ICS 03.220.20;35.240.15
R 07
备案号:

JT

中华人民共和国交通运输行业标准

JT/T 978.2—2015

城市公共交通IC卡技术规范 第2部分:卡片

Technical specification on IC card for urban public transport—Part 2:Card

2015-05-21 发布　　2015-07-15 实施

中华人民共和国交通运输部　发布

目　　次

前　言

JT/T 978《城市公共交通IC卡技术规范》由7个部分组成：

——第1部分：总则；

——第2部分：卡片；

——第3部分：读写终端；

——第4部分：信息接口；

——第5部分：非接触接口通信；

——第6部分：安全；

——第7部分：检测项目。

本部分为JT/T 978的第2部分。

本部分按GB/T 1.1—2009给出的规则起草。

本部分由中华人民共和国交通运输部运输服务司提出。

本部分由全国城市客运标准化技术委员会(SAC/TC 529)归口。

本部分起草单位：交通运输部公路科学研究院、中国交通通信信息中心、交通运输部科学研究院、北京市政交通一卡通有限公司、南京市市民卡有限公司、武汉城市一卡通有限公司、泰州市凤城一卡通有限公司、广东岭南通股份有限公司、中国银联股份有限公司、中钞信用卡产业发展有限公司、北京中电华大电子设计有限责任公司、武汉天喻信息产业股份有限公司、北京握奇数据系统有限公司、恒宝股份有限公司。

本部分主要起草人：杨蕴、王刚、梅新明、王立岩、李岚、唐猛、沈伟彬、司徒文翰、谷云辉、张永军、陈文革、惠思涌、莫若、嵇云峰、徐锋、李斌、丁吉、孟秋霞、王晓燕、丹明波、邱峥。

城市公共交通 IC 卡技术规范

第 2 部分:卡片

1 范围

JT/T 978 的本部分规定了城市公共交通 IC 卡卡片介质、卡片文件、电子现金应用、电子钱包应用、电子现金双币应用等要求。

本部分适用于城市公共交通 IC 卡卡片的设计、研发与生产。

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 4880.1 语种名称代码 第 1 部分:字母代码

GB/T 12406 表示货币和资金的代码

GB/T 14916 识别卡 物理特性

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 15273 信息处理八位单字节编码图形字符集

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 16649.5 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 17552 识别卡 金融交易卡

JT/T 978.1 城市公共交通 IC 卡技术规范 第 1 部分:总则

JT/T 978.3 城市公共交通 IC 卡技术规范 第 3 部分:读写终端

JT/T 978.5 城市公共交通 IC 卡技术规范 第 5 部分:非接触接口通信

JT/T 978.6 城市公共交通 IC 卡技术规范 第 6 部分:安全

3 术语和定义

JT/T 978.1 界定的以及下列术语和定义适用于本文件。

3.1

复合应用 complex application

结合电子钱包应用的交通应用模式,适用于使用分时分段扣费、换乘优惠等应用场景。

3.2

扩展应用 comprehensive application

结合电子现金应用的交通应用模式,适用于使用分时分段扣费、换乘优惠等的应用场景。

3.3

押金抵扣 deposit deduction

当卡片内余额不足且消费金额小于发卡机构给予持卡人的押金额度时,持卡人使用押金完成交易

的过程。

3.4

发卡机构行为代码　issuer action code

发卡机构写入卡片供终端进行动作选择的代码。

4　符号和缩略语

下列符号和缩略语适用于本文件。

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——应用专用文件(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)

APDU——应用协议数据单元(Application Protocol Data Unit)

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)

BER——基本编码规则(Basic Encoding Rules)

CAPP——扩展应用(Comprehensive Application)/复合应用(Complex Application)

CDA——复合动态数据认证(Combined DDA)/应用密文生成(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)

cn——压缩数字型

CRT——中国余数定理(Chinese Remainder Theorem)

CTTA——累计脱机交易总金额(Cumulative Total Transaction Amount)

CTTAL——累计脱机交易总金额限制(Cumulative Total Transaction Amount Limit)

CTTAUL——累计脱机交易总金额上限(Cumulative Total Transaction Amount Upper Limit)

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)

DF——专用文件(Dedicated File)

DOL——数据对象列表(Data Object List)

EC——电子现金(Electronic Cash)

EF——基本文件(Elementary File)

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)

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——终端应用层在情况3或情况4命令中发出数据的实际长度
注:情况3或情况4参见JR/T 0025.6。
Le——响应数据中的最大期望长度
MAC——报文鉴别码(Message Authentication Code)
n——数字型
P1——参数1
P2——参数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)
RSA——Rivest、Sharmir和Adleman提出的一种非对称密钥算法的简称
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)
TAL——终端应用层(Terminal Application Layer)
TC——交易证书(Transaction Certificate)
TLV——表示标签、长度以及值的组合(Tag Length Value)
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 Key)

5 卡片介质要求

5.1 卡片介质

城市公共交通IC卡(以下简称“卡片”)为非接触式集成电路卡,符合JT/T 978.5要求,CPU卡的可写数据存储器容量不少于20kB。

5.2 卡体材料

卡体材料应符合GB/T 14916的规定。

5.3 卡片外形规格

卡片尺寸应符合GB/T 14916规定的ID-1型卡的尺寸。

5.4 卡面要求

卡片正面应包括城市公共交通IC卡标识及卡号。
城市公共交通IC卡标识位于卡片正面右侧,可分为下置格式和上置格式两种设计方案,下置格式

见图1,上置格式见图2。

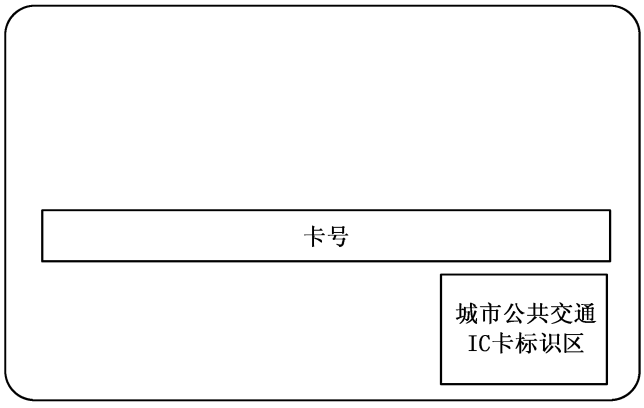


图1　城市公共交通IC卡标识下置格式

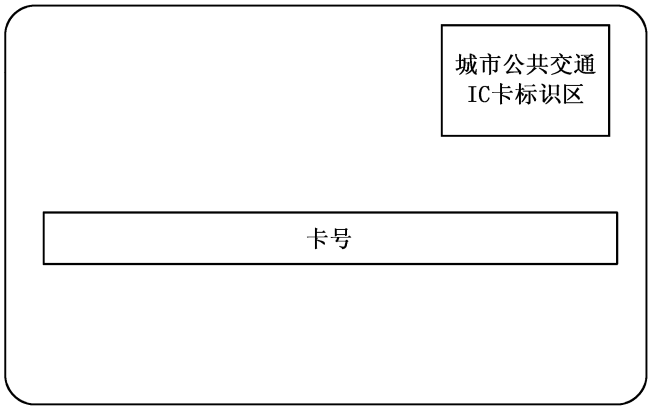


图2　城市公共交通IC卡标识上置格式

6　卡片文件要求

6.1　文件

6.1.1　概述

卡片的每个应用都包括一系列信息项,文件中的数据信息以记录方式或二进制方式存储。文件结构及引用方式由文件的用途决定,支持ADF和AEF两种文件。

6.1.2　应用专用文件(ADF)

应用专用文件(ADF)的树形结构应符合以下要求:

a)　能够将数据文件与应用联系起来;

b)　能够确保应用之间的独立性;

c)　通过应用选择实现对其逻辑结构的访问。

6.1.3　应用基本文件(AEF)

