

中华人民共和国交通运输部

城市公共交通 IC 卡卡片技术规范 (试行)

中华人民共和国交通运输部 发布

目 次

前言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	2
4 符号和缩略语	4
5 文件、数据元、数据对象列表	6
5.1 文件	6
5.2 数据元	9
5.3 电子现金数据对象列表	10
6 通用卡片技术要求	10
6.1 功能要求	10
6.2 命令要求	12
7 电子现金卡片技术要求	13
7.1 卡片通用要求	13
7.2 应用选择要求	14
7.3 卡片初始应用处理要求	15
7.4 交易时间	15
8 电子钱包卡片技术要求	16
8.1 卡片通用要求	16
8.2 应用选择要求	16
8.3 交易时间	18
9 电子现金双币应用（可选）	18
9.1 基于城市公共交通 IC 卡应用的电子现金双币应用	18
9.2 支持电子现金双币应用的分时分段扣费流程	20
9.3 基于城市公共交通 IC 卡应用的电子现金双币应用	21
附录 A（规范性附录） 应用指令	23
附录 B（规范性附录） 电子现金扩展应用文件短文件标识符定义	73
附录 C（规范性附录） 卡片与发卡机构数据元	74
附录 D（规范性附录） 应用数据与文件	99
附录 E（资料性附录） 交易应用举例	131
附录 F（规范性附录） 电子现金支持的密文版本	142
附录 G（规范性附录） 算法标识	143
附录 H（资料性附录） 行业应用开通指南	144

目次

附录 I（规范性附录）	电子现金快速 DDA（fDDA）	145
-------------	------------------------	-----

前 言

城市公共交通IC卡系列技术规范由5个规范组成：

- 《城市公共交通IC卡卡片技术规范》；
- 《城市公共交通IC卡读写终端技术规范》；
- 《城市公共交通IC卡信息接口技术规范》；
- 《城市公共交通IC卡非接触接口通讯技术规范》；
- 《城市公共交通IC卡安全技术规范》。

本规范由中华人民共和国交通运输部提出。

本规范主要起草单位：

本规范主要起草人：

本规范为首次发布。

城市公共交通 IC 卡卡片技术规范

1 范围

本规范对应用于道路运输领域基于智能卡支付应用做出了相关要求和规定，主要应用于公共电汽车、出租车、轨道交通、停车场、城际客运、城际铁路、轮渡等应用场景，支持包括圈存、标准快速支付、分时分段扣费、脱机预授权、单次扣款优惠等交易。

本规范适用于开展基于城市公共交通IC卡应用的地区、发卡机构以及收单机构。其使用对象主要是与城市公共交通IC卡应用相关的卡片设计、制造、管理、发行、受理以及应用系统的研制、开发、集成和维护等相关部门（单位）。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 2659 世界各国和地区名称代码(GB/T 2659—2000)

GB/T 4880.1 语种名称代码 第1部分:2字母代码(GB/T 4880.1—2005)

GB/T 12406 表示货币和资金的代码(GB/T 12406—2008)

GB/T 15150 产生报文的银行卡 交换报文规范 金融交易内容(GB/T 15150—1994)

GB/T 16649.4 识别卡 带触点的集成电路卡 第4部分：用于交换的结构、安全和命令（GB/T 16649.4—2010）

GB/T 16649.5 识别卡 带触点的集成电路卡 第5部分：应用标识符的编号系统和注册程序(GB/T 16649.5—2002)

GB/T 16649.6 识别卡 带触点的集成电路卡 第6部分：行业间数据元（GB/T 16649.6—2001）

GB/T 21078.1 银行业务 个人识别码的管理与安全 第1部分:ATM和POS系统中联机PIN处理的基本原则和要求(GB/T 21078.1—2007)

GB/T 17552 识别卡 金融交易卡(GB/T 17552—1998)

GB/T 15273 信息处理八位单字节编码图形字符集

JR/T 0025.4 中国金融集成电路（IC）卡规范 第4部分： 借记/贷记应用规范

JR/T 0025.5 中国金融集成电路（IC）卡规范 第5部分： 借记/贷记应用卡片规范

JR/T 0025.7 中国金融集成电路（IC）卡规范 第7部分： 借记/贷记应用安全规范

JR/T 0025.12 中国金融集成电路（IC）卡规范 第12部分：非接触式IC卡支付规范

JR/T 0025.13 中国金融集成电路（IC）卡规范 第13部分：基于借记贷记应用的小额支付规范

JR/T 0025.14 中国金融集成电路（IC）卡规范 第14部分：非接触式IC卡小额支付扩展应用规范

JR/T 0025.15 中国金融集成电路（IC）卡规范 第15部分：电子现金双币支付应用规范

JR/T 0025.17 中国金融集成电路（IC）卡规范 第17部分：借记/贷记应用安全增强规范

3 术语和定义

下列术语和定义适用于本规范。

3.1

应用 application

卡片和终端之间的应用协议和相关的数据集。

3.2

CAPP 记录 CAPP records

扩展应用专用文件的记录，包括扩展应用循环记录文件和扩展应用专用文件的记录。

3.3

命令 command

终端向城市公共交通IC卡发出的一条报文，该报文启动一个操作或请求一个响应。

3.4

复合应用 complex application

结合电子钱包应用和其它应用的应用模式。

3.5

扩展应用专用文件 comprehensive application specified file

扩展应用专用文件用于存储特定的行业应用信息，通常情况下是变长记录结构文件。

3.6

中国余数定理私钥模式 CRT

中国余数定理又称孙子定理，是中国古代求解一次同余式组的方法，对于提高RSA算法的模幂运算效率作用显著。

3.7

扩展应用循环记录文件 comprehensive application cyclic file

扩展应用循环记录文件作为一些日志类的数据记录存储，是循环记录结构文件。每次交易，UPDATE CAPP DATACACHE命令只更新第一条记录。

3.8

密文 cryptogram

密码加密运算的结果。

3.9

电子现金 (EC) electronic cash (EC)

基于城市公共交通IC卡应用上实现的小额支付功能。

3.10

电子现金余额 electronic cash balance

一个计数器，表示卡片上可脱机消费的金额。该计数器的值与电子钱包余额保持一致。

3.11

电子现金余额上限 electronic cash funds limit

持卡人可用来脱机消费的最大金额。

3.12

电子钱包（EP） electronic purse

一种为方便持卡人小额消费而设计的金融IC卡应用。它支持圈存、消费等交易。

3.13

电子钱包余额 electronic purse balance

一个计数器，表示卡片上可脱机消费的金额。该计数器的值与电子现金余额保持一致。

3.14

押金抵扣 deposit deduction

押金抵扣是指发卡机构可以给予持卡人一定的押金额度，该金额不计入电子现金的实际金额，但是当持卡人卡片内电子现金余额不足且小于押金额度时，持卡人可以选择使用押金来完成交易。

3.15

ID 号 identify number

用于区分同一行业在不同地区的应用。

3.16

集成电路（IC） integrated circuit (IC)

具有处理和/或存储功能的电子器件。

3.17

发卡机构行为代码 issuer action code

发卡机构根据TVR的内容选择的动作。

3.18

圈存 load

增加卡中电子现金/电子钱包余额的过程, 圈存后的电子现金余额不能超过电子现金/电子钱包余额上限。

3.19

支付系统环境 payment system environment

当符合本规范的支付系统应用被选择，或者用于支付系统应用目的的目录定义文件（DDF）被选择后，城市公共交通IC卡中所确立的逻辑条件集合。

3. 20

近距离支付系统环境 proximity payment systems environment

支持的应用标识、应用标签和应用优先指示器的一个列表，可以通过非接触界面访问。该列表包括所有目录的入口，由卡片在SELECT PPSE（“2PAY.SYS.DDF01”）响应的FCI中返回。

3. 21

响应 response

城市公共交通IC卡处理完收到的命令报文后，返回给终端的报文。

3. 22

脱机预授权交易 offline pre-authorization

脱机预授权交易是指受理方将预估的消费金额置入交易命令中发送给卡片，卡片通过风险控制和额度检查，批准交易，并冻结卡内对应电子现金额度。

3. 23

脱机预授权完成交易 offline pre-authorization completion

脱机预授权完成交易是指受理方在预授权有效期内以发送交易命令发送给卡片，卡片通过风险控制和额度检查，批准交易，并返还卡内对应的电子现金额度。

3. 24

分段扣费 section purchase

分段扣费是在原来的标准城市公共交通IC卡应用交易流程的基础上，在GPO命令处理和READ RECORD命令处理之间，增加了更新扩展应用数据的UPDATE CAPP DATA CACHE命令。以满足脱机小额快速支付应用中可能遇到的分时、分段计费的需求。

3. 25

交易终止 transaction terminated

规范规定的流程被执行完毕，但卡片、终端或发卡机构出于某些因素的考虑（包括但不限于风险管理、业务规则、政策因素）不允许该笔交易的发生。

3. 26

交易拒绝 transaction declined

规范规定的流程被执行完毕，但卡片、终端或发卡机构处于某些因素的考虑（包括但不限于风险管理、业务规则、政策因素）不允许该笔交易的发生。

3. 27

圈提 unload

持卡人将电子钱包中的全部资金提取。圈提交易必须在特定的终端上联机进行。

4 符号和缩略语

下列符号和缩略语表示适用于本文件。

AAC	应用认证密文 (Application Authentication Cryptogram)
AC	应用密文 (Application Cryptogram)
ADA	应用缺省行为 (Application Default Action)
ADF	应用定义文件 (Application Definition File)
AEF	应用基本文件 (Application Elementary File)
AFL	应用文件定位器 (Application File Locator)
AID	应用标识符 (Application Identifier)
ARPC	授权响应密文 (Authorization Response Cryptogram)
ARQC	授权请求密文 (Authorization Request Cryptogram)
ATC	应用交易计数器 (Application Transaction Counter)
APDU	应用协议数据单元 (Application Protocol Data Unit)
ATC	应用交易计数器 (Application Transaction Counter)
AUC	应用用途控制 (Application Usage Control)
BER	基本编码规则 (Basic Encoding Rules)
C	条件 (Condition)
CAPP	扩展应用 (Comprehensive Application) / 复合应用 (Complex Application)
CAM	卡片认证方法 (Card Authentication Method)
CDA	复合动态数据认证/应用密文生成 (Combined DDA/AC Generation)
CDOL	卡片风险管理数据对象列表 (Card Risk Management Data Object List)
CLA	命令报文的类别字节 (Class Byte of the Command Message)
CID	密文信息数据 (Cryptogram Information Data)
cn	压缩数字型 (Compressed Numeric)
CVM	持卡人验证方法 (Cardholder Verification Method)
CVR	卡片验证结果 (Card Verification Results)
DDA	动态数据认证 (Dynamic Data Authentication)
DDOL	动态数据认证数据对象列表 (Dynamic Data Authentication Data Object List)
DDF	目录定义文件 (Directory Definition File)
DF	专用文件 (Dedicated File)
DIR	目录 (Directory)
DOL	数据对象列表 (Data Object List)
EC	电子现金 (Electronic Cash)
EF	基本文件 (Elementary File)
EP	电子钱包 (Electronic Purse)
FCI	文件控制信息 (File Control Information)
fDDA	快速动态数据认证 (Fast DDA)
GPO	获取处理选项 (Get Processing Options)
IAC	发卡机构行为代码 (Issuer Action Code)
IC	集成电路 (Integrated Circuit)
ICC	集成电路卡 (Integrated Circuit Card)
IDD	发卡机构自定义数据 (Issuer Defined Data)
INS	命令报文的指令字节 (Instruction Byte of Command Message)
Lc	终端应用层 (TAL) 在情况 3 或情况 4 命令中发出数据的实际长度 (Exact Length of

	Data Sent by the TAL in a Case 3 or 4 Command)
Le	响应数据中的最大期望长度 (Maximum Length of Data Expected)
M	必备 (Mandatory)
MAC	报文鉴别码 (Message Authentication Code)
MDK	主密钥 (Master DEA Key)
MF	主文件 (Master File)
n	数字型 (Numeric)
P1	参数 1 (Parameter 1)
P2	参数 2 (Parameter 2)
PAN	主账号 (Primary Account Number)
PDOL	处理选项数据对象列表 (Processing Options Data Object List)
PIN	个人识别码 (Personal Identification Number)
PIX	扩展的专用应用标识符 (Proprietary Application Identifier Extension)
PPSE	近距离支付系统环境 (Proximity Payment Systems Environment)
RFU	预留 (Reserved for Future Use)
RID	注册的应用提供商标识 (Registered Application Provider Identifier)
R-MAC	响应数据的报文鉴别码 (Response Message Authentication Code)
SAM	安全认证模块 (Secure Authentication Module)
SFI	短文件标示符 (Short File Identifier)
SW1	状态字 1 (Status Word One)
SW2	状态字 2 (Status Word Two)
TAC	交易验证码 (Transaction Authorization Cryptogram)
TC	交易证书 (Transaction Certificate)
TLV	标签、长度、值 (Tag Length Value)
TSI	交易状态信息 (Transaction Status Information)
TDOL	交易证书数据对象列表 (Transaction Certificate Data Object List)
TVR	终端验证结果 (Terminal Verification Results)
UDK	子密钥 (Unique DEA Key)
YYYYMMDD	年、月、日 (Year, Month, Day)

5 文件、数据元、数据对象列表

5.1 文件

本规范的文件组织结构来自且符合GB/T 16649.4的基本组织结构。

本部分描述了符合城市公共交通IC卡技术应用规范的IC卡应用文件结构。

城市公共交通IC卡中的能够读/写的文件中的数据对象是以记录方式保存的。文件的结构和引用方法取决于该文件的用途。文件的结构和引用的方法将在下面描述。除了下一条描述的目录文件以外，其它的城市公共交通IC卡可读/写数据文件的布局均由发卡机构定义。

5.1.1 应用定义文件

ADF的树形结构：

——能够将数据文件与应用联系起来；

- 确保应用之间的独立性；
- 可以通过应用选择实现对其逻辑结构的访问。

5.1.2 应用基本文件

短文件标识符（SFI）范围为1-10的AEF，包含一个基本数据对象或由多个“基本编码规则—标签长度值”（BER-TLV）的数据对象组成的结构BER-TLV数据对象（记录）。一旦选定之后，范围为1-10的AEF只能如5.1.5.2所述通过它的短文件标识符（SFI）来引用。

本规范中，一个数据文件包括一组按记录号引用的记录序列。1-10号SFI引用的数据文件中只包括那些不由卡片解释的数据，即不在卡片内部过程中使用的数据。这种文件的结构定义成线性结构。根据GB/T 16649.44规定，文件结构既可以固定的，也可以是线性可变的。这由发卡机构自行选择，并且根据本规范不会影响对文件的读操作。

5.1.3 文件到 GB/T 16649.4 的文件结构的映射

使用下列到GB/T 16649.4的映射：

- 一个 GB/T 16649.4 定义的专用文件（DF）映射为一个 ADF 或一个 DDF。可以通过它来访问基本文件和 DF。在卡片中处于最高层的 DF 称为主文件（MF）。
- GB/T 16649.4 定义的一个基本文件（EF）对应一个 AEF。EF 永远不会成为另一个文件的入口点。

在本规范中，如果嵌入了DF，对与之相连的EF的访问是透明的。

5.1.4 目录结构

当卡片上存在支付系统环境（PPSE）时，城市公共交通IC卡必须为PPSE中发卡机构希望通过目录选择的应用列表提供一个目录结构。目录结构允许以应用标识符（AID）检索一个应用，或以AID的前n个字节作为DDF名检索一组应用。

- 本部分描述的一个或多个应用模板（标签为‘61’）。
- 可能在目录自定义模板（标签为‘73’）中出现的其他数据对象，此模板中包含的数据对象不在本规范的范围内定义。

城市公共交通IC卡中的目录是可选的，但对可能存在的目录数目没有限制。其中每个目录的位置由每个DDF中的FCI的目录SFI数据对象指定。

城市公共交通IC卡文件结构如图1所示：

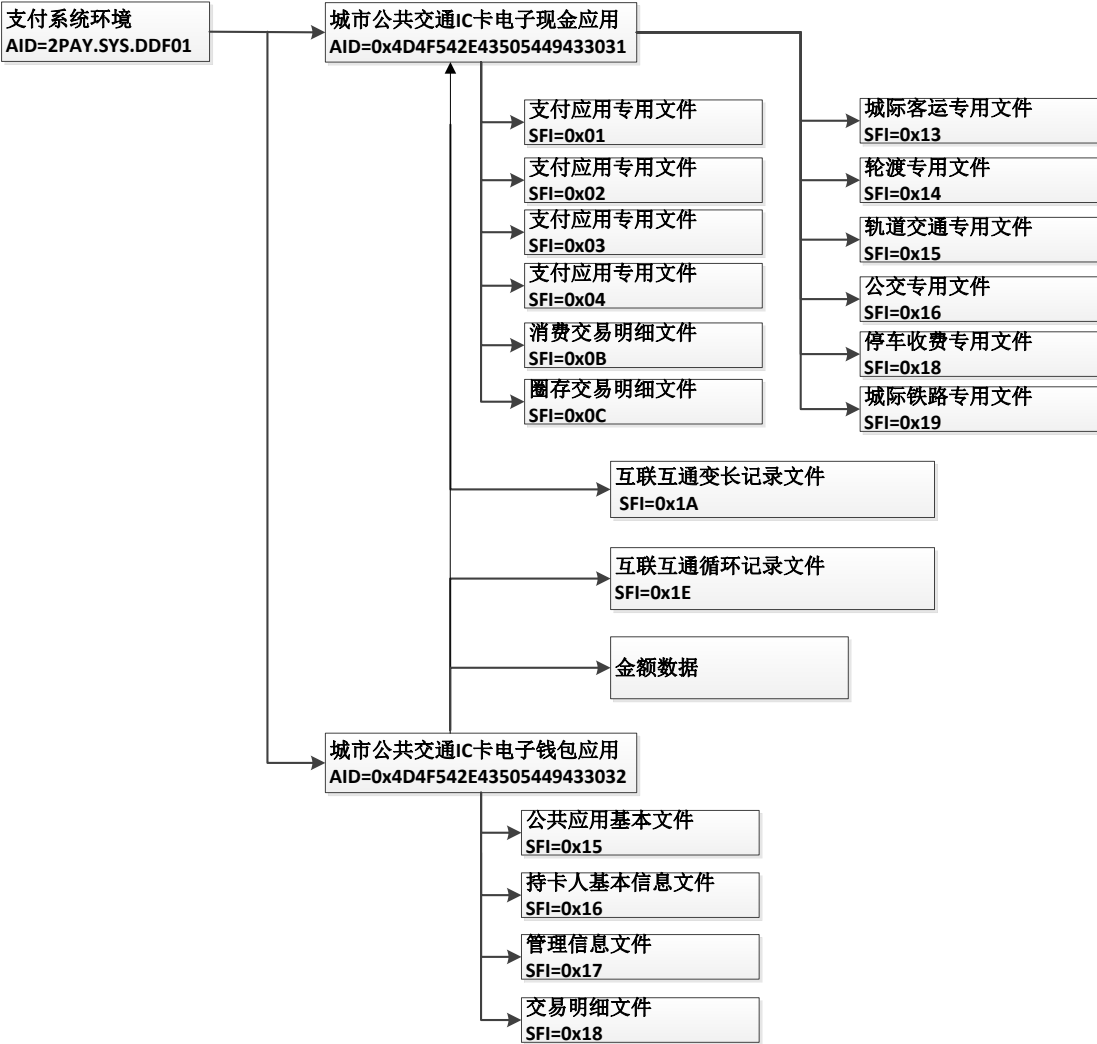


图1 城市公共交通 IC 卡文件结构示意图

城市公共交通IC卡中同时存在电子现金应用和电子钱包应用,两个应用公用金额与互联互通专用文件。互联互通专用文件(0x1A、0x1E)将同时存在于电子现金应用和电子钱包应用,两个应用能共同对这两个文件进行读写。此外,两个应用拥有各自独立的文件结构、安全体系与交易流程。

以下电子现金命令会导致公用金额的更新:

- PUT DATA (设置数据) 命令。
- 支付流程最后的READ RECORD (读记录) 命令。

以下电子钱包命令会导致公用金额的更新:

- CREDIT FOR LOAD (圈存) 命令。
- DEBIT FOR PURCHASE (消费) 命令。
- DEBIT FOR UNLOAD (圈提) 命令。
- UPDATE OVERDRAW LIMIT (修改透支限额) 命令。

以下电子现金命令会导致互联互通专用文件的更新:

- APPEND RECORD (新增记录) 命令。
- UPDATE CAPP DATA CACHE (更新数据缓存) 命令。
- UPDATE RECORD (修改记录) 命令。

以下电子钱包命令会导致互联互通专用文件的更新:

- APPEND RECORD (新增记录) 命令。
- UPDATE CAPP DATA CACHE (更新数据缓存) 命令。
- UPDATE RECORD (修改记录) 命令。

电子现金扩展应用文件短文件标识符定义见附录B。

5.1.5 文件引用

根据文件的种类,文件可以通过文件名或SFI引用。

5.1.5.1 通过文件名引用

卡片中的任何ADF或DDF都可以通过它的DF名引用。ADF的DF名与它的AID对应或以AID作为DF名的开头。卡片中的每个DF名字必须在该卡内是唯一的。

5.1.5.2 通过 SFI 引用

SFI用于选择AEF。在一个给定的应用中可以通过SFI来引用任何一个AEF。该SFI使用5个位(bit)来编码,其值在1~30的范围内。SFI编码将在使用它的各命令中描述。SFI的结构见表1。

表1 SFI 结构

数值	意义
1~10	规范定义
11~20	城市公共交通 IC 卡系统定义
21~30	发卡机构定义

每个SFI在一个应用以内必须是唯一的。范围为11~20的SFI引用的AEF由城市公共交通IC卡系统分配管理。

5.2 数据元

定义并解释城市公共交通IC卡应用数据交换过程中卡片所需的相关数据元。包括数据元的名称、标识及功能等，见附录C。

5.3 电子现金数据对象列表

有时，终端应卡片的要求需要建立可变的数据元列表用来向卡片发送。为了减少城市公共交通IC卡电子现金应用对这些数据的处理，这个列表不需要进行TLV编码，而只是把若干数据单元连接成一个复合域。因为复合域中的数据单元不是TLV编码的，所以当城市公共交通IC卡电子现金应用收到数据时，城市公共交通IC卡电子现金应用必须知道该复合域的格式。因此，需要在城市公共交通IC卡电子现金应用内包含一个数据对象列表（DOL）来定义复合域中的数据格式。本规范用的DOL包括：

- 卡风险管理数据对象列表 1（CDOL1）：在第一次 GENERATE AC 命令中需要传送给卡片的数据对象列表。CDOL1 是终端在读应用记录处理过程中从卡片中读出的；
- 卡风险管理数据对象列表 2（CDOL2）：在第二次 GENERATE AC 命令中需要传送给卡片的数据对象列表。CDOL2 是终端在读应用记录处理过程中从卡片中读出的；
- 交易证书数据对象列表（TDOL）：列出生成交易证书（TC）哈希计算的数据对象（标签和长度）；
- 动态脱机数据认证对象列表（DDOL）：指定在 INTERNAL AUTHENTICATE 指令中，卡片要求终端送入卡片的终端数据标签和长度列表。

一个DOL是用一些条目连接而成的列表。每个条目代表一个加入复合域的单个数据元。每个条目的格式包括1~2个字节的标签来表明需要的数据对象，然后是1个字节的长度部分，表明本数据对象在命令数据中占据的字节长度。只有那些在附录A中定义为基本数据对象的标签才可以在DOL中使用。

终端必须完成下列步骤以建立结构域：

- 从城市公共交通 IC 卡读取 DOL。
- 连接 DOL 中列出的所有数据单元。按照下列规则进行连接：
 - 如果 DOL 中指出的数据对象的标签无法被终端识别，或这个标签代表了一个结构数据对象，终端将提供一个长度为 DOL 指定长度的数据元，并必须把该数据元所有的数值部分设置为 16 进制的 0。
 - 如果该列表上的一个数据对象在终端上可以识别，但是表现为城市公共交通 IC 卡上不出现的可选静态数据，那么在命令区域上代表数据对象的部分必须用 16 进制的 0 来填满。
 - 如果在 DOL 条目中指出的长度小于实际数据对象的长度，则需要将实际的数据对象削减至 DOL 指出的长度。如果数据对象是数字格式（n）的，则从数据单元的的最左端开始削减字节。如果数据对象是其它格式的，则从数据单元的最右端开始削减字节。如果指出的长度比实际的数据长度大，需要把实际的数据填充至指定长度：
 - 如果数据对象是数字格式（n）的，则从数据单元头部开始填充 16 进制的 0；
 - 如果数据对象是压缩数字型（cn）的，则在数据单元的末尾填充 16 进制的 FF；
 - 如果数据对象是其它格式的，则在数据单元的末尾填充 16 进制的 0。
 - 如果表上的一个数据对象在终端可以识别，但不代表在当前交易中适用的数据，代表该数据对象的命令域部分将填充 16 进制的 0。

数据单元在表上的连接顺序应该与相应的数据对象在DOL中出现的顺序一一对应。

6 通用卡片技术要求

6.1 功能要求

电子支付应用卡片应支持表2中列出的必备功能。可选功能由发卡机构或者市场需求来决定。如果相关条件满足，有条件的功能也要支持。

表2 卡片功能需求

功能	卡片支持
应用选择	必备
a) 目录选择方式	可选
b) 直接选择方式	必备
应用初始化	必备
读应用记录	必备
脱机数据认证	可选
c) 标准 DDA	必备
d) 复合 DDA/应用密文生成	可选
处理限制	必备
e) 应用版本号检查	必备
f) 应用用途控制检查	可选
g) 生效日期检查	可选
h) 失效日期检查	必备
持卡人验证	可选
i) 单独的 CVM	可选
终端风险管理	必备
j) 终端异常文件检查	n/a（卡片没有处理）
k) 商户强制联机	n/a（卡片没有处理）
l) 最低限额检查	n/a（卡片没有处理）
m) 交易日志	n/a（卡片没有处理）
n) 随机选择	n/a（卡片没有处理）
o) 频度检查	可选
p) 新卡检查	可选
终端行为分析	IAC 需要（城市公共交通 IC 卡应用）
卡片行为分析	必备
q) 联机/脱机决定	必备
r) 卡片风险管理	必备
s) 通知报文	可选
t) 应用密文	提供算法选择 提供多算法选择
联机处理	必备
u) 联机能力	必备
v) 发卡机构认证	可选
交易结束	必备
发卡机构到卡片脚本处理	可选
w) 安全报文	仅支持一种脚本形式

6.2 命令要求

卡片支持的命令在表3中描述。

表3 命令支持需求

命令	卡片支持
应用锁定 APPLICATION BLOCK	应用锁定功能可选，如果支持，推荐使用应用锁定命令
应用解锁 APPLICATION UNBLOCK	应用解锁功能可选，如果支持，推荐使用应用解锁命令
卡片锁定 CARD BLOCK	卡片锁定是推荐功能，可通过卡片锁定命令实现
外部认证 EXTERNAL AUTHENTICATE	有条件的——如果支持发卡机构认证
生成应用密文 GENERATE AC	必备
取数据 GET DATA	必备
获取处理选项 GET PROCESSING OPTIONS	必备
内部认证 INTERNAL AUTHENTICATE	有条件的——如果支持 DDA
PIN 修改/解锁 PIN CHANGE / UNBLOCK	如果支持脱机 PIN。则 PIN 解锁功能必备，可使用 PIN 修改/解锁命令实现 PIN 修改功能可选，如果使用则应在发卡机构可控的环境下
设置数据 PUT DATA	必备
读记录 READ RECORD	必备
选择 SELECT	必备
修改记录 UPDATE RECORD	可选
验证 VERIFY	有条件的——如果支持脱机 PIN
读扩展应用数据 READ CAPP DATA	必备
更新数据缓存 UPDATE CAPP DATA CACHE	必备
新增记录 APPEND RECORD	必备
取脱机交易应用密文 GET TRANS PROVE	必备

取随机数 GET CHALLENGE	必备
内部认证 INTERNAL AUTHENTICATION	必备
读二进制文件 READ BINARY	必备
修改二进制文件 UPDATE BINARY	必备
圈存 CREDIT FOR LOAD	必备
消费 DEBIT FOR PURCHASE	必备
圈提 DEBIT FOR UNLOAD	必备
查询余额 GET BALANCE	必备
取交易认证 GET TRANSACTION PROVE	必备
初始化圈存 INITIALIZE FOR LOAD	必备
初始化圈提 INITIALIZE FOR UNLOAD	必备
初始化消费 INITIALIZE FOR PURCHASE	必备
修改初始化 INITIALIZE FOR UPDATE	必备
修改透支限额 UPDATE OVERDRAW LIMIT	必备

7 电子现金卡片技术要求

7.1 卡片通用要求

7.1.1 通用的卡片要求

- 卡片应支持城市公共交通 IC 卡电子现金应用；
- 电子现金应用支持联机交易、标准快速支付交易、分时分段扣费交易、脱机预授权交易、单次扣款优惠交易功能。
- 卡片应该符合《城市公共交通 IC 卡非接触接口通讯技术规范》，至少支持 type A 或 Type B 中的一种；
- 发卡机构基本信息数据对于城市公共交通 IC 卡应用是必备的；
- 支持城市公共交通 IC 卡应用的卡片应支持 fDDA；
- 为了使目前的芯片满足时间要求，卡片以中国余数定理模式存放与使用 RSA 私钥。

7.1.2 通用卡片选项

卡片可选支持非接触界面城市公共交通IC卡应用应用。

卡片应支持记录交易日志的功能，该功能可在个人化时通过卡片附加处理开启或关闭。

当卡片附加处理（标签“9F68”）中第2字节第5位为‘1’时，表示脱机批准的交易，卡片记录交易日志；当卡片附加处理（标签“9F68”）中第2字节第5位为‘0’时，表示脱机批准的交易，卡片不记录交易日志。

是否启用交易日志功能由发卡机构决定。

7.2 应用选择要求

所有非接触卡片应符合下列选择非接触支付应用的要求。在初始化应用处理阶段，确定用于处理交易的方法（非接触式城市公共交通IC卡应用）。

7.2.1 卡片应用选择要求

下面的卡片要求允许选择非接触应用。本部分描述了多个非接触应用的行为。为了将应用选择时间最小化，建议对个人化在FCI中的应用数量进行限制。

- 应使用文件名“2PAY.SYS.DDF01”将PPSE个人化到所有的非接触卡片中；
- 应当在具有城市公共交通 IC 卡应用 AID 的单个卡片应用中，支持非接触式城市公共交通 IC 卡应用和城市公共交通 IC 卡应用路径；
- 如果一个以上的应用被个人化到 FCI 中，则应用优先指示器应被个人化到所有的应用中。在本部分中，应用优先指示器 Bits 8-5 应设为“0000”；
- 卡片中的非接触应用的 AID，应在 SELECT PPSE 命令响应的 FCI 中返回。
- 所有非接触应用的个人化都应存在 PDOL，该 PDOL 至少要包含标签为“9F66”（终端交易属性）的数据元；
- 如果支持单一的非接触应用，AID 的长度应至少有 7 字节。

7.2.2 近距离支付系统环境（PPSE）

表4定义了单一应用和多个应用的PPSE格式。建议对个人化的应用的数量进行限制。

表4 近距离支付系统环境（PPSE）

标签	值		长度	出现条件
“6F”	FCI 模板		变长	M
	“84”	“2PAY.SYS.DDF01”	0E	M
	“A5”	FCI 专用模板	变长	M
	“BF0C”	FCI 发卡机构自定义数据	变长	M
	“61”	目录入口	变长	M
	“4F”	DF 名（AID）	07-08	M
	“50”	应用标签	04-10	O
	“87”	应用优先指示器	01	C*
	“61”	目录入口	变长	C*

标签	值			长度	出现条件
		“4F”	DF 名 (AID)	07-08	C
		“50”	应用标签	04-10	C
		“87”	应用优先指示器	01	C
	“61”	目录入口		变长	C*
		“4F”	DF 名 (AID)	07-08	C
		“50”	应用标签	04-10	C
		“87”	应用优先指示器	01	C

