用信息记录	128	
6	公共自行车应用信息记录	128	
7	停车收费应用信息记录	112	
8	长途客运应用信息记录	128	
9	轮渡应用信息记录	128	
10	城际铁路应用信息记录	128	
11	民航应用信息记录	128	
12	高速公路收费应用信息记录	128	
13	优惠信息记录	30	
14	本规范预留记录 1	128	
15	本规范预留记录 2	128	
16	本规范预留记录 3	128	
17	本规范预留记录 4	128	
18	本规范预留记录 5	128	

(6) 公共交通过程信息循环记录文件

文件标识（SFI）	0x1E		
文件类型	循环记录文件		
记录长度	48*30		
文件存取控制	读 = 自由	改写 = 应用维护密钥计算MAC	
字节	数据元	长度（字节）	数据格式
1	交易类型	1	BCD
2～9	终端编号	8	BCD
10～17	交易流水号	8	BCD
18～21	交易金额	4	HEX(高字节在前)
22～25	交易后余额	4	HEX(高字节在前)
26～32	交易日期时间	7	YYYYMMDDhhmmss
33～34	受理方城市代码	2	BCD
35～42	受理方机构标识	8	BCD

43～48	本规范预留	6	初始为 00

6. 终端交易流程

2.1 POS 代理充值流程

1、 调用会话连接报文

2、 卡片上电

3、 选择 MF 应用，命令：00A404000E 325041592E5359532E4444463031

4、 选择钱包应用，命令：00A4040008 A000000632010105

5、 读取 15H 文件，命令：00B0950A0A，根据返回数据截取相应卡应用序列号，后 8 字节为卡应用序列号

6、 读取卡钱包余额，命令：805C000204，返回数据为 4 字节余额，需要将返回的十六进制余额转换为十进制数，十进制余额/100 可以换算成“元”显示

7、 校验卡 PIN，命令：0020000003 123456

8、 圈存初始化，命令：805000020B[1 字节密钥索引][4 节交易金额][6 字节终端机号][0x10]
返回数据依次是：4 字节旧余额，2 字节卡联机交易序号，1 字节密钥版本，1 字节算法标识，4 字节随机数，4 字节 MAC1

9、 用圈存初始化的返回数据调用“POS 充值申请”接口，获得 MAC2

10、 圈存，8052000000B[7 字节交易日期时间][4 字节 MAC2][0x04]
返回数据是：4 字节交易 TAC

11、 调用“POS 充值提交”接口

2.1 充值防拔流程

防拔处理：防拔功能用于保证卡片在交易处理的任何情况下，甚至是在更新 EEPROM 过程中掉电的情况下，仍能保持数据的完整性。 在终端发给 IC 卡一个命令以更新 ED 或 EP 余额时，卡片总会回送一个报文鉴别代码 MAC 或交易验证码 TAC，以证明更新已经发生。一旦余额更新成功，可以通过 GET TRANSACTION PROVE 命令获得此 MAC 或 TAC。 若在命令已执行完毕，而终端未收到响应之前，卡片突然拔出，终端将会处于不知卡片是否

更新的不定状态。这种情况下，终端可以用 GET TRANSACTION PROVE 命令进行恢复。首先，终端提醒持卡人重新插入卡片，通过检查发卡方标识和应用序列号以确认插入的卡片与前面拔出的卡片是否为同一张卡片，如果是同一张卡片，终端发出 GET TRANSACTION PROVE 命令取回 MAC 或/和 TAC。如果返回'9000'，取回 MAC 或/和 TAC，终端即完成交易处理，如果不返回'9000'则表示卡内余额没被修改，交易需从初始化命令重新开始。