按GB/T 16649.4的规定创建。

6.1.4 文件结构的映射

文件结构的映射应符合以下要求：

a) GB/T 16649.4 规定的专用文件(DF)映射为一个 ADF；

b) GB/T 16649.4 规定的一个基本文件(EF)对应一个 AEF。

6.1.5 文件引用

6.1.5.1 概述

文件可以通过文件名或 SFI 引用。

6.1.5.2 通过文件名引用

卡片中的 ADF 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 名应在该卡内是唯一的。

6.1.5.3 通过 SFI 引用

SFI 用于选择 AEF，每个 SFI 在一个应用内应是唯一的。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 bit 来编码，其值在 0x01 ~0x1E 的范围内。SFI 编码将在使用它的各命令中描述。SFI 的分配范围见表 1。

表 1 SFI 分配范围

数 值	说 明
0x1A,0x1E	该 SFI 对应的文件可以由发卡机构按本规范要求予以使用
0x15 ~0x19	在电子现金应用中，该 SFI 对应的文件可以由发卡机构自行定义使用
0x05 ~0x08,0x19	在电子钱包应用中，该 SFI 对应的文件可以由发卡机构自行定义使用
其他	本规范预留

6.2 数据对象列表

在交易过程中，终端根据流程要求，建立可变的数据元列表，并发送给卡片，卡片数据对象列表见 JT/T 978.3。

6.3 数据元

卡片交易过程中的相关数据元，包括数据元的名称、标识及功能等，见附录 A。

数据元的推荐值见附录 B，发卡机构可根据应用需求选择不同的数据模板。

6.4 文件结构

6.4.1 卡片中应同时存在电子现金和电子钱包两个应用，两个应用拥有独立的文件结构，两个应用的文件结构应符合 JT/T 978.3 交易流程及 JT/T 978.6 安全体系，两个应用均可访问共用余额文件、公共交通过程信息变长记录文件(0x1A)和公共交通过程信息循环记录文件(0x1E)，本规范未定义的应用不允许访问。电子现金应用和电子钱包应用共享以下数据信息：实际余额、透支限额、已透支金额、余额上限。卡片文件结构见图 3。

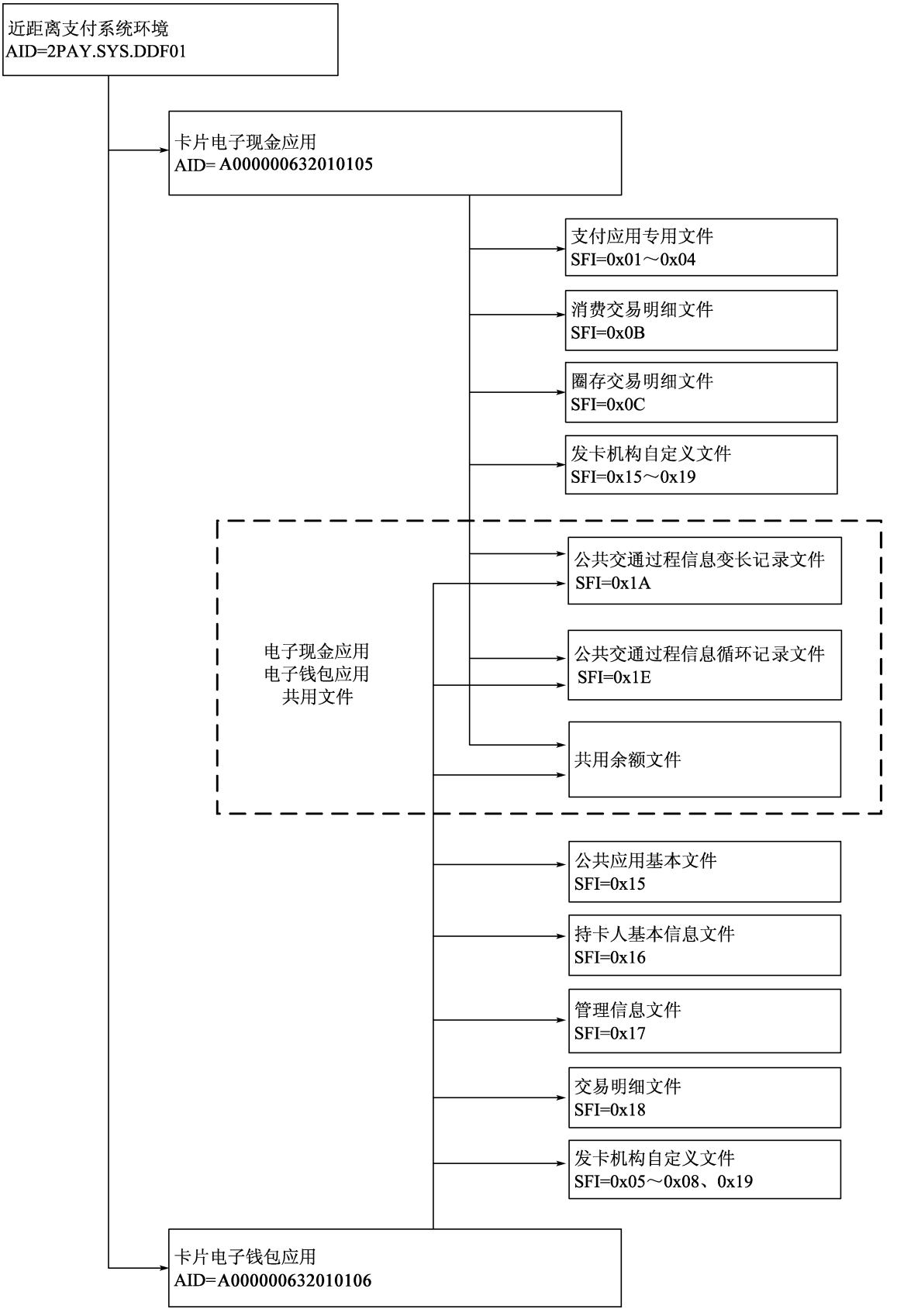

近距离支付系统环境
AID=2PAY.SYS.DDF01
卡片电子现金应用
AID= A000000632010105
支付应用专用文件
SFI=0x01～0x04
消费交易明细文件
SFI=0x0B
圈存交易明细文件
SFI=0x0C
发卡机构自定义文件
SFI=0x15～0x19
电子现金应用
电子钱包应用
共用文件
公共交通过程信息变长记录文件
SFI=0x1A
公共交通过程信息循环记录文件
SFI=0x1E
共用余额文件
公共应用基本文件
SFI=0x15
持卡人基本信息文件
SFI=0x16
管理信息文件
SFI=0x17
交易明细文件
SFI=0x18
发卡机构自定义文件
SFI=0x05～0x08、0x19
卡片电子钱包应用
AID=A000000632010106

图 3　卡片文件结构示意

6.4.2 共用余额文件存放卡片余额,电子现金应用更新共用余额文件命令见 7.3,电子钱包应用更新共用余额文件命令见 8.3。

6.4.3 公共交通过程信息循环记录文件,为循环记录结构,在换乘优惠等交通应用模式下,用于保存相应的换乘记录等信息,应按 C.2.5 的信息创建。

6.4.4 公共交通过程信息变长记录文件存放的交通信息记录见表 2,详细结构说明见 C.2.4.1,文件结构件见 C.2.4。电子现金应用读写公共交通过程信息变长记录文件命令见 7.3,电子钱包应用读写公共交通过程信息变长记录文件命令见 8.3。