条件——如果一个以上的应用个人化到卡片中，则每个应用的个人化应具有应用优先指示器。应用优先指示器的Bit 8-5位应置为“0000”。

7.2.3 SELECT 命令

SELECT命令报文编码见表5。

表5 SELECT 命令报文

代码	值
CLA	‘00’
INS	‘A4’
P1	引用控制参数（见表6）
P2	SELECT 命令选项（见表7）
Lc	‘05’ – ‘10’
Data	AID
Le	‘00’

表6 SELECT 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0				
					1			通过名称选择
						0	0	

表7 SELECT 命令可选参数

b8	b7	b6	b5	b4	b3	b2	b1	含义
						0	0	第1个或仅有一个
						1	0	下一个（未用）

7.3 卡片初始应用处理要求

在初始应用处理阶段，终端向卡片发出GP0命令，命令中包括卡片在应用选择时返回PDOL中所要求的所有数据。GP0命令详细描述见附录A。

7.3.1 GP0 命令

获取处理选项（GET PROCESSING OPTIONS）命令格式如表8所示。

表8 GP0 命令

编码	值
CLA	‘80’
INS	‘A8’
P1	‘00’；其它值预留
P2	‘00’；其它值预留
Lc	变长
数据域	处理选项数据对象列表（PDOL）相关数据
Le	‘00’

7.4 交易时间

基于卡片和终端之间的交互，单次脱机的交易时间不能超过350毫秒。这个时间是从终端寻获卡片并上电成功，到终端接收到卡片返回的最后一条指令为止，不包括联机认证或终端脱机数据认证中验证静态或动态签名所需的时间。

8 电子钱包卡片技术要求

8.1 卡片通用要求

8.1.1 通用的卡片要求

- 卡片应支持城市公共交通 IC 卡电子钱包应用；
- 电子钱包应用支持圈存交易、圈提交易、消费交易、复合应用消费交易、查询交易、应用维护功能；
- 卡片应该符合《城市公共交通 IC 卡非接触接口通讯技术规范》，至少支持 type A 或 Type B 中的一种。

8.2 应用选择要求

卡片必须支持支付系统环境（PPSE）选择和直接选择。

8.2.1 卡片应用选择要求

下面的卡片要求允许选择非接触应用。本部分描述了多个非接触应用的行为。为了将应用选择时间最小化，建议对个人化在FCI中的应用数量进行限制。

- 应使用文件名“2PAY.SYS.DDF01”将 PPSE 个人化到所有的非接触卡片中；
- 应当在具有城市公共交通 IC 卡应用 AID 的单个卡片应用中，支持非接触式城市公共交通 IC 卡应用和城市公共交通 IC 卡应用路径；
- 如果一个以上的应用被个人化到 FCI 中，则应用优先指示器应被个人化到所有的应用中。在本部分中，应用优先指示器 Bits 8-5 应设为“0000”；
- 卡片中的非接触应用的 AID，应在 SELECT PPSE 命令响应的 FCI 中返回；
- 如果支持单一的非接触应用，AID 的长度应至少有 7 字节。

8.2.2 近距离支付系统环境（PPSE）

表9定义了单一应用和多个应用的PPSE格式。建议对个人化的应用的数量进行限制。

表9 近距离支付系统环境（PPSE）

标签	值		长度	出现条件
“6F”	FCI 模板		变长	M
“84”	“2PAY.SYS.DDF01”		0E	M
“A5”	FCI 专用模板		变长	M
“BF0C”	FCI 发卡机构自定义数据		变长	M
“61”	目录入口		变长	M
“4F”	DF 名（AID）		07-08	M
“50”	应用标签		04-10	O
“87”	应用优先指示器		01	C*
“61”	目录入口		变长	C*
“4F”	DF 名（AID）		07-08	C
“50”	应用标签		04-10	C
“87”	应用优先指示器		01	C
“61”	目录入口		变长	C*
“4F”	DF 名（AID）		07-08	C
“50”	应用标签		04-10	C
“87”	应用优先指示器		01	C

8.2.3 SELECT 命令

SELECT 命令报文编码见表 10。

表10 SELECT 命令报文

代码	值
CLA	‘00’
INS	‘A4’
P1	引用控制参数（见表 11）
P2	‘00’ 第一个或仅有一个 ‘02’ 下一个
Lc	‘05’ - ‘10’
Data	文件名
Le	‘00’

表11定义了命令报文中的引用控制参数。

表11 SELECT 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含 义
0	0	0	0	0				

					1			通过文件名选择
						0	0	

8.3 交易时间

基于卡片和终端之间的交互，单次脱机的交易时间不能超过300毫秒。这个时间是从终端寻获卡片并上电成功，到终端接收到卡片返回的最后一条指令为止。

9 电子现金双币应用（可选）

电子现金双币应用是在城市公共交通 IC 卡应用基础上，在卡中增加一组第二币种相关数据元(参见附录 C)，交易时卡片根据交易货币代码，选择对应币种的数据元进行风险检查和余额更新。发卡机构主机，应能通过交易货币代码来区分对应币种的电子现金账户。

9.1 基于城市公共交通 IC 卡应用的电子现金双币应用

基于城市公共交通IC卡应用的电子现金双币应用仅适用于“支持小额检查”选项(卡片附加处理选项，标签“9F68”)，不适用“支持小额和CTTA检查”和“支持小额或CTTA检查”选项。当“支持小额和CTTA检查”或“支持小额或CTTA检查”选项打开时，卡片应关闭第二币种电子现金功能，并按照城市公共交通IC卡应用流程处理。

9.1.1 个人化要求

电子现金双币应用应将新增的第二币种相关数据元个人化至卡片中，PDOL应满足相关要求，并至少包含交易货币代码（标签“5F2A”）。卡片附加处理选项（标签“9F68”）中第1字节第7位“支持小额和CTTA检查”和第1字节第6位“支持小额或CTTA检查”应设置为‘0’，第1字节第8位“支持小额检查”应设置为‘1’。发卡机构应用数据（标签“9F10”）中的发卡机构自定义数据(IDD)不应包含以下选项：

- CTTA，IDD ID 为 0x02；
- 电子现金余额和 CTTA，IDD ID 为 0x03；
- CTTA 和 CTTAL，IDD ID 为 0x04。

9.1.2 卡片风险管理

卡片在接收到GPO命令后开始进行风险管理。在卡片风险管理的第一步“设置货币匹配或不匹配”中，卡片应使用交易货币代码进行电子现金的币种匹配和数据元选择。具体过程如图2所示：

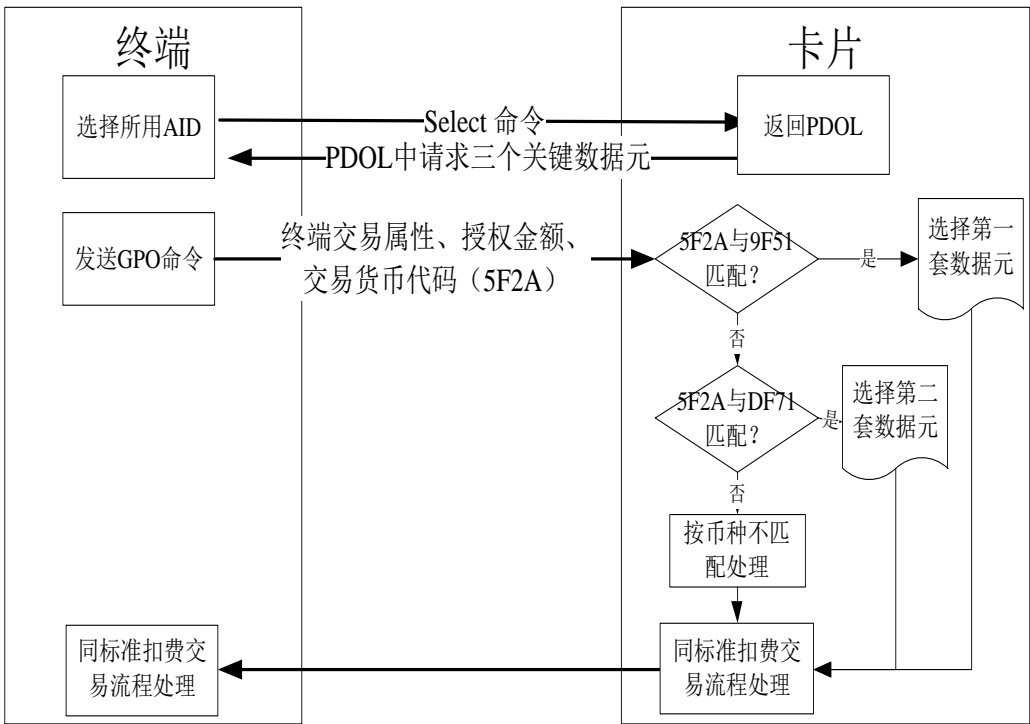


图2 卡片风险管理

卡片在接收到GPO命令后，首先将交易货币代码（标签“5F2A”）与应用货币代码（标签“9F51”）进行比较，如果匹配，则在后续流程中使用第一币种相关数据元进行处理；如果不匹配，则将交易货币代码（标签“5F2A”）与第二币种电子现金应用货币代码（标签“DF71”）进行比较：如果与第二币种电子现金应用货币代码匹配，则在后续流程中使用第二币种相关数据元代替第一币种相关数据元进行处理，否则仍然使用第一币种相关数据元按照标准快速支付流程中币种不匹配的情况处理。

卡片在风险管理结束后，返回GPO命令的响应数据时：

- 如响应数据中包括可用脱机消费金额（标签“9F5D”），则卡片应根据卡片风险管理过程中币种匹配的结果选择使用电子现金余额（标签“9F79”）或第二币种电子现金余额（标签“DF79”）参与“9F5D”的计算；
- 如卡片需要在发卡机构自定义数据中返回电子现金余额（标签“9F79”）或脱机可用余额（标签“9F5D”），则卡片应根据卡片风险管理过程中币种匹配的结果选择电子现金余额（标签“9F79”）或第二币种电子现金余额（标签“DF79”）参与计算。

9.1.3 读应用数据

对于第二币种电子现金交易，卡片完成GPO 命令的处理后：

- 当终端以 GET DATA 命令读取电子现金余额（标签“9F79”）时，卡片应将第二币种电子现金余额（标签“DF79”）的值返回；
- 当终端以 GET DATA 命令读取电子现金重置阈值（标签“9F6D”）时，卡片应将第二币种电子现金重置阈值（标签“DF76”）的值返回；
- 当终端以 GET DATA 命令读取电子现金余额上限（标签“9F77”）时，卡片应将第二币种电子现金余额上限（标签“DF77”）的值返回；
- 当终端以 GET DATA 命令读取电子现金单笔交易限额（标签“9F78”）时，卡片应将第二币种电

子现金单笔交易限额（标签“DF78”）的值返回；

——当终端以 GET DATA 命令读取脱机可用余额（标签“9F5D”）时，卡片应使用第二币种电子现金余额（标签“DF79”）的值参与计算；

——当终端以 GET DATA 命令读取卡片 CVM 限额（标签“9F6B”）时，卡片应使用第二币种卡片 CVM 限额（标签“DF72”）的值参与计算。

如果没有收到GPO命令或者收到的GPO中交易货币代码与第二币种应用货币代码（标签“DF71”）不匹配，则卡片在处理GET DATA命令时仍按标准快速支付流程处理。

此设计的目的是为保证终端在不做任何流程上的改变的情况下，能够通过GET DATA命令正确识别并获取本次交易所使用的与币种相关的数据元。

9.2 支持电子现金双币应用的分时分段扣费流程

支持电子现金双币应用的分时分段扣费流程是基于城市公共交通 IC 卡应用的电子现金双币应用，本部分仅描述电子现金双币应用的分时分段扣费流程与标准分段扣费交易流程的差异，未提及部分请参考《城市公共交通 IC 卡读写终端技术规范》分时分段扣费交易流程。

9.2.1 支持分段扣费押金抵扣功能的特殊处理

在分段扣费交易模式下，发卡机构可选择支持押金抵扣功能，并需在个人化时增加双币分段扣费抵扣限额（DF82）和双币分段扣费已抵扣金额（DF83）两个数据。同时，在标准分时、分段扣费交易的部分流程中，对具有押金抵扣功能的卡片进行如下特殊处理。

a) 应用选择

对于支持押金抵扣交易的终端，在进行交易前，应获取第二币种电子现金余额（DF79）进行校验。如果当前第二币种电子现金余额(DF79)大于 0，终端继续交易；如果当前第二币种电子现金余额(DF79)等于 0，表示卡内余额为 0 或者已经进行过押金抵扣交易，终端可根据自身业务逻辑决定继续交易或者终止交易。

b) 初始化应用

当收到 GPO 命令，进入分段扣费流程时，如果卡片支持分段扣费押金抵扣功能，则当前实际可用电子现金余额=第二币种电子现金余额（DF79）+双币分段扣费抵扣限额（DF82）-双币分段扣费已抵扣金额（DF83）；如果卡片不支持分段扣费押金抵扣功能，则当前实际可用电子现金余额=第二币种电子现金余额（DF79）。

c) 读取卡片数据内容

终端根据 GPO 返回的 AFL，向卡片发送 READ RECORD 命令时，如果卡片支持押金抵扣功能，且第二币种电子现金余额（DF79）小于当前交易金额，则进行押金抵扣，交易后的双币分段扣费已抵扣金额（DF83）=交易前双币分段扣费已抵扣金额（DF83）+ 交易金额 - 交易前第二币种电子现金余额（DF79）。如果交易后的双币分段扣费已抵扣金额（DF83）小于电子现金双币应用分段扣费抵扣限额（DF82），则在最后一个记录被成功读取后，将交易后的双币分段扣费已抵扣金额（DF83）进行更新，同时将交易后的第二币种电子现金余额（DF79）设置为零，完成交易；否则交易失败。

d) 圈存操作

——发卡机构后台圈存流程保持与现有流程一致。

——卡片收到发卡机构发送的修改余额的脚本命令时，需自动计算并同时设置第二币种电子现金余额（DF79）和双币分段扣费已抵扣金额（DF83）。

——如果当前第二币种电子现金余额（DF79）等于 0；

——当修改余额脚本中指定的金额大于双币分段扣费已抵扣金额（DF83），则圈存后的第二币种电

子现金余额 (DF79) = 修改余额脚本中指定的金额 - 双币分段扣费已抵扣金额 (DF83)，同时将双币分段扣费已抵扣金额 (DF83) 清零；

- 当修改余额脚本中指定的金额小于等于双币分段扣费已抵扣金额 (DF83)，则圈存后的双币分段扣费已抵扣金额 (DF83) = 圈存前双币分段扣费已抵扣金额 (DF83) - 修改余额脚本中指定的金额，第二币种电子现金余额 (DF79) 值保持不变；
- 如果当前第二币种电子现金余额 (DF79) 大于 0，按标准圈存流程处理。

e) 查询操作

- 标准终端只能支持第二币种电子现金余额 (DF79) 的查询；
- 支持分段扣费押金抵扣功能的终端，可单独查询第二币种电子现金余额 (DF79)、双币分段扣费抵扣限额 (DF82) 与双币分段扣费已抵扣金额 (DF83)，根据实际业务需求显示查询余额。

f) 更新分段扣费抵扣限额操作

卡片收到发卡机构发送的修改双币分段扣费抵扣限额 (DF82) 的脚本命令时，如果修改分段扣费抵扣限额的脚本中指定的双币分段扣费抵扣限额 (DF82) 小于双币分段扣费已抵扣金额 (DF83)，则返回 6A80；否则，用脚本中指定的值完成双币分段扣费抵扣限额 (DF82) 的更新。

9.3 基于城市公共交通 IC 卡应用的电子现金双币应用

本部分仅描述电子现金双币应用在城市公共交通 IC 卡应用流程下与标准快速支付交易流程的差异，未提及部分请参考《城市公共交通 IC 卡读写终端技术规范》标准快速支付交易流程。

9.3.1 初始化应用

卡片在接收到 GP0 命令后，应根据一系列条件判断交易是否为电子现金交易。如卡片支持电子现金双币应用，则应首先判断交易货币代码与应用货币代码是否匹配。具体判断过程如图 3 所示：

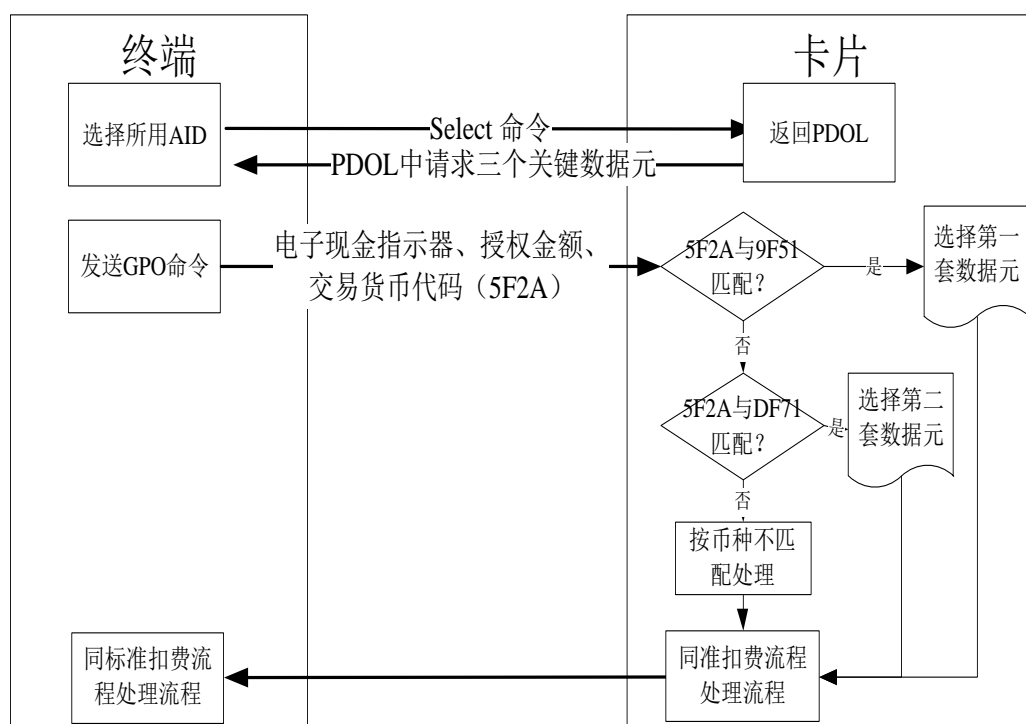


图3 卡片风险管理

卡片在接收到 GP0 命令后，首先将交易货币代码（标签“5F2A”）与应用货币代码（标签“9F51”）进行比较，如果匹配，则在后续流程中使用第一币种相关数据元进行处理；如果不匹配，则将交易货币代码（标签“5F2A”）与第二币种电子现金应用货币代码（标签“DF71”）进行比较：如果与第二币种电子现金应用货币代码匹配，则在后续流程中使用第二币种相关数据元代替第一币种相关数据元进行处理，否则仍然使用第一币种相关数据元按照标准电子现金流程中币种不匹配的情况处理。

后续处理流程与标准快速支付交易流程保持一致。

9.3.2 读应用数据

如果终端读取的记录数据中包含电子现金发卡机构授权码（标签“9F74”），则终端将通过 GET DATA 读取电子现金余额（标签“9F79”）和电子现金重置阈值（标签“9F6D”），用于终端风险管理中的处理。对于第二币种电子现金交易，卡片完成 GP0 命令的处理后：

- 当终端以 GET DATA 命令读取电子现金余额（标签“9F79”）时，卡片应将第二币种电子现金余额（标签“DF79”）的值返回；
- 当终端以 GET DATA 命令读取电子现金重置阈值（标签“9F6D”）时，卡片应将第二币种电子现金重置阈值（标签“DF76”）的值返回；
- 当终端以 GET DATA 命令读取电子现金余额上限（标签“9F77”）时，卡片应将第二币种电子现金余额上限（标签“DF77”）的值返回；
- 当终端以 GET DATA 命令读取电子现金单笔交易限额（标签“9F78”）时，卡片应将第二币种电子现金单笔交易限额（标签“DF78”）的值返回；

如果没有收到 GP0 命令或者 GP0 命令中收到的交易货币代码与第二币种应用货币代码（标签“DF71”）不匹配，则卡片在处理 GET DATA 命令时仍按标准快速支付交易情况处理。此设计的目的是为保证终端在不做任何流程上的改变的情况下，能够通过 GET DATA 命令正确识别并获取本次交易所使用的与币种相关的数据元。

9.3.3 卡片行为分析

电子现金双币应用卡片行为分析和标准快速支付交易中卡片行为分析流程相同，差异部分如下：卡片在响应 GAC 命令时，卡片应根据初始化应用处理过程中币种匹配的情况决定在发卡机构应用数据（标签“9F10”）中返回电子现金余额（标签“9F79”）还是返回第二币种电子现金余额（标签“DF79”）。

9.3.4 发卡机构脚本处理

卡片需支持发卡机构通过发卡机构脚本命令 PUT DATA 修改第二币种相关数据元。例如发卡机构脚本命令 PUT DATA 的 P1 P2 参数为“DF79”，则卡片直接修改第二币种电子现金余额（标签“DF79”）对应的值。

附录 A (规范性附录) 应用指令

此附录中描述了各个章条中使用到的卡片命令。

A.1 通用指令

A.1.1 SELECT（选择）命令

A.1.1.1 定义和范围

选择（SELECT）命令通过文件名或AID来选择城市公共交通IC卡中的PPSE或ADF。
成功执行该命令设定PPSE或ADF的路径。后续命令作用于与用SFI选定的PPSE或ADF相联系的AEF。
从城市公共交通IC卡返回的响应报文包含回送FCI。

A.1.1.2 命令报文

表A.1 Select 命令报文

代码	值
CLA	‘00’
INS	‘A4’
P1	‘04’
P2	‘00’
Lc	‘05’ - ‘10’
Data	文件名
Le	‘00’

A.1.1.3 命令报文数据域

命令报文数据域应包括所选择的PPSE名、DF名或AID。

A.1.1.4 响应报文数据域

A.1.1.4.1 PPSE的响应报文数据域

表A.2定义了成功选择PPSE后回送的FCI。

表A.2 选择 PPSE 的响应报文（FCI）

标签	值		长度	出现条件
“6F”	FCI 模板		变长	M
	“84”	“2PAY.SYS.DDF01”	0E	M
	“A5”	FCI 专用模板	变长	M
	“BF0C”	FCI 发卡机构自定义数据	变长	M
	“61”	目录入口	变长	M
	“4F”	DF 名（AID）	07-08	M

标签	值		长度	出现条件	
		“50”	应用标签	04-10	O
		“87”	应用优先指示器	01	C*
	“61”	目录入口		变长	C*
		“4F”	DF 名（AID）	07-08	C
		“50”	应用标签	04-10	C
		“87”	应用优先指示器	01	C
	“61”	目录入口		变长	C*
		“4F”	DF 名（AID）	07-08	C
		“50”	应用标签	04-10	C

A. 1. 1. 4. 2 电子现金的响应报文数据域

表A. 3定义了电子现金应用的响应报文数据域。

表A. 3 选择电子现金应用的响应报文 (FCI)

标签	值		存在性
‘6F’	FCI 模板		M
	‘84’	DF 名	M
	‘A5’	FCI 数据专用模板	M
	‘50’	应用标签	M
	‘87’	应用优先指示器	O
	‘9F38’	PDOL	O
	‘5F2D’	首选语言	O
	‘9F11’	发卡机构代码表索引	O
	‘9F12’	应用优先名称	O
	‘BF0C’	发卡机构自定义数据（FCI）	O

对于多应用卡片，应在响应报文中包含“应用标签”数据元，使得在终端用“AID列表”方法进行应用选择时，能方便持卡人选择/确认应用。

A. 1. 1. 4. 3 电子钱包的响应报文数据域

表A. 4定义了成功选择电子钱包应用后回送的FCI：

表A. 4 选择电子钱包应用的响应报文 (FCI)

标签	值		存在性方式
‘6F’	FCI 模板		M
	‘84’	DF 名	M

	‘A5’	FCI 数据专用模板		M
	‘50’	应用标签		O
	‘87’	应用优先指示符		O
	‘9F08’	应用版本号		M
	‘9F12’	应用优先名称		O
	‘BF0C’	发卡机构自定义数据（FCI），见表 A.5		O

表A.5 FCI 发卡机构专用数据

数据字段的描述	长度（字节）
发卡机构标识符	8
应用类型标识	1
发卡机构应用版本号	1
应用序列号	10
应用启用日期	4
应用有效日期	4
发卡机构自定义 FCI 数据	2

A.1.1.5 响应报文的状态字

响应报文状态字见A.6。

表A.6 Select 指令的响应报文状态字

SW1	SW2	含 义
‘64’	‘00’	标志状态位没变
‘67’	‘00’	P1、P2 与 Lc 不一致
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘86’	P1 和 P2 错误
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘03’	应用永久锁定

A.1.2 GET RESPONSE（取数据）命令

A.1.2.1 定义和范围

该指令只用于T=0协议卡片。

当APDU不能用现有协议传输时，GET RESPONSE命令提供了一种从卡片向接口设备传送APDU（或APDU的一部分）的传输方法。

A.1.2.2 命令报文

GET RESPONSE命令报文编码见表A.7。

表A.7 GET RESPONSE 命令报文

代码	值
CLA	‘00’
INS	‘C0’
P1	‘00’
P2	‘00’
Lc	不存在
Data	不存在
Le	响应的期望数据最大长度

A.1.2.3 命令报文数据域

命令报文数据域不存在。

A.1.2.4 响应报文数据域

响应报文数据域的长度由Le的值决定。

如果Le的值为零，在附加数据有效时，卡片必须回送状态字“6CXX”，否则回送状态字“6F00”。

A.1.2.5 响应报文状态字

此命令执行成功的状态字是“9000”。

表A.8列出正常处理情况。

表A.8 GET RESPONSE 正常状态

SW1	SW2	含 义
‘61’	‘XX’	表示正常处理，‘XX’表示可以通过后续 GET RESPONSE 命令得到的额外数据长度

IC卡可能回送的警告状态字见表A.9。

表A.9 GET RESPONSE 警告状态

SW1	SW2	含 义
‘62’	‘81’	回送的数据可能有错

IC卡可能回送的错误状态字见表A.10。

表A.10 GET RESPONSE 错误状态

SW1	SW2	含 义
‘67’	‘00’	长度错误（Le 不正确）
‘6A’	‘86’	P1 和 P2 错误
‘6C’	‘XX’	长度错误（Le 不正确，‘XX’表示实际长度）
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘6F’	‘00’	数据无效

A.1.3 READ RECORD（读记录）命令

A. 1. 3. 1 定义和范围

读记录（READ RECORD）命令从一个线性文件中读一条文件记录。

从城市公共交通IC卡返回的响应中将包含这条被读出的记录。

A. 1. 3. 2 命令报文

读记录（READ RECORD）命令报文根据表A. 11编码。

表A. 11 读记录（READ RECORD）命令报文

编码	值
CLA	‘00’
INS	‘B2’
P1	记录号
P2	引用控制参数，见表 A.12
Lc	不存在
数据域	不存在
Le	‘00’

表A. 12定义了命令报文的引用控制参数。

表A. 12 读记录（READ RECORD）命令引用控制参数

b8	B7	b6	b5	b4	b3	b2	b1	意义
x	x	x	x	x				SFI
					1	0	0	读 P1 指定记录

A. 1. 3. 3 命令报文的数据域

命令报文中没有数据域。

A. 1. 3. 4 响应报文的数据域

任何成功的读记录（READ RECORD）命令的响应报文的数据域都包含读出的记录值。对于在1-10范围内的SFI，这个记录是一个标签为‘80’的BER-TLV结构数据对象。除本规范有特别定义，对于不在1-10范围内的SFI的读记录命令响应报文，不在本规范的范围描述范围内。

A. 1. 3. 5 响应报文的响应字

“9000” 编码表示命令成功执行。

A. 1. 4 UPDATE RECORD（修改记录）命令

A. 1. 4. 1 定义和范围

修改记录（UPDATE RECORD）命令用来修改文件中一条记录的内容，修改的内容在命令数据域中。

A. 1. 4. 2 命令报文

修改记录（UPDATE RECORD）命令报文编码见表A. 13。

表A. 13 修改记录（UPDATE RECORD）命令报文

代码	值
CLA	‘00’或‘04’
INS	‘DC’
P1	记录号
P2	引用控制参数，见表 A.14
Lc	后续数据域的长度
Data	更新原有记录的新记录+报文鉴别码（MAC）数据元（4 字节）
Le	不存在

CLA=‘00’ 不需要安全报文。

CLA=‘04’ 需要安全报文。

表A. 14定义了命令报文的引用控制参数。

表A. 14 修改记录（UPDATE RECORD）命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	意义
x	x	x	x	x				SFI
					1	0	0	P1 为记录号

A. 1. 4. 3 命令报文的数据域

数据域中是要修改的新记录内容。如果需要安全报文，则MAC长度为4字节。算法参考《城市公共交通IC卡安全技术规范》。

A. 1. 4. 4 响应报文的数据域

响应报文没有数据域。

A. 1. 4. 5 响应报文的响应字

“9000” 编码表示命令成功执行。

表A. 15列出了命令可能返回的警告信息。

表A. 15 修改记录（UPDATE RECORD）命令的警告响应码

SW1	SW2	含义
62	00	没有信息返回
62	81	数据可能被破坏

表A. 16列出了命令可能返回的错误信息。

表A. 16 修改记录（UPDATE RECORD）命令的错误响应码

SW1	SW2	含义
64	00	没有准确诊断
65	81	内存失败
67	00	长度错误

68	82	不支持安全报文
69	81	命令与文件结构不匹配
69	82	安全状态不满足
69	86	命令不允许
69	87	安全报文数据对象丢失
69	88	安全报文数据对象不正确
6A	81	功能不支持
6A	82	文件没找到
6A	83	记录没找到
6A	84	文件中没有足够空间
6A	85	Lc 和 TLV 结构不一致

A.2 电子现金应用指令

- 应用锁定 (APPLICATION BLOCK) (发卡机构脚本命令)；
- 应用解锁 (APPLICATION UNBLOCK) (发卡机构脚本命令)；
- 卡片锁定 (CARD BLOCK) (发卡机构脚本命令)；
- 外部认证 (EXTERNAL AUTHENTICATE)；
- 生成应用密文 (GENERATE APPLICATION CRYPTGRAM (AC))；
- 取数据 (GET DATA)；
- 获取处理选项 (GPO)；
- 内部认证 (INTERNAL AUTHENTICATE)；
- PIN 修改/解锁 (PIN CHANGE/UNBLOCK) (发卡机构脚本命令)；
- 设置数据 (PUT DATA) (发卡机构脚本命令)；
- 读记录 (READ RECORD)；
- 选择 (SELECT)；
- 修改记录 (UPDATE RECORD) (发卡机构脚本命令)；
- 验证 (VERIFY)；
- 读取扩展应用数据 (READ CAPP DATA)；
- 更新数据缓存 (UPDATE CAPP DATA CACHE)；
- 新增记录 (APPEND RECORD)；
- 安全方式更新 (SECURITY UPDATE) (发卡机构脚本命令)；
- 取脱机交易应用密文 (GET TRANS PROVE)。

上述命令可以在其它情况下使用，例如个人化卡片。

终端发送命令给卡片，卡片处理完毕后，返回命令响应给终端。每个命令包括的 CLA、INS 字节标明了命令类型，参数字节 P1 P2 提供了处理信息。命令还可能包括一个数据域。

命令响应包括两个状态字 SW1 和 SW2，描述了命令运行结果。当命令执行成功，SW1 和 SW2 等于“9000”，其它值说明命令执行错误。命令的响应中还可以包括响应数据。

A.2.1 APPLICATION BLOCK (应用锁定) 命令

A.2.1.1 定义和范围

APPLICATION BLOCK命令是使当前被选择的应用无效的一个发卡机构脚本命令。

在成功的APPLICATION BLOCK命令之后：

- 对选择（SELECT）命令，无效的应用应该返回状态字节“选择文件无效”（SW1 SW2= “6283”）；
- 对生成应用密文（GENERATE AC）命令，一个无效的应用应该返回 AAC 代替 AC 作为响应。

A. 2. 1. 2 命令报文

APPLICATION BLOCK命令报文根据表A. 17编码。

表A. 17 APPLICATION BLOCK 命令报文

编码	值
CLA	‘84’
INS	‘1E’
P1	‘00’；其它值保留
P2	‘00’；其它值保留
Lc	数据域字节长度
数据域	4 字节 MAC 值
Le	不存在