命令：805A000102 +"要取的 MAC 或 TAC 所对应的 ED/EP 联机或脱机交易序号 "+ 08

返回数据是：4 字节全 0 + 4 字节交易 TAC

说明：要取的 MAC 或 TAC 所对应的 ED/EP 联机或脱机交易序号是圈存初始化时 2 字节卡联机交易序号加 1（2 字节十六进制）

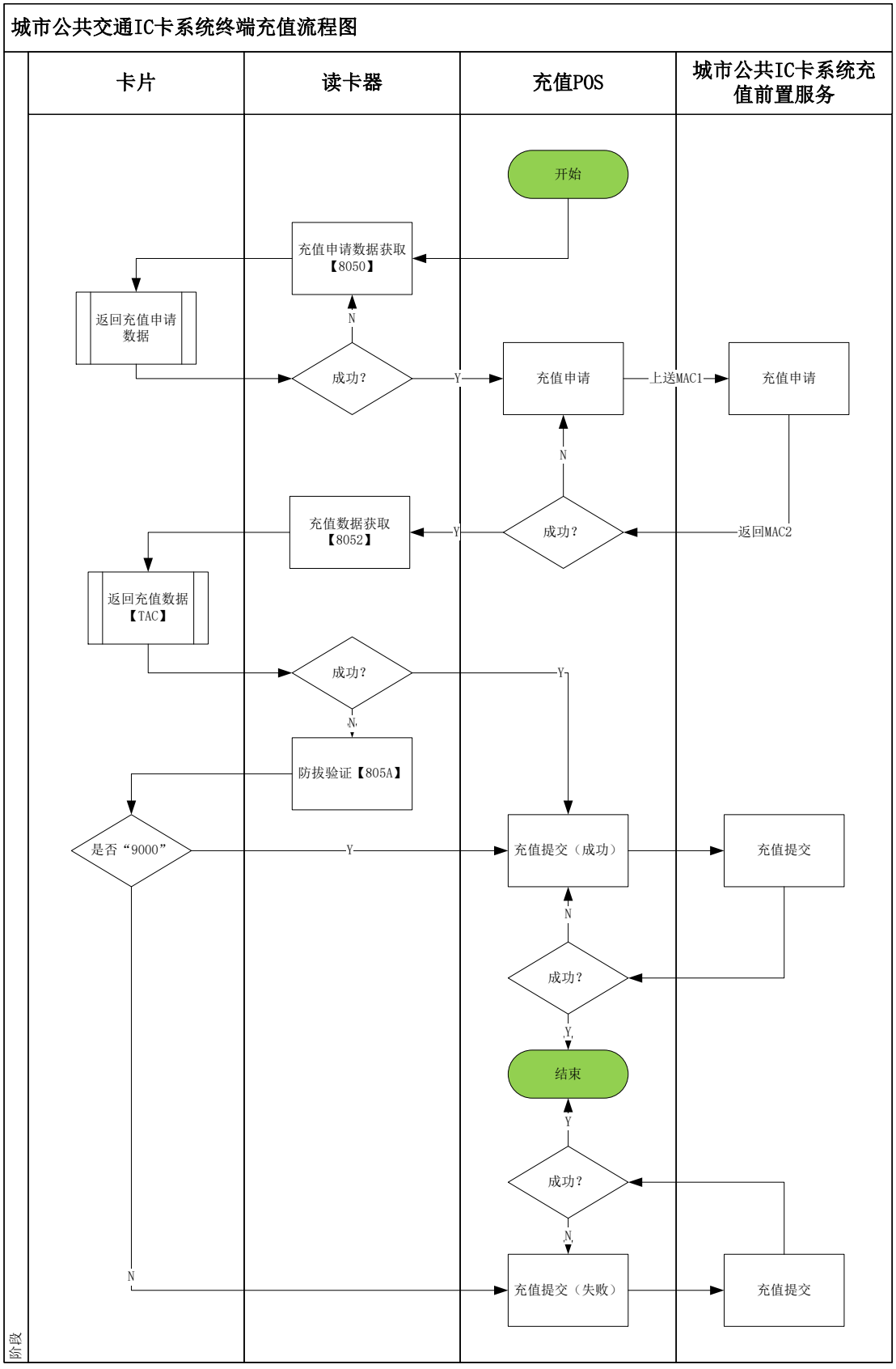
如命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

响应报文状态码如图 5-89 所示。

返回错误码	解　释
6E00	CLA 不正确
6581	内存失败
6985	使用的条件不满足
9406	所需 MAC 不可用
9303	应用已被永久锁定
6A81	功能不支持（卡片或应用被锁定）
6901	命令不接受（无效状态）

图 5-89 取交易认证码状态码

2.1 充值流程图


城市公共交通IC卡系统终端充值流程图
卡片
读卡器
充值POS
城市公共IC卡系统充值前置服务
开始
充值申请数据获取【8050】
返回充值申请数据
N
成功？
Y
充值申请
上送MAC1
充值申请
N
充值数据获取【8052】
Y
成功？
返回MAC2
返回充值数据【TAC】
成功？
Y
N
防拔验证【805A】
是否“9000”
Y
充值提交（成功）
充值提交
N
成功？
Y
结束
Y
成功？
N
N
充值提交（失败）
充值提交
阶段

附录一

字段名	编码规则
卡种类型	01H：普通卡 02H：学生卡 03H：老人卡 04H：夕阳红卡 05H：稽查证卡 06H：成人卡 07H：军人卡 08H：伤残卡 09H：退休干部卡 10H：特殊卡 11H：教师卡 21H：员工卡 51H：司机卡 52H：线路卡 53H：采集卡
交易类型标志	02H：圈存 03H：圈提 06H：消费 07H：修改透支限额； 09H：复合应用消费。
分段标识	00H：不分段 01H：规则分段 02H：不规则分段
行车方向	00H：上行 01H：下行