表 2 公共交通过程信息变长记录文件 (0x1A)的交通信息记录

记 录 号	记 录 描 述
1	城市轨道应用信息记录
2	公共汽电车应用信息记录
3	城市水上客运应用信息记录
4	出租汽车应用信息记录
5	租赁汽车应用信息记录
6	公共自行车应用信息记录
7	停车收费应用信息记录
8	长途客运应用信息记录
9	轮渡应用信息记录
10	城际铁路应用信息记录
11	民航应用信息记录
12	高速公路收费应用信息记录
13	优惠信息记录
14	本规范预留信息记录 1
15	本规范预留信息记录 2
16	本规范预留信息记录 3
17	本规范预留信息记录 4
18	本规范预留信息记录 5

6.5 应用选择

终端通过选择 DF 名称(AID)“2PAY.SYS.DDF01”选择近场支付系统环境(PPSE),根据卡片返回的应用信息和 AID,判断选择电子现金应用或电子钱包应用。终端发送选择(SELECT)命令选择应用,卡片返回相应的文件控制信息(FCI)。应用选择流程见 JT/T 978.3,SELECT 命令见 C.1.1。

7 电子现金应用要求

7.1 基本要求

电子现金应用基本要求如下:

a) 应具备联机交易、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;

b) 应具备 fDDA 功能,详细过程见附录 D;

c) 为缩短交易时间,卡片的 RSA 私钥以 CRT 模式存放和使用。

7.2 功能要求

7.2.1 电子现金应用应符合表 3 中列出的功能。

表 3 电子现金应用功能

功 能	条 件
应用选择	M
a)目录选择方式	O
b)直接选择方式	M
初始化应用	M
读应用记录	M
脱机数据认证	M
a)标准 DDA	M
b)复合 DDA/应用密文生成	O
处理限制	M
a)应用版本号检查	M
b)应用用途控制检查	O
c)生效日期检查	O
d)失效日期检查	M
持卡人验证	O
单独的 CVM	O
终端风险管理	M
a)终端异常文件检查	N/A
b)商户强制联机	N/A
c)最低限额检查	N/A
d)交易日志	N/A
e)随机选择	N/A
f)频度检查	O
g)新卡检查	O
终端行为分析	C-当需要验证 IAC 时需具备
卡片行为分析	M
a)联机/脱机决定	M
b)卡片风险管理	M
c)通知报文	O
d)应用密文	提供算法选择,算法标识见附录 E
联机处理	M
a)联机能力	M
b)发卡机构认证	O
交易结束	M
发卡机构到卡片脚本处理 安全报文	O 仅具备一种脚本形式
注:M-必备,O-可选,C-有条件,N/A 不适用。	

7.2.2 卡片应具备记录交易日志功能选项,该功能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。

7.2.3 启用交易日志功能由发卡机构决定。

7.3 命令要求

7.3.1 卡片的电子现金应用命令,见表4。

表4 电子现金应用命令

命 令	条 件
应用锁定(APPLICATION BLOCK)	O-若具备,推荐使用应用锁定命令
应用解锁(APPLICATION UNBLOCK)	O-若具备,推荐使用应用解锁命令
卡片锁定(CARD BLOCK)	O-可通过卡片锁定命令实现
外部认证(EXTERNAL AUTHENTICATE)	C-具备发卡机构认证
生成应用密文(GENERATE AC)	M
取数据(GET DATA)	M
获取处理选项(GET PROCESSING OPTIONS)	M
内部认证(INTERNAL AUTHENTICATE)	C-具备 DDA
PIN 修改/解锁(PIN CHANGE/UNBLOCK)	C-电子现金应用,具备脱机 PIN。 PIN 解锁功能必备,使用 PIN 修改/解锁命令实现; PIN 修改功能可选,应在发卡机构可控的环境下使用
设置数据(PUT DATA)	M
验证(VERIFY)	C-电子现金应用,具备脱机 PIN
读扩展应用数据(READ CAPP DATA)	M
更新数据缓存(UPDATE CAPP DATA CACHE)	M
新增记录(APPEND RECORD)	M
取脱机交易应用密文(GET TRANS PROVE)	M
安全方式更新(SECURITY UPDATE)	M

7.3.2 电子现金应用应使用下述命令更新共用余额文件:

a) 设置数据(PUT DATA)命令;

b) 支付流程最后一条读记录(READ RECORD)命令。

7.3.3 电子现金应用应使用下述命令更新公共交通过程信息变长记录文件和公共交通过程信息循环记录文件:

a) 新增记录(APPEND RECORD)命令;

b) 更新应用数据缓存(UPDATE CAPP DATA CACHE)命令;

c) 修改记录(UPDATE RECORD)命令。

7.4 交易流程

电子现金应用交易流程见JT/T 978.3。非接触小额支付的分时分段扣费交易在特定环境中的应

用示例参见附录 F,行业应用的开通方式参见附录 G。

7.5 交易时间

单次脱机交易时间是从终端寻获卡片并上电成功后开始,到终端接收到卡片返回的最后一个字节为止,不包括终端脱机数据认证中验证静态或动态签名所需的时间。

单次脱机交易时间要求:采用 1 024 位 RSA 算法时,标准快速支付交易时间应不超过 400ms,更新一条过程记录的分时分段扣费交易时间应不超过 500ms。

8 电子钱包应用要求

8.1 基本要求

电子钱包应用基本要求如下:

a) 电子钱包应用具备圈存交易、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;

b) 电子钱包应用的金额数据、公共交通过程信息变长记录文件和公共交通过程信息循环记录文件的详细定义见附录 B。

8.2 功能要求

电子钱包应用应符合表 5 中列出的功能。

表 5 电子钱包应用功能

功 能	条 件
应用选择 a)目录选择方式 b)直接选择方式	M O M
消费	M
复合消费	M
圈提	M
修改透支限额	M
应用锁定	M
应用解锁	M

8.3 命令要求

8.3.1 卡片的电子钱包应用命令,见表 6。

表 6 电子钱包应用命令

命 令	条 件
应用锁定(APPLICATION BLOCK)	O-若具备,使用应用锁定命令
应用解锁(APPLICATION UNBLOCK)	O-若具备,使用应用解锁命令
外部认证(EXTERNAL AUTHENTICATE)	C-若具备,发卡机构认证时使用

表6(续)

命　令	条　件
取随机数(GET CHALLENGE)	M
内部认证(INTERNAL AUTHENTICATION)	M
读二进制文件(READ BINARY)	M
修改二进制文件(UPDATE BINARY)	M
圈存(CREDIT FOR LOAD)	M
消费(DEBIT FOR PURCHASE)	M
圈提(DEBIT FOR UNLOAD)	M
查询余额(GET BALANCE)	M
取交易认证(GET TRANSACTION PROVE)	M
初始化圈存(INITIALIZE FOR LOAD)	M
初始化消费(INITIALIZE FOR PURCHASE)	M
初始化圈提(INITIALIZE FOR UNLOAD)	M
修改初始化(INITIALIZE FOR UPDATE)	M
初始化复合应用消费(INITIALIZE FOR CAPP PURCHASE)	M
更新复合应用数据缓存(UPDATE CAPP DATA CACHE)	M
复合应用消费(DEBIT FOR CAPP PURCHASE)	M
新增记录(APPEND RECORD)	M
修改透支限额(UPDATE OVERDRAW LIMIT)	M
国密/国际算法操作(CRYPTOGRAPHIC OPERATION)	O

8.3.2　电子钱包应用应使用下述命令更新共用余额文件：

a)　圈存(CREDIT FOR LOAD)命令；

b)　消费(DEBIT FOR PURCHASE)命令；

c)　复合应用消费(DEBIT FOR CAPP PURCHASE)命令；

d)　圈提(DEBIT FOR UNLOAD)命令；

e)　修改透支限额(UPDATE OVERDRAW LIMIT)命令。

8.3.3　电子钱包应用应使用下述命令更新公共交通过程信息变长记录文件和公共交通过程信息循环记录文件：

a)　新增记录(APPEND RECORD)命令；

b)　更新复合应用数据缓存(UPDATE CAPP DATA CACHE)命令；

c)　修改记录(UPDATE RECORD)命令。

8.4　交易流程

电子钱包应用包括圈存交易、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，其交易流程见JT/T 978.3。电子钱包在一特定环境中的应用示例，参见附录F。