A. 2. 1. 3 命令报文的数据域

命令报文的数据域中包含了根据密钥与安全规范中描述的安全报文格式编码的MAC数据。

A. 2. 1. 4 响应报文的数据域

响应报文没有数据域。

A. 2. 1. 5 响应报文的状况字

不论应用是否有效，“9000”编码总表示命令成功执行。

A. 2. 2 APPLICATION UNBLOCK（应用解锁）命令

A. 2. 2. 1 定义和范围

APPLICATION UNBLOCK命令是一个发卡机构脚本命令，用来恢复当前被选择的应用。

当APPLICATION UNBLOCK命令成功执行后，此前通过应用锁定附加在该应用上的限制被解除。

A. 2. 2. 2 命令报文

APPLICATION UNBLOCK命令报文通过表A. 18编码。

表A. 18 APPLICATION UNBLOCK 命令报文

编码	值
CLA	‘84’
INS	‘18’
P1	‘00’；其它值保留
P2	‘00’；其它值保留

Lc	数据域字节长度
数据域	4 字节 MAC 值
Le	不存在

A. 2. 2. 3 命令报文的数据域

命令报文的数据域中包含了根据安全规范中描述的安全报文格式编码的MAC数据。

A. 2. 2. 4 响应报文的数据域

响应报文中没有数据域。

A. 2. 2. 5 响应报文的状态字

■ 不论应用是否有效，“9000”编码表示命令成功执行。

A. 2. 3 CARD BLOCK（卡片锁定）命令

A. 2. 3. 1 定义和范围

CARD BLOCK命令是一个发行后命令，用来永久地停止城市公共交通IC卡中所有的应用。

CARD BLOCK命令停止城市公共交通IC卡中所有的应用，包括那些被隐式选中的应用。

当一个CARD BLOCK命令成功后，所有随后的选择命令都将收到状态字节为“功能不支持”（SW1 SW2=“6A81”）的反馈，并且不执行任何其它动作。

A. 2. 3. 2 命令报文

CARD BLOCK命令报文根据表A. 19编码。

表A. 19 CARD BLOCK 命令报文

编码	值
CLA	‘84’
INS	‘16’
P1	‘00’；其它值保留
P2	‘00’；其它值保留
Lc	数据域字节长度
数据域	4 字节 MAC 值
Le	不存在

A. 2. 3. 3 命令报文的数据域

命令报文的数据域中包含了根据安全规范中描述的安全报文格式编码的MAC数据。

A. 2. 3. 4 响应报文的数据域

■ 响应报文没有数据域。

A. 2. 3. 5 响应报文的状态字

不论卡是否已经被锁，“9000”编码都表示命令成功执行。

A. 2. 4 EXTERNAL AUTHENTICATE（外部认证）命令

A. 2. 4. 1 定义和范围

外部认证（EXTERNAL AUTHENTICATE）命令要求城市公共交通IC卡中的应用认证一个密文。
城市公共交通IC卡的响应应该包括该命令的处理状态。
一次交易中只执行最多一次外部认证命令。

A. 2. 4. 2 命令报文

外部认证（EXTERNAL AUTHENTICATE）命令报文根据表A. 20编码。

表A. 20 外部认证（EXTERNAL AUTHENTICATE）命令报文

编码	值
CLA	‘00’
INS	‘82’
P1	‘00’
P2	‘00’
Lc	8—16
数据域	发卡机构认证数据
Le	不存在

在外部认证（EXTERNAL AUTHENTICATE）命令中的引用算法（P1）值为‘00’，表示该域无信息。对算法的引用或者在使用本命令前就已经完成，或者在本命令的数据域中定义。

A. 2. 4. 3 命令报文的数据域

按照本规范的规定，本命令报文的数据域包含标签为‘91’的值域，编码如下：
——前 8 个字节为必选的授权响应密文 ARPC；
——附加的 1-8 个可选字节是专有数据。
在本规范中，发卡机构认证数据包括下列两个数据元：
——ARPC（8 字节）；
——授权响应码（2 字节）。

A. 2. 4. 4 响应报文的数据域

响应报文没有数据域。

A. 2. 4. 5 响应报文的状况字

“9000” 编码表示命令成功执行。
如果验证失败，返回“6300”，如果在本次交易中卡片已经接收过外部认证命令，卡片返回“6985”。

A. 2. 5 GENERATE AC（生成应用密文）命令

A. 2. 5. 1 定义和范围

生成应用密文（GENERATE AC）命令传送交易相关数据到城市公共交通IC卡，城市公共交通IC卡计算并且返回一个密文。这个密文是一个由本规范定义的应用密文（AC），表A. 21列出了密文类型。

表A. 21 生成应用的密文类型

类型	意义
应用认证密文（AAC）	拒绝交易
授权请求密文（ARQC）	请求联机授权
交易证书（TC）	批准交易

由城市公共交通IC卡返回的密文可能由于城市公共交通IC卡的内部处理过程而与命令报文中要求的密文不一样。

A. 2. 5. 2 命令报文

生成应用密文（GENERATE AC）命令报文根据表A. 22编码。

表A. 22 生成应用密文（GENERATE AC）命令报文

编码	值
CLA	‘80’
INS	‘AE’
P1	引用控制参数（见表 A.23）
P2	‘00’
Lc	Var.
数据域	交易相关数据
Le	‘00’

生成应用密文（GENERATE AC）命令中的引用控制参数根据表A. 23编码。

表A. 23 GENERATE AC 引用控制参数

b8	b7	B6	b5	b4	b3	b2	b1	意义
0	0							AAC
0	1							TC
1	0							ARQC
1	1							保留
			0					未明确请求复合动态数据认证/应用密文生成
			1					请求复合动态数据认证/应用密文生成
		x		x	x	x	x	保留

A. 2. 5. 3 命令报文的数据域

命令报文的数据域是用来生成应用密文的终端数据，具体的数据内容在附录D中描述。

A. 2. 5. 4 响应报文的数据域

密文的生成算法在附录D中描述。

响应报文的数据域包含一个BER-TLV编码的数据对象。这个数据对象需要按照以下两种格式之一编码。

格式1:

响应报文中的数据对象是一个标签为‘80’的基本数据对象。数据域由表A. 24所示的数据对象连接而成，各数据对象之间没有分隔符（标签和长度）。

表A. 24 GENERATE AC 响应报文数据域格式 1

值	存在性
密文信息数据	必备
应用交易计数器（ATC）	必备
应用密文（AC）	必备
发卡机构应用数据	可选

格式2:

响应报文的数据对象是一个标签为‘77’的结构数据对象。数据域中可以包含多个BER-TLV编码对象，但是应包括密文信息数据、应用交易序号和由城市公共交通IC卡计算出的密文（可以是应用密文或专有密文）。对于响应报文中可能包含的专有数据对象的应用和解释，不在本规范的范围之内。

如果响应报文是如《城市公共交通IC卡安全技术规范》定义的签名数据，对CDA的响应，则采用格式2。该响应数据单元格式见本部分附录C。

如果卡片不执行CDA，命令的响应报文数据域中的数据对象按照格式1编码。如果卡片执行CDA，命令的响应报文数据域中的数据对象按照格式2编码。

以上两种格式中，在生成应用密文命令的响应报文中包括的密文数据按照表A. 25的方式编码。

表A. 25 密文信息数据编码

b8	b7	b6	b5	b4	b3	b2	b1	意义
0	0							AAC
0	1							TC
1	0							ARQC
1	1							RFU
		x	x					城市公共交通 IC 卡系统密文
				0				未请求通知
				1				请求通知
					x	x	x	原因/通知/授权参考码
					0	0	0	无信息
					0	0	1	不允许服务
					0	1	0	PIN 重试超限
					0	1	1	发卡机构鉴定失败
					x	x	x	其它值保留

A. 2. 5. 5 响应报文的状态字

“9000”编码表示命令成功执行。

一次交易卡片最多处理两个生成应用密文命令，如果收到三个及以上个数，卡片返回“6985”。

A. 2. 6 GET DATA（取数据）命令

A. 2. 6. 1 定义和范围

下面描述的是在非支付交易过程中在特殊设备上使用取数据（GET DATA）命令访问到的数据和一个支付交易过程中，使用取数据（GET DATA）命令访问数据。

——特殊设备

表A. 26列出的静态数据可以在发卡机构控制的特殊设备上通过取数据（GET DATA）命令访问。普通终端不能用取数据命令获得。

表A. 26 使用取数据（GET DATA）命令访问的静态数据

数据元
应用货币代码（9F51）
应用缺省行为（9F52）
连续脱机交易限制数（国际-国家）（9F72）
连续脱机交易限制数（国际-货币）（9F53）
累计脱机交易金额限制数（9F54）
累计脱机交易金额限制数（双货币）（9F75）
累计脱机交易金额上限（9F5C）
货币转换因子（9F73）
发卡机构认证指示位（9F56）
发卡机构国家代码（9F57）
连续脱机交易下限（9F58）
连续脱机交易上限（9F59）
第2应用货币代码（9F76）
电子现金分段扣费抵扣限额（DF62）
电子现金分段扣费已抵扣额（DF63）

——支付交易

取数据（GET DATA）命令用来从当前应用中取得一个没有封装在记录中的基本数据对象。取数据（GET DATA）命令可以用来获取基本数据对象ATC（标签为“9F36”）、上次联机ATC寄存器（标签为“9F13”）或PIN重试计数器（标签为“9F17”）、交易日志格式（标签为“9F4F”）。

A. 2. 6. 2 命令报文

取数据（GET DATA）命令报文根据表A. 27编码。

表A. 27 取数据（GET DATA）命令报文

编码	值
CLA	‘80’
INS	‘CA’
P1 P2	要访问数据的标签
Lc	不存在
数据域	不存在

Le	‘00’
----	------

A. 2. 6. 3 命令报文的数据域

命令报文没有数据域。

A. 2. 6. 4 响应报文的数据域

响应报文的数据域中包含有如命令报文的P1、P2所述的基本数据对象。（即包括它的标签和它的长度）。

A. 2. 6. 5 响应报文的状况字

“9000” 编码表示命令成功执行。
如果命令中请求的数据是专有数据不能返回，卡片返回 “6A88” 。

A. 2. 7 GET PROCESSING OPTIONS（获取处理选项）命令

A. 2. 7. 1 定义和范围

获取处理选项（GP0）命令用来启动城市公共交通IC卡内的交易。
城市公共交通IC卡的响应报文中包含应用交互特征（AIP）和应用文件定位器（AFL）。

A. 2. 7. 2 命令报文

获取处理选项（GP0）命令报文根据表A. 28编码。

表A. 28 获取处理选项（GP0）命令报文

编码	值
CLA	‘80’
INS	‘A8’
P1 P2	‘00’
Lc	‘00’
数据域	PDOL 相关数据（如果存在）或 8300
Le	‘00’

A. 2. 7. 3 命令报文的数据域

命令报文的数据域根据城市公共交通IC卡提供的处理选项数据对象列表（PDOL）编码。PDOL通过标签“83” 标记。 当城市公共交通IC卡没有提供数据对象列表时，这个模板的长度域设置为 ‘0’ 。否则，这个模板的数据长度域的值等于传输给城市公共交通IC卡的数据对象的值域的总长度。

A. 2. 7. 4 响应报文的数据域

响应报文的数据域包含一个BER-TLV编码数据对象。
卡片可以任选下列两种格式之一来编码：
格式1：
响应报文中的数据对象是一个标签为 ‘80’ 的基本数据对象。数据域为应用交互特征（AIP）和应用文件定位器（AFL）。

格式2:

响应报文中的数据对象是一个标签为‘77’的基本数据对象。数据域可以包含多个BER-TLV编码的对象，但至少包含应用交互特征（AIP）和应用文件定位器（AFL）。

应用交互特征定义了可以被城市公共交通IC卡中的应用支持的功能。

AFL包括一个不含有分隔符的由文件与记录组成的列表。

A. 2. 7. 5 响应报文的状态字

“9000”编码表示命令成功执行。

A. 2. 8 INTERNAL AUTHENTICATE（内部认证）命令

A. 2. 8. 1 定义和范围

内部认证（INTERNAL AUTHENTICATE）命令引发卡片使用从IFD收到的随机数、数据和卡片中储存的私钥来计算出“签名动态应用数据”的过程。

A. 2. 8. 2 命令报文

- 内部认证（INTERNAL AUTHENTICATE）命令根据表 A.29 编码。

表A. 29 内部认证（INTERNAL AUTHENTICATE）命令报文

编码	值
CLA	‘00’
INS	‘88’
P1	‘00’
P2	‘00’
Lc	认证相关数据长度
数据域	认证相关数据
Le	‘00’

在内部认证（INTERNAL AUTHENTICATE）命令中的算法引用（P1）域值为‘00’，这表示该值无意义。对算法的引用应该或者在使用本命令前就已经完成，或者在本命令的数据域中定义。

A. 2. 8. 3 命令报文的数据域

命令报文的数据域包括该应用专有的与认证有关的数据。它是根据附录D中定义的动态数据认证数据对象列表（DDOL）规则来编码的。

为了确保内部认证（INTERNAL AUTHENTICATE）命令返回数据在256字节限制内，签名的动态应用数据加上可选的TLV格式编码的长度应该限制在《城市公共交通IC卡安全技术规范》中定义的范围内。

A. 2. 8. 4 响应报文的数据域

响应报文的数据域包括一个BER-TLV编码数据对象。这个数据对象的编码格式为：

响应报文中的数据对象是一个标签为‘80’的基本数据对象。数据域中包括签名动态应用数据。签名动态应用数据按照附录D中的规则定义。

A. 2. 8. 5 响应报文的状态字

“9000” 编码表示命令成功执行。

A. 2. 9 PIN CHANGE/UNBLOCK (PIN修改/解锁) 命令

A. 2. 9. 1 定义和范围

PIN CHANGE/UNBLOCK命令是一个发卡机构脚本命令。它的目的是让发卡机构解锁PIN或同时既改变PIN也解锁PIN。

当PIN CHANGE/UNBLOCK命令成功后，卡片将执行下列功能：

——PIN 尝试计数器的值将复位到 PIN 尝试限制数（最大值）；

——如果有请求，脱机 PIN 值将被设置为新的 PIN 值。

为了保密，如果本命令包含有PIN数据，则该数据应该加密。

注：脱机PIN是存储在卡中与应用相关的PIN，它用来验证在验证命令中传来的PIN数据。

A. 2. 9. 2 命令报文

PIN CHANGE/UNBLOCK命令报文根据表A. 30编码。

表A. 30 PIN CHANGE/UNBLOCK 命令报文

编码	值
CLA	‘84’
INS	‘24’
P1	‘00’
P2	‘00’、‘01’或‘02’
Lc	数据字节数
数据	加密 PIN 数据成员（如果存在）和 MAC 数据
Le	不存在

当P2为“00”，PIN尝试计数器复位。

当P2为“01”，PIN尝试计数器复位同时PIN修改，PIN修改时使用当前的PIN。

当P2为“02”，PIN尝试计数器复位同时PIN修改，PIN修改是不使用当前的PIN。

A. 2. 9. 3 命令报文的数据域

本命令报文的数据域包括PIN加密数据，后面可以加上4到8字节的安全报文MAC数据。

如果P2等于‘00’，参考PIN解锁，PIN尝试计数器被复位到PIN尝试限制数。命令数据域只包含MAC。因为PIN修改/解锁命令中不包含新的PIN值，所以PIN不会更新。

P2等于‘01’或‘02’的值的处理步骤分别在B. 10. 1和B. 10. 2中描述。

A. 2. 9. 3. 1 使用当前PIN修改PIN值

如果命令中的P2参数等于“01”，命令数据域包括PIN加密数据和MAC，PIN加密数据的产生过程按照下列步骤进行：

步骤 1：发卡机构确定用来给数据进行加密的安全报文加密主密钥，并分散生成卡片的安全报文加密子密钥：ENC UDK-A 和 ENC UDK-B；

步骤 2：生成过程密钥 Ks；

步骤 3：生成 8 字节 PIN 数据块 D3；

表A. 31 8 字节数据块 D1

字节 1		字节 2		字节 3		字节 4		字节 5	字节 6	字节 7	字节 8
0	0	0	0	0	0	0	0	ENC UDK-A 的最右边 4 个字节			

表A. 32 8 字节数据块 D2

字节 1		字节 2		字节 3		字节 4		字节 5		字节 6		字节 7		字节 8	
0	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

——N: 新 PIN 的数字个数 (16 进制)

——P: 新 PIN 值, 长度 4-12 个数字 (2-6 字节)

——D1 和 D2 执行异或得到 D3

步骤 4: 使用当前 PIN 生成 8 字节数据块 D4;

表A. 33 使用当前 PIN 生成 8 字节数据块 D4

字节 1		字节 2		字节 3		字节 4		字节 5		字节 6		字节 7		字节 8	
P	P	P	P	P/0	P/0	P/0	P/0	P/0	P/0	P/0	P/0	0	0	0	0

步骤 5: 将数据块 D3 和 D4 执行异或得到 D;

步骤 6: 用 Ks 对 D 进行加密, 得到 PIN 加密数据。

A. 2. 9. 3. 2 不使用当前PIN修改PIN值

如果命令中的P2参数等于“02”, 命令数据域包括PIN加密数据和MAC, PIN加密数据的产生过程按照下列步骤进行:

步骤 1: 发卡机构确定用来给数据进行加密的安全报文加密主密钥, 并分散生成卡片的安全报文加密子密钥: ENC UDK-A 和 ENC UDK-B;

步骤 2: 生成过程密钥 Ks;

步骤 3: 生成 8 字节 PIN 数据块 D3:

表A. 34 8 字节数据块 D1

字节 1		字节 2		字节 3		字节 4		字节 5	字节 6	字节 7	字节 8
0	0	0	0	0	0	0	0	ENC UDK-A 的最右边 4 个字节			

表A. 35 生成第 2 个 8 字节数据块 D2

字节 1		字节 2		字节 3		字节 4		字节 5		字节 6		字节 7		字节 8	
0	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

——N: 新 PIN 的数字个数 (16 进制);

——P: 新 PIN 值, 长度 4-12 个数字 (2-6 字节)。

——D1 和 D2 执行异或得到 D。

步骤 4: 用 Ks 对 D 进行加密, 得到 PIN 加密数据。

A. 2. 9. 4 响应报文的数据域

响应报文没有数据域。

A. 2. 9. 5 响应报文的状态字

“9000”编码表示命令成功执行。

A. 2. 10 PUT DATA（设置数据）命令

A. 2. 10. 1 定义和范围

设置数据（PUT DATA）命令用来修改卡片中的一些基本数据对象的值。只有有标签的数据才能使用这条命令修改。此命令不能用来修改结构数据对象。

A. 2. 10. 1. 1 可以用设置数据命令修改的数据

表A. 36列出的数据可以使用此命令修改。

表A. 36 使用设置数据（PUT DATA）命令修改的数据

数据元
连续脱机交易限制数（国际-国家）（9F72）
连续脱机交易限制数（国际-货币）（9F53）
累计脱机交易金额限制数（9F54）
累计脱机交易金额限制数（双货币）（9F75）
累计脱机交易金额上限（9F5C）
货币转换因子（9F73）
连续脱机交易下限（9F58）
连续脱机交易上限（9F59）
电子现金分段扣费抵扣限额（DF62）

A. 2. 10. 2 命令报文

设置数据（PUT DATA）命令报文根据表A. 37编码。

表A. 37 设置数据（PUT DATA）命令报文

编码	值
CLA	‘04’
INS	‘DA’
P1 P2	要修改的数据对象的标签
Lc	数据域字节数
数据域	数据对象的新值（不包括标签和长度）和 MAC 数据
Le	不存在

A. 2. 10. 3 命令报文的数据域

命令数据域中包括的是要修改的数据对象的值，后面加一个4到8字节的MAC。MAC的计算见《城市公共交通IC卡安全技术规范》。

A. 2. 10. 4 响应报文的数据域

响应报文没有数据域。

A. 2. 10. 5 响应报文的状态字

“9000” 编码表示命令成功执行。

表A. 38列出了命令可能返回的警告信息。

表A. 38 设置数据（PUT DATA）命令的警告响应码

SW1	SW2	含义
62	00	没有信息返回
62	81	数据可能被破坏

表A. 39列出了命令可能返回的错误信息。

表A. 39 设置数据（PUT DATA）命令的错误响应码

SW1	SW2	含义
64	00	没有准确诊断
65	81	内存失败
67	00	长度错误
68	82	不支持安全报文
69	82	安全状态不满足
69	86	命令不允许
69	87	安全报文数据对象丢失
69	88	安全报文数据对象不正确
6A	80	错误的参数
6A	81	功能不支持
6A	84	文件中没有足够空间
6A	85	Lc 和 TLV 结构不一致

A. 2. 11 VERIFY（验证）命令

A. 2. 11. 1 定义和范围

验证（VERIFY）命令引发城市公共交通IC卡将命令报文数据域内的交易PIN数据和与该应用相关的参考PIN数据进行比较验证。验证方式由城市公共交通IC卡中的应用自行决定。当从CVM列表中选择持卡人验证方法（CVM）是脱机PIN时，使用验证（VERIFY）命令。

A. 2. 11. 2 命令报文

验证（VERIFY）命令报文根据表A. 40编码。

表A. 40 验证（VERIFY）命令报文

编码	值
CLA	‘00’
INS	‘20’

P1	‘00’
P2	参考数据定义
Lc	var.
数据	交易 PIN 数据
Le	不存在

表A. 41定义了参考数据（P2）的意义。

表A. 41 验证（VERIFY）命令参考数据定义（P2）

b8	b7	b6	b5	b4	b3	b2	b1	意义
0	0	0	0	0	0	0	0	ISO/IEC 7816-4 定义 ¹
1	0	0	0	0	0	0	0	明文 PIN，格式如下
1	0	0	0	0	x	x	x	保留
1	0	0	0	1	0	0	0	保留
1	0	0	0	1	0	x	x	保留
1	0	0	0	1	1	x	x	城市公共交通 IC 卡系统保留
1	0	0	1	x	x	x	x	发卡机构保留

城市公共交通IC卡明文脱机PIN数据块按表A. 42格式组织。

表A. 42 脱机 PIN 数据块

字节 1								字节 2							
b8	b7	b6	b5	b4	b3	b2	b1	b8	b7	b6	b5	b4	b3	b2	b1
C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

脱机PIN数据块含义如表A. 43所示。

表A. 43 脱机 PIN 数据块

对应项	名称	值
C	控制域	值为 0010 的四位二进制数（hex. 2）
N	PIN 长度	值在 0100 到 1100 之间的 4 位二进制数（hex. ‘4’到‘C’）
P	PIN 数字	值在 0000 到 1001 之间的 4 位二进制数（hex. ‘0’到‘9’）
P/F	PIN/填充位	由 PIN 长度决定
F	填充位	值为 1111 的四位二进制数（hex. ‘F’）

P2=‘00’表示没有使用特别的限定符。城市公共交通IC卡中处理验证命令的应用应该知道怎样明白无误的找到PIN数据。

A. 2. 11. 3 命令报文的数据域

命令报文的数据域中包含标签‘99’的值域。

A. 2. 11. 4 响应报文的数据域

响应报文中没有数据域。

1) ¹未采用 P2= ‘00’。

A. 2. 11. 5 响应报文的状态字

“9000”编码表示命令成功执行。

如果对当前选择的应用，通过验证命令对交易 PIN 数据和参考 PIN 数据进行的比较失败了，城市公共交通 IC 卡会返回 SW2=‘Cx’，‘x’代表还可以重新验证的次数；如果城市公共交通 IC 卡返回了‘C0’，意味着不能再验证了，CVM 会被锁死。随后，在这个应用中进行的所有验证命令都会失败，并返回 SW1 SW2= “6983”。

A. 2. 12 READ CAPP DATA（读取扩展应用数据）命令

A. 2. 12. 1 定义和范围

READ CAPP DATA 命令用于扩展应用交易中，终端判断卡片是否支持相应行业应用，同时可获得上笔扩展应用交易信息。

终端通过扩展应用的所属的 ID 号（ID 号由城市公共交通 IC 卡系统定义，不足位数后补 0）和扩展应用行业类型，决定读取某一扩展应用文件的指定记录，在同一个 SFI 下，ID 应保持唯一。

卡片在接收到 READ CAPP DATA 命令后，将进行以下操作：

- 根据 P2 指定的 SFI 选取相应的 EF 文件。如果文件不存在，卡片回送状态字‘6A82’（未找到文件）。
- 如果 EF 文件不是变长记录文件，卡片回送状态字‘6981’（文件类型不符）。

A. 2. 12. 2 命令报文

此命令报文见表 A.44：

表A. 44 READ CAPP DATA 命令报文

代码	值
CLA	‘80’
INS	‘B4’
P1	‘00’
P2	见表 A. 45
Lc	‘02’ 或 ‘0A’
Data	详见说明
Le	‘00’

此命令报文中的引用控制参数 P2 定义如表 A.45 所示：

表A. 45 READ CAPP DATA 命令报文中引用控制参数 P2 定义

B8	B7	B6	B5	B4	B3	B2	B1	含义
0	0	0	0	0	—	—	—	RFU
x	x	x	x	x	—	—	—	SFI
1	1	1	1	1	—	—	—	RFU
—	—	—	—	—	0	0	0	第一个区号出现的记录
—	—	—	—	—	0	0	1	同一区号的下一条记录
—	—	—	—	—	x	x	x	RFU
其它值								RFU

A. 2. 12. 3 命令报文数据域

当卡片不支持扩展应用记录的 R-MAC 保护时，命令报文数据域包括 2 个字节的 ID 号；当卡片支持扩展应用记录的 R-MAC 保护时，命令报文数据域包括 2 个字节的 ID 号和 8 个字节的终端随机数。

A. 2. 12. 4 响应报文数据域

当卡片不支持扩展应用记录的 R-MAC 保护时，响应报文数据包括指定 ID 号的记录内容；当卡片支持扩展应用记录的 R-MAC 保护时，响应报文数据域包括指定 ID 号的记录内容和 4 个字节的 R-MAC 值。

响应报文数据中的 R-MAC，由卡片根据《城市公共交通 IC 卡安全技术规范》中关于报文鉴别码的描述，使用行业应用管理密钥对响应数据进行加密生成，其初始向量为命令报文数据域中的终端随机数。

A. 2. 12. 5 响应报文的状态字

命令执行成功的状态字是‘9000’。

城市公共交通 IC 卡可能回送的错误状态字见表 A.46：

表A. 46 READ CAPP DATA 错误状态字表

SW1	SW2	含 义
‘65’	‘81’	内存失败（修改失败）
‘67’	‘00’	长度错误（Lc 域为空）
‘69’	‘81’	命令与文件结构不相容
‘69’	‘86’	不满足命令执行的条件（不是当前的 EF 文件）
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到记录
‘6A’	‘84’	文件中存储空间不够
‘94’	‘07’	应用禁止

A. 2. 13 UPDATE CAPP DATA CACHE(更新数据缓存)命令

A. 2. 13. 1 定义和范围

UPDATE CAPP DATA CACHE 命令用于扩展应用交易中更新应用数据缓存。

卡片在收到 UPDATE CAPP DATA CACHE 命令后，将进行以下操作：

- 根据 P2 指定的 SFI 选取相应的 EF 文件。如果文件不存在，卡片回送状态字‘6A82’
- （未找到文件）。终端应终止此次扩展应用交易。
- 检查扩展应用专用文件的使用条件，若该命令的前续命令不是 GP0 命令或另一条 UPDATE CAPP DATA CACHE 命令，则回送状态字‘6985’（使用条件不满足）。终端应终止此次扩展应用交易。
- 若待更新的扩展应用专用文件是变长记录文件，则根据命令数据域中的 ID 号，查询扩展应用专用文件中是否存在相同 ID 号的记录。如果不存在，则回送状态字‘6A83’（未找到记录）。终端应终止此次扩展应用交易。
- 检查命令中的数据域长度是否大于扩展应用专用文件中相应记录的长度。如果大于，则回送状态字‘6A84’（文件中存储空间不够）；如果小于，则回送状态‘6A80’（数据域不正确）。终端应终止此次扩展应用交易。

在通过以上检查后，卡片应暂存命令中的 SFI、记录号和应用数据。扩展应用专用文件中相应记录的数据不得通过此命令更新。

允许多次执行 UPDATE CAPP DATA CACHE 命令，来完成多条记录的更新。

扩展应用专用文件可以是变长记录结构，也可以是循环记录结构。若是变长记录结构，在使用 UPDATE CAPP DATA CACHE 命令更新扩展应用数据之前，必须保证文件中存在相应的记录；若是循环记录结构，每次执行该指令，将更新最新的一条记录，然后循环使用。

该命令必须采用安全报文方式。

A. 2. 13. 2 命令报文

此命令报文见表 A.47:

表A. 47 UPDATE CAPP DATA CACHE 命令报文

代码	值
CLA	' 84/C4'
INS	'DE'
P1	'00'
P2	见表 A. 48
Lc	后续数据域的长度
Data	详见说明
Le	'00'

此命令报文中的参数 CLA 高半字节第 2 位定义加密算法类型，0 表示采用《城市公共交通 IC 卡安全技术规范》描述的 DES 算法，1 表示采用《城市公共交通 IC 卡安全技术规范》描述的 SM4 算法。

此命令报文中的引用控制参数 P2 定义如表 A.48:

表A. 48 UPDATE CAPP DATA CACHE 命令报文中引用控制参数 P2 定义

B8	B7	B6	B5	B4	B3	B2	B1	含义
0	0	0	0	0	—	—	—	RFU
x	x	x	x	x	—	—	—	SFI
1	1	1	1	1	—	—	—	RFU
—	—	—	—	—	0	0	0	第一个 ID 号出现的记录(变长记录文件) 或最新的一条记录(循环记录文件)
—	—	—	—	—	0	0	1	下一个 ID 号出现的记录(变长记录文件)
—	—	—	—	—	x	x	x	RFU
其它值								RFU

A. 2. 13. 3 命令报文数据域

命令报文数据域包含记录内容和安全报文。

若当前文件为变长记录文件，记录内容包含 ID 号、记录长度等扩展应用信息和扩展应用数据；若当前文件是循环记录文件，命令报文数据域包含扩展应用数据。

A. 2. 13. 4 响应报文数据域

当卡片不支持扩展应用记录的 R-MAC 保护时，响应报文数据域不存在；当卡片支持扩展应用记录的 R-MAC 保护时，响应报文数据为 4 字节的 MAC 值。

响应报文数据中的 R-MAC，由卡片根据《城市公共交通 IC 卡安全技术规范》中关于报文鉴别码的描述，使用行业应用管理密钥对响应报文的状态字进行加密生成，其初始向量为 ‘00’||‘00’||‘00’||‘00’|| 命令报文数据域中的 MAC。

A. 2. 13. 5 响应报文的状态字

此命令执行成功的状态字是 ‘9000’ 。

城市公共交通 IC 卡可能回送的错误状态字见表 A.49：

表A. 49 UPDATE CAPP DATA CACHE 错误状态字表

SW1	SW2	含 义
‘65’	‘81’	内存失败（修改失败）
‘67’	‘00’	长度错误（Lc 域为空）
‘69’	‘81’	命令与文件结构不相容
‘69’	‘86’	不满足命令执行的条件（不是当前的 EF 文件）
‘6A’	‘80’	数据域不正确
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到记录
‘6A’	‘84’	文件中存储空间不够
‘94’	‘07’	应用禁止

A. 2. 14 APPEND RECORD (新增记录) 命令

A. 2. 14. 1 定义和范围

APPEND RECORD 命令用于扩展应用开通时，向扩展应用文件中增加行业应用记录。可以用于向循环记录文件中添加记录，也可以用于向扩展应用循环记录文件中初始化第一条记录，记录空间在 APPEND RECORD 命令时动态分配。

卡片接收到 APPEND RECORD 命令后，将进行如下处理：

- 判断新增记录长度是否超过文件记录最大长度限制，如果超过，卡片回送状态字 ‘6A80’ ；
- 判断文件剩余空间是否足够，如果空间不足，卡片回送状态字 ‘6A84’ ；