8.5 交易时间

电子钱包脱机交易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个字节为止的时间。电子钱包脱机消费交易时间应不超过300ms。

9 电子现金双币应用要求

9.1 概述

电子现金双币应用是在电子现金应用基础上,在卡中增加一组第二币种相关数据元(见附录A),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。发卡机构通过交易货币代码来区分对应币种的电子现金账户。此应用为可选应用。

9.2 基本要求

9.2.1 一般要求

电子现金双币应用仅适用于“具备小额检查”选项(卡片附加处理选项,标签“9F68”),不适用“具备小额和CTTA检查”和“具备小额或CTTA检查”选项。当“具备小额和CTTA检查”或“具备小额或CTTA检查”选项打开时,卡片应关闭第二币种电子现金功能。

9.2.2 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至少包含交易货币代码(标签“5F2A”)。卡片附加处理选项中第1字节第7位“具备小额和CTTA检查”和第1字节第6位“具备小额或CTTA检查”应设置为‘0’,第1字节第8位“具备小额检查”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)应包含以下选项:

a) CTTA,IDD ID为0x02;
b) 电子现金余额和CTTA,IDD ID为0x03;
c) CTTA和CTTAL,IDD ID为0x04。

9.3 电子现金双币应用标准快速支付交易流程

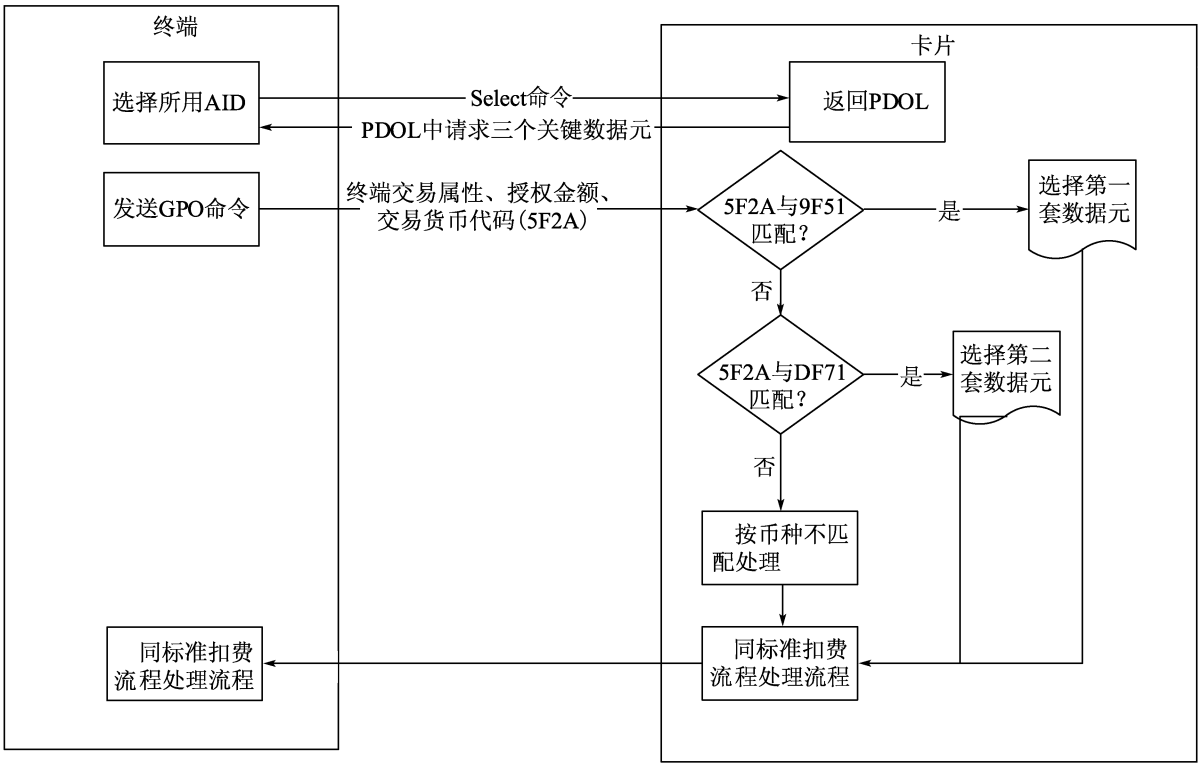
9.3.1 一般要求

电子现金双币应用的标准快速支付交易流程,应符合JT/T 978.3,交易时卡片应按9.3.2~9.3.4处理。

9.3.2 卡片风险管理

9.3.2.1 卡片在接收到终端发出的GPO命令后开始进行风险管理。如卡片具备电子现金双币应用功能,则应首先判断交易货币代码与应用货币代码数据的匹配。具体判断过程见图4。

9.3.2.2 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。



注1：三个关键数据元——由终端给卡片传的相关交易数据——包括：终端交易属性、授权金额和交易货币代码。

注2：第一套数据元——即第一货币对应的数据元。

注3：第二套数据元——即第二货币对应的数据元。

图4　卡片风险管理判断过程

9.3.2.3　卡片在风险管理结束后，返回GPO命令的响应数据时：

a）　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（标签“9F5D”）的计算；

b）　如卡片需要在发卡机构自定义数据中返回电子现金余额或脱机可用余额，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或第二币种电子现金余额参与计算。

9.3.3　读应用数据

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”），通过GET DATA读取电子现金余额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GPO命令的处理如下：

a）　当终端以GET DATA命令读取电子现金余额时，卡片应将第二币种电子现金余额的值返回；

b）　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；

c）　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；

d）　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；

e）　当终端以GET DATA命令读取脱机可用余额时，卡片应使用第二币种电子现金余额的值参与计算；

f) 当终端以 GET DATA 命令读取卡片 CVM 限额(标签“9F6B”)时,卡片应将第二币种卡片 CVM 限额(标签“DF72”)的值返回。

注:若未收到 GPO 命令或者 GPO 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。保证终端在不作流程上改变的情况下,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。

9.3.4 发卡机构脚本处理

卡片应支持发卡机构通过 PUT DATA 命令修改第二币种相关数据元。

9.4 电子现金双币应用的分时分段扣费交易流程

9.4.1 一般要求

电子现金双币应用的分时分段扣费交易流程,应符合 JT/T 978.3,交易时卡片应按 9.4.2 处理。

9.4.2 分时分段扣费押金抵扣功能的特殊处理

在分时分段扣费交易模式下,发卡机构可选择具备押金抵扣功能,并需在个人化时增加双币分时分段扣费抵扣限额(标签“DF82”)和双币分段扣费已抵扣金额(标签“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:
   1) 对具备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进行校验;
   2) 如果当前第二币种电子现金余额大于 0,终端继续交易;若当前第二币种电子现金余额等于 0,表示卡内余额为 0 或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终止交易。
b) 初始化应用:
   1) 当收到 GPO 命令时,进入分时分段扣费流程;
   2) 若卡片具备分时分段扣费押金抵扣功能,则当前实际可用电子现金余额等于第二币种电子现金余额加双币分时分段扣费抵扣限额减双币分时分段扣费已抵扣金额;
   3) 若卡片不具备分时分段扣费押金抵扣功能,则当前实际可用电子现金余额等于第二币种电子现金余额。
c) 读取卡片数据内容:
   1) 终端根据 GPO 返回的 AFL,向卡片发送 READ RECORD 命令;
   2) 若卡片具备押金抵扣功能,且第二币种电子现金余额小于当前交易金额,则进行押金抵扣,交易后的双币分时分段扣费已抵扣金额等于交易前双币分时分段扣费已抵扣金额加交易金额减交易前第二币种电子现金余额;
   3) 若交易后的双币分时分段扣费已抵扣金额小于电子现金双币应用分时分段扣费抵扣限额,则在最后一个记录被成功读取后,将交易后的双币分时分段扣费已抵扣金额进行更新,同时将交易后的第二币种电子现金余额设置为零,完成交易;否则交易失败。
d) 圈存操作:
   1) 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和双币分时分段扣费已抵扣金额;
   2) 若当前第二币种电子现金余额等于 0,则卡片应按如下处理:当修改余额脚本中指定的金额大于双币分时分段扣费已抵扣金额时,则圈存后的第二币种电子现金余额等于修改余额脚本中指定的金额减双币分时分段扣费已抵扣金额时,同时将双币分时分段扣费已抵扣金额清零;当修改余额脚本中指定的金额大于双币分时分段扣费已抵扣金额时,则圈

存后的第二币种电子现金余额等于修改余额脚本中指定的金额减双币分时分段扣费已抵扣金额,同时将双币分时分段扣费已抵扣金额(标签“DF83”)清零;

3) 若当前第二币种电子现金余额大于0,则按标准圈存流程处理。

e) 查询操作:

1) 标准终端只能具备第二币种电子现金余额的查询;

2) 具备分时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、双币分时分段扣费抵扣限额与双币分时分段扣费已抵扣金额,根据查询结果显示余额。

f) 更新分时分段扣费抵扣限额操作:

1) 卡片收到发卡机构发送的修改双币分时分段扣费抵扣限额的脚本命令;

2) 若修改分时分段扣费抵扣限额的脚本中指定的双币分时分段扣费抵扣限额小于双币分时分段扣费已抵扣金额,则返回‘6A80’;否则,用脚本中指定的值完成双币分时分段扣费抵扣限额的更新。

附 录 A
（规范性附录）
卡片数据元

A.1 数据元格式

数据元格式包括：数字型（n）、压缩数字型（cn）、二进制（b）、字母数字（an）、特殊字母数字（ans）。

A.2 补位规则

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：

a） 数字型（n）格式的数据元右对齐，左补 0；

b） 压缩数字型（cn）格式的数据元左对齐，右补 F；

c） 字母数字（an）格式的数据元左对齐，右补 0；

d） 特殊字母数字（ans）格式的数据元左对齐，右补 0。

A.3 卡片电子现金标准数据元

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，都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。卡片的数据元见表 A.1～表 A.5。

表 A.1 卡片电子现金标准数据元

名字	格式	标签	长度（字节）	条 件	描 述	值（十六进制）
应用密文（AC）	b64	9F26	8	R	生成应用密文命令返回的密文	
应用货币代码	n3	9F42	2	C 如果 CVM 中要求金额检查，需要此数据	按 GB/T 12406 编码要求	
应用货币代码	n3	9F51	2	C 如果执行频度检查	本部分专有数据。按 GB/T 12406 编码要求	
应用货币指数	n1	9F44	1	O	指出金额数据中小数点从最右边开始第几个位置	
应用缺省行为（ADA）	b16	9F52	2	C 如果具备发卡机构认证	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	
应用自定义数据	b8-256	9F05	1～32	O	和卡片应用有关的发卡机构指定数据	
应用生效日期	n6-YYMMDD	5F25	3	O	卡片中应用启用日期	
应用失效日期	n6-YYMMDD	5F24	3	M	卡片中应用的失效日期	

表 A.1（续）

名字	格式	标签	长度（字节）	条　件	描　　述	值（十六进制）
应用文件定位器（AFL）	变长	94	变长：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）	
应用标识符（AID）	b40-128	4F	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）	b16	82	2	M	一个列表，说明此应用中卡片具备指定功能的能力	
应用标签	ans1-16	50	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	ans1-16	9F12	1～16	O	和 AID 相关的便于记忆的数据。如果终端具备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）	变长：最大 cn19	5A	变长：最大 10	M	持卡人有效账号	
应用主账号序列号	n2	5F34	1	O	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	b8	87	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	a）位 8： 1）1-没有持卡人确认应用不能选择； 2）0-没有持卡人确认应用可以选择。 b）位 7～5：RFU（000） c）位 4～1： 1）0000-不指定优先级； 2）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	b	61	变长：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	b16	9F36	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	b16	9F07	2	O	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	

表 A.1（续）

名字	格式	标签	长度（字节）	条　件	描　　述	值（十六进制）
应用版本号	b16	9F08	2	M	应用版本号	
授权响应码	an2	8A	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： a）Y1-脱机接受； b）Z1-脱机拒绝； c）Y3-不能联机（脱机接受）； d）Z3-不能联机（脱机拒绝）
卡片风险管理数据对象列表 1（CDOL1）	b	8C	变长：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）	b	8D	变长：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）	b32		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	
持卡人姓名	ans2-26	5F20	2～26	R	如果持卡人姓名小于或等于 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	ans27-45	9F0B	27～45	O	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	an40	9F61	1～40	O	持卡人证件号	

表 A.1（续）

名字	格式	标签	长度（字节）	条　件	描　　述	值（十六进制）
持卡人证件类型	cn1	9F62	1	O	表明持卡人证件类型	a）00-身份证； b）01-军官证； c）02-护照； d）03-入境证； e）04-临时身份证； f）其他
持卡人验证方法（CVM）列表	b	8E	变长：最大 252	R	按优先顺序列出卡片应用具备的所有持卡人验证方法。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）	b8	8F	1	C 如果具备 SDA 或 DDA	在 SDA 或 DDA 过程中，和 RID 一起使用，用来标识 CA 公钥	
连续脱机交易计数器（国际—货币）	b8		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）	b8	9F53	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）	b8		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）	b8	9F72	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	b8	9F27	1	R	表明卡片返回的密文类型并指出终端要进行的操作	
密文版本号	n2		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	n12		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
累计脱机交易金额限制数	n12	9F54	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	

表 A.1（续）

名字	格式	标签	长度（字节）	条　件	描　　述	值(十六进制)
累计脱机交易金额（双货币）	n12		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）	n12	9F75	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	n12	9F5C	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	8n	9F73	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	a)字节 1： 1)位 8～5：小数点位置。从右边开始移动的位数； 2)位 4～1：转换因子的第 1 个数字； b)字节 2～4：剩下的 6 个数字
数据认证码	b16	9F45	2	O	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	b128		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加密时使用	
专用文件(DF)名称	b40-128	84	5～16	R	按 GB/T 16649.4 规定的，DF 的名字	
分散密钥索引(DKI)	b8		1	O	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	发卡机构指定。 如果不存在，缺省值为 0

表 A.1（续）

名字	格式	标签	长度（字节）	条　件	描　　述	值（十六进制）
目录自定义模板	变长	73	变长：最大 252	O	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）	b	9F49	变长：最大 252	C 如果具备 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	b1			C 如果具备 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	变长	BF0C	变长：最大 222	O	FCI 中的发卡机构自定义部分	
文件控制信息（FCI）专用模板	变长	A5	变长	R	按 GB/T 16649.4，标识 FCI 模板中，专用于本部分的数据对象	
文件控制信息（FCI）模板	变长	6F	变长：最大 252	R	按 GB/T 16649.4，标识 FCI 模板	
卡片动态数据			变长	C 如果具备 DDA	卡片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	
IC 动态数	b	9F4C	2～8	C 如果具备 DDA	DDA 处理过程中，卡片生成的随时间变化不同的随机数。包括在签名动态数据中送到终端，由终端恢复	
卡片私钥	b		NIC	C 如果具备 DDA	卡片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	
卡片 RSA 公钥指数	b	9F47	1/3	C 如果具备 DDA	卡片 RSA 公钥指数用于验证签名的动态应用数据	
卡片公钥证书	b	9F46	NI	C 如果具备 DDA	发卡机构认证过的卡片公钥	
卡片 RSA 公钥余数	b	9F48	NIC-Ni+42	C 如果需要	没有放入卡片公钥证书的卡片 RSA 公钥部分	
发卡机构行为代码（IAC）-缺省	b40	9F0D	5	R 将变成必备	指定当交易请求联机但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	b40	9F0E	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