通过以上判断，卡片将根据命令数据域的记录数据长度，分配记录空间，将新的记录数据写入文件。

A. 2. 14. 2 命令报文

此命令报文见表 A. 50：

表A. 50 APPEND RECORD 命令报文

代码	值
CLA	‘04’
INS	‘E2’
P1	‘00’
P2	见表 A. 51
Lc	后续数据域的长度

Data	16 字节记录修改密钥（由应用开通密钥加密）+新增的记录内容 + MAC
Le	不存在

此命令报文中的引用控制参数 P2 定义见表 A.51:

表A. 51 APPEND RECORD 命令报文中引用控制参数 P2 定义

B8	B7	B6	B5	B4	B3	B2	B1	含义
0	0	0	0	0	—	—	—	RFU
x	x	x	x	x	—	—	—	SFI
1	1	1	1	1	—	—	—	RFU
—	—	—	—	—	x	x	x	RFU
其它值								RFU

A. 2. 14. 3 命令报文数据域

此命令报文数据域由加密后的 16 字节的记录修改密钥、新增的记录内容（扩展应用数据）和 MAC 组成。

A. 2. 14. 4 响应报文数据域

响应报文数据域不存在。

A. 2. 14. 5 响应报文的状态字

此命令执行成功的状态字是‘9000’。

城市公共交通 IC 卡可能回送的错误状态字见表 A.52 所示:

表A. 52 APPEND RECORD 错误状态字表

SW1	SW2	含 义
‘65’	‘81’	内存失败（修改失败）
‘67’	‘00’	长度错误（Lc 域为空）
‘69’	‘81’	命令与文件结构不相容
‘69’	‘86’	不满足命令执行的条件（不是当前的 EF 文件）
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到记录
‘6A’	‘84’	文件中存储空间不够
‘94’	‘07’	应用禁止

A. 2. 15 GET TRANS PROVE (取脱机交易应用密文) 命令

A. 2. 15. 1 定义和范围

GET TRANS PROVE 命令用于获取指定的 ATC（应用交易计数器）对应扩展应用交易的 TC(脱机交易应用密文)。使用场景为，终端在无法接收到最后一条交易指令响应数据的情况下，重新上电并发送此命令，获取上笔失败交易的 TC，如果命令响应成功，则终端判断上笔交易成功，否则，按交易失败处理。

该命令只能获取最近一笔卡片成功完成的扩展应用交易的 TC。如果最近一笔交易是脱机预授权交易，则返回的 TC 为零。

A. 2. 15. 2 命令报文

此命令报文见表 A.53:

表A. 53 GET TRANS PROVE 命令报文

代码	值
CLA	‘80’
INS	‘5A’
P1	‘00’
P2	‘00’
Lc	‘02’
Data	终端指定的交易 ATC
Le	‘08’

A. 2. 15. 3 命令报文数据域

命令报文数据域由终端指定的交易 ATC 组成。

A. 2. 15. 4 响应报文数据域

响应报文数据域返回终端指定交易 ATC 对应的 TC（8 字节）。

A. 2. 15. 5 响应报文的状况字

此命令执行成功的状态字是 ‘9000’ 。

城市公共交通 IC 卡可能回送的错误状态字见表 A.54 所示:

表A. 54 GET TRANS PROVE 错误状态字表

SW1	SW2	含义
‘65’	‘81’	内存失败
‘67’	‘00’	长度错误
‘69’	‘85’	使用条件不满足
‘6D’	‘00’	命令不存在
‘6E’	‘00’	命令类型不支持
‘94’	‘06’	所需 TC 不可用

A. 3 电子钱包应用指令

A. 3. 1 APPLICATION BLOCK（应用锁定）命令

A. 3. 1. 1 定义和范围

APPLICATION BLOCK命令使当前选择的应用失效，该指令只能在特殊终端上使用。

当APPLICATION BLOCK命令成功地完成应用临时锁定后，用SELECT命令选择已临时锁定的应用，将回送状态字“选择文件无效”（SW1 SW2= “6283” ）。同时回送FCI（对于T=0卡片，需要用GET RESPONSE指令取回）。

当APPLICATION BLOCK命令成功完成应用永久锁定后，此后电子钱包应用执行所有命令，卡片将回送状态字“应用永久锁定”（SW1 SW2= “9303” ）。

对其他命令的影响根据不同应用而定。

A.3.1.2 命令报文

APPLICATION BLOCK命令报文编码见表A. 55。

表A. 55 APPLICATION BLOCK 命令报文

代码	值
CLA	‘84’
INS	‘1E’
P1	‘00’，其他值预留
P2	‘00’或‘01’
Lc	数据字节数
Data	报文鉴别码（MAC）数据元
Le	不存在

P2=‘00’：此命令执行成功后可锁定应用，但该应用可以用APPLICATION UNBLOCK命令解锁。

P2=‘01’：此命令执行成功后将永久锁定应用。

A.3.1.3 命令报文数据域

报文鉴别码（MAC）数据元。根据《城市公共交通IC卡安全技术规范》，由应用维护过程密钥计算。

A.3.1.4 响应报文数据域

响应报文数据域不存在。

A.3.1.5 响应报文状态字

无论应用是否已经失效，此命令执行成功的状态字是“9000”。

IC卡可能回送的状态字见表A. 56。

表A. 56 APPLICATION BLOCK 状态字表

SW1	SW2	含 义
‘62’	‘00’	无信息提供
‘62’	‘81’	回送数据可能出错
‘62’	‘83’	选择文件无效
‘6A’	‘81’	不支持此功能
‘93’	‘03’	应用永久锁定
‘64’	‘00’	状态标志位未变
‘65’	‘81’	内存失败
‘67’	‘00’	Lc 长度错误
‘69’	‘82’	不满足安全状态
‘69’	‘84’	引用数据无效
‘69’	‘87’	安全报文数据项丢失
‘69’	‘88’	安全报文数据项不正确
‘6A’	‘86’	P1 和 P2 错误
‘6A’	‘88’	未找到引用数据

‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

A.3.2 APPLICATION UNBLOCK（应用解锁）命令

A.3.2.1 定义和范围

APPLICATION UNBLOCK命令用于恢复当前电子钱包应用，该指令只能在特殊终端上使用。

当APPLICATION UNBLOCK命令成功地完成后，由APPLICATION BLOCK命令产生的对应用命令响应的限制将被取消。

A.3.2.2 命令报文

APPLICATION UNBLOCK命令报文编码见表A.57。

表A.57 APPLICATION UNBLOCK 命令报文

代码	值
CLA	‘84’
INS	‘18’
P1	‘00’，其他值预留
P2	‘00’，其他值预留
Lc	数据字节数
Data	报文鉴别码（MAC）数据元
Le	不存在

A.3.2.3 命令报文数据域

报文鉴别码（MAC）数据元。根据《城市公共交通IC卡安全技术规范》，由应用解锁过程密钥计算。

A.3.2.4 响应报文数据域

响应报文数据域不存在。

A.3.2.5 响应报文状态字

当应用被临时锁定时，此命令执行成功的状态字是“9000”。

当应用未被临时锁定，此命令执行返回的状态字是使用条件不满足（SW1 SW2=“6985”）。

IC卡可能回送的错误状态字见表A.58。

表A.58 APPLICATION UNBLOCK 错误状态

SW1	SW2	含 义
‘64’	‘00’	标志状态位未变
‘65’	‘81’	内存失败
‘67’	‘00’	Lc 错误
‘69’	‘82’	不满足安全状态
‘69’	‘84’	未取随机数
‘69’	‘85’	使用条件不满足
‘69’	‘87’	安全报文数据项丢失

‘69’	‘88’	安全报文数据项不正确
‘6A’	‘82’	文件未找到
‘6A’	‘86’	P1 和 P2 错误
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘03’	应用已被永久锁定

A. 3.3 EXTERNAL AUTHENTICATION（外部认证）命令

A. 3.3.1 定义和范围

EXTERNAL AUTHENTICATION命令要求IC卡中的应用验证密码。

IC卡的响应包括命令处理状态的回送。

A. 3.3.2 命令报文

EXTERNAL AUTHENTICATION命令报文编码见表A. 59。

表A. 59 EXTERNAL AUTHENTICATION 命令报文

代码	值
CLA	‘00’
INS	‘82’
P1	‘00’
P2	‘00’
Lc	8-16
Data	发卡机构认证数据
Le	不存在

EXTERNAL AUTHENTICATION命令使用的算法参考值（P1）编码为‘00’表示无信息。算法参考值在命令发出之前是已知的，或者在数据域中提供。

EXTERNAL AUTHENTICATION命令的参数P2为‘00’时的含义是无信息。P2的值可事先得到，也可以在数据域中提供。

A. 3.3.3 命令报文数据域

命令报文数据域中包含8-16字节的数据：

- 前 8 个必备型字节包含密码；
- 可选的 1-8 个附加字节是专用的信息。

A. 3.3.4 响应报文数据域

响应报文数据域不存在。

A. 3.3.5 响应报文状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的警告状态字见表A. 60。

表A. 60 EXTERNAL AUTHENTICATION 警告状态

SW1	SW2	含 义
-----	-----	-----

‘63’	‘CX’	认证失败（X 代表剩余尝试次数）
------	------	------------------

IC卡可能回送的错误状态字见表A. 61。

表A. 61 EXTERNAL AUTHENTICATION 错误状态

SW1	SW2	含 义
‘67’	‘00’	Lc 不正确
‘69’	‘83’	认证方法锁定
‘6A’	‘86’	P1 和 P2 错误
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

A. 3. 4 GET CHALLENGE（取随机数）命令

A. 3. 4. 1 定义和范围

GET CHALLENGE命令请求一个用于安全相关过程（如安全报文）的随机数。

该随机数只能用于下一条指令，无论下一条指令是否使用了该随机数，该随机数都将立即失效。

A. 3. 4. 2 命令报文

GET CHALLENGE命令报文编码见表A. 62。

表A. 62 GET CHALLENGE 命令报文

代码	值
CLA	‘00’
INS	‘84’
P1	‘00’
P2	‘00’
Lc	不存在
Data	不存在
Le	‘04’ 或 ‘08’

A. 3. 4. 3 命令报文数据域

命令报文数据域不存在。

A. 3. 4. 4 响应报文数据域

响应报文数据域包括随机数，长度为4字节或8字节。

A. 3. 4. 5 响应报文状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的错误状态字见表A. 63。

表A. 63 GET CHALLENGE 错误状态

SW1	SW2	含 义
‘6A’	‘81’	不支持此功能
‘6A’	‘86’	P1 和 P2 错误

'6D'	'00'	INS 不支持或错误
'6E'	'00'	CLA 不支持或错误

A. 3.5 INTERNAL AUTHENTICATION (内部认证) 命令

A. 3.5.1 定义和范围

INTERNAL AUTHENTICATION命令提供了利用接口设备发来的随机数和自身存储的相关密钥进行数据认证的功能。

A. 3.5.2 命令报文

INTERNAL AUTHENTICATION命令报文编码见表A. 64。

表A. 64 INTERNAL AUTHENTICATION 命令报文

代码	值
CLA	'00'
INS	'88'
P1	'00'
P2	'00'
Lc	认证数据的长度
Data	认证数据
Le	'00'

INTERNAL AUTHENTICATION命令的参数P1为'00'时的含义是无信息。P1的值可事先得到，也可以在数据域中提供。

INTERNAL AUTHENTICATION命令的参数P2为'00'时的含义是无信息。P2的值可事先得到，也可以在数据域中提供。

A. 3.5.3 命令报文数据域

命令报文数据域的内容是应用专用的认证数据。

A. 3.5.4 响应报文数据域

响应报文数据域内容是相关认证数据，其格式和定义不在JR/T 0025的范围之内。

A. 3.5.5 响应报文状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的警告状态字见表A. 65。

表A. 65 INTERNAL AUTHENTICATION 警告状态

SW1	SW2	含 义
'62'	'81'	回送的数据可能有错

IC卡可能回送的错误状态字见表A. 67。

表A. 66 INTERNAL AUTHENTICATION 错误状态

SW1	SW2	含 义
'64'	'00'	标志状态位未变

‘67’	‘00’	Lc 域不存在
‘68’	‘82’	不支持安全报文
‘69’	‘85’	不满足使用条件
‘6A’	‘80’	数据域参数不正确
‘6A’	‘86’	P1 和 P2 错误
‘6D’	‘00’	INS 不支持或错误

A.3.6 READ BINARY（读二进制文件）命令

A.3.6.1 定义和范围

READ BINARY命令用于读取二进制文件的内容（或部分内容）。

A.3.6.2 命令报文

READ BINARY命令报文编码见表A. 67。

表A. 67 READ BINARY 命令报文

代码	值
CLA	‘00’ 或 ‘04’
INS	‘B0’
P1	见表 A. 69
P2	从文件中读取的第一个字节的偏移地址
Lc	不存在；（CLA=‘04’ 时除外）
Data	不存在；（CLA=‘04’ 时，应包括 MAC）
Le	‘00’

表A. 68定义了命令报文中的引用控制参数。

表A. 68 READ BINARY 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含 义
X								读取模式： -用 SFI 方式
1								
	0	0						RFU（如果 b8=1）
			X	X	X	X	X	SFI（取值范围 21-30）

A.3.6.3 命令报文数据域

一般情况下，命令报文数据域不存在。当使用安全报文时，命令报文数据域中应包含MAC。MAC的计算方法和长度由应用决定。

A.3.6.4 响应报文数据域

当Le的值为零时，只要文件的最大长度在256（短长度）或65536（扩展长度）之内，则其全部字节将被读出。

A.3.6.5 响应报文状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的警告状态字见表A. 69。

表A. 69 READ BINARY 警告状态

SW1	SW2	含 义
‘62’	‘81’	部分回送的数据可能有错
‘62’	‘82’	文件长度<Le

IC卡可能回送的错误状态字见表A. 70。

表A. 70 READ BINARY 错误状态

SW1	SW2	含 义
‘67’	‘00’	长度错误（Lc 域为空）
‘69’	‘81’	命令与文件结构不相容
‘69’	‘82’	不满足安全状态
‘69’	‘86’	不满足命令执行的条件（非当前 EF）
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘86’	P1 和 P2 错误
‘6B’	‘00’	参数错误（偏移地址超出了 EF）
‘6C’	‘XX’	长度错误（Le 错误；‘XX’ 为实际长度）
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

A. 3. 7 UPDATE BINARY（更新二进制文件）命令

A. 3. 7. 1 定义和范围

UPDATE BINARY命令报文使用C-APDU中给定的数据修改EF文件中已有的数据。

A. 3. 7. 2 命令报文

UPDATE BINARY命令报文编码见表A. 71。

表A. 71 UPDATE BINARY 命令报文

代码	值
CLA	‘00’ 或 ‘04’
INS	‘D6’
P1	见表 A. 73
P2	要修改的第一个字节的偏移地址
Lc	后续数据域的长度
Data	修改用的数据+报文鉴别码（MAC）数据元（4 字节）
Le	不存在

CLA=‘00’ 不需要安全报文。

CLA=‘04’ 需要安全报文。

表A. 72定义了命令报文中的引用控制参数。

表A. 72 UPDATE BINARY 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含 义
X								读取模式：
1								-用 SFI 方式
	0	0						RFU（如果 b8=1）
			X	X	X	X	X	SFI（取值范围 21-30）

A. 3. 7. 3 命令报文数据域

命令报文数据域：包括更新原有数据的新数据。

报文鉴别码（MAC）数据元：4字节。

A. 3. 7. 4 响应报文数据域

响应报文数据域不存在。

A. 3. 7. 5 响应报文状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的警告状态字见表A. 73。

表A. 73 UPDATE BINARY 警告状态

SW1	SW2	含 义
‘63’	‘CX’	使用内部重试程序更新成功，其中 X 表示剩余重试次数。

IC卡可能回送的错误状态字见表A. 75。

表A. 74 UPDATE BINARY 错误状态

SW1	SW2	含 义
‘65’	‘81’	内存失败（修改失败）
‘67’	‘00’	长度错误（Lc 域为空）
‘69’	‘81’	命令与文件结构不相容
‘69’	‘82’	不满足安全状态
‘69’	‘84’	引用数据无效
‘69’	‘86’	不满足命令执行的条件（不是当前的 EF）
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘86’	P1 和 P2 参数错误
‘6B’	‘00’	参数错误（偏移地址超出了 EF）
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘03’	应用永久锁定

A. 3. 8 CREDIT FOR LOAD（圈存）命令

A. 3. 8. 1 定义和范围

圈存（CREDIT FOR LOAD）命令用于圈存交易。

A.3.8.2 命令报文

圈存 (CREDIT FOR LOAD) 命令报文见表A.75。

表A.75 圈存 (CREDIT FOR LOAD) 命令报文

代码	值
CLA	‘80’
INS	‘52’
P1	‘00’
P2	‘00’
L _c	‘0B’
Data	见表 A.77
L _e	‘04’

A.3.8.3 命令报文数据域

表A.76描述了命令报文数据域。

表A.76 圈存 (CREDIT FOR LOAD) 命令报文数据域

说明	长度 (字节)
交易日期 (主机)	4
交易时间 (主机)	3
MAC2	4

A.3.8.4 响应报文数据域

圈存 (CREDIT FOR LOAD) 响应报文数据域见表A.77。

如果命令执行不成功, 则只在响应报文中回送SW1和SW2。

表A.77 圈存 (CREDIT FOR LOAD) 响应报文数据域

说明	长度 (字节)
TAC	4

A.3.8.5 响应报文的状况字

此命令执行成功的状态字是“9000”。

表A.78描述了IC卡可能回送的错误状态。

表A.78 圈存 (CREDIT FOR LOAD) 错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘01’	命令不接受 (无效状态)
‘69’	‘85’	使用条件不满足
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘02’	MAC 无效

A.3.9 DEBIT FOR PURCHASE (消费) 命令

A.3.9.1 定义和范围

消费（DEBIT FOR PURCHASE）命令用于消费交易。

A.3.9.2 命令报文

消费（DEBIT FOR PURCHASE）命令报文见表A.79。

执行初始化消费（INITIALIZE FOR PURCHASE）后即选择了消费交易。

表A.79 消费（DEBIT FOR PURCHASE）命令报文

代码	值
CLA	‘80’
INS	‘54’
P1	‘01’
P2	‘00’
L _c	‘0F’
Data	见表 A.81
L _e	‘08’

A.3.9.3 命令报文数据域

表A.80描述了命令报文数据域。

表A.80 消费 DEBIT FOR PURCHASE 命令报文数据域

说明	长度（字节）
终端交易序号	4
交易日期（终端）	4
交易时间（终端）	3
MAC1	4

A.3.9.4 响应报文数据域

此命令执行成功的响应报文数据域见表A.81。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表A.81 消费 DEBIT FOR PURCHASE 响应报文数据域

说明	长度（字节）
TAC	4
MAC2	4

A.3.9.5 响应报文的狀態字

此命令执行成功的状态字是“9000”。

表A.82描述了IC卡可能回送的错误状态。

表A.82 消费（DEBIT FOR PURCHASE）错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误

‘69’	‘01’	命令不接受（无效状态）
‘69’	‘85’	使用条件不满足
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘02’	MAC 无效

A. 3. 10 DEBIT FOR UNLOAD（圈提）命令

A. 3. 10. 1 定义和范围

圈提（DEBIT FOR UNLOAD）命令用于圈提交易。该指令只能在特殊终端上使用。

A. 3. 10. 2 命令报文

圈提（DEBIT FOR UNLOAD）命令报文见表A. 83。

表A. 83 圈提（DEBIT FOR UNLOAD）命令报文

代码	值
CLA	‘80’
INS	‘54’
P1	‘03’
P2	‘00’
L _c	‘0B’
Data	见表 A. 85
L _e	‘04’

A. 3. 10. 3 命令报文数据域

表A. 84定义了命令报文数据域。

表A. 84 圈提（DEBIT FOR UNLOAD 命）令报文数据域

说明	长度（字节）
交易日期（主机）	4
交易时间（主机）	3
MAC2	4

A. 3. 10. 4 响应报文数据域

此命令执行成功的响应报文数据域见表A. 85。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表A. 85 圈提（DEBIT FOR UNLOAD）响应报文数据域

说明	长度（字节）
MAC3	4

A. 3. 10. 5 响应报文的状态字

此命令执行成功的状态字是“9000”。

表A. 86描述了IC卡可能回送的错误状态。

表A. 86 圈提（DEBIT FOR UNLOAD）错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘01’	命令不接受（无效状态）
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘02’	MAC 无效

A. 3. 11 GET BALANCE（查询余额）命令

A. 3. 11. 1 定义和范围

查询余额（GET BALANCE）命令用于读取电子钱包余额，实现查询余额交易。

A. 3. 11. 2 命令报文

查询余额（GET BALANCE）命令报文见表A. 87。

表A. 87 查询余额（GET BALANCE）命令报文

代码	值
CLA	‘80’
INS	‘5C’
P1	‘00’
P2	‘02’
Lc	不存在
Data	不存在
Le	‘04’

A. 3. 11. 3 响应报文数据域

命令执行成功的响应报文数据域见表A. 88。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表A. 88 查询余额（GET BALANCE）响应报文数据域

说明	长度（字节）
电子钱包余额	4

A. 3. 11. 4 响应报文的响应字

此命令执行成功的响应字是“9000”。

表A. 89描述了IC卡可能回送的错误状态。

表A. 89 查询余额（GET BALANCE）错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘69’	‘85’	使用条件不满足
‘69’	‘82’	安全条件不满足

‘6A’	‘86’	P1 和 P2 参数不正确
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

A. 3. 12 GET TRANSACTION PROVE（取交易认证）命令

A. 3. 12. 1 定义和范围

取交易认证（GET TRANSACTION PROVE）命令提供了一种在交易处理过程中拔出并重插卡后卡片的恢复机制。该命令的用法在5. 6中说明。

A. 3. 12. 2 命令报文

取交易认证（GET TRANSACTION PROVE）命令报文见表A. 90。

表A. 90 取交易认证（GET TRANSACTION PROVE）命令报文

代码	值
CLA	‘80’
INS	‘5A’
P1	‘00’
P2	要取的 MAC 或/和 TAC 所对应的交易类型标识。
Lc	‘02’
Data	见表 A. 92
Le	‘08’

A. 3. 12. 3 命令报文数据域

表A. 91定义了命令报文数据域。

表A. 91 取交易认证（GET TRANSACTION PROVE）命令报文数据域

说明	长度（字节）
要取的 MAC 或/和 TAC 所对应的交易序号。	2

如果命令中指定的交易类型标识和交易序号对应的MAC或TAC可用，则响应报文数据域见表A. 93。

表A. 92 取交易认证（GET TRANSACTION PROVE）响应报文数据域

说明	长度
MAC	4
TAC	4

A. 3. 12. 4 响应报文的状态字

此命令执行成功的状态字是“9000”。

表A. 93描述了IC卡可能回送的错误状态。

表A. 93 取交易认证（GET TRANSACTION PROVE）错误状态

SW1	SW2	含义
‘65’	‘81’	内存错误
‘69’	‘85’	使用条件不满足
‘6D’	‘00’	INS 不支持或错误

‘6E’	‘00’	CLA 不支持或错误
‘94’	‘06’	所需 MAC 不可用

A. 3. 13 INITIALIZE FOR LOAD（初始化圈存）命令

A. 3. 13. 1 定义和范围

初始化圈存（INITIALIZE FOR LOAD）命令用于初始化圈存交易。

A. 3. 13. 2 命令报文

初始化圈存（INITIALIZE FOR LOAD）命令报文见表A. 94。

表A. 94 初始化圈存（INITIALIZE FOR LOAD）命令报文

代码	值
CLA	‘80’
INS	‘50’
P1	‘00’
P2	‘02’
L _c	‘0B’
Data	见表 A. 96
L _e	‘10’

A. 3. 13. 3 命令报文数据域

表A. 95定义了命令报文数据域。

表A. 95 初始化圈存（INITIALIZE FOR LOAD）命令报文数据域

说明	长度（字节）
密钥索引号	1
交易金额	4
终端机编号	6

A. 3. 13. 4 响应报文数据域

此命令执行成功的响应报文数据域见表A. 96。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表A. 96 初始化圈存（INITIALIZE FOR LOAD）响应报文

说明	长度（字节）
电子钱包余额	4
交易序号	2
密钥版本号（DLK）	1
算法标识（DLK）	1
伪随机数（IC 卡）	4
MAC1	4

A. 3. 13. 5 响应报文的状态字

此命令执行成功的状态字是“9000”。

表A. 97描述了IC卡可能回送的错误状态。

表A. 97 初始化圈存（INITIALIZE FOR LOAD）错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘85’	使用条件不满足
‘6A’	‘81’	功能不支持
‘6A’	‘86’	P1 和 P2 参数不正确
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘94’	‘03’	密钥索引不支持

A. 3. 14 INITIALIZE FOR PURCHASE（初始化消费）命令

A. 3. 14. 1 定义和范围

初始化消费（INITIALIZE FOR PURCHASE）命令用于初始化消费交易。

A. 3. 14. 2 命令报文

初始化消费（INITIALIZE FOR PURCHASE）命令报文见表A. 98。

表A. 98 初始化消费（INITIALIZE FOR PURCHASE）命令报文

代码	值
CLA	‘80’
INS	‘50’
P1	‘01’
P2	‘02’
L _c	‘0B’
Data	见表 A. 100
L _e	‘0F’

A. 3. 14. 3 命令报文数据域

表A. 99定义了命令报文的数据域。

表A. 99 初始化消费（INITIALIZE FOR PURCHASE）命令报文数据域

说明	长度（字节）
密钥索引号	1
交易金额	4
终端机编号	6

A. 3. 14. 4 响应报文数据域

此命令执行成功的响应报文数据域见表A. 100。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表A. 100 初始化消费（INITIALIZE FOR PURCHASE）响应报文数据域

说明	长度（字节）
电子钱包余额	4
交易序号	2
透支限额	3
密钥版本号（DPK）	1
算法标识（DPK）	1
伪随机数（IC 卡）	4

A. 3. 14. 5 响应报文的状态字

此命令执行成功的状态字是“9000”。

表A. 101描述了IC卡可能回送的错误状态。

表A. 101 初始化消费（INITIALIZE FOR PURCHASE）错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘69’	‘85’	使用条件不满足
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘94’	‘01’	金额不足
‘94’	‘03’	密钥索引不支持

A. 3. 15 INITIALIZE FOR UNLOAD（初始化圈提）命令

A. 3. 15. 1 定义和范围

初始化圈提（INITIALIZE FOR UNLOAD）命令用于初始化圈提交易。

A. 3. 15. 2 命令报文

初始化圈提（INITIALIZE FOR UNLOAD）命令报文见表A. 102。

表A. 102 初始化圈提（INITIALIZE FOR UNLOAD）命令报文

代码	值
CLA	‘80’
INS	‘50’
P1	‘05’
P2	‘02’
L _c	‘0B’
Data	见表 A. 104
L _e	‘10’

A. 3. 15. 3 命令报文数据域

表A. 103定义了命令报文的数据域。

表A. 103 初始化圈提（INITIALIZE FOR UNLOAD）命令报文数据域

说明	长度（字节）
密钥索引号	1
交易金额	4
终端机编号	6

A. 3. 15. 4 响应报文数据域

此命令执行成功的响应报文数据域见表A. 104。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表A. 104 初始化圈提（INITIALIZE FOR UNLOAD）响应报文数据域

说明	长度（字节）
电子钱包余额	4
交易序号	2
密钥版本号（DULK）	1
算法标识（DULK）	1
伪随机数（IC 卡）	4
MAC1	4

A. 3. 15. 5 响应报文的状态字

此命令执行成功的状态字是“9000”。

表A. 105描述了IC卡可能回送的错误状态。

表A. 105 初始化圈提（INITIALIZE FOR UNLOAD）错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘85’	使用条件不满足
‘6A’	‘86’	P1 和 P2 参数不正确
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘94’	‘01’	金额不足
‘94’	‘03’	密钥索引不支持

A. 3. 16 INITIALIZE FOR UPDATE（修改初始化）命令

A. 3. 16. 1 定义和范围

INITIALIZE FOR UPDATE命令用于初始化修改透支限额交易。

A. 3. 16. 2 命令报文

INITIALIZE FOR UPDATE命令报文见表A. 106。

表A. 106 修改初始化（INITIALIZE FOR UPDATE）命令报文

代码	值
CLA	‘80’
INS	‘50’
P1	‘04’
P2	‘01’
L _c	‘07’
Data	见表 A. 108
L _e	‘13’

A. 3. 16. 3 命令报文数据域

表A. 107定义了命令报文的数据域。

表A. 107 修改初始化（INITIALIZE FOR UPDATE）命令报文数据域

说明	长度（字节）
密钥索引号	1
终端机编号	6

A. 3. 16. 4 响应报文数据域

命令执行成功的响应报文数据域见表A. 108。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表A. 108 修改初始化（INITIALIZE FOR UPDATE）响应报文数据域

说明	长度（字节）
电子钱包余额	4
交易序号	2
原透支限额	3
密钥版本号（DUK）	1
算法标识（DUK）	1
伪随机数（IC 卡）	4
MAC1	4

A. 3. 16. 5 响应报文的状态字

此命令执行成功的状态字是“9000”。

表A. 109描述了IC卡可能回送的错误状态。

表A. 109 修改初始化（INITIALIZE FOR UPDATE）错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘85’	使用条件不满足
‘6A’	‘86’	P1 和 P2 参数不正确
‘6D’	‘00’	INS 不支持或错误

‘6E’	‘00’	CLA 不支持或错误
‘94’	‘03’	密钥索引不支持

A. 3. 17 INITIALIZE FOR CAPP PURCHASE（初始化复合应用消费）命令

A. 3. 17. 1 定义和范围

INITIALIZE FOR CAPP PURCHASE命令用于初始化复合应用消费交易。

A. 3. 17. 2 命令报文

INITIALIZE FOR CAPP PURCHASE命令报文见表A. 110。

表A. 110 INITIALIZE FOR CAPP PURCHASE 命令报文格式

代码	值
CLA	‘80’
INS	‘50’
P1	‘03’
P2	‘02’
Lc	‘0B’
Data	见 A. 112
Le	‘0F’

A. 3. 17. 3 命令报文数据域

此命令报文的数据域定义见表A. 111。

表A. 111 INITIALIZE FOR CAPP PURCHASE 命令报文的数据域定义

说明	长度（字节）
密钥索引号	1
交易金额	4
终端机编号	6

A. 3. 17. 4 响应报文数据域

此命令执行成功的响应报文数据域见表A. 112。

表A. 112 INITIALIZE FOR CAPP PURCHASE 命令执行成功的响应报文数据域

说明	长度（字节）
电子钱包余额	4
电子钱包交易序号	2
透支限额	3
密钥算法版本号（DPK）	1
密钥标识（DPK）	1
伪随机数（IC 卡）	4

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

A. 3. 17. 5 响应报文的状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的错误状态见表A. 113。

表A. 113 INITIALIZE FOR CAPP PURCHASE 命令可能回送的错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘69’	‘85’	使用条件不满足
‘94’	‘01’	金额不足
‘94’	‘03’	密钥索引不支持
‘94’	‘02’	交易计数器达到最大值
‘94’	‘08’	应用灰锁锁定

A. 3. 18 UPDATE CAPP DATA CACHE（更新复合用数据缓存）命令

A. 3. 18. 1 定义和范围

UPDATE CAPP DATA CACHE命令用于复合应用消费交易中更新复合应用数据缓存，缓存数据将被DEBIT FOR CAPP PURCHASE命令用于改写复合应用专用文件中相关记录。

A. 3. 18. 2 命令报文

此命令报文见表A. 114。

表A. 114 UPDATE CAPP DATA CACHE 命令报文

代码	值
CLA	‘80’
INS	‘DC’
P1	复合应用类型标识符
P2	见表 A. 116
Lc	后续数据域的长度
Data	记录内容
Le	不存在

此命令报文中的引用控制参数P2定义见表A. 115。

表A. 115 UPDATE CAPP DATA CACHE 命令报文中的引用控制参数 P2 定义

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	—	—	—	RFU
x	x	x	x	x	—	—	—	SFI
1	1	1	1	1	—	—	—	RFU
—	—	—	—	—	0	0	0	第一个标识符出现的记录
—	—	—	—	—	x	x	x	RFU
其它值								RFU