表 A.1（续）

名字	格式	标签	长度（字节）	条　件	描　　述	值(十六进制)
发卡机构行为代码(IAC)-联机	b40	9F0F	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	b	9F10	变长:最大32	R	在一个联机交易中,要传送到发卡机构的专有应用数据。 第1字节是自定义数据长度。 格式内容: a)长度(07)(1字节); b)分散密钥索引(1字节); c)密文版本号(1字节); d)卡片验证结果(CVR)(4字节); e)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	b64-128	91	8～16	O	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: a)ARPC(8字节); b)授权响应码(2字节)	
发卡机构认证失败指示位	b1			C 如果具备发卡机构认证	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: a)发卡机构认证执行但失败; b)发卡机构认证没有执行但必备	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	b8	9F56	-1	C 如果具备发卡机构认证	专有数据。标明当具备发卡机构认证时,是必备还是可选	a)位8: 1)发卡机构认证必备; 2)发卡机构认证可选。 b)位7～1:RFU(0000000)

表 A.1（续）

名字	格式	标签	长度（字节）	条　件	描　　述	值(十六进制)
发卡机构代码表索引	n2	9F11	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	a)01-GB/T 15273-1; b)02-GB/T 15273-2; c)03-GB/T 15273-3; d)04-GB/T 15273-4; e)05-GB/T 15273-5; f)06-GB/T 15273-6; g)07-GB/T 15273-7; h)08-GB/T 15273-8; i)09-GB/T 15273-9; j)10-GB/T 15273-10
发卡机构国家代码	n3	5F28	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	n3	9F57	2	C 如果具备卡片频度检查	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	b	90	NCA	C 如果具备 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	b	9F32	1/3	C 如果具备 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卡片公钥证书	
发卡机构 RSA 公钥余数	b	92	NI－NCA +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	b	86	变长:最大 261	O	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 C 中的命令描述	见附录 C
发卡机构脚本命令计数器	b4			C 如果具备发卡机构脚本	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	a)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; b)'F'-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	b1			C 如果具备发卡机构脚本	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 2	b	72	变长	C 如果具备发卡机构脚本	最后的生成应用密文命令后,包括发送到卡片的发卡机构专用数据	

表 A.1（续）

名字	格式	标签	长度（字节）	条　件	描　　述	值（十六进制）
发卡机构 URL	ans	5F50	变长	O	存放发卡机构服务器在互联网上的位置	
发卡机构 URL2	ans	9F5A	变长	O	本部分定义的。存放发卡机构服务器在互联网上的位置	
首选语言	an2	5F2D	2～8	O	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	b16	9F13	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	b16	9F4D	2	O	提供交易日志文件的 SFI 和交易日志文件记录个数	a）字节 1：交易日志循环记录文件的 SFI； b）字节 2：交易日志文件中的记录个数
交易日志格式	b	T：9F4F	变长	O	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	b8	9F14	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	b8	9F58	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	b128		16	C 如果具备发卡机构脚本使用安全报文	专有数据。双长度安全报文鉴别（MAC）密钥，16 字节。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	b1			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	b1			C 如果卡片具备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，需要联机授权但没有实现
卡片请求联机指示位	b1			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	

表 A.1（续）

名字	格式	标签	长度（字节）	条　件	描　　述	值（十六进制）
PIN 尝试计数器	b8	9F17	1	C 如果具备脱机 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	b8		1	C 如果具备脱机 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）	b	9F38	变长	C 在终端进行初始化应用时需要	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）	b		0～11	R	按 GB/T 16649.5 规定的，AID 的组成部分之一	
脱机 PIN	b		8	C 如果具备脱机 PIN	专有数据。在卡片个人化时由发卡机构写入卡片	
注册的应用提供商标识（RID）	b		5	R	按 GB/T 16649.5 规定的，AID 的组成部分之一	
响应报文模板格式 1	变长	80	变长	R	卡片命令响应信息，包括数据对象（不包括标签和长度）	
响应报文模板格式 2	变长	77	变长	C 如果具备 CDA	卡片命令响应信息，包括数据对象（包括标签和长度）	
第 2 应用货币代码	n3	9F76	2	C 如果具备双货币频度检查	第 2 种货币，要转换成应用指定货币。按 GB/T 12406 编码	
服务码	n3	5F30	2	O	按 GB/T 17552 的规定	
短文件标识符（SFI）	b8	88	1	R	命令中用于标识文件。字节中高三位为 0	a）1～10：规范定义； b）11～20：卡片系统定义； c）21～30：发卡机构定义
签名的动态应用数据	b	9F4B	NIC	C 如果具备 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）	b	93	NI	C 如果具备 SDA	发卡机构签名的数据签名。用卡片内的指定数据生成	

表 A.1（续）

名字	格式	标签	长度（字节）	条　件	描　　述	值（十六进制）
静态数据认证（SDA）失败指针	b1			C 如果具备 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
静态数据认证标签列表		9F4A	变长	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卡片公钥证书中	可以只包括应用交互特征（AIP）的标签
发卡机构自定义数据	ans	9F1F	变长	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	b	57	a）变长：最大 19； b）变长：最大 19； c）1； d）n4； e）n3； f）0 或 n5； g）n。 16 进制格式。	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： a）应用主账号（PAN）； b）分隔符（“D”）； c）失效日期（YYMM）； d）服务码； e）PIN 验证域； f）自定义数据； g）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）	b	97	变长：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	b128		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	b8	9F23	1	C 如果具备终端频度	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	b8	9F59	1	C 如果无法联机，卡片风险管理可以得出交易拒绝结论	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值	
自定义数据	b56		变长：7～9	R	发卡机构应用数据的一部分，包括： a）一个长度字节； b）分散密钥索引； c）密文版本号； d）卡片验证结果。 在生成应用密文命令中返回给终端	

表 A.1（续）

名字	格式	标签	长度（字节）	条　件	描　　述	值(十六进制)
产品标识信息	b128	9F63	16	O	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	a)字节 1～8:发卡机构代码; b)字节 9:产品标识: 1)位 8:1 = 市民卡; 2)位 7:1 = 军人卡; 3)位 6:1 = 积分卡; 4)位 5:1 = 交通卡; 5)位 4:1 = 社保卡; 6)位 3:1 = 学生卡; 7)位 2:1 = 航空卡; 8)位 1:1 = 公共缴费类卡; c)字节 10:产品标识,移动支付规范保留; d)字节 11:产品标识,发卡机构保留; e)字节 12～14:本部分保留; f)字节 15～16:发卡机构保留
SM 算法具备指示器	b8	DF69	1	C 如果卡片具备 SM 国密算法	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	b	DF11	32	O	应用选择返回的发卡机构特殊数据元信息	a)字节 01～08:发卡机构代码; b)字节 09: 应用主账号序列号; c)字节 10～19:应用主账号; d)字节 20:卡种类型: 1)0x01-普通卡; 2)0x02-学生卡; 3)0x03-老人卡; 4)0x04-测试卡; 5)0x05-军人卡; 6)0x96～0xC8 本规范保留; 7)其他:发卡机构自定义; e)字节 21:卡状态字;

表 A.1（续）

名字	格式	标签	长度（字节）	条　件	描　　述	值（十六进制）
发卡机构特殊数据元	b	DF11	32	O	应用选择返回的发卡机构特殊数据元信息	f）字节 22～25：国际代码； g）字节 26～27：省级代码； h）字节 28～29：城市代码； i）字节 30～31：互通卡种； j）字节 32：预留
注：R-需求，数据应存在，在读应用数据过程中，终端不检查。						

表 A.2　电子现金专用数据元

名字	格式	标签	长度（字节）	条件	描　　述	备份	获取	值（十六进制）
可用脱机消费金额	n12	9F5D	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度，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	a）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； b）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）； c）如果卡片的私钥的长度大于 1 024 位，则此数据元通过读记录指令（READ RECORD）而不是通过 GPO 读出
卡片附加处理	b32	9F68	4	如果具备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，在此条件下应具备	指出卡片处理需求和参数选择	N	GET DATA（SD）	a）字节 1： 1）位 8：1-具备小额检查； 2）位 7：1-具备小额和 CTTA 检查； 3）位 6：1-具备小额或 CTTA 检查； 4）位 5：1-具备新卡检查； 5）位 4：1-具备 PIN 重试次数超过检查； 6）位 3：1-允许货币不匹配的脱机交易； 7）位 2：1-卡优先选择接触式联机；

表 A.2(续)

名字	格式	标签	长度(字节)	条件	描　　述	备份	获取	值(十六进制)
卡片附加处理	b32	9F68	4	如果具备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,在此条件下应具备	指出卡片处理需求和参数选择	N	GET DATA (SD)	8)位 1:1-返回可用脱机消费金额。 b)字节 2: 1)位 8:1-具备预付; 2)位 7:1-不允许不匹配货币交易; 3)位 6:1-如果是新卡且终端仅具备脱机则拒绝交易; 4)位 5:1-脱机批准的交易,卡片记录交易日志; 5)位 4～1:保留。 c)字节 3: 1)位 8:1-匹配货币的交易具备联机 PIN; 2)位 7:1-不匹配货币的交易具备联机 PIN; 3)位 6:1-对于不匹配货币交易,卡要求 CVM; 4)位 5:1-具备签名; 5)位 4～1:保留; d)保留
卡片 CVM 限额	n12	9F6B	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
卡片内部指示器	b16		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: 1)位 8 中断; 2)位 7 脱机只具备终端; 3)位 6 匹配货币
卡片交易属性	b16	9F6C	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	a)字节 1: 1)位 8:1-需要联机 PIN; 2)位 7:1-需要签名; 3)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; 4)位 5:1-如果脱机数据认证失败而且终端具备的卡片应用则终止; 5)位 4～1:保留。 b)字节 2 位 8～1 保留

表 A.2（续）

名字	格式	标签	长度（字节）	条件	描　　述	备份	获取	值(十六进制)
应用交互特征	b16	82	2	必备卡片数据元	说明此应用中卡片具备指定功能的能力	N	GPO	a)字节 1： 1)位 8:RFU； 2)位 7:1-具备 SDA； 3)位 6:1-具备 DDA； 4)位 5:1-具备持卡人验证； 5)位 4:1-具备终端风险管理； 6)位 3:1-具备发卡机构认证； 7)位 2:1-RFU； 8)位 1:1-具备 CDA。 b)字节 2： a)位 8:0； b)位 7～1:RFU
上次联机应用交易计数器	b16	9F13	2	可选卡片数据元	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	n12		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	
非接触终端交易限额	n12		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，允许在其他界面尝试此交易	N/A	N/A	
终端执行 CVM 限额	n12		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	b32	9F66	4	必备终端数据元	指示终端能力，对卡片的参数选择	N/A	N/A	见 JT/T 978.3
电子现金余额	n12	9F79	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	n12	9F77	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

表 A.2（续）

名字	格式	标签	长度（字节）	条件	描　　述	备份	获取	值（十六进制）
电子现金重置阈值	n12	9F6D	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	n12	9F78	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	a6	9F74	6	可选卡片数据元	电子现金交易或卡片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	b16	9F08	2	必备数据元	应用的版本号	N	READ RECORD	系统定义

表 A.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（字节）	格式
第二币种电子现金应用货币代码	DF71	2	n4
第二币种电子现金余额	DF79	6	n12
第二币种电子现金余额上限	DF77	6	n12
第二币种电子现金单笔交易限额	DF78	6	n12
第二币种电子现金重置阈值	DF76	6	n12

表 A.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	1～15	N/A	发卡机构指定固定数据	无

表 A.5　电子钱包数据元

数据域	说　　明	来源	格式	长度（字节）	值（十六进制）
算法标识（DLK）	用来标识圈存交易的加密算法	卡片	b	1	
算法标识（DPK）	用来标识消费和取现交易的加密算法	卡片	b	1	

表 A.5（续）

数据域	说　明	来源	格式	长度(字节)	值(十六进制)
算法标识（DTK）	用来标识在交易中计算 TAC 使用的加密算法	卡片	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	卡片	b	1	
算法标识（DULK）	用来标识在圈提交易中使用的加密算法	卡片	b	1	
应用有效日期	该日期后卡应用终止	卡片	cn CCYYMMDD	4	
应用标识符	用于标识一个应用，并符合 GB/T 16649.5	卡片 终端	b	5～16	
应用主账号	发卡机构分配的一个数字	卡片	cn	10	
应用生效日期	指示应用生效日期	卡片	cn CCYYMMDD	4	
应用类型标识	卡片具备的表示卡存在的应用	卡片	cn	1	02
应用版本号	表示卡片当前使用的应用版本的一个数字	卡片	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	卡片	n	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	卡片	b	1	
持卡人类型标识		卡片	cn	1	a)00-普通卡； b)01-学生卡； c)02-老人卡； d)03-军人卡； e)04-内部员工卡； f)其他-保留； g)所有其他值预留
持卡人证件号码	用来标识持卡人	卡片	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	卡片	cn	1	a)00-身份证； b)01-军官证； c)02-护照； d)03-入境证（仅限香港/澳门/台湾居民使用）； e)04-临时身份证； f)05-其他
持卡人姓名	根据 GB/T 17552 格式，标识持卡人姓名	卡片	an	20	
电子钱包余额	卡片中电子钱包的当前余额	卡片	b	4	

表 A.5（续）

数据域	说　明	来源	格式	长度(字节)	值(十六进制)
交易计数器	卡片中的一个计数器,每发生一次交易时就增加	卡片	b	2	
发卡机构标代码	用来唯一标识发卡机构的一个数字	卡片	cn	4	
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	卡片	b	2	
密钥索引号	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	卡片 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	卡片	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	卡片	b	1	
密钥版本号(DTK)	用来唯一标识计算 TAC 所用的密钥版本	卡片	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	卡片	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	卡片	b	1	
透支限额	发卡机构给持卡人指定的最大透支额度	卡片	b	3	
伪随机数(卡片)	卡片随机产生的一个数字	卡片	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 卡片	cn	1	a)02-圈存; b)03-圈提; c)06-消费; d)07-修改透支限额; e)09-复合应用消费

附 录 B
（规范性附录）
应用数据与文件

B.1 应用数据

B.1.1 联机应用数据

B.1.1.1 卡片数据对象

卡片数据对象列表见表 B.1。

表 B.1 卡片数据对象列表

数据名称	数据格式	标签	长度（字节）	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	说明此应用中卡片具备的功能	M			
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	M			
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	初始设置为 00 30	行业主管部门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	M			M
卡片内部数据	变长				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		1bit	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		1bit	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		1bit	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				
发卡机构认证失败指示位	b		1bit	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				
静态数据认证(SDA)失败指示位	b		1bit	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		1bit	初始设置为 0	标明当上次交易拒绝时 DDA 是否失败				

表 B.1（续）

数据名称	数据格式	标签	长度（字节）	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		M		
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，卡片应用规范提供推荐值：0B 0A a）字节 1：循环交易日志文件的 SFI，为 11（十进制）； b）字节 2：交易日志文件中的记录个数，为 10（十进制）	M			
日志格式	b	9F4F	变长	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	M			
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		M		
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		M		
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				