A. 3. 18. 3 命令报文数据域

此命令报文数据域由更新原有记录的新记录组成。

A. 3. 18. 4 响应报文数据域

响应报文数据域不存在。

A. 3. 18. 5 响应报文的状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的错误状态字见表A. 116。

表A. 116 UPDATE CAPP DATA CACHE 可能回送的错误状态字

SW1	SW2	含 义
‘65’	‘81’	内存失败（修改失败）
‘67’	‘00’	长度错误（Lc 域为空）
‘69’	‘81’	命令与文件结构不相容
‘69’	‘82’	不满足安全状态
‘69’	‘86’	不满足命令执行的条件（不是当前的 EF）
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到记录
‘6A’	‘84’	文件中存储空间不够
‘94’	‘07’	复合应用禁止

A. 3. 19 DEBIT FOR CAPP PURCHASE（复合应用消费）命令

A. 3. 19. 1 定义和范围

DEBIT FOR CAPP PURCHASE命令用于复合应用消费交易。

A. 3. 19. 2 命令报文

此命令报文见表 A.117。

表A. 117 DEBIT FOR CAPP PURCHASE 命令报文

代码	值
CLA	‘80’
INS	‘54’
P1	‘01’
P2	‘00’
Lc	‘0F’
Data	见表 A. 119
Le	‘08’

A. 3. 19. 3 命令报文数据域

此命令报文的数据域定义见表A. 118。

表A. 118 DEBIT FOR CAPP PURCHASE 命令报文的数据域定义

说明	长度（字节）
终端交易序号	4

交易日期	4
交易时间	3
MAC1	4

A. 3. 19. 4 响应报文数据域

此命令执行成功的响应报文数据域见表A. 119。

表A. 119 DEBIT FOR CAPP PURCHASE 命令执行成功的响应报文数据域

说明	长度（字节）
TAC	4
MAC2	4

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

A. 3. 19. 5 响应报文的狀態字

此命令执行成功的状态字是“9000”。

IC卡可能回送的错误状态见表A. 120。

表A. 120 DEBIT FOR CAPP PURCHASE 可能回送的错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘01’	命令不接受（无效状态）
‘69’	‘85’	使用条件不满足
‘93’	‘01’	金额不足
‘93’	‘02’	MAC 无效

A. 3. 20 APPEND RECORD（增加记录命令）

A. 3. 20. 1 定义和范围

APPEND RECORD命令用于对变长记录文件追加新记录。

A. 3. 20. 2 命令报文

增加记录命名报文编码在表A. 121中。

表A. 121 APPEND RECORD 命令报文编码

代码	值
CLA	‘04’ 或 ‘00’
INS	‘E2’
P1	‘00’
P2	见表 F. 2
Lc	后续数据域的长度
Data	追加的新记录+报文鉴别码（MAC）数据元（4 字节）
Le	不存在

表A. 122定义了命令报文中的引用控制参数。

表A. 122 APPEND RECORD 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含义
x	x	x	x	x				SFI
					0	0	0	追加新记录

A. 3. 20. 3 命令报文数据域

命令报文数据域由追加的新记录和报文鉴别码（MAC）组成。

A. 3. 20. 4 响应报文数据域

响应报文数据域不存在。

A. 3. 20. 5 响应报文状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的错误状态字如表A. 123所示。

表A. 123 APPEND RECORD 错误状态

SW1	SW2	含义
65	81	内存失败
67	00	长度错误
69	81	命令与文件结构不相容
69	82	不满足安全状态
6A	81	不支持此功能
6A	82	未找到文件
6A	84	文件中存储空间不够

A. 3. 21 UPDATE OVERDRAW LIMIT（修改透支限额）命令

A. 3. 21. 1 定义和范围

UPDATE OVERDRAW LIMIT命令用于修改透支限额交易。

A. 3. 21. 2 命令报文

修改透支限额（UPDATE OVERDRAW LIMIT）命令报文见表A. 124。

表A. 124 修改透支限额（UPDATE OVERDRAW LIMIT）命令报文

代码	值
CLA	‘80’
INS	‘58’
P1	‘00’
P2	‘00’
LC	‘0E’
Data	见表 A. 126
Le	‘04’

A. 3. 21. 3 命令报文数据域

表A. 125定义了命令报文的数据域。

表A. 125 修改透支限额（UPDATE OVERDRAW LIMIT）命令报文数据域

说明	长度（字节）
新透支限额	3
交易日期（发卡方）	4
交易时间（发卡方）	3
MAC2	4

A. 3. 21. 4 响应报文数据域

此命令执行成功的响应报文数据域见表A. 126。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表A. 126 修改透支限额（UPDATE OVERDRAW LIMIT）响应报文数据域

说明	长度（字节）
TAC	4

A. 3. 21. 5 响应报文的状态字

此命令执行成功的状态字是“9000”。

表A. 127描述了IC卡可能回送的错误状态。

表A. 127 修改透支限额（UPDATE OVERDRAW LIMIT）错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘00’	不能处理
‘69’	‘01’	命令不接受（无效状态）
‘69’	‘85’	使用条件不满足
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘02’	MAC 无效

附 录 B
(规范性附录)

电子现金扩展应用文件短文件标识符定义

对扩展应用文件短文件标识符 (SFI) 做出如表 B.1 所示。

表 B.1 扩展应用文件短文件标识符及开通密钥定义

扩展应用类型	扩展应用文件 SFI	开通密钥
城际客运应用	0x13	预设
轮渡应用	0x14	预设
轨道交通应用	0x15	预设
公共汽电车应用	0x16	预设
停车收费咪表应用	0x18	预设
城际铁路应用	0x19	预设
城市公共交通 IC 卡互联互通应用	0x1A、0x1E	预设
保留应用	0x1C、0x1D	预设

附 录 C

（规范性附录）

卡片与发卡机构数据元

本章节列出了本规范所用的卡片和发卡机构数据元，包括的格式有：格式（F）、标签（T）和长度（L）。

支持的格式有：

- n（数字型）；
- cn（压缩数字型）；
- b（二进制）；
- an（字母数字）；
- ans（特殊字母数字）。

当数据定义的长度超过数据实际长度，而位数没有占满时，补位规则如下：

- 格式 n 的数据元右对齐，左补 0；
- 格式 cn 的数据元左对齐，右补 F；
- 格式 an 的数据元左对齐，右补 0；
- 格式 ans 的数据元左对齐，右补 0。

需求列中列出的是对数据元的需求情况：

- M（必备）：此数据应存在并提供给终端，终端在读应用数据过程中，如果没有读到必备数据，终端终止交易；
- R（需求）：数据应存在，在读应用数据过程中，终端不检查；
- C（有条件）：在一定条件下应存在；
- O（可选）：可选数据元。

当一个数据元从一方传递到另一方时（例如：从卡片传递到终端），不论该数据元原来是如何被存储的，应当将该数据元从高字节至低字节传递。构造数据时也应遵循此规则。

表C.1 卡片电子现金标准数据元

名字（格式、标签和长度）	需求	描述	值
应用密文（AC） F: b64 T: 9F26 L: 8	R	生成应用密文命令返回的密文	
应用货币代码 F: n3 T: 9F42 L: 2	C 如果 CVM 中要求金额检查，需要此数据。	按 GB/T 12406 编码	
应用货币代码 F: n3 T: 9F51 L: 2	C 如果执行频度检查	本规范专有数据。按 GB/T 12406 编码	
应用货币指数 F: n1	O	指出金额数据中小数点从最右边开始第几个位置	

名字(格式、标签和长度)	需求	描述	值
T: 9F44 L: 1			
应用缺省行为 (ADA) F: b16 T: 9F52 L: 2	C 如果支持发卡机构认证。专有数据。	定义在一些特定条件下卡片执行的发卡机构指定的行为。如果卡片中没有此数据, 缺省认为全零	字节 1: 位 8: 1=如果发卡机构认证失败, 下次联机交易 位 7: 1=如果发卡机构认证执行但失败, 拒绝交易 位 6: 1=如果发卡机构认证必备但没有收到 ARPC, 拒绝交易 位 5: 1=如果交易拒绝, 生成通知 位 4: 1=如果 PIN 在本次交易中尝试次数超限而且交易拒绝, 生成通知 位 3: 1=如果因为发卡机构认证失败或没有执行导致交易拒绝, 生成通知 位 2: 1=如果是新卡, 联机交易 位 1: 1=如果是新卡, 当交易无法联机时拒绝交易 字节 2: 位 8: 1=如果 PIN 在本次交易中尝试次数超限, 应用锁定 位 7: 1=如果 PIN 在前次交易中尝试次数超限, 拒绝交易 位 6: 1=如果 PIN 在前次交易中尝试次数超限, 联机交易 位 5: 1=如果 PIN 在前次交易中尝试次数超限, 当交易无法联机时拒绝交易 位 4: 1=如果发卡机构脚本命令在前次交易中失败, 联机交易 位 3: 1=如果 PIN 在前次交易中尝试次数超限, 拒绝交易并锁应用 位 2 - 1: RFU (000)
应用自定义数据 F: b8 - 256 T: 9F05 L: 1 - 32	0	和卡片应用有关的发卡机构指定数据	
应用生效日期 F: n6 YYMMDD T: 5F25 L: 3	0	卡片中应用启用日期	
应用失效日期 F: n6 YYMMDD	M	卡片中应用的失效日期	

名字(格式、标签和长度)	需求	描述	值
T: 5F24 L: 3			
应用文件定位器 (AFL) F: var. T: 94 L: var. 最大 252	R	指出和应用相关的数据存放位置(短文件标识符和记录号)	对于每一个要读的文件, AFL 包括 4 个字节: 字节 1: 位 8-4=SFI 短文件标识符 位 3-1=000 字节 2: 文件中要读的第 1 个记录的记录号(不能为 0) 字节 3: 文件中要读的最后一个记录的记录号(等于或大于字节 2) 字节 4: 从字节 2 中的记录号开始, 存放认证用静态数据记录的个数(值从 0 到字节 3-字节 2+1 的值)
应用标识符 (AID) F: b40-128 T: 4F L: 5-16	R	按 GB/T 16649.5 规定标识应用。由注册的应用提供商标识 (RID) 和扩展的专用应用标识符 (PIX) 组成	
应用交互特征 (AIP) F: b16 T: 82 L: 2	M	一个列表, 说明此应用中卡片支持指定功能的能力	字节 1: 位 8: 1=RFU 位 7: 1=支持 SDA 位 6: 1=支持 DDA 位 5: 1=支持持卡人认证 位 4: 1=执行终端风险管理 位 3: 1=支持发卡机构认证 位 2: RFU (0) 位 1: 1=支持 CDA 字节 2: RFU (“00”)
应用标签 F: ans1-16 T: 50 L: 1-16	R	和 AID 相关的便于记忆的数据。 用于应用选择。存在于 ADF 的 FCI 中(可选)和 ADF 目录入口中(必备)	
应用首选名称 F: ans1-16 T: 9F12 L: 1-16	0	和 AID 相关的便于记忆的数据。如果终端支持在发卡机构代码表索引数据中指定的字符类型, 终端在应用选择过程中显示应用首选名称	
应用主账号 (PAN) F: var. 最大 cn19	M	持卡人有效账号	

名字(格式、标签和长度)	需求	描述	值
T: 5A L: var. 最大 10			
应用主账号序列号 F: n2 T: 5F34 L: 1	0	用来表示卡片中使用同一个账号的不同应用	
应用优先指示器 F: b8 T: 87 L: 1	C	如果卡片中有多个应用, 指出同一目录中的应用的优先级	位 8 1: 没有持卡人确认应用不能选择 0: 没有持卡人确认应用可以选择 位 7-5: RFU (000) 位 4-1: 0000: 不指定优先级 xxxx: 应用显示和选择的顺序, 从 1-15.1 的优先级最高
应用模板 F: b T: 61 L: var. 最大 252	C 如果有 PPSE	按 GB/T 16649.5 的规定, 包含和应用目录入口相关的 1 个或多个数据对象	
应用交易计数器 F: b 16 T: 9F36 L: 2.	R	记录个人化以后交易处理的次数。由卡片中的应用维护	初始值为 0, 执行一次交易加 1
应用用途控制 F: b 16 T: 9F07 L: 2	0	标明发卡机构指定的卡片应用上的一些限制, 包括地域使用和服务类型等。	字节 1: 位 8: 1=国内现金交易有效 位 7: 1=国际现金交易有效 位 6: 1=国内商品有效 位 5: 1=国际商品有效 位 4: 1=国内服务有效 位 3: 1=国际服务有效 位 2: 1=RFU 位 1: 1=RFU 字节 2: 位 8: 1=允许国内返现 位 7: 1=允许国际返现 位 6-1: RFU (000000) 限制: 字节 1 中, 位 4, 6 值相同; 位 3, 5 值相同
应用版本号 F: b16 T: 9F08	M	城市公共交通 IC 卡系统给应用分配的版本号	

名字(格式、标签和长度)	需求	描述	值
L: 2			
授权响应码 F: an2 T: 8A L: 2	来自发卡机构或终端	标明了交易结果	发卡机构生成的代码, 按 GB/T 15150 标准下面的代码由终端生成: Y1: 脱机接受 Z1: 脱机拒绝 Y3: 不能联机(脱机接受) Z3: 不能联机(脱机拒绝)
卡片风险管理数据对象列表 1 (CDOL1) F: b T: 8C L: var. 最大 252	M	列出第 1 个生成应用密文命令中, 卡片请求终端传送的数据。 内容是终端数据对象(标签和长度)	
卡片风险管理数据对象列表 2 (CDOL2) F: b T: 8D L: var. 最大 252	M	列出第 2 个生成应用密文命令中, 卡片请求终端传送的数据。 内容是终端数据对象(标签和长度)	
卡片验证结果 (CVR) F: b32 T: - L: 4.	M	专有数据。记录卡片在本次和上次交易中出现的异常情况。要作为发卡机构应用数据的一部分返回给终端	字节 1: 长度字节 03 字节 2: 位 8 - 7: 00=第 2 个 GENERATE AC 返回 AAC 01=第 2 个 GENERATE AC 返回 TC 10=不请求第 2 个 GENERATE AC 11=RFU 位 6 - 5: 00=第 1 个 GENERATE AC 返回 AAC 01=第 1 个 GENERATE AC 返回 TC 10=第 1 个 GENERATE AC 返回 ARQC 11=不能返回 11 位 4: 1=发卡机构认证执行但失败 位 3: 1 =脱机 PIN 执行 位 2: 1=脱机 PIN 认证失败 位 1: 1 =不能联机 字节 3: 位 8: 1=上次联机交易没有完成 位 7: 1=PIN 锁定 位 6: 1=超过频率检查 位 5: 1=新卡 位 4: 1=上次联机交易发卡机构认证失败

名字(格式、标签和长度)	需求	描述	值
			位 3: 1=联机授权后, 发卡机构认证没有执行 位 2: 1=由于 PIN 锁卡片锁定应用 位 1: 1=上次交易 SDA 失败交易拒绝 字节 4: 位 8-5: 上次交易第 2 个生成应用密文(GENERATE AC) 命令后收到的带有安全报文的发卡机构脚本命令 位 4: 1 =上次交易发卡机构脚本处理失败指针 位 3: 1=上次交易 DDA 失败交易拒绝 位 2: 1 =DDA 执行 位 1: RFU (0) 在应用初始化时, 字节 2-4 置零
持卡人姓名 F: ans2 - 26 T: 5F20 L: 2 - 26	R	如果持卡人姓名小于等于 26 字节, 此时不应使用标签 9F0B, 完整的持卡人姓名应当存放在该标签下。 按 GB/T 17552 的规定。	
持卡人姓名扩展 F: ans 27 - 45 T: 9F0B L: 27-45	0	如果持卡人姓名大于 26 字节, 此时不应使用标签 5F20, 完整的持卡人姓名应当存放在该标签下。按 GB/T 17552 的规定。	
持卡人证件号 F: an40 T: 9F61 L: 1-40	0	持卡人证件号	
持卡人证件类型 F: cn1 T: 9F62 L: 1	0	表明持卡人证件类型	00: 身份证 01: 军官证 02: 护照 03: 入境证 04: 临时身份证 05: 其它
持卡人验证方法 (CVM) 列表 F: b T: 8E L: var. 最大 252	R	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注: 一个应用中可以有多个 CVM 列表, 例如一个用于国内交易, 一个用于国际交易	字节 1 - 4: 金额 X (二进制) 字节 5 - 8: 金额 Y (二进制) 字节 9 (CVM Code): 位 8: 0=只有符合此规范的取值 (如果为 1, 说明有自定义的值) 位 7: 1=如果此 CVM 失败, 应用后续的 0 = 如果此 CVM 失败, 则持卡人验证失败

名字(格式、标签和长度)	需求	描述	值
			位 6 - 1 (CVM Type): 000000=CVM 失败处理 000001=卡片执行明文 PIN 核对 000010=联机加密 PIN 验证 000011=卡片执行明文 PIN 核对+签名(纸上) 000100=保留 000101=保留 011110=签名(纸上) 011111=无需 CVM 000110 - 011101=保留给加入的城市公共交通 IC 卡系统 100000 - 101111=保留给各自独立的城市公共交通 IC 卡系统 110000 - 111110=保留给发卡机构 111111=RFU 定义: 100000 =持卡人证件出示 字节 10 (CVM Condition Code): 00=总是 01=RFU 02=RFU 03=如果终端支持这个 CVM 04=如果是人工值守现金交易 05=如果是返现交易 06=如果交易货币等于应用货币代码而且小于 X 值 07=如果交易货币等于应用货币代码而且大于 X 值 08 =如果交易货币等于应用货币代码而且小于 Y 值 09=如果交易货币等于应用货币代码而且大于 Y 值 0A - 7F: RFU 80 - FF: RFU 保留给各个城市公共交通 IC 卡系统 下一个 CVM 用另两个 CVM 码和 CVM 条件字节表示
CA 公钥索引 (PKI) F: b8 T: 8F L: 1	C 如果支持 SDA 或 DDA	在 SDA 或 DDA 过程中, 和 RID 一起使用, 用来标识 CA 公钥	

名字(格式、标签和长度)	需求	描述	值
连续脱机交易计数器(国际-货币) F: b8 T: - L: 1	C 如果执行国际-货币频度检查	专有数据元。记录自从上次联机后, 不使用指定应用货币的脱机交易次数	初始值为 0, 每接受一次国际-货币交易脱机后加 1
连续脱机交易限制数(国际-货币) F: b8 T: 9F53 L: 1	C 如果执行国际-货币频度检查	专有数据元。不使用指定应用货币的连续脱机交易次数最大数, 超过后交易请求联机	
连续脱机交易计数器(国际-国家) F: b8 T: - L: 1	C 如果执行国际-国家频度检查	专有数据元。记录自从上次联机后, 不在发卡机构所在国家内进行的脱机交易次数	初始值为 0, 每接受一次国际-国家交易脱机后加 1
连续脱机交易限制数(国际-国家) F: b8 T: 9F72 L: 1	C 如果执行国际-国家频度检查	专有数据元。不在发卡机构所在国家的连续脱机交易次数最大数, 超过后交易请求联机	
密文信息数据 F: b8 T: 9F27 L: 1	R	表明卡片返回的密文类型并指出终端要进行的操作	位 8 - 7: 00=AAC 01=TC 10=ARQC 11=AAR (不支持) 位 6 - 5: RFU (00) 位 4: 1=需要通知 位 3 - 1 (原因/通知/授权参考码): 000=无信息 001 = 不允许服务 010=PIN 尝试次数超过 011=发卡机构认证失败 xxx = RFU
密文版本号 F: n2 T: - L: 1	R	专有数据。标明生成密文的算法版本。作为发卡机构应用数据的一部分传送	指定密文版本号 01 (‘01’)
累计脱机交易金额 F: n12 T: - L: 6	C 如果执行累计金额频度检查	专有数据。记录自从上次联机交易完成后, 使用应用指定货币的脱机交易累计金额	初始值为 0。累加每次使用应用指定货币的脱机交易的授权金额。在某些联机交易后可以被复位成零

名字(格式、标签和长度)	需求	描述	值
累计脱机交易金额限制数 F: n12 T: 9F54 L: 6	C 如果执行累计金额频度检查	专有数据。累计脱机交易金额的最大限制。超过交易请求联机	
累计脱机交易金额(双货币) F: n12 T: - L: 6	C 如果执行累计金额(双货币)频度检查	专有数据。记录自从上次联机交易完成后,使用应用指定货币和第 2 应用货币的脱机交易累计金额	初始值为 0。累加每次使用应用指定货币或第 2 应用货币的脱机交易的授权金额。在某些联机交易后可以被复位成零
累计脱机交易金额限制数(双货币) F: n12 T: 9F75 L: 6	C 如果执行累计金额(双货币)频度检查	专有数据。累计脱机交易金额(双货币)的最大限制。超过交易请求联机	
累计脱机交易金额上限 F: n 12 T: 9F5C L: 6	C 如果执行累计金额频度检查	专有数据。累计脱机交易金额和累计脱机交易金额(双货币)的最大限制数。如果超过而且交易无法联机时,拒绝交易	
货币转换因子 F: 8n T: 9F73 L: 4	C 如果执行双货币频度检查	用来将第 2 应用货币转换成指定应用货币的 10 进制数	字节 1 位 8-5: 小数点位置。从右边开始移动的位数 位 4-1: 转换因子的第 1 个数字 字节 2-4: 剩下的 6 个数字
数据认证码 F: b 16 T: 9F45 L: 2	0	发卡机构指定数值。在 SDA 过程中,终端从签名的静态应用数据中恢复出来。作为签名的静态应用数据保存在卡片中	
安全报文加密密钥 F: b 128 T: - L: 16	C 如果执行修改 PIN	自定义数据元。双长度的安全报文加密密钥,16 字节。发卡机构脚本命令中的数据域需要加密时使用	
专用文件(DF)名称 F: b 40-128 T: 84 L: 5-16	R	按 GB/T 16649.4 规定的,DF 的名字	
分散密钥索引(DKI) F: b 8 T: -	0	专有数据。发卡机构用来明确使用哪个主密钥分散得到卡片中的子密钥。用	发卡机构指定。 如果不存在,缺省值为 0

名字(格式、标签和长度)	需求	描述	值
L: 1		于卡片联机处理和发卡机构认证。在发卡机构应用数据中返回给终端	
目录自定义模板 F: var. T: 73 L: var. 最大 252	0	按 GB/T 16649.5, 目录中发卡机构自定义部分	
动态数据认证数据对象列表 (DDOL) F: b T: 9F49 L: var. 最大 252	C 如果支持 DDA	在内部认证命令中需要终端送到卡片中的数据列表, 包括数据对象的标签和长度	
动态数据认证 (DDA) 失败指示位 F: b 1 T: - L: -	C 如果支持 DDA	专有数据。标明当上次交易拒绝时 DDA 是否失败	位 1: 1=上次交易 DDA 失败而且交易拒绝
文件控制信息 (FCI) 发卡机构自定义数据 F: var. T: BF0C L: var. 最大 222	0	FCI 中的发卡机构自定义部分	
文件控制信息 (FCI) 专用模板 F: var. T: A5 L: var.	R	按 GB/T 16649.4, 标识 FCI 模板中, 专用于本规范的数据对象	
文件控制信息 (FCI) 模板 F: var. T: 6F L: var. 最大 252	R	按 GB/T 16649.4, 标识 FCI 模板	
城市公共交通 IC 卡动态数据 F: - T: - L: var.	C 如果支持 DDA	城市公共交通 IC 卡生成或保存的动态数据。在签名的动态应用数据中传送给终端。终端用来证明脱机动态数据认证执行了	
IC 动态数 F: b	C 如果支持 DDA	DDA 处理过程中, 卡片生成的随时间变化不同的随机	

名字(格式、标签和长度)	需求	描述	值
T: 9F4C L: 2 - 8		数。包括在签名动态数据中送到终端, 由终端恢复	
城市公共交通 IC 卡私钥 F: b T: - L: N_{IC}	C 如果支持 DDA	城市公共交通 IC 卡公私钥对中的私钥部分。用于脱机动态数据认证。有两种格式: 模/私钥指数形式和中国余数定理 (CRT) 形式	
城市公共交通 IC 卡 RSA 公钥指数 F: b T: 9F47 L: 1 or 3	C 如果支持 DDA	城市公共交通 IC 卡 RSA 公钥指数用于验证签名的动态应用数据	
城市公共交通 IC 卡公钥证书 F: b T: 9F46 L: N_i	C 如果支持 DDA	发卡机构认证过的城市公共交通 IC 卡公钥	
城市公共交通 IC 卡 RSA 公钥余数 F: b T: 9F48 L: $N_{IC} - N_i + 42$	C 如果需要	没有放入城市公共交通 IC 卡公钥证书的城市公共交通 IC 卡 RSA 公钥部分	
发卡机构行为代码 (IAC) -缺省 F: b40 T: 9F0D L: 5	R 将变成必备	指定当交易请求联机但是终端不能完成联机上送的交易拒绝的条件	值和终端验证结果 (TVR) 中的每一位对应
发卡机构行为代码 (IAC) -拒绝 F: b40 T: 9F0E L: 5	R 将变成必备	指定交易不进行联机直接拒绝的条件	值和终端验证结果 (TVR) 中的每一位对应
发卡机构行为代码 (IAC) -联机 F: b40 T: 9F0F L: 5	R 将变成必备	指定交易联机上送的条件	值和终端验证结果 (TVR) 中的每一位对应
发卡机构应用数据 F: b T: 9F10	R	在一个联机交易中, 要传送到发卡机构的专有应用数据。	

名字(格式、标签和长度)	需求	描述	值
L: var. 最大 32		第 1 字节是自定义数据长度。 格式内容: 长度 (07) (1 字节) 分散密钥索引 (1 字节) 密文版本号 (1 字节) 卡片验证结果 (CVR) (4 字节) 算法标识 (1 字节) 如果有发卡机构自定义数据。在上述数据后跟一个发卡机构自定义数据长度字节和 1-15 字节的发卡机构自定义数据。	
发卡机构认证数据 F: b64 - 128 T: 91 L: 8 - 16	0	用于发卡机构认证的数据, 从发卡机构传来由终端送入卡片。 发卡机构认证数据包括两部分: ARPC (8 字节) 授权响应码 (2 字节)	
发卡机构认证失败指示位 F: b1 T: - L: -	C 如果支持发卡机构认证	专有数据元。表明上次交易出现的发卡机构认证错误的情况。有: 发卡机构认证执行但失败 发卡机构认证没有执行但是必备	位 1: 1 = 上次联机交易发卡机构验证失败
发卡机构认证指示位 F: b8 T: 9F56 L: - 1	C 如果支持发卡机构认证	专有数据。标明当支持发卡机构认证时, 是必备还是可选	位 8: 1=发卡机构认证必备 0=发卡机构认证可选 位 7 - 1: RFU (0000000)
发卡机构代码表索引 F: n2 T: 9F11 L: 1	C 如果有应用首选名称	按 GB/T 15273, 显示应用首选名称的代码表	01 = GB/T 15273-1 02 = GB/T 15273-2 03 = GB/T 15273-3 04 = GB/T 15273-4 05 = GB/T 15273-5 06 = GB/T 15273-6 07 = GB/T 15273-7 08 = GB/T 15273-8

名字(格式、标签和长度)	需求	描述	值
			09 = GB/T 15273-9 10 = GB/T 15273-10
发卡机构国家代码 F: n 3 T: 5F28 L: 2	C 如果有应用用途控制	按 GB/T 2659 指出发卡机构的国家	
发卡机构国家代码 F: n3 T: 9F57 L: 2	C 如果支持卡片频率检查	专有数据。按 GB/T 2659 指出发卡机构的国家	
发卡机构公钥证书 F: b T: 90 L: N_{CA}	C 如果支持 SDA, DDA	CA 认证过的发卡机构公钥。用于脱机数据认证	
发卡机构 RSA 公钥指数 F: b T: 9F32 L: 1 或 3	C 如果支持 SDA, DDA	发卡机构 RSA 公钥指数, 用来验证签名的静态应用数据和城市公共交通 IC 卡公钥证书	
发卡机构 RSA 公钥余数 F: b T: 92 L: $N_I - N_{CA} + 36$	C 如果需要	没有放入发卡机构公钥证书中的发卡机构 RSA 公钥部分	
发卡机构脚本命令 F: b T: 86 L: var 最大 261	0	从发卡机构到终端, 由终端送入卡片。包括在授权响应中的发卡机构脚本中。见附录 A 中的命令描述	见附录 A
发卡机构脚本命令计数器 F: b4 T: - L: -	C 如果支持发卡机构脚本	专有数据。记录上次交易中, 卡片处理的带安全报文的发卡机构脚本命令个数	位 4-1: 第 2 个生成应用密文命令后收到的有安全报文的脚本命令个数 值 'F' 表示有 15 个或更多的发卡机构脚本命令
发卡机构脚本失败指示位 F: b1 T: - L: -	C 如果支持发卡机构脚本	专有数据。当上次交易发卡机构脚本处理失败时设置	位 1: 上次交易发卡机构脚本处理失败
发卡机构脚本模板	C	最后的生成应用密文命令	

名字(格式、标签和长度)	需求	描述	值
2 F: b T: 72 L: var.	如果支持发卡机构脚本	后, 包括发送到卡片的发卡机构专用数据	
发卡机构 URL F: ans T: 5F50 L: var.	0	存放发卡机构服务器在互联网上的位置	
发卡机构 URL2 F: ans T: 9F5A L: var.	0	本规范定义的。存放发卡机构服务器在互联网上的位置	
首选语言 F: an2 T: 5F2D L: 2 - 8	0	顺序存放的 1-4 种语言。根据 GB/T 4880.1 编码	
上次联机应用交易计数器 (ATC) 寄存器 F: b16 T: 9F13 L: 2	C 如果卡片或终端执行频度检查或新卡检查	上次联机上送交易时的 ATC 值	初始值为 0
交易日志入口 F: b16 T: 9F4D L: 2	0	提供交易日志文件的 SFI 和交易日志文件记录个数	字节 1: 交易日志循环记录文件的 SFI 字节 2: 交易日志文件中的记录个数
交易日志格式 F: b T: 9F4F L: var.	0	列出交易日志记录中数据对象的标签和长度	
连续脱机交易下限 F: b8 T: 9F14 L: 1	C 如果执行终端频度检查	发卡机构指定的有联机能力的终端允许连续脱机交易的最大次数	
连续脱机交易下限 F: b8 T: 9F58 L: 1	C 如果执行卡片频度检查	专有数据。发卡机构指定的有联机能力的终端允许连续脱机交易的最大次数	
安全报文鉴别 (MAC) 密钥	C 如果支持发卡机	专有数据。双长度安全报文鉴别 (MAC) 密钥, 16 字	

名字(格式、标签和长度)	需求	描述	值
F: b128 T: - L: 16	构脚本使用安全报文	节。当发卡机构脚本需要安全报文时用来计算 MAC	
卡片请求脱机拒绝指示位 F: b1 T: - L: -	C 如果卡片风险管理检查允许得出拒绝结论	专有数据。在交易处理过程中, 当卡片决定交易拒绝时设置	
联机授权指示位 F: b1 T: - L: -	C 如果卡片支持发卡机构授权或发卡机构脚本处理	专有数据。如果卡片请求 ARQC 但是终端不能完成时设置	位 1: 1=本次或上次交易中, 需要联机授权但是没有实现
卡片请求联机指示位 F: b1 T: - L: -	R	专有数据。在交易处理过程中, 当卡片决定交易联机时设置	
PIN 尝试计数器 F: b8 T: 9F17 L: 1	C 如果支持脱机 PIN	剩余的 PIN 尝试次数	初始值为 PIN 尝试限制数。验证失败一次减 1。验证成功或发卡机构修改/解锁成功则复位到最大值 (PIN 尝试限制数)
PIN 尝试限制数 F: b8 T: - L: 1	C 如果支持脱机 PIN	自定义数据。发卡机构指定的 PIN 允许的连续错误次数	
处理选项数据对象列表 (PDOL) F: b T: 9F38 L: var.	C 在终端进行应用初始化时需要	指定在取处理选项命令中终端送入卡片的数据。包括终端数据对象 (标签和长度)	
扩展的专用应用标识符 (PIX) F: b T: - L: 0-11	R	按 GB/T 16649.5 规定的, AID 的组成部分之一	
脱机 PIN F: b T: - L: 8	C 如果支持脱机 PIN	专有数据。在卡片个性化时由发卡机构写入卡片	
注册的应用提供商	R	按 GB/T 16649.5 规定的,	

名字(格式、标签和长度)	需求	描述	值
标识 (RID) F: b T: - L: 5		AID 的组成部分之一	
响应报文模板格式 1 F: var. T: 80 L: var.	R	城市公共交通 IC 卡命令响应信息, 包括数据对象(不包括标签和长度)	
响应报文模板格式 2 F: var. T: 77 L: var.	C 如果支持 CDA	城市公共交通 IC 卡命令响应信息, 包括数据对象(包括标签和长度)	
第 2 应用货币代码 F: n3 T: 9F76 L: 2	C 如果支持双货币 频度检查。	第 2 种货币, 要转换成应用指定货币。按 GB/T 12406 编码	
服务码 F: n3 T: 5F30 L: 2	0	按 GB/T 17552 的规定	
短文件标识符(SFI) F: b 8 T: 88 L: 1	R	命令中用于标识文件。字节中高三位为 0	1 - 10: 规范定义 11 - 20: 城市公共交通 IC 卡系统定义 21 - 30: 发卡机构定义
签名的动态应用数据 F: b T: 9F4B L: N _{ic}	C 如果支持 DDA	卡片生成的动态数据签名。在 DDA 过程中由终端验证	
签名的静态应用数据 (SAD) F: b T: 93 L: N _i	C 如果支持 SDA	发卡机构签名的数据签名。用卡片内的指定数据生成。	
静态数据认证(SDA)失败指针 F: b1 T: -	C 如果支持 SDA	专有数据。标明当上次交易拒绝时 SDA 是否失败	位 1: 1 =上次交易 SDA 失败而且交易拒绝

名字(格式、标签和长度)	需求	描述	值
L: -			
静态数据认证标签列表 F: - T: 9F4A L: var.	C	列出基本数据对象标签, 标签的值包括在签名的静态应用数据中或城市公共交通 IC 卡公钥证书中	可以只包括应用交互特征 (AIP) 的标签
发卡机构自定义数据 F: ans T: 9F1F L: var.	R 将会改为可选	按 GB/T 17552 规定的自定义数据	
发卡机构基本信息数据 F: b T: 57 L: var. 最大 19 n, var. 最大 19 1 n4 n3 0 或 n5 n, var. hex.	M	按 GB/T 17552 的规定, 发卡机构基本信息数据不包括起始位、结束位和 LRC (验证码), 包括: 应用主账号 (PAN) 分隔符 ("D") 失效日期 (YYMM) 服务码 PIN 验证域 自定义数据 (由城市公共交通 IC 卡系统定义) 补 F (如果不是偶数个)	发卡机构基本信息数据要保存在短文件标识符位 1, 记录 1 中
交易证书数据对象列表 (TDOL) F: b T: 97 L: var. 最大 252	C 如果需要预先哈希	终端使用列出的数据对象 (标签和长度) 生成 TC 哈希值	
应用密文 (AC) 密钥 F: b128 T: - L: 16	M	专有数据。双长度应用密文密钥, 16 字节。用于卡片联机授权, 发卡机构联机授权和生成应用密文	
连续脱机交易上限 F: b8 T: 9F23 L: 1	C 如果支持终端频率检查	发卡机构指定的卡片需要联机处理前允许连续脱机交易次数最大值	
连续脱机交易上限 F: b 8 T: 9F59	C 如果无法联机, 卡片风险管理可	专有数据。发卡机构指定的卡片需要联机处理前允许连续脱机交易次数最大	

名字(格式、标签和长度)	需求	描述	值
L: 1	以得出交易拒绝结论	值	
自定义数据 F: b56 T: - L: var 7-9	R	发卡机构应用数据的一部分。包括一个长度字节、分散密钥索引、密文版本号 and 卡片验证结果。在生成应用密文命令中返回给终端	
产品标识信息 F: b 128 T: 9F63 L: 16	0	用于标识发卡机构和卡片产品种类，在联机交易时上送发卡机构。	字节 1—字节 8: 发卡机构标识码 字节 9—11: 产品标识 字节 9: 位 8: 1=市民卡 位 7: 1=军人卡 位 6: 1=积分卡 位 5: 1=交通卡 位 4: 1=社保卡 位 3: 1=学生卡 位 2: 1=航空卡 位 1: 1=公共缴费类卡 字节 10: 移动支付规范保留 字节 11: 发卡机构保留 字节 12—14: 本规范保留 字节 15—16: 发卡机构保留
SM2 算法支持指示器 F: b8 T: DF69 L: 1	C 如果卡片支持 SM2 算法	专有数据。卡片在应用选择过程中返回给终端。	
发卡机构特殊数据元 F: b T: 7F01 L: 32	0	应用选择返回的发卡机构特殊数据元信息	字节 01—04: 发卡机构代码 字节 05—08: 发卡地区代码 字节 09—12: 制卡信息代码 字节 13: 卡片类型标识 00: 普通卡 01: 学生卡 02: 老人卡 03: 军人卡 04: 内部员工卡 其他: 保留 字节 14—20: 本规范保留

名字(格式、标签和长度)	需求	描述	值
			字节 21—32: 发卡机构保留

表C.2 电子现金专用数据元

名字	格式 标签 长度	需求	描述	备份	获取	值
可用脱机消费金额 Available Offline Spending Amount	F: n 12 T: “9F5D” L: 6	可选卡片数据元	一个计算区域, 用来允许终端打印或显示卡内的可用的脱机交易额, 除非此标签被个人化为 ‘1’, 否则卡片将不会允许此标签被包括在可被终端读出的记录中或对 GPO 的响应中, 对于此数据的个人化并不影响它包含在发卡机构定义数据中	N	GET DATA GPO READ RECORD	如果个人化的值大于零, 对此数据元的获取数据 (GET DATA) 操作被允许 如果此数据元被个人化为 ‘1’ 并且卡片应用处理(第 1 字节第 1 位) 有值为 ‘1’, 则此数据元包含在 GPO 中, 并且允许读记录 (READ RECORD) 如果城市公共交通 IC 卡的私钥的长度大于 1024 位, 则此数据元通过读记录指令 (READ RECORD) 而不是通过 GPO 读出

名字	格式 标签 长度	需求	描述	备份	获取	值
卡片附加处理 Card Additional Processes	F: b 32 T: “9F68” L: 4	条件卡片数据元 如果支持脱机并且是小额选项而不是默认值或没有卡片风险管理选项所支持	指出卡片处理需求和参数选择	N	GET DATA (SD)	字节 1 位 8 1= 支持小额检查 位 7 1= 支持小额和 CTTA 检查 位 6 1= 支持小额或 CTTA 检查 位 5 1= 支持新卡检查 位 4 1= 支持 PIN 重试次数超过检查 位 3 1= 允许货币不匹配的脱机交易 位 2 1= 卡优先选择接触式联机 位 1 1= 返回可用脱机消费金额 字节 2 位 8 1= 支持预付 位 7 1= 不允许不匹配货币交易 位 6 1= 如果是新卡且终端仅支持脱机则拒绝交易 位 5 1= 脱机批准的交易，卡片记录交易日志 位 4~1 保留 字节 3 位 8 1= 匹配货币的交易支持联机 PIN 位 7 1= 不匹配货币的交易支持联机 PIN 位 6 1= 对于不匹配货币交易，卡要求 CVM 位 5 1= 支持签名 位 4~1 保留
卡片 CVM 限额 Card CVM Limit	F: n 12 T: “9F6B” L: 6	可选卡片数据元	如果出现表示当卡片和终端货币类型匹配且一个非接触交易超过这个值，则需要由卡片提供 CVM 本部分定义的持卡人验证是联机 PIN 和签名	N	GET DATA (SD)	此标签应可以被 PUT DATA 命令修改。

名字	格式 标签 长度	需求	描述	备份	获取	值
卡片内部指示器 Card Internal Indicators	F: b 16 T: – L: 2	必备卡片内部数据元	用于控制卡片内部过程	Y	N	字节 1 位 8 中断 位 7 脱机只支持终端 位 6 匹配货币
卡片交易属性 Card Transaction Qualifiers	F: b 16 T: “9F6C” L: 2	可选卡片数据元	在本部分中用于向设备指明卡片要求哪一个 CVM	N	GPO	字节 1 位 8 1= 需要联机 PIN 位 7 1= 需要签名 位 6 1= 如果脱机数据认证失败而且终端可联机则要求联机 位 5 1= 如果脱机数据认证失败而且终端支持城市公共交通 IC 卡应用则终止 位 4~1 保留 字节 2 位 8~1 保留
应用交互特征 Application Interchange Profile (AIP)	F: b 16 T: “82” L: 2	必备卡片数据元	说明此应用中卡片支持指定功能的能力	N	GPO	字节 1 位 8 RFU 位 7 1= 支持 SDA 位 6 1= 支持 DDA 位 5 1= 支持持卡人验证 位 4 1= 支持终端风险管理 位 3 1= 支持发卡机构认证 位 2 1= RFU 位 1 1= 支持 CDA 字节 2 位 8 = 0 位 7~1 RFU
上次联机应用 交易计数器 (ATC) 寄存器 Last Online ATC Register	F: b 16 T: “9F13” L: 2	可选卡片数据元 如果执行新卡检查	上次联机上送交易时的 ATC 值	Y 或缺省为 1	GET DATA	
非接触终端脱机最低限额 Terminal Contactless Floor Limit	F: n 12 T: – L: 6	可选终端数据元	指示终端中的非接触最低限额	N/A	N/A	

名字	格式 标签 长度	需求	描述	备份	获取	值
非接触终端交易限额 Terminal Contactless Transaction Limit	F: n 12 T: – L: 6	可选终端数据元	如果非接触交易的数值大于或等于此数值，则交易终止允许在其它界面尝试此交易	N/A	N/A	
终端执行 CVM 限额	F: n 12 T: – L: 6	可选终端数据元	如果非接触交易超过此值，终端要求一个持卡人验证方法（CVM） 联机 PIN 和签名是本部分定义的持卡人验证方法（CVM）	N/A	N/A	
终端交易属性 Terminal Transaction Qualifiers	F: b 32 T: “9F66” L: 4	必备终端数据元	指示终端能力，需求和对卡片的参数选择	N/A	N/A	详见《城市公共交通 IC 卡读写终端技术规范》
电子现金余额 Electronic Cash Balance	F: n 12 T: “9F79” L: 6	可选卡片数据元	如果授权金额超过了电子现金余额，则所有交易应通过联机授权或脱机拒绝	N	GET DATA	不应在 READ RECORD 命令中返回
电子现金余额上限 Electronic Cash Balance Limit	F: n 12 T: “9F77” L: 6	可选卡片数据元	如果授权金额加上电子现金余额超出此限制，卡片要求联机处理	N	GET DATA (SD)	不应在 READ RECORD 命令中返回

名字	格式 标签 长度	需求	描述	备份	获取	值
电子现金重置阈值 EC Reset Threshold	F: n 12 T: “9F6D” L: 6	可选卡片数据元	如果授权金额大于电子现金余额减去此阈值，则卡片要求联机处理	N	GET DATA	不应在 READ RECORD 命令中返回
电子现金单笔交易限额 EC Single Transaction Limit	F: n 12 T: “9F78” L: 6	可选卡片数据元		N	GET DATA (SD)	不应在 READ RECORD 命令中返回
电子现金发卡机构授权码 EC Issuer Authorization Code	F: a 6 T: “9F74” L: 6	可选卡片数据元	电子现金交易或城市公共交通 IC 卡应用脱机批准的交 易，卡片应当返回此数据元	N	READ RECORD	
应用版本号 Application Version Number	F: b16 T: “9F08” L: 2	必备数据元	城市公共交通 IC 卡系统给应用分配的版本号。	N	READ RECORD	由城市公共交通 IC 卡系统定义

表C.3 电子现金双币应用新增的卡片数据元

数据元名称	标签	长度	格式
第二币种电子现金应用货币代码 (EC Secondary Application Currency Code)	DF71	2	n4
第二币种电子现金余额 (EC Secondary Application Balance)	DF79	6	n12
第二币种电子现金余额上限 (EC Secondary Application Balance Limit)	DF77	6	n12
第二币种电子现金单笔交易限额 (EC Secondary Application Single Transaction Limit)	DF78	6	n12
第二币种电子现金重置阈值 (EC Secondary Application Reset Threshold)	DF76	6	n12

表C.4 电子现金扩展应用专用数据元

发卡机构自定义数据选项	长度 (字节)	IDD ID	金额域	MAC 字节数
电子现金余额	10	0x01	标签 “9F79” 的值 (低 5 位字节)	4
累计交易总金额 (CTTA)	10	0x02	值，此数据无标签 (低 5 位字节)	4
电子现金余额和 CTTA	15	0x03	值 (10 字节, “9F79” 值在第 1 位置)	4
CTTA 和 CTTAL	15	0x04	值 (10 字节, CTTA 值在第 1 位置)	4

可用脱机消费金额	10	0x05	标签“9F5D”的值（低 5 位字节）	4
静态	1 to 15	N/A	发卡机构指定固定数据	无

表C.5 电子钱包数据元

数据域	说明	来源	格式	长度(字节)	值
算法标识 (DLK)	用来标识圈存交易的加密算法。	IC 卡	b	1	
算法标识 (DPK)	用来标识消费和取现交易的加密算法。	IC 卡	b	1	
算法标识 (DTK)	用来标识在交易中计算 TAC 使用的加密算法。	IC 卡	b	1	
算法标识 (DUBK)	用来标识在解除应用锁定中使用的加密算法。	IC 卡	b	1	
算法标识 (DULK)	用来标识在圈提交易中使用的加密算法。	IC 卡	b	1	
应用有效日期	该日期后卡应用终止。	IC 卡	cn CCYYMMDD	4	
应用标识符	用于标识一个应用，并符合 GB/T 16649.5	IC 卡 终端	b	5-16	
应用序列号	发卡机构分配的一个数字。	IC 卡	cn	10	
应用启用日期	指示应用生效日期。	IC 卡	cn CCYYMMDD	4	
应用类型标识	IC 卡支持的表示卡存在的应用。	IC 卡	cn	1	值： 02
应用版本号	表示 IC 卡当前使用的应用版本的一个数字。	IC 卡	b	1	
发卡机构应用版本号	表示发卡机构当前使用的应用版本的一个数字。	IC 卡	b	1	
本机构职工标识	用来表示持卡人是否是机构职员的一个标识。该标识可用来获得某种优惠。	IC 卡	n	1	
卡类型标识		IC 卡	cn	1	值： 00：个人卡 10：单位卡 所有其他值预留
持卡人证件号码	用来标识持卡人。	IC 卡	an	32	
持卡人证件类型	用于区分持卡人证件类型而分配的值。	IC 卡	cn	1	值： 00：身份证 01：军官证 02：护照 03：入境证（仅限香港/台湾居民使用）

城市公共交通 IC 卡卡片技术规范

数据域	说明	来源	格式	长度(字节)	值
					04: 临时身份证 05: 其他
持卡人姓名	根据 GB/T 17552 格式, 标识持卡人姓名。	IC 卡	an	20	
电子钱包余额	IC 卡中电子钱包的当前余额。	IC 卡	b	4	
交易计数器	IC 卡中的一个计数器, 每发生一次交易时就增加。	IC 卡	b	2	
发卡机构标识	用来唯一标识发卡机构的一个数字	IC 卡	cn	8	
发卡机构自定义 FCI 数据	发卡机构在其自己终端上用于特殊处理的自定义数据	IC 卡	b	2	
密钥索引号	为了唯一标识在一个密钥版本中的密钥索引号而分配的一个数字。	IC 卡终端	cn	1	
密 钥 版 本 号 (DLK)	用来唯一标识圈存交易的密钥版本。	IC 卡	b	1	
密 钥 版 本 号 (DPK)	用来唯一标识一个消费或取现交易的密钥版本。	IC 卡	b	1	
密 钥 版 本 号 (DTK)	用来唯一标识计算 TAC 所用的密钥版本。	IC 卡	b	1	
密 钥 版 本 号 (DUBK)	用来唯一标识一个解除应用锁定的密钥版本。	IC 卡	b	1	
密 钥 版 本 号 (DULK)	用来唯一标识一个圈提交易的密钥版本。	IC 卡	b	1	
透支限额	发卡机构给持卡人指定的最大透支额度。	IC 卡	b	3	
伪随机数(IC 卡)	IC 卡随机产生的一个数字。	IC 卡	b	4	
交易日期(发卡机构)	交易发生日期。	发 卡 机构	cn CCYYMMDD	4	
交易日期(终端)	交易发生日期。	终端	cn CCYYMMDD	4	
交易时间	交易发生时间。	终端	cn	3	
交 易 类 型 标 识 (TTI)	用于标识持卡人选择的交易类型(例如: 圈存、圈提及消费等)而分配的一个值。	终端、IC 卡	cn	1	值: 02: 圈存 03: 圈提 06: 消费 07: 修改透支限额 09: 复合应用消费

附 录 D
(规范性附录)
应用数据与文件

D.1 应用数据

D.1.1 联机应用数据

D.1.1.1 卡片数据对象

表D.1 卡片数据对象列表

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡机构通用数据	卡或持卡人特殊数据	数据存储 在文件记录中
应用交互特征(AIP)	b	'82'	2	7C00	说明此应用中卡片支持的功能。	✓			
应用优先指示器	b	'87'	1	01	如果卡片中有多个应用,指出同一目录中的应用的优先级。	✓			
应用交易计数器(ATC)	b	'9F36'	2	初始设置为 0	记录个人化以后交易处理的次数。				
应用版本号	b	'9F08'	2	初始化好的。 00 20	城市公共交通 IC 卡系统给应用分配的版本号,为以后增加新功能提供一种移值的途径。终端会比较自己与卡片的版本号。	✓			✓
卡片内部数据	var.	—			用于发卡机构提供交易处理信息和影响交易结果的卡片内部计数器和指示器。				
上次联机交易未完成指示位	b	—	1 bit	初始设置为 0	表明上次联机交易没有完成。				
卡片请求联机指示位	b	—	1 bit	初始设置为 0	在交易处理过程中,当卡片决定交易联机时设置。				
卡片请求脱机拒绝指示位	b	—	1 bit	初始设置为 0	在交易处理过程中,当卡片决定交易拒绝时设置。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板 缺省 设置	发卡机 构通用 数据	卡或持 卡人特 殊数据	数据存储 在文件记 录中
发卡机构认证失败指示位	b	—	1 bit	初始设置为 0	表明上次交易出现的发卡机构认证错误的情况。				
动态数据认证 (SDA) 失败指示位	b	—	1 bit	初始设置为 0	标明当上次交易拒绝时 SDA 是否失败。				
动态数据认证 (DDA) 失败指示位	b	—	1 bit	初始设置为 0	标明当上次交易拒绝时 DDA 是否失败。				
发卡机构认证指示位	b	'9F56'	1	00 或 80 推荐 00	交易联机后控制交易如何处理的指示器。发卡机构认证可以是可选 ('00') 或强制 ('80')。如果是强制但没有授权响应密文返回, 则发卡机构可以选择不管联机返回报文结果如何, 拒绝本次交易。		✓		
上次联机应用交易计数器 (ATC) 寄存器	b	'9F13'	2	初始设置为 0	上次联机上送交易时的 ATC 值				
日志入口	b	'9F4D'	2	0B 0A	提供日志文件的 SFI 和日志文件记录个数, 城市公共交通 IC 卡应用规范提供推荐值: 0B 0A 字节 1: 循环交易日志文件的 SFI, 为 11 (十进制) 字节 2: 交易日志文件中的记录个数, 为 10 (十进制)	✓			

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡机构通用数据	卡或持卡人特殊数据	数据存储在文件记录中
日志格式	b	'9F4F'	Var.	9A03 9F2103 9F0206 9F0306 9F1A02 5F2A02 9F4E14 9C01 9F3602	列出日志记录中数据对象的标签和长度	✓			
连续脱机交易限制数 (国际-货币)	b	'9F53'	1	发卡机构模板 推荐值 0	不使用指定应用货币的连续脱机交易次数最大数, 超过后交易请求联机		✓		
连续脱机交易限制数 (国际-国家)	b	'9F72'	1	发卡机构模板, 推荐值 0	不在发卡机构所在国家的连续脱机交易次数最大数, 超过后交易请求联机		✓		
累计交易计数器 (国际-货币)	b	—	1	初始设置为 0	国际脱机交易计数器。当计数器超过累计脱机交易限制数时, 卡片请求交易联机。				
累计交易金额 (国内)	n	—	6	初始设置为 0	记录自从上次联机交易完成后, 使用应用指定货币的脱机交易累计金额				
累计脱机交易金额限制数	n	'9F54'	6	发卡机构模板 推荐值 00 00 00 00 00 00	累计脱机交易金额的最大限制数。超过交易请求联机		✓		

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板 缺省 设置	发卡机 构通用 数据	卡或持 卡人特 殊数据	数据存储 在文件记 录中
累计脱机交易金额上限	n	'9F5C'	6	发卡机构模板 推荐值 00 00 00 00 00	累计脱机交易金额和累计脱机交易金额(双货币)的最大限制数。如果超过而且交易无法联机时, 拒绝交易。		✓		
连续脱机交易下限 (LCOL)	b	'9F58'	1	发卡机构模板 推荐值 0	在申请联机授权之前, 卡片允许的最大连续脱机交易限制数。		✓		
连续脱机交易上限 (UCOL)	b	'9F59'	1	发卡机构模板 推荐值 0	发卡机构指定的卡片需要联机处理前允许连续脱机交易次数最大值, 超过此值如果交易要求联机但联机不成功, 则拒绝交易。		✓		
卡片风险管理数据对象列表 1 (CDOL1)	b	'8C'	27	9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03 9F4E 14	列出第一个生成应用密文命令中, 卡片请求终端传送的数据。用于支持密文版本01和授权控制处理过程。内容是终端数据对象(标签和长度), 数据包括: 授权金额, 其他金额, 终端国家代码, 终端验证结果, 交易货币代码, 交易日期, 交易类型, 终端不可预知数, 交易时间和商户名称。	✓			✓

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板 缺省 设置	发卡机 构通用 数据	卡或持 卡人特 殊数据	数据存储 在文件记 录中
卡片风险管理 数据对象列表 2 (CDOL2)	b	'8D'	26	8A02 9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03	列出第二个生成应用 密文命令中, 卡片请求 终端传送的数据。内容 是终端数据对象(标签 和长度), 包括: 发卡 机构响应码, 授权金 额, 其他金额, 终端国 家代码, 终端验证结 果, 交易货币代码, 交 易日期, 交易类型, 终 端不可预知数和交易 时间。	✓			✓
密文信息数据	b	'9F27'	1	初始设置 为 0	表明卡片返回的密文 类型	✓			
发卡机构行为 代码(IAC)-拒绝	b	'9F0E' ,	5	00 10 98 00 00	指定交易不进行联机 直接拒绝的条件。	✓			✓
发卡机构行为 代码(IAC)-联机	b	'9F0F'	5	D8 68 04 F8 00	指定交易联机上送的 条件。	✓			✓
发卡机构行为 代码(IAC)-缺省	b	'9F0D' ,	5	D8 60 04 A8 00	指定当交易请求联机 但是终端不能完成联 机上送的交易拒绝的 条件。	✓			✓
发卡机构应用 数据	b	'9F10'	8	07__ 01 03 00 00 00 01 0A 01	在一个联机交易中, 要 传送到发卡机构的专 有应用数据。		✓		
发卡机构国家 代码	b	'5F28'	2	发卡机构 模板	指明卡片发行者的国 家。		✓		✓
首选语言	ans	'5F2D' ,	2	发卡机构 模板	当终端支持多种语言 时, 终端根据发卡机构 首选语言显示终端信 息。		✓		

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板 缺省 设置	发卡机 构通用 数据	卡或持 卡人特 殊数据	数据存储 在文件记 录中
应用货币码	n	'9F51'		发卡机构模板	发卡机构的国内货币。		✓		✓
应用标识符 (AID)	b	'4F'	5-16	初始化好的	4D4F542E43505449 433031 4D4F542E43505449 433032				
应用标签	ans	'50'	1-16	发卡机构模板	终端显示给消费者一个可选应用列表的时候应用的名称。		✓		
应用用途控制	b	'9F07'	2	FF 00	标明发卡机构指定的卡片应用上的一些限制, 包括地域使用和服务类型等。 用于提供更灵活的卡片服务控制(类似服务代码)。	✓			✓
应用主帐户序列号	n	'5F34'	1	发卡机构基本信息数据文件中提供	用来表示卡片中使用同一个账号的不同应用			✓	✓
持卡人姓名	ans	'5F20'	2-26	从发卡机构基本信息数据文件提供				✓	✓
持卡人姓名扩展	ans	'9F0B',	1—19	从发卡机构基本信息数据文件提供	如果持卡人姓名大于26 字节, 多出部分放在此数据元中。			✓	✓
持卡人证件号	an	'9F61'	1-40	从发卡机构基本信息数据文件提供	持卡人证件号			✓	✓

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板 缺省 设置	发卡机 构通用 数据	卡或持 卡人特 殊数据	数据存储 在文件记 录中
持卡人证件类型	cn	'9F62'	1	从发卡机构基本信息数据文件提供	表明持卡人证件类型			✓	✓
应用失效日期	n	'5F24'	3	发卡机构基本信息数据文件提供	卡片应用失效日期			✓	✓
应用生效日期	n	'5F25'	3	发卡机构模板	卡片中应用启用日期。		✓		✓
应用主帐户 (PAN)	cn	'5A'	最大 10	发卡机构基本信息数据文件提供				✓	✓
服务码	n	'5F30'	2	发卡机构基本信息数据文件提供				✓	✓
发卡机构自定义数据	ans	'9F1F'	var.	发卡机构基本信息数据文件提供				✓	✓
发卡机构基本信息数据	var.	'57'	最大 19	发卡机构基本信息数据文件提供				✓	✓
持卡人验证方法(CVM)列表	b	'8E'	12	0000 0000 0000 0000 0203 1F00	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意：一个应用中可以有多个 CVM 列表，例如一个用于国内交易，一个用于国际交易。	✓			✓
CA 公钥索引 (PKI)	b	'8F'	1	发卡机构模板	在 SDA 或 DDA 过程中，和 RID 一起使用，用来标识 CA 公钥		✓		✓

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡机构通用数据	卡或持卡人特殊数据	数据存储在文件记录中
发卡机构公钥 (IPK) 证书	b	'90'	N_{CA}	发卡机构模板	CA 认证过的发卡机构公钥。用于脱机数据认证		✓		✓
发卡机构公钥余数 (如果需要)	b	'92'	$N_1 - N_{CA} + 36$	发卡机构模板	没有放入发卡机构公钥证书中的发卡机构公钥部分		✓		✓
发卡机构公钥指数	b	'9F32'	1 to $N_1/4$	发卡机构模板	发卡机构公钥指数, 用来验证签名的静态应用数据和城市公共交通 IC 卡公钥证书		✓		✓
签名的静态应用数据 (SAD)	b	'93'	var.	发卡机构模板	用发卡机构签名的应用数据。			✓	✓
城市公共交通 IC 卡公钥证书	b	'9F46'	N_i	发卡机构模板	发卡机构认证过的城市公共交通 IC 卡公钥。			✓	✓
城市公共交通 IC 卡公钥指数	b	'9F47'	1 or 3	发卡机构模板	城市公共交通 IC 卡公钥指数用于验证签名的动态应用数据。			✓	✓
城市公共交通 IC 卡公钥余数	b	'9F48'	$N_{ic} - N_i + 42$	发卡机构模板	没有放入城市公共交通 IC 卡公钥证书的城市公共交通 IC 卡公钥部分			✓	✓
城市公共交通 IC 卡私钥	b	—	N_{ic}	发卡机构模板	城市公共交通 IC 卡公钥对中的私钥部分。用于脱机动态数据认证。 有两种格式: 模/私钥指数形式和中国余数定理 (CRT) 形式。			✓	
动态数据认证数据对象列表 (DDOL)	b	'9F49'	最大 252	发卡机构模板	在内部认证命令中需要终端送到卡片中的数据列表, 包括数据对象的标签和长度。		✓		✓

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板 缺省 设置	发卡机 构通用 数据	卡或持 卡人特 殊数据	数据存储 在文件记 录中
应用缺省行为 (ADA)	b	'9F52'	2	C000	如果支持发卡机构认证。城市公共交通 IC 卡应用专有数据。定义在一些特定条件下卡片执行的发卡机构指定的行为。如果卡片中没有此数据,缺省认为全零	✓			
子密钥 (UDK) A	b	—	8	发卡机构 模板	由每个发卡机构唯一的主密钥分散生成每张卡片唯一的子密钥。			✓	
子密钥 (UDK) B	b	—	8	发卡机构 模板	由每个发卡机构唯一的主密钥分散生成每张卡片唯一的子密钥。			✓	
子密钥(ENC Key)A	b	—	8	发卡机构 模板	用于发卡机构脚本的加密密钥,由每个发卡机构唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(ENC Key)B	b	—	8	发卡机构 模板	用于发卡机构脚本的加密密钥,由每个发卡机构唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(MAC Key)A	b	—	8	发卡机构 模板	用于发卡机构脚本的安全报文密钥,由每个发卡机构唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(MAC Key)B	b	—	8	发卡机构 模板	用于发卡机构脚本的安全报文密钥,由每个发卡机构唯一的主密钥分散生成每张卡片唯一的子密钥。				

D. 1. 1. 2 应用交互特征 (AIP) 设置

应用交互特征(AIP)建议设置为‘7C00’。

表D.2 应用交互特征(AIP)

字节	位	值	含义
1	8	0	RFU
1	7	1	支持SDA
1	6	1	支持DDA
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡机构认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	0000 0000	RFU

D.1.1.3 应用优先指示器

应用优先指示器建议设置为‘01’。

表D.3 应用优先指示器

字节	位	值	含义
1	8	0	没有持卡人确认应用可以选择。
1	7-5	000	RFU
1	4-1	0001	最高优先级

D.1.1.4 卡片内部数据

表D.4 卡片内部数据

卡片内部数据	保留	初始值	Tag
联机授权指示位	1 bit	0	-
卡片请求ARQC指示位	1 bit	0	-
卡片请求AAC指示位	1 bit	0	-
发卡机构认证失败指示位	1 bit	0	-
静态数据(SDA)认证失败指示位	1 bit	0	-
动态数据认证(DDA)失败指示位	1 bit	0	-
发卡机构脚本失败指示位	1 bit		-

卡片内部数据	保留	初始值	Tag
发卡机构认证指示位 (bit8 0=可选 1=强制)	1 字节	00或80 推荐00	'9F56'
发卡机构脚本命令计数器	4 bits		-
连续脱机交易下限	1 字节	发卡机构模板 =0	'9F58'
连续脱机交易上限	1 字节	>=连续脱机交易下限, =0	'9F59'
上次联机应用交易计数器 (ATC) 寄存器	2 字节	0	'9F13'
连续脱机交易限制数 (国际-货币)	1 字节	发卡机构模板 =0	'9F53'
连续脱机交易限制数 (国际-国家)	1 字节	发卡机构模板 =0	'9F72'
累计脱机交易计数器 (国际)	1 字节	0	-
PIN尝试限制数	1 字节	发卡机构模板	-
PIN尝试次数计数器	1 字节	= PIN尝试限制数	'9F17'
累计脱机交易金额数 (国内)	6 字节	0	-
累计脱机交易金额限制数 (国内)	6 字节	发卡机构模板=0	'9F54'
累计脱机交易上限	6 字节	>=累计脱机交易金额限制数 (国内), =0	'9F5C'

注：为了支持DDA, SDA, 发卡机构认证和授权控制处理, 带阴影的指示位应当在个人化时设置。

D. 1. 1. 5 日志格式

日志格式建议设置为‘9A 03 9F21 03 9F02 06 9F03 06 9F1A 02 5F2A 02 9F4E 14 9C 01 9F36 02’。

表D. 5 日志格式的标签和长度

数据对象名称	Tag(标签)	长度
交易日期	9A	3
交易时间	9F21	3
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2

数据对象名称	Tag(标签)	长度
交易货币代码	5F2A	2
商户名称	9F4E	20
交易类型	9C	1
应用交易计数器 (ATC)	9F36	2

D. 1. 1. 6 卡片风险管理数据对象列表 (CDOL) 1

卡片风险管理数据对象列表 (CDOL) 1 建议设置为‘9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03 9F4E 14’。

表D. 6 卡片风险管理数据对象列表 (CDOL) 1 的标签和长度

数据对象名称	Tag(标签)	长度
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3
商户名称	9F4E	20

D. 1. 1. 7 卡片风险管理数据对象列表 (CDOL) 2

卡片风险管理数据对象列表 (CDOL) 2 建议设置为‘8A 02 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03’。

表D. 7 卡片风险管理数据对象列表 (CDOL) 2 的标签和长度

数据对象名称	Tag(标签)	长度
授权响应码	8A	2
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2

数据对象名称	Tag(标签)	长度
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3

D.1.1.8 发卡机构行为代码（IAC）(拒绝、联机 and 缺省)

发卡机构行为代码建议按如下设置：

‘00 10 98 00 00’（发卡机构行为代码-拒绝）；

‘D8 68 04 F8 00’（发卡机构行为代码-联机）；

‘D8 60 04 A8 00’（发卡机构行为代码-缺省）。

表D.8 发卡机构行为代码

条件	结果		
	IAC拒绝- 脱机拒绝	IAC 联机 – 要求联机	IAC 缺省 – 如果不能联机的话 脱机拒绝
未进行脱机数据认证	0	1	1
脱机静态数据认证（SDA）失败	0	1	1
城市公共交通IC卡数据缺失	0	0	0
卡片出现在终端异常文件中	0	1	1
脱机动态数据认证（DDA）失败	0	1	1
复合动态数据认证/应用密码生成（CDA）失败	0	0	0
RFU	00	00	00
城市公共交通IC卡和终端应用版本不一致	0	0	0
应用已过期	0	1	1
应用尚未生效	0	1	1
卡片不允许所请求的服务	1	0	0
新卡	0	1	0
RFU	000	000	000
持卡人验证失败	1	0	0
未知的CVM	0	0	0
PIN重试次数超限	0	0	0
要求输入PIN但密码键盘不存在或不工作	1	0	0
要求输入PIN，密码键盘存在，但未输入PIN	1	0	0

条件	结果		
	IAC拒绝- 脱机拒绝	IAC 联机 – 要求联机	IAC 缺省 – 如果不能联机的话 脱机拒绝
输入联机PIN	0	1	1
RFU	00	00	00
交易超过最低限额	0	1	1
超过连续脱机交易下限	0	1	0
超过连续脱机交易上限	0	1	1
交易被随机选择联机处理	0	1	0
商户要求联机处理	0	1	1
RFU	000	000	000
使用缺省的TDOL	0	0	0
发卡机构认证失败	0	0	0
最后一次GENERATE AC 命令之前脚本处理失败	0	0	0
最后一次GENERATE AC 命令之后脚本处理失败	0	0	0
RFU	0000	0000	0000

D. 1. 1. 9 发卡机构应用数据

表D. 9 发卡机构应用数据

字节	Bit	十六进制初始值	条件
1	8-1	07	长度
2	8-1	发卡机构模板	分散密钥索引
3	8-1	01	密文版本号
4-7	8-1	03 00 00 00	卡片验证结果(CVR)
8	8-1	01	算法标识
9	8-1	0A	发卡机构自定义数据(IDD)-自定义数据长度 (最长15)
10	8-1	01	IDD ID
11-15	8-1	初始设置为0	金额域
16-19	8-1	初始设置为0	MAC
20-24	8-1		其它的发卡机构自定义数据

D. 1. 1. 10 应用标识符和应用标签

表D. 10 应用标识符与应用标签

应用标识符 (AID)	应用标签
4D4F542E43505453414D3031	城市公共交通IC卡电子现金应用
4D4F542E43505453414D3032	城市公共交通IC卡电子钱包应用

D. 1. 1. 11 应用用途控制

应用用途控制建议设置为‘FF00’。

表D. 11 应用用途控制

字节	b8	b7	b6	b5	b4	b3	b2	B1	用法
1	1	0	0	0	0	0	0	0	国内现金交易有效
1	0	1	0	0	0	0	0	0	国际现金交易有效
1	0	0	1	0	0	0	0	0	国内商品有效
1	0	0	0	1	0	0	0	0	国际商品有效
1	0	0	0	0	1	0	0	0	国内服务有效
1	0	0	0	0	0	1	0	0	国际服务有效
1	0	0	0	0	0	0	1	0	RFU
1	0	0	0	0	0	0	0	1	RFU
2	0	0	0	0	0	0	0	0	允许国内返现
2	0	0	0	0	0	0	0	0	允许国际返现
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU

注：表中相应位设置为1，表示该服务是被允许的。此处设置的值是服务代码设置为2时的例子，如果设置为6，则只有国内功能被允许。

D. 1. 1. 12 持卡人验证方法 (CVM) 列表

持卡人验证方法 (CVM) 列表建议设置为‘0000 0000 0000 0000 0203 1F00’。

表D. 12 持卡人验证方法 (CVM) 列表

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0000 0010 0000 0011	联机PIN	1	如果终端支持	CVM处理过程失败
0001 1111 0000 0000	不需要持卡人验证	2	总是	不会失败

D. 1. 1. 13 动态数据对象列表 (DDOL)

动态数据对象列表 (DDOL) 建议设置为‘9F37 04’。

表D. 13 动态数据对象列表 (DDOL) 数据对象的标签和长度

值	标签(Tag)	长度
不可预知数	9F37	4

D. 1. 1. 14 应用缺省行为

应用缺省行为建议设置为‘C000’。

表D. 14 应用缺省行为

字节	位	值	含义
1	8	1	如果发卡机构认证失败，下次联机交易。
1	7	1	如果发卡机构认证执行但失败，拒绝交易。
1	6	0	如果发卡机构认证必需但没有收到ARPC，不拒绝交易。
1	5	0	如果交易拒绝，不生成通知。
1	4	0	如果PIN在本次交易中已锁而且交易拒绝，不生成通知。
1	3	0	如果因为发卡机构认证失败或没有执行导致交易拒绝，不生成通知。
1	2	0	如果是新卡，不联机交易。
1	1	0	如果是新卡，当交易无法联机时不拒绝交易。
2	8	0	如果PIN在本次交易中锁定，应用不锁定。
2	7	0	如果PIN在前次交易中锁定，不拒绝交易。
2	6	0	如果PIN在前次交易中锁定，不联机交易。
2	5	0	如果PIN在前次交易中锁定，当交易无法联机时不拒绝交易。
2	4	0	如果发卡机构脚本命令在前次交易中失败，不联机交易。
2	3	0	如果PIN在前次交易中锁定，不拒绝交易并不锁应用。
2	2-1	00	RFU

注：带阴影的指示位表示支持卡片与发卡机构认证和授权控制处理。

D. 1. 2 脱机应用数据

D. 1. 2. 1 卡片数据对象

表D. 15 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板 缺省 设置	发卡机 构通用 数据	卡或持 卡人特 殊数据	数据存储 在文件记 录中
电子现金余额	n	'9F79 ,	6	初始设置 为 0	保存了可供脱机消费的 剩余总额。				
电子现金余额 上限	n	'9F77 ,	6	发卡机构 模板	表示在电子现金应用 中, 持卡人可脱机消费 的最大累积额度, 也即 卡片充值所能达到的上 限。			✓	
电子现金发卡 机构授权码	an	'9F74 ,	6	ECC001	卡片上用于标识批准电 子现金交易的代码。	✓			✓
电子现金单笔 交易限额	n	'9F78 ,	6	发卡机构 模板	卡片上单笔电子现金交 易额的上限, 用于控制 单笔电子现金交易风 险。			✓	
电子现金重置 阈值	n	'9F6 D'	6	发卡机构 模板	触发卡片进行自动充值 的可用余额下限。			✓	
处理选项数据 对象列表 (PDOL)	b	'9F38 ,	10	9F7A 01 9F02 06 5F2A 02 DF69 01	指定在取处理选项命令 中终端送入卡片的数据。 包括终端数据对象 (标签和长度)。	✓			✓
持卡人验证方 法(CVM)列表	b	'8E'	10	0000 0000 0000 0000 1F03	按照优先顺序列出卡片 应用支持的所有持卡人 验证方法 注意: 一个应用中可以 有多个 CVM 列表, 例 如一个用于国内交易, 一个用于国际交易。	✓			✓
发卡机构行为 代码(IAC)-拒 绝	b	'9F0 E'	5	00 10 80 00 00	指定交易不进行联机直 接拒绝的条件。	✓			✓
发卡机构行为 代码(IAC)-联 机	b	'9F0F ,	5	D8 68 3C F8 00	指定交易联机上送的条 件。	✓			✓

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板 缺省 设置	发卡机 构通用 数据	卡或持 卡人特 殊数据	数据存储 在文件记 录中
发卡机构行为 代码(IAC)-缺 省	b	'9F0 D'	5	D8 60 3C A8 00	指定当交易请求联机但是终端不能完成联机上送的交易拒绝的条件。	✓			✓

D. 1. 2. 2 处理选项数据对象列表 (PDOL)

处理选项数据对象列表 (PDOL) 建议设置为‘9F7A 01 9F02 06 5F2A 02 DF69 01’。

表D. 16 处理选项数据对象列表 (PDOL)

数据对象名称	Tag(标签)	长度
电子现金终端支持指示器	9F7A	1
授权金额	9F02	6
交易货币代码	5F2A	2
SM2算法支持指示器	DF69	1

D. 1. 2. 3 持卡人验证方法 (CVM) 列表

持卡人验证方法 (CVM) 列表建议设置为‘0000 0000 0000 0000 1F03’。

表D. 17 持卡人验证方法 (CVM) 列表

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0001 1111 0000 0011	不需要持卡人验证	1	如果终端支持	CVM处理过程失败

D. 1. 2. 4 发卡机构行为代码 (IAC) (拒绝、联机和缺省)

发卡机构行为代码建议按如下设置：

‘00 10 80 00 00’ (发卡机构行为代码-拒绝)；

‘D8 68 3C F8 00’ (发卡机构行为代码-联机)；

‘D8 60 3C A8 00’ (发卡机构行为代码-缺省)。

表D. 18 发卡机构行为代码

条件	结果		
	IAC拒绝- 脱机拒绝	IAC 联机 – 要求联机	IAC 缺省 – 如果不能联机的话 脱机拒绝
未进行脱机数据认证	0	1	1

条件	结果		
	IAC拒绝- 脱机拒绝	IAC 联机 – 要求联机	IAC 缺省 – 如果不能联机的话 脱机拒绝
脱机静态数据认证（SDA）失败	0	1	1
城市公共交通IC卡数据缺失	0	0	0
卡片出现在终端异常文件中	0	1	1
脱机动态数据认证（DDA）失败	0	1	1
复合动态数据认证/应用密码生成（CDA）失败	0	0	0
RFU	00	00	00
城市公共交通IC卡和终端应用版本不一致	0	0	0
应用已过期	0	1	1
应用尚未生效	0	1	1
卡片不允许所请求的服务	1	0	0
新卡	0	1	0
RFU	000	000	000
持卡人验证失败	1	0	0
未知的CVM	0	0	0
PIN重试次数超限	0	1	1
要求输入PIN但密码键盘不存在或不工作	0	1	1
要求输入PIN，密码键盘存在，但未输入PIN	0	1	1
输入联机PIN	0	1	1
RFU	00	00	00
交易超过最低限额	0	1	1
超过连续脱机交易下限	0	1	0
超过连续脱机交易上限	0	1	1
交易被随机选择联机处理	0	1	0
商户要求联机处理	0	1	1
RFU	000	000	000
使用缺省的TDOL	0	0	0
发卡机构认证失败	0	0	0
最后一次GENERATE AC 命令之前脚本处理失败	0	0	0
最后一次GENERATE AC 命令之后脚本处理失败	0	0	0
RFU	0000	0000	0000

D. 1. 3 非接触式应用数据

D. 1. 3. 1 卡片数据对象

表D. 19 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板 缺省 设置	发卡机 构通用 数据	卡或持 卡人特 殊数据	数据存储 在文件记 录中
卡片附加处理	b	'9F68'	4	81 00 00 00	指出卡片处理需求和参数选择。				
卡片内部指示器	b	—	2	初始设置为 0	用于控制城市公共交通 IC 卡应用卡片内部过程。				
卡片交易属性	b	'9F6C'	2	初始设置为 00 00	主要用于向终端指明卡片要求的 CVM。				
脱机消费可用余额	n	'9F5D'	6	初始设置为 1	一个计算域, 可用于终端显示卡片的脱机可用额度、或用于发卡机构风险管控。				
应用交互特征 (AIP)	b	'82'	2	7C00	说明此应用中卡片支持的功能。	✓			
处理选项数据对象 列表(PDOL)	b	'9F38'	18	9F66 04 9F02 06 9F37 04 5F2A 02 DF60 01 DF69 01	指定在取处理选项命令中终端送入卡片的数据。包括终端数据对象(标签和长度)。	✓			✓
发卡机构应用数据	b	'9F10'	8	07 _ 17 03 00 00 00 01 0A 01	在一个联机交易中, 要传送到发卡机构的专有应用数据。		✓		

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板 缺省 设置	发卡机 构通用 数据	卡或持 卡人特 殊数据	数据存储 在文件记 录中
CAPP 交易指示位	b	'DF 60'	1	初始设置 为 00	如果卡片支持电子现金 CAPP 扩展应用交易, 则需在 PDOL 中指明此数据 00: 表示终端不支持电子现金扩展应用 01: 表示选择或执行分段扣费交易 02: 表示选择或执行脱机预授权交易 03: 表示选择或执行脱机预授权完成交易				
分段扣费应用标识	b	'DF 61'	1	01/02	如果卡片仅支持分段扣费交易时, 发卡机构在 BFOC 中进行个人化 1: 表示卡片仅支持分段扣费交易 2: 表示卡片同时支持分段扣费交易和预授权交易功能				
电子现金分段扣费抵扣限额	cn	'DF 62'	6	初始设置 为 0	如果卡片支持分段扣费抵扣功能, 表示卡片在分段扣费交易中可抵扣的最大额度				
电子现金分段扣费已抵扣额	cn	'DF 63'	6	初始设置 为 0	如果卡片支持分段扣费抵扣功能, 表示卡片当前已抵扣的额度				

D. 1. 3. 2 应用交互特征 (AIP) 设置

应用交互特征 (AIP) 建议设置为 '7C00'。

表D. 20 应用交互特征 (AIP)

字节	位	值	含义
1	8	0	RFU
1	7	1	支持SDA
1	6	1	支持fDDA

字节	位	值	含义
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡机构认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	00000000	RFU

D. 1. 3. 3 处理选项数据对象列表 (PDOL)

处理选项数据对象列表 (PDOL) 建议设置为‘9F66 04 9F02 06 9F37 04 5F2A 02 DF60 01’。

表D. 21 处理选项数据对象列表 (PDOL)

数据对象名称	Tag(标签)	长度
终端交易属性	9F66	4
授权金额	9F02	6
不可预知数	9F37	4
交易货币代码	5F2A	2
CAPP交易指示位	DF60	1
SM2算法支持指示器	DF69	1

D. 1. 3. 4 卡片附加处理

卡片附加处理建议设置为‘81 40 00 00’。

表D. 22 卡片附加处理

字节	位	值	含义
1	8	1	支持小额检查
1	7	0	不支持小额和CTTA检查
1	6	0	不支持小额或CTTA检查
1	5	0	不支持新卡检查
1	4	0	不支持PIN重试次数超过检查
1	3	0	不允许货币不匹配的脱机交易
1	2	0	卡片不优先选择接触式应用联机

字节	位	值	含义
1	1	1	返回脱机消费可用额度
2	8	0	不支持预付
2	7	1	不允许不匹配货币的交易
2	6	0	如果是新卡且读卡器仅支持脱机，不拒绝交易
2	5-1	00000	RFU
3	8	0	匹配货币的交易不支持联机PIN
3	7	0	不匹配货币的交易不支持联机PIN
3	6	0	对于不匹配货币交易，卡不要求CVM
3	5	0	不支持签名
3	4-1	0000	RFU
4	8-1	00000000	RFU

D. 1. 3. 5 卡片交易属性

卡片交易属性建议设置为‘00 00’。

表D. 23 卡片交易属性

字节	位	值	含义
1	8	0	不需要联机PIN
1	7	0	不需要签名
1	6	0	如果脱机数据认证失败且终端可联机，不要求联机
1	5	0	如果脱机数据认证失败且终端支持接触式城市公共交通IC卡应用，不终止
1	4-1	0000	RFU
2	8-1	00000000	RFU

D. 1. 3. 6 发卡机构应用数据

表D. 24 发卡机构应用数据

字节	Bit	十六进制初始值	条件
1	8-1	07	长度
2	8-1	发卡机构模板	分散密钥索引
3	8-1	17(十六进制)	密文版本号

字节	Bit	十六进制初始值	条件
4-7	8-1	03 00 00 00	卡片验证结果(CVR)
8	8-1	01	算法标识
9	8-1	0A	发卡机构自定义数据(IDD)-自定义数据长度 (最长15)
10	8-1	01	IDD ID
11-15	8-1	初始设置为0	金额域
16-19	8-1	初始设置为0	MAC
20-24	8-1		其它的发卡机构自定义数据

D.2 应用文件

D.2.1 电子现金专用文件

D.2.1.1 专用文件1 (SFI=0x01)

表D.25 记录 1: 应用基本数据

Tag	Length	Value
'57'	Up to 19	发卡机构基本信息数据
'5F20'	2-26	持卡人姓名
'9F1F'	可变	发卡机构自定义数据
'9F61'		持卡人证件号
'9F62'		持卡人证件类型

表D.26 记录 2: 数据认证数据

Tag	Length	Value
'90'	128(设)	发卡机构公钥证书

表D.27 记录 3: 数据认证数据

Tag	Length	Value
'9F32'		发卡机构公钥指数
'92'	可变	发卡机构公钥余项
'8F'	1	认证中心公钥索引

D.2.1.2 专用文件2 (SFI=0x02)

表D.28 记录 1: 联机交易卡片风险管理数据

Tag	Length	Value
'5F24'	3	应用失效日期
'5A'	可变	应用主账号(PAN)
'5F34'	1	应用 PAN 序列号

‘9F07’	2	应用使用控制
‘8E’	可变	持卡人验证方法(CVM)列表
‘9F0D’	5	发卡机构行为码(IAC)默认
‘9F0E’	5	发卡机构行为码(IAC)拒绝
‘9F0F’	5	发卡机构行为码(IAC)联机
‘5F28’	2	发卡机构国家代码

表D. 29 记录 2：数据认证数据

Tag	Length	Value
‘93’	128(设)	签名的静态认证数据

表D. 30 记录 3：签名的静态认证数据

Tag	Length	Value
‘9F46’	128(设)	ICC 公钥证书

表D. 31 记录 4：ICC 公钥数据

Tag	Length	Value
‘9F47’	1 或 3	ICC 公钥指数
‘9F48’	可变	ICC 钥余项
‘9F49’	可变	DDOL
‘9F4A’	1	静态签名数据列表（只包含 82 数据元）

D. 2. 1. 3 专用文件3 (SFI=0x03)

表D. 32 记录 1：脱机交易卡片风险管理数据

Tag	Length	Value
‘5F24’	3	应用失效日期
‘5A’	可变	应用主账号(PAN)
‘5F34’	1	应用 PAN 序列号
‘9F07’	2	应用使用控制
‘8E’	可变	持卡人验证方法(CVM)列表
‘9F0D’	5	发卡机构行为码(IAC)默认
‘9F0E’	5	发卡机构行为码(IAC)拒绝
‘9F0F’	5	发卡机构行为码(IAC)联机
‘5F28’	2	发卡机构国家代码

表D. 33 记录 1：数据认证数据

Tag	Length	Value
‘93’	128(设)	签名的静态认证数据

表D. 34 记录 2：签名的静态认证数据

Tag	Length	Value
‘9F46’	128(设)	ICC 公钥证书

表D. 35 记录 3: ICC 公钥数据

Tag	Length	Value
‘9F47’	1 或 3	ICC 公钥指数
‘9F48’	可变	ICC 公钥余项
‘9F49’	可变	DDOL
‘9F4A’	1	静态签名数据列表（只包含 82 数据元）

D. 2. 1. 4 专用文件4 (SFI=0x04)

表D. 36 记录 1: 电子现金相关数据

Tag	Length	Value
‘9F74’	6	电子现金发卡机构授权码

D. 2. 2 电子钱包专用文件

表D. 37 公共应用信息文件

文件标识 (FID)		0x15
文件类型		二进制数据文件
文件大小		30
文件存取控制		读=自由
字节	数据元	长度
1-8	发卡机构标识	8
9	应用类型标识	1
10	发卡机构应用版本	1
11-20	应用序列号	10
21-24	应用启用日期 (YYYYMMDD)	4
25-28	应用有效日期 (YYYYMMDD)	4
29-30	发卡机构自定义 FCI 数据	2

表D. 38 持卡人基本信息文件

文件标识 (FID)		0x16
文件类型		二进制数据文件
文件大小		55
文件存取控制		读=自由
字节	数据元	长度
1	卡类型标识	1
2	本行职工标识	2
3-22	持卡人姓名	3-22
23-54	持卡人证件号码	23-54

55	持卡人证件类型	55
----	---------	----

表D. 39 管理信息文件

文件标识 (FID)		0x17
文件类型		二进制数据文件
文件大小		60
文件存取控制		读=自由
字节	数据元	长度
1-4	国际代码	4
5-6	省级代码	2
7-8	城市代码	2
9-10	互通卡种	2
11	卡类型	1
12-60	预留	49

说明：互通卡种暂定 FFFF

表D. 40 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。

交易明细必须允许卡对其循环修改。

对明细中所有数据元的修改必须考虑数据完整性和安全要求。

文件标识符 (FID)		0018
文件类型		循环文件
记录大小		10×23
文件安全控制		读：自由
字节	数据元	长度
1-2	ED 或 EP 联机或脱机交易序号	2
3-5	透支限额	3
6-9	交易金额	4
10	交易类型标识	1
11-16	终端机编号	6
17-20	交易日期（终端）	4
21-23	交易时间（终端）	4

表D. 41 电子钱包应用相关密钥

密钥名称（类型）	密钥索引	密钥长度	算法	错误计数器
应用主控	00	16 字节	3DES	33
应用维护	00/01	16 字节	3DES	33
消费子密钥	01	16 字节	3DES	-
消费子密钥	02	16 字节	3DES	-
圈存子密钥	01	16 字节	3DES	-

圈存子密钥	02	16 字节	3DES	-
PIN 解锁子密钥	00	16 字节	3DES	33
PIN 重装子密钥	00	16 字节	3DES	33
TAC 子密钥	01	16 字节	3DES	-
TAC 子密钥	02	16 字节	3DES	-
口令密钥	00	16 字节	3DES	33

D.2.3 金额数据

卡内以安全方式存储的，由卡片操作系统和应用自动进行维护的，电子现金应用和电子钱包应用共用的一个余额数值。

D.2.4 互联互通变长记录文件

互联互通变长记录文件是变长记录结构，在换乘优惠应用模式下，可增加一个循环记录文件，用于保存相应的换乘记录等信息。

该应按表 D.42 创建。

表D.42 互联互通变长记录文件

文件名称	互联互通变长记录文件——交易应用数据文件		
文件标识	SFI=0x1A	文件类型	变长记录文件
文件大小 (bytes)	510		
文件权限	读取	自由	
	更新	保护	
记录号	记录描述		长度 (bytes)
1	租车应用信息		96
2	停车应用信息		84
3	公共交通应用信息		100
4	优惠信息		30
5	自定义信息记录1		100
6	自定义信息记录2		100

租车应用信息记录的记录格式见表 D.43。

表D.43 租车应用信息记录

记录名称	租车应用信息	记录大小	96
字节	数据元	长度 (bytes)	数据格式
1-2	记录ID标识	2	2701
3	记录长度	1	固定为0x5D
4	应用有效标识	1	固定为0x01
5	互联互通标识	1	1表示本应用采用分段扣费/复合消费 2表示应用采用预授权消费
6	应用锁定标志 (0表示应用没有锁定；1表示应用锁定)	1	BCD

7	PAN 序列号	1	BCD
8-17	PAN 号	10	BCD
18-25	交易流水号	8	BCD
26	交易状态	1	BCD
27-28	借车城市代码	2	BCD
29-30	还车城市代码	2	BCD
31-38	借车受理机构标识	8	BCD
39-46	还车受理机构标识	8	BCD
47-54	借车终端编号	8	BCD
55-62	还车终端编号	8	BCD
63-70	车辆标识	8	BCD
71-77	租车时间	7	YYYYMMDDhhmmss
78-84	还车时间	7	YYYYMMDDhhmmss
85-88	预授权金额	4	HEX（高字节在前）
89-96	预留	8	初始为00

停车应用信息记录的记录格式见表 D.44。

表D. 44 停车应用信息记录

记录名称	停车应用信息	记录大小	84
字节	数据元	长度 (bytes)	数据格式
1-2	记录ID标识	2	2702
3	记录长度	1	固定为0x51
4	应用有效标识	1	固定为0x01
5	互联互通标识	1	1表示本应用采用分段扣费/复合消费 2表示应用采用预授权消费
6	应用锁定标志（0表示应用没有锁定；1表示应用锁定）	1	BCD
7	PAN 序列号	1	BCD
8-17	PAN 号	10	BCD
18-25	交易流水号	8	BCD
26	交易状态	1	BCD
27-28	城市代码	2	BCD
29-36	末次受理机构标识	8	BCD
37-44	入场终端编号	8	BCD
45-52	出场终端编号	8	BCD
53-60	车辆标识	8	BCD
61-67	入场时间	7	YYYYMMDDhhmmss
68-74	出场时间	7	YYYYMMDDhhmmss
75-78	最大消费金额	4	HEX（高字节在前）
79-84	预留	6	初始为00

公共交通信息记录的记录格式见表D.45。

表D. 45 公共交通应用信息记录

记录名称	公共交通信息	记录大小	100
字节	数据元	长度 (bytes)	数据格式
1-2	记录ID标识	2	2703
3	记录长度	1	固定为0x61
4	应用有效标识	1	固定为0x01
5	互联互通标识	1	1表示本应用采用分段扣费/复合消费 2表示应用采用预授权消费
6	应用锁定标志（0表示应用没有锁定；1表示应用锁定）	1	BCD
7	PAN 序列号	1	BCD
8-17	PAN 号	10	BCD
18-25	交易流水号	8	BCD
26	交易状态	1	BCD
27-28	进闸城市代码	2	BCD
29-30	出闸城市代码	2	BCD
31-38	进闸机构标识	8	BCD
39-46	出闸机构标识	8	BCD
47-54	进闸站点	8	BCD
55-62	出闸站点	8	BCD
63-70	进闸终端编号	8	BCD
71-78	出闸终端编号	8	BCD
79-85	进闸时间	7	YYMMDDhhmmss
86-92	出闸时间	7	YYMMDDhhmmss
93-96	最大消费金额	4	HEX（高字节在前）
97-100	预留	4	初始为00

优惠信息记录的记录格式见表D.46。

表D. 46 优惠信息记录

记录名称	优惠信息	记录大小	30
字节	数据元	长度 (bytes)	数据格式
1-2	记录ID标识	2	2704
3	记录长度	1	固定为0x1B
4	应用有效标识	1	固定为0x01
5	互联互通标识	1	1表示本应用采用分段扣费/复合消费 2表示应用采用预授权消费
6	应用锁定标志（0表示应用没有锁定；1表示应用锁定）	1	BCD
7	优惠类型	1	BCD
8-11	优惠开始时间	4	YYMMDD

12-15	优惠截止时间	4	YYYYMMDD
16	优惠计次	1	BCD
17-30	预留	14	初始为00

自定义信息记录的记录格式见表 D.47 和 D48。

表D. 47 自定义信息记录 1

记录名称	自定义信息1	记录大小	100
字节	数据元	长度(bytes)	数据格式
1-2	记录ID标识	2	2705
3	记录长度	1	固定为0x63
4	应用有效标识	1	固定为0x01
5	互联互通标识	1	1表示本应用采用分段扣费/复合消费 2表示应用采用预授权消费
6	应用锁定标志（0表示应用没有锁定；1表示应用锁定）	1	BCD
7-100	预留	1	各自城市自定义

表D. 48 自定义信息记录 2

记录名称	自定义信息2	记录大小	100
字节	数据元	长度(bytes)	数据格式
1-2	记录ID标识	2	2706
3	记录长度	1	固定为0x63
4	应用有效标识	1	固定为0x01
5	互联互通标识	1	1表示本应用采用分段扣费/复合消费 2表示应用采用预授权消费
6	应用锁定标志（0表示应用没有锁定；1表示应用锁定）	1	BCD
7-100	预留	1	各自城市自定义

D. 2. 5 互联互通循环记录文件

互联互通循环记录文件，为循环记录结构。建议按表 D.49 信息创建。

本文件也可用于行业的其他自定义应用。

表D. 49 互联互通循环记录文件

文件名称	互联互通循环记录文件——交易信息记录文件		
文件标识	SFI=0x1E	文件标识	SFI=0x1E
文件大小 (bytes)	40*30		
文件权限	读取	文件权限	
	更新		
字节	数据元	字节	数据元
1	交易类型	1	交易类型

2-9	终端编号	2-9	终端编号
10-17	交易流水号	10-17	交易流水号
18-21	交易金额	18-21	交易金额
22-25	交易后余额	22-25	交易后余额
26-32	交易日期时间	26-32	交易日期时间
33-34	受理方城市代码	33-34	受理方城市代码

支持换乘优惠的应用应将本次交易明细记录在互联互通循环记录文件中。在换乘优惠时，可读取循环记录文件中的内容作为换乘优惠的依据。

附录 E

（资料性附录）

交易应用举例

本附录以基于非接触小额支付的分段扣费交易在特定应用环境中的应用为范例，描述扣费交易的实际应用模式。

E.1 电子现金公共汽车/轨道交通/停车场/城际客运班车/城际铁路/轮渡应用

出租车收费应用是标准快速支付模式；公共汽车、轨道交通、城际客运班车、城际铁路收费应用是分段收费模式；停车咪表应用是分时收费模式，但以上所有应用其交易流程是一致的。本条将重点以出租收费应用为例表述基于非接触小额支付应用的交易流程，以地铁收费应用为例描述基于非接触小额支付特定分段扣费应用的交易流程。整个交易分为进闸交易（即进消费区交易）和出闸交易（即出消费区交易）。关于终端上CVM的设置，参照电子现金要求执行。

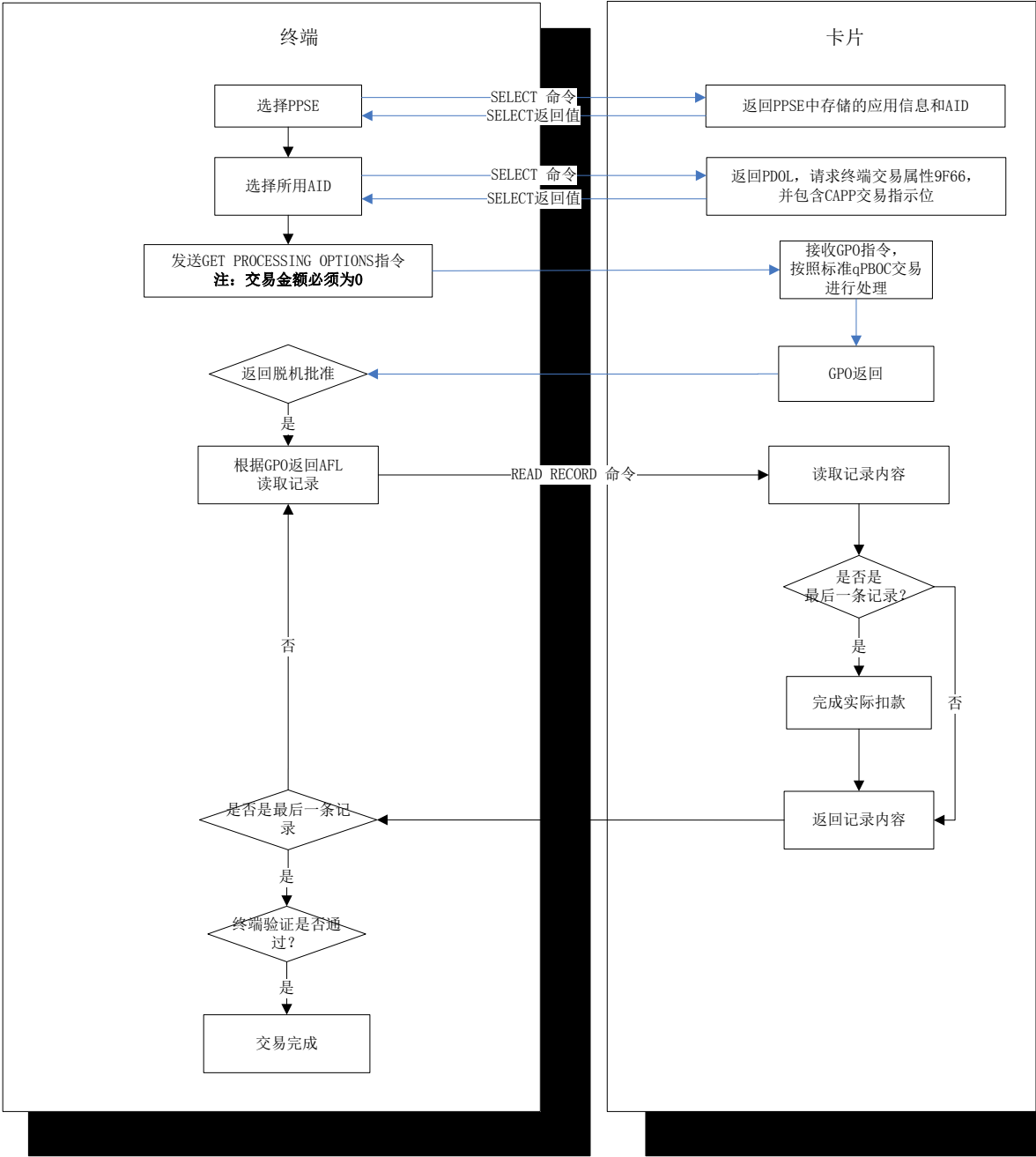
E.1.1 出租收费应用

——描述

出租汽车收费为标准快速支付交易，其基本流程为：选择 PPSE 支付环境，然后选择电子支付应用，发送 GPO 指令，根据消费金额进行扣费。

——流程图

出租车收费交易流程见图 E.1 所示。



图E.1 出租车消费应用交易流程

E. 1. 2 公共汽电车/地铁收费应用

注：以下范例描述的前提是终端支持特定的分段扣费交易应用。

E. 1. 2. 1 进闸交易流程

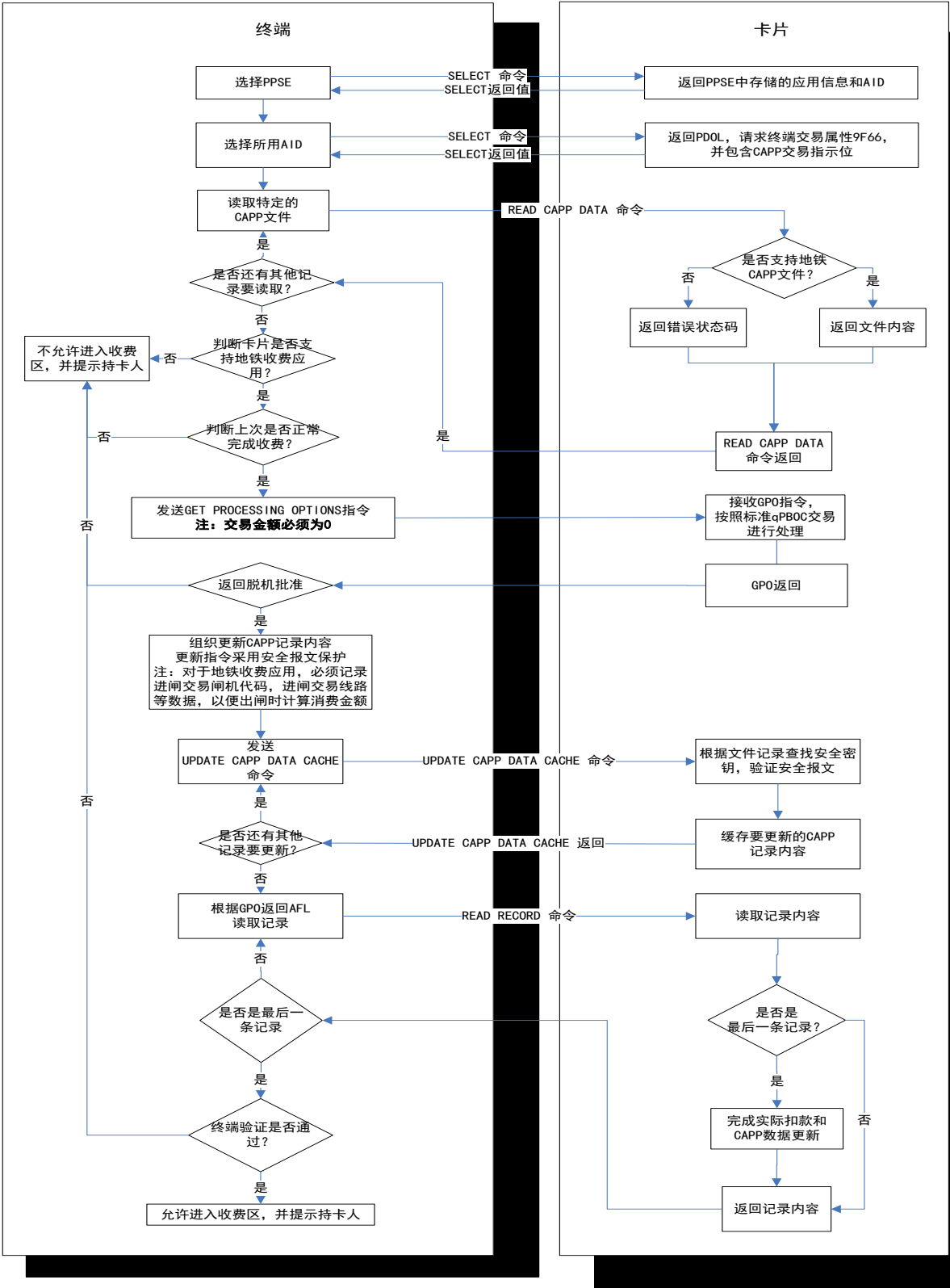
——描述

进闸交易的基本流程为：选择 PPSE 支付环境，然后选择电子支付应用，读取扩展应用专用文件，判断上次交易是否正常完成。若上次交易正常完成，则进行零金额消费，并更新文件；否则返回错误提示，提示持卡人不能进入收费区。

终端也可以根据实际需求进行预处理，例如可以事先获取卡片中的余额，来判断是否允许持卡人进站。

——流程图

公共汽车/地铁进闸交易流程见图 E.2 所示。



图E.2 公共汽电车/地铁消费应用的进闸交易流程

——流程说明

持卡人使用城市公共交通 IC 卡在地铁消费应用环境中进行进闸交易时，终端将作如下处理：

- 1) 终端首先选择和激活卡片，并通过 AID 选择判断卡片是否支持基于非接触小额支付的扩展应用交易。
- 2) 终端发出 READ CAPP RECORD 命令查询，判断卡片是否支持地铁收费应用。如支持，终端应读取此特定专用数据，并根据数据进行处理，如判断上次是否离开收费区等。如处理结果为不允许进行进闸交易，终端应提示持卡人。如处理结果允许进行进闸交易，终端进行分段扣费交易，其中交易金额为 0。
- 3) 终端根据其自身情况，在 UPDATE CAPP DATA CACHE 中更新地铁收费专用数据，填写城市代码、运营企业代码、记录格式版本号、交易标志、进收费区交易时间、进收费区交易线路代码、进收费区交易站点代码、进收费区交易闸机代码、进收费区交易序号和专用 TAC 等字段，并保留出收费区交易时间、出收费区交易线路代码、出收费区交易站点代码、出收费区交易闸机代码、出收费区交易金额、出收费区交易序号等记录原值。
- 4) 交易最后，终端根据交易过程中卡片返回的数据，对卡片进行动态数据认证。只有卡片通过认证，终端才允许持卡人进入收费区。

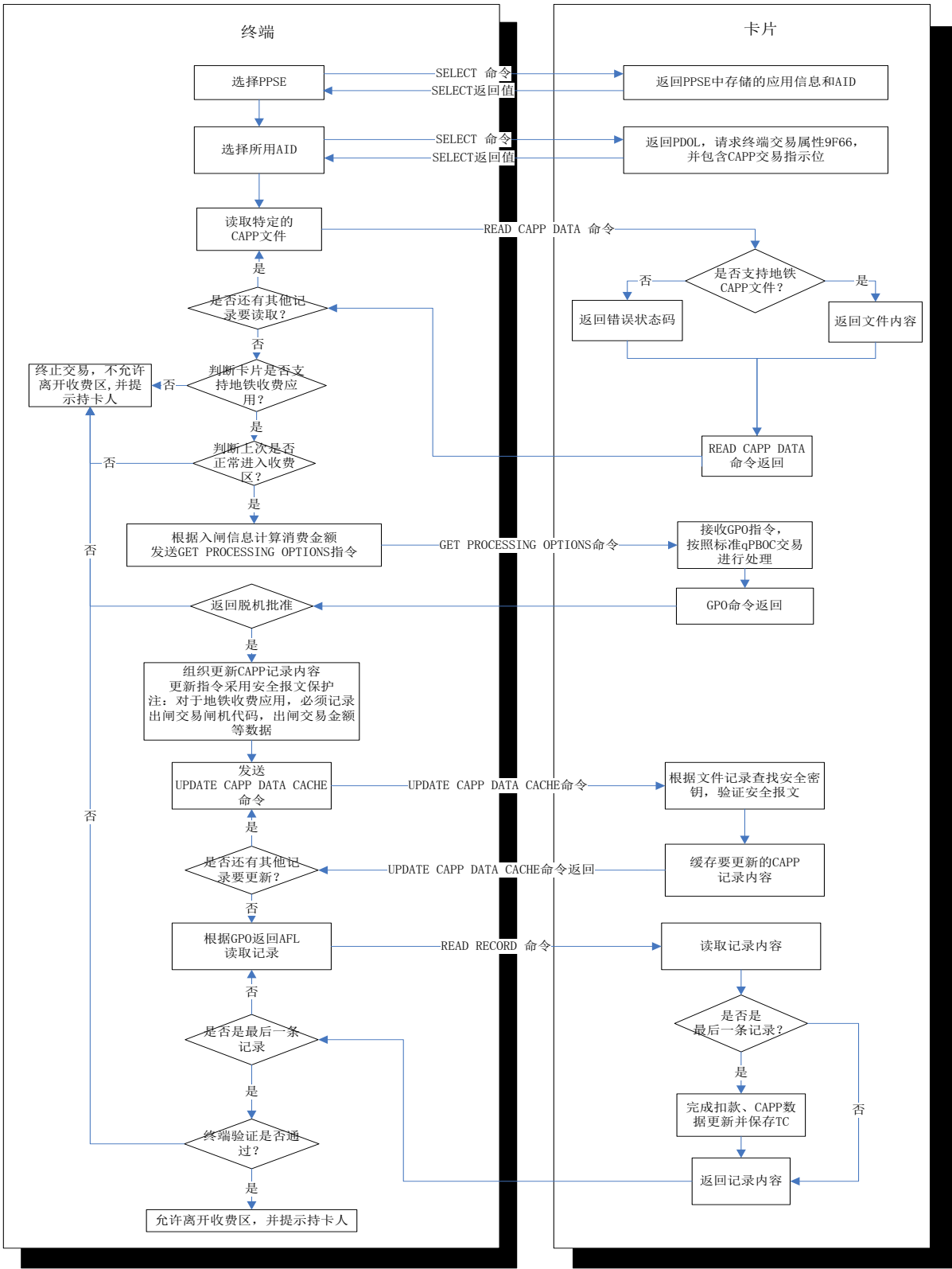
E.1.2.2 出闸交易流程

——描述

出闸交易的基本流程为：选择 PPSE 支付环境，然后选择电子支付应用，读取扩展应用专用文件，判断文件内容是否正确，若正确，则根据入闸信息，计算消费金额。然后进行扣款消费，并更新扩展应用专用文件，表示正常完成交易，同时提示持卡人离开收费区。

——流程图

公共汽电车/地铁出闸交易见流程图 E.3 所示。



图E.3 公共汽车/地铁消费应用的出闸交易流程

——流程说明

持卡人使用城市公共交通 IC 卡在地铁消费应用环境中进行出闸交易时，终端将作如下处理：

- 1) 终端首先选择和激活卡片，并通过 AID 选择判断卡片是否支持基于非接触小额支付的扩展应用交易。
- 2) 终端发出 READ CAPP RECORD 命令查询，判断卡片是否支持地铁收费应用。如支持，终端应读取地铁收费专用数据，并根据数据进行处理，如判断上次是否正常进入收费区等，若是，则根据扩展应用专用文件中的入闸信息计算消费金额。如处理结果为不允许进行出收费区交易，终端应提示持卡人。如处理结果允许进行出收费区交易，终端进行分段扣费交易，并更新扩展应用专用文件，其中交易金额为计算所得的消费金额。
- 3) 终端根据其自身情况，在 UPDATE CAPP DATA CACHE 中更新地铁收费专用数据，填写出收费区交易时间、出收费区交易线路代码、出收费区交易站点代码、出收费区交易闸机代码、出收费区交易金额、出收费区交易序号、专用 TAC 等记录，并保留城市代码、运营企业代码、记录格式版本号、交易标志、进收费区交易时间、进收费区交易线路代码、进收费区交易站点代码、进收费区交易闸机代码、进收费区交易序号等字段记录原值。
- 4) 交易最后，终端根据交易过程中卡片返回的数据，对卡片进行动态数据认证。只有卡片通过认证，终端才允许持卡人离开收费区。

E.1.3 停车咪表应用

停车咪表应用的交易流程与地铁收费应用的交易流程一样，可以将交易分为停车交易和收费交易，等同于进闸交易和出闸交易。但地铁收费应用是按旅客的乘坐路段收费，而停车咪表应用是按顾客的停车时间收费，所以对于停车咪表应用，在停车交易时，对交易咪表代码和停车交易时间等的记录非常重要，这些信息是在收费交易时，计算扣款金额的依据。

E.2 电子现金公交日票/月票交易流程说明

除分时、分段扣费交易外，扩展应用还可以通过读取扩展应用专用文件，实现公交日票/月票应用功能。

E.2.1 公交日票/月票应用

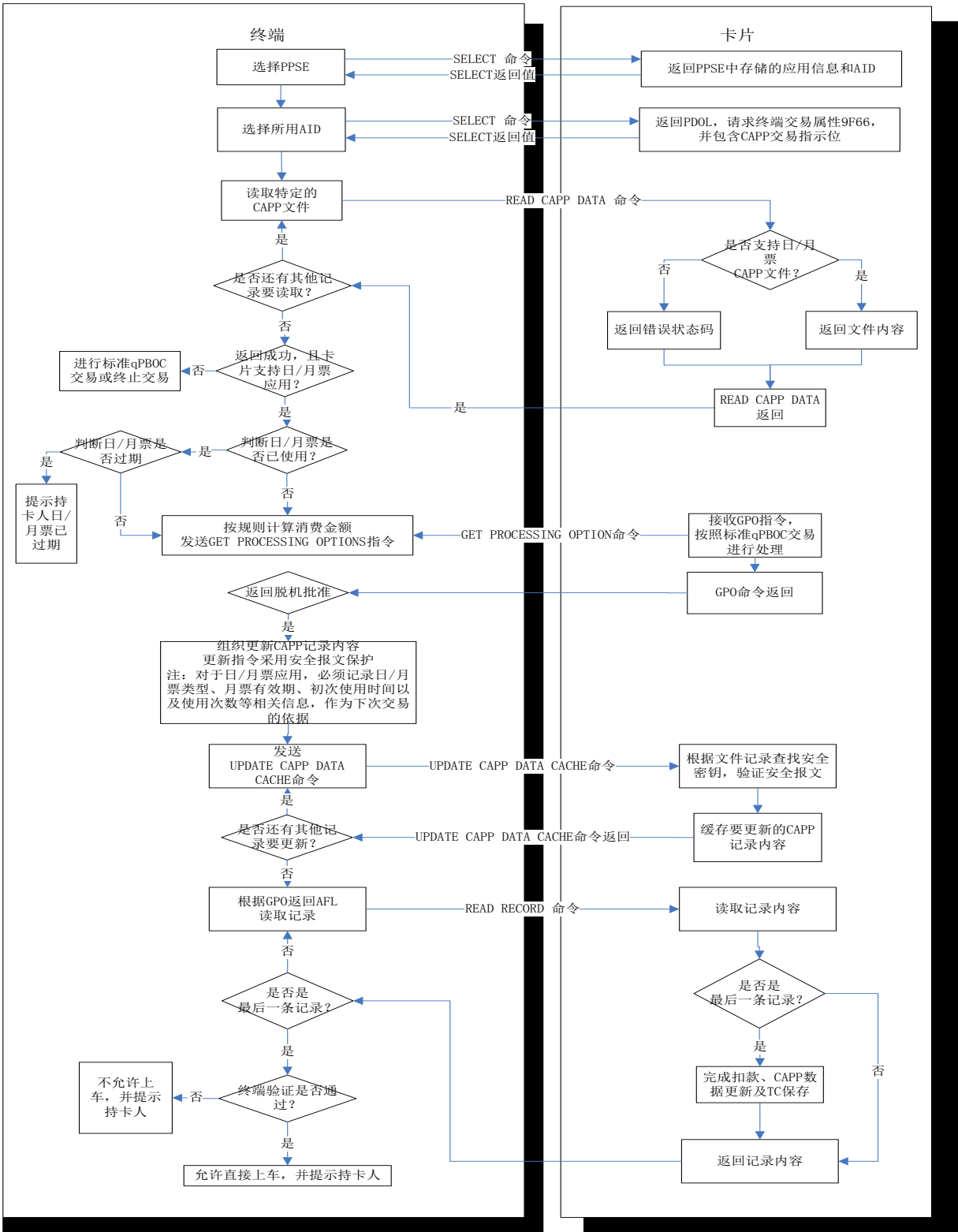
——描述

扩展应用在公交日/月票领域的应用包括以下两种类型：限定次数型和不限次数型。其中，限定次数型表示限定日/月票在当日/月内的使用次数，每次进行等额消费，消费金额为日/月票总额与限定次数的比值；不限次数型表示不限定日/月票在当日/月内的使用次数，且在第一次使用时一次性扣减当天/整月的金额，以后每次进行 0 额消费。

日/月票交易的基本流程为：读取扩展应用专用文件，判断卡片是否支持公交日/月票应用，若支持，判断公交日/月票是否已使用；若未使用，则进行日/月票消费交易；若已使用，根据初次使用时间和（/或）使用次数，判断日/月票是否已过期，如果是则提示持卡人日/月票已过期，否则继续进行日/月票消费交易。

——流程图

公交日票/月票消费交易流程见图 E.4 所示。



——流程说明

持卡人使用城市公共交通 IC 卡在日/月票应用环境中进行公交日/月票交易时，终端将作如下处理：

- a) 终端首先选择和激活卡片，并通过返回信息选择判断卡片是否支持基于非接触小额支付的扩展应用交易。
- b) 终端发出 READ CAPP RECORD 命令查询行业文件，判断卡片是否支持公交日/月票应用。如支持，终端应读取公交日/月票专用数据，并根据数据进行处理：首先判断公交日/月票是否已使用：若未使用，则根据规则，计算消费金额并进行日/月票消费交易；若已经使用，则根据初次使用的时间和（/或）使用的次数判断日/月票是否过期，如果过期则交易停止，并提示持卡人日/月票过期，如果未过期则根据规则，计算消费金额并进行日/月票消费交易。
- c) 对于日/月票应用，扩展应用专用文件中必须记录日/月票的类型，日/月票的有效期，初次使用的时间以及使用的次数等相关信息，作为下次交易的依据。
- d) 如果日/月票限定必须在某日/月使用，则可以在充值/发卡时，对 CAPP 文件进行更新。

E.3 电子钱包复合应用消费举例

本附录以非接触式金融IC卡电子钱包应用在一特定应用环境中的应用为范例，描述复合应用的一种实际应用模式。在这一特定应用环境中，空间被分割为收费区和非收费区。持卡人在进入收费区时，终端将在IC卡中写入特定信息；当持卡人离开收费区时，终端根据特定信息计算所需支付费用，并从电子钱包中扣除等额金额。

E.3.1 基础定义

以下定义复合应用所需基础定义：定义此复合应用的复合应用类型标识符为‘13’。

复合应用记录格式见表E.1。

表 E.1 复合应用专用文件

字段名	长度	字节
城市代码	4	1—4
运营企业代码	6	5—10
记录格式版本号	1	11
交易标志	1	12
进收费区交易时间	4	13—16
进收费区交易线路代码	1	17
进收费区交易站点代码	1	18
进收费区交易闸机代码	1	19
进收费区交易序号	4	20—23
出收费区交易时间	4	24—27
出收费区交易线路代码	1	28
出收费区交易站点代码	1	29
出收费区交易闸机代码	1	30
出收费区交易金额	3	31—34
出收费区交易序号	4	35—38
专用 TAC	4	39—42

E.3.2 交易流程

E.3.2.1 增加复合应用类型

持卡人如需使用非接触式金融IC卡在特定应用环境中进行交易，需先在卡片中增加相应复合应用类型，即启用此类型的复合应用。

增加复合应用操作必须在支持复合应用的终端上联机完成。

具体处理流程为：

- 终端在激活卡片后，由持卡人选择进入增加复合应用增加操作界面，终端向持卡人提示其支持的所有复合应用类型，其中包括此特定复合应用；
- 当持卡人选择增加此特定复合应用后，终端使用 READ RECORD 命令查询卡片是否支持复合应用，是否支持此特定复合应用。如不支持复合应用，可联机创建复合应用专用文件。如卡片已支持此特定复合应用，终端应提示持卡人。

如卡片支持复合应用，但不支持此特定复合应用或此特定复合应用已锁定，则终端在卡片中增加此特定复合应用，即创建以‘13’为记录号的长度为43字节的记录，并将记录内所有字节初始化为0。

E.3.2.2 进收费区交易流程

进收费区交易有两种实现方式：交易方式和文件改写方式。其中交易方式将完成一次完整的消费交易。文件改写方式则直接改写复合应用专用文件中的相关记录。

E.3.2.2.1 交易方式

持卡人使用非接触式金融IC卡在此特定应用环境中进行进收费区交易时，终端将作如下处理：

- 终端首先选择和激活卡片，判断卡片为非接触式金融 IC 卡，并通过 AID 选择进入电子钱包应用目录；
- 终端发出 READ RECORD 命令查询复合应用，判断卡片是否支持复合应用，是否支持此特定复合应用。

如支持，终端应读取此特定复合应用专用数据，并根据数据进行处理，如判断上次是否未出收费区等等。如处理结果为不允许进行进收费区交易，终端应提示持卡人。

如处理结果允许进行进收费区交易，终端进行复合应用消费交易，其中交易金额为0。

终端根据其自身情况，在UPDATE CAPP DATA CACHE中更新此特定复合应用专用数据，填写城市代码、运营企业代码、记录格式版本号、交易标志、进收费区交易时间、进收费区交易线路代码、进收费区交易站点代码、进收费区交易闸机代码、进收费区交易序号和专用TAC等字段，并保留出收费区交易时间、出收费区交易线路代码、出收费区交易站点代码、出收费区交易闸机代码、出收费区交易金额、出收费区交易序号等记录原值。

交易成功后，终端应允许持卡人进收费区。

E.3.2.2.2 文件改写方式

持卡人使用非接触式金融IC卡在此特定应用环境中进行进收费区交易时，终端将作如下处理：

- 终端首先选择和激活卡片，判断卡片为非接触式金融 IC 卡，并通过 AID 选择进入电子钱包应用目录；
- 终端发出 READ RECORD 命令查询复合应用，判断卡片是否支持复合应用，是否支持此特定复合应用。

如支持，终端应读取此特定复合应用专用数据，并根据数据进行处理，如判断上次是否未出收费区等等。如处理结果为不允许进行进收费区交易，终端应提示持卡人。

如处理结果允许进行进收费区交易，则终端向卡片发出GET CHALLENGE命令获取卡片随机数，并利用随机数和消费密钥DPK生成更改后的此特定复合应用专用数据MAC。终端向卡片发出包含更改后的此特定复合应用专用数据及MAC的UPDATE RECORD命令，更新复合应用专用文件记录。

更新成功即表示进收费区交易成功，终端应允许持卡人进收费区。

E.3.2.3 出收费区交易

持卡人使用非接触式金融IC卡在此特定应用环境中进行出收费区交易时，终端将作如下处理：

- 终端首先选择和激活卡片，判断卡片为非接触式金融 IC 卡，并通过 AID 选择进入电子钱包应用目录；
- 终端发出 READ RECORD 命令查询复合应用，判断卡片是否支持复合应用，是否支持此特定复合应用。

如支持，终端应读取此特定复合应用专用数据，并根据数据进行处理，如判断上次是否未进收费区等等，并计算需消费金额。如处理结果为不允许进行出收费区交易，终端应提示持卡人。

如处理结果允许进行出收费区交易，终端根据7.4条进行复合应用消费交易，其中交易金额为计算所得的消费金额。

终端根据其自身情况，在UPDATE CAPP DATA CACHE中更新此特定复合应用专用数据，填写出收费区交易时间、出收费区交易线路代码、出收费区交易站点代码、出收费区交易闸机代码、出收费区交易金额、出收费区交易序号、专用TAC等记录，并保留城市代码、运营企业代码、记录格式版本号、交易标志、进收费区交易时间、进收费区交易线路代码、进收费区交易站点代码、进收费区交易闸机代码、进收费区交易序号等字段记录原值。

交易成果后，终端应允许持卡人出收费区。

附 录 F
(规范性附录)
电子现金支持的密文版本

本规范定义的密文版本为01（0x01）和17（0x17）。密文版本01和密文版本17均使用安全规范中定义的对称密钥算法计算应用密文，不同点是使用的数据元不同。

F.1 密文版本 01 的数据元

表F.1列出的是密文版本01中生成TC/AAC和ARQC的数据元和顺序。

表 F.1 密文版本 01 生成 TC/AAC 和 ARQC 的数据

数据元	来自终端的数据	卡片内数据
授权金额	✓	
其它金额	✓	
终端国家代码	✓	
终端验证结果	✓	
交易货币代码	✓	
交易日期	✓	
交易类型	✓	
不可预知数	✓	
应用交互特征（AIP）		✓
应用交易计数器（ATC）		✓
卡片验证结果（CVR）		✓

F.2 密文版本 17 的数据元

表F.2列出的是密文版本17中生成TC/AAC和ARQC的数据元和顺序。

表F.2密文版本17生成TC/AAC和ARQC的数据

数据元	来自终端的数据	卡片内数据
授权金额	✓	
不可预知数	✓	
应用交易计数器（ATC）		✓
发卡机构自定义数据		✓

附 录 G
(规范性附录)
算法标识

G.1 公钥算法标识

表 G.1 列出了本部分使用的公钥签名算法标识。

表 G.1 公钥签名算法标识

公钥签名算法标识	签名算法	对应哈希算法
‘00’	无	无
‘01’	RSA	SHA-1
‘04’	SM2（数字签名算法）	SM3

表 G.2 列出了本部分使用的公钥加密算法标识。

表 G.2 公钥加密算法标识

公钥加密算法标识	加密算法	对应哈希算法
‘00’	无	无
‘01’	RSA	SHA-1
‘04’	SM2（公钥加密算法）	SM3

G.2 哈希算法标识

表 G.3 列出了本部分使用的哈希标识。

表 G.3 哈希算法标识

哈希算法标识	哈希算法
‘01’	SHA-1
‘07’	SM3

G.3 发卡机构自定义数据（对称密钥算法标识）

发卡机构自定义数据元中有一个自定义数据“算法标识”。此数据定义了卡片计算应用密文和安全报文采用的算法。长度为1个字节。取值情况见表G.4。

表 G.4 对称算法标识

算法	值（16 进制）
3DES	01
SM4	04

附 录 H
(资料性附录)
行业应用开通指南

行业应用开通主密钥一般由发卡机构管理，且各个行业应用由独立的行业应用开通主密钥控制，以确保各个行业的独立性。城市公共交通 IC 卡应用开通密钥的分散方法见《城市公共交通 IC 卡安全技术规范》中关于子密钥分散的描述部分，由行业应用开通主密钥通过支付应用 PAN 号、PAN 序列号进行分散得到。

行业应用管理和开通的流程如下：

- a) 发卡机构在其城市公共交通 IC 卡密钥管理系统中产生行业应用开通主密钥。
- b) 发卡机构在进行城市公共交通 IC 卡数据准备时，由行业应用开通主密钥通过支付应用 PAN 号、PAN 序列号进行分散，得到城市公共交通 IC 卡行业应用开通密钥。
- c) 发卡机构在个人化时，预先创建扩展应用文件，预置相应的城市公共交通 IC 卡行业应用开通密钥。
- d) 持卡人在指定的终端上，在行业应用开通密钥的保护下，通过 APPEND RECORD 命令新增行业应用记录，开通行业应用。

开通行业应用可以通过如下途径：

- 终端机具认证方式开通行业应用：终端上存放有行业应用开通主密钥，通过 PAN 号、PAN 序列号进行分散，获得城市公共交通 IC 卡行业应用开通密钥。终端在城市公共交通 IC 卡行业应用开通密钥的控制下，创建行业应用记录（行业应用管理密钥由发卡机构、行业协商产生，通过城市公共交通 IC 卡行业应用开通密钥加密后写入城市公共交通 IC 卡）。
- 发卡机构后台认证方式开通行业应用：终端上不存放行业应用开通主密钥，行业应用开通主密钥存放在发卡机构后台，由卡片与发卡机构后台进行联机交互认证，其开通行业应用流程同终端机具认证方式。该方式适合通过远程进行行业应用开通。

附 录 I
(规范性附录)
电子现金快速 DDA (fDDA)

在非接触支付环境中，快速交易速度（1秒或者更低）是业务上的需要。DDA作为一种可选方法，用于脱机预防伪卡。

在这个方法中，卡片通过PDOL向终端请求不可预知的随机数。卡片通过GPO命令收到终端的随机数。对于脱机交易，卡片用随机数和ATC生成动态签名，动态签名通过GPO的响应返回（当IC卡私钥的长度大于1024Bits，用记录的方式）。

在GPO中返回的AFL指向的记录包含RSA的证书和相关的DDA数据。一旦最后的记录被终端读取，卡片就不再需要保持在通讯区域。终端认证DDA的动态签名数据。如果认证失败，脱机交易被拒绝。

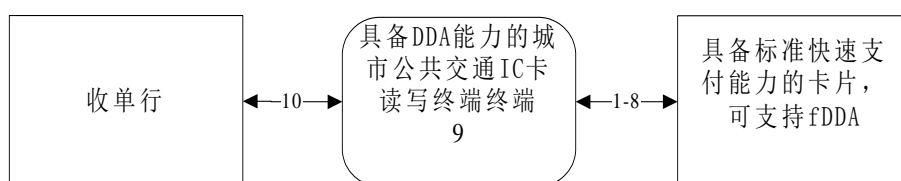


图 I.1 快速 DDA (fDDA) 示例

- a) 终端选择 PPSE;
- b) 卡片返回唯一的城市公共交通 IC 卡电子现金应用 AID;
- c) 终端选择城市公共交通 IC 卡电子现金应用 AID;
- d) 卡片返回请求：
 - 终端交易属性（标签“9F66”）；
 - 随机数（标签“9F37”）；
 - 其它和 fDDA 无关的标签。
- e) 终端发出 GPO，提供：
 - 标签“9F66”指明仅支持标准快速支付；
 - 标签“9F37”随机数；
 - 其它和 fDDA 无关的请求的数据。
- f) 卡片响应：
 - 交易证书（TC）；
 - 动态签名；
 - 同脱机数据认证（fDDA）相关的 AFL 列表记录；
 - 其它和 fDDA 无关的数据。
- g) 终端读取 AFL 指定的记录；
- h) 卡片提供 RSA 证书和数据，用来认证静态数据的哈希；此时卡片可以离开通讯区域。
- i) 终端认证动态签名；
- j) 如果 DDA 认证通过，终端提供清算消息。
 - 交易证书（TC）；
 - 相关数据。

如果DDA认证失败，交易被拒绝。