表 B.1（续）

数据名称	数据格式	标签	长度（字节）	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		M		
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 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		M		
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		M		
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		M		
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。用于具备密文版本 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： a）授权金额； b）其他金额； c）终端国家代码； d）终端验证结果； e）交易货币代码； f）交易日期； g）交易类型； h）终端不可预知数； i）交易时间和商户名称	M			M
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	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： a）发卡机构响应码； b）授权金额； c）其他金额； d）终端国家代码；	M			M

表 B.1（续）

数据名称	数据格式	标签	长度（字节）	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	9A03 9C01 9F37 04 9F21 03	e）终端验证结果； f）交易货币代码； g）交易日期； h）交易类型； i）终端不可预知数； j）交易时间	M			M
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	M			
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	M			M
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	M			M
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终端不能完成联机上送的交易拒绝的条件	M			M
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		M		
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		M		M
首选语言	ans	5F2D	2	发卡机构模板	当终端具备多种语言时，终端根据发卡机构首选语言显示终端信息		M		
应用货币码	n	9F51		发卡机构模板	发卡机构的国内货币		M		M
应用标识符（AID）	b	4F	8～16	初始化好的	A0000000632010105 A0000000632010106				
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		M		
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）	M			M
应用主帐号序列号	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			M	M

表 B.1（续）

数据名称	数据格式	标签	长度（字节）	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
持卡人姓名	ans	5F20	2～26	从发卡机构基本信息数据文件提供				M	M
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			M	M
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			M	M
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			M	M
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			M	M
应用生效日期	n	5F25	3	发卡机构模板	卡片中应用启用日期		M		M
应用主账户（PAN）	cn	5A	最大 10	发卡机构基本信息数据文件提供				M	M
服务码	n	5F30	2	发卡机构基本信息数据文件提供				M	M
发卡机构自定义数据	ans	9F1F	变长	发卡机构基本信息数据文件提供				M	M
发卡机构基本信息数据	变长	57	最大 19	发卡机构基本信息数据文件提供				M	M
持卡人验证方法（CVM）列表	b	8E	12	0000 0000 0000 0000 0203 1F00	按优先顺序列出卡片应用具备的所有持卡人验证方法	M			M
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		M		M
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		M		M

表 B.1（续）

数据名称	数据格式	标签	长度（字节）	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
发卡机构公钥余数(如果需要)	b	92	$N_I - N_{CA} + 36$	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		M		M
发卡机构公钥指数	b	9F32	1 to $N_I/4$	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卡片公钥证书		M		M
签名的静态应用数据(SAD)	b	93	变长	发卡机构模板	用发卡机构签名的应用数据			M	M
卡片公钥证书	b	9F46	NI	发卡机构模板	发卡机构认证过的卡片公钥			M	M
卡片公钥指数	b	9F47	1/3	发卡机构模板	卡片公钥指数用于验证签名的动态应用数据			M	M
卡片公钥余数	b	9F48	NIC – NI + 42	发卡机构模板	没有放入卡片公钥证书的卡片公钥部分			M	M
卡片私钥	b		NIC	发卡机构模板	卡片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			M	
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		M		M
应用缺省行为(ADA)	b	9F52	2	C000	如果具备发卡机构认证。卡片应用专有数据。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	M			
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			M	
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			M	
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				

表 B.1（续）

数据名称	数据格式	标签	长度（字节）	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
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				
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。									

B.1.1.2　应用交互特征（AIP）设置

应用交互特征（AIP）宜设置为‘7C00’，见表 B.2。

表 B.2　应用交互特征（AIP）

字　　节	位	值	说　　明
1	8	0	RFU
1	7	1	具备 SDA
1	6	1	具备 DDA
1	5	1	具备持卡人认证
1	4	1	具备终端风险管理
1	3	1	具备发卡机构认证
1	2	0	RFU
1	1	0	不具备 CDA
2	8～1	0000　0000	RFU

B.1.1.3　应用优先指示器

应用优先指示器宜设置为‘01’，见表 B.3。

表 B.3　应用优先指示器

字　　节	位	值	意　　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

B.1.1.4 卡片内部数据

卡片内部数据见表 B.4。

表 B.4 卡片内部数据

卡片内部数据	保 留	初 始 值	标 签
联机授权指示位	1bit	0	
卡片请求 ARQC 指示位	1bit	0	
卡片请求 AAC 指示位	1bit	0	
发卡机构认证失败指示位	1bit	0	
静态数据(SDA)认证失败指示位	1bit	0	
动态数据认证(DDA)失败指示位	1bit	0	
发卡机构脚本失败指示位	1bit		
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	4bits		
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

B.1.1.5 日志格式

日志格式宜设置为‘9A 03 9F21 03 9F02 06 9F03 06 9F1A 02 5F2A 02 9F4E 14 9C 01 9F36 02’,见表 B.5。

表 B.5 日志格式的标签和长度

数据对象名称	标 签	长度(字节)
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
交易货币代码	5F2A	2

表 B.5 （续）

数据对象名称	标　签	长度(字节)
商户名称	9F4E	20
交易类型	9C	1
应用交易计数器(ATC)	9F36	2

B.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 宜设置为‘9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03 9F4E 20’,见表 B.6。

表 B.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	标　签	长度(字节)
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

B.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 宜设置为‘8A 02 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03’,见表 B.7。

表 B.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	标　签	长度(字节)
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
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

B.1.1.8 发卡机构行为代码（IAC)(拒绝、联机和缺省)

发卡机构行为代码宜按如下设置：

a) ‘00 10 98 00 00’(发卡机构行为代码-拒绝)；

b) ‘D8 68 04 F8 00’(发卡机构行为代码-联机)；

c) ‘D8 60 04 A8 00’(发卡机构行为代码-缺省)。

发卡机构行为代码见表 B.8。

表 B.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
卡片数据缺失	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
卡片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
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

表 B.8(续)

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
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

B.1.1.9　发卡机构应用数据

发卡机构应用数据见表 B.9。

表 B.9　发卡机构应用数据

字节	位	值(十六进制)	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		其他的发卡机构自定义数据

B.1.1.10　应用标识符和应用标签

应用标识符和应用标签见表 B.10。

表 B.10　应用标识符和应用标签

应用标识符 (AID)	应用标签
A000000632010105	电子现金应用
A000000632010106	电子钱包应用

B.1.1.11　应用用途控制

应用用途控制宜设置为‘FF00’,见表 B.11。

表 B.11　应用用途控制

字节	b8	b7	b6	b5	b4	b3	b2	B1	说　明
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

表 B.11(续)

字节	b8	b7	b6	b5	b4	b3	b2	B1	说　明
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	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
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。									

B.1.1.12　持卡人验证方法(CVM)列表

持卡人验证方法(CVM)列表宜设置为‘0000 0000 0000 0000　0203 1F00’,见表 B.12。

表 B.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	如果终端具备	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

B.1.1.13　动态数据对象列表(DDOL)

动态数据对象列表(DDOL)宜设置为‘9F37 04’,见表 B.13。

表 B.13　动态数据对象列表(DDOL)数据对象的标签和长度

值	标　签	长度(字节)
不可预知数	9F37	4

B.1.1.14　应用缺省行为

应用缺省行为宜设置为‘C000’,见表 B.14。

表 B.14　应用缺省行为

字节	位	值	说　明
1	8	1	如果发卡机构认证失败,下次联机交易

表 B.14(续)

字节	位	值	说　明
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

B.1.2　脱机应用数据

B.1.2.1　卡片数据对象

卡片数据对象列表见表 B.15。

表 B.15　卡片数据对象

数据名称	数据格式	标签	长度(字节)	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,即卡片充值所能达到的上限			M	
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	M			M
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			M	
电子现金重置阈值	n	9F6D	6	发卡机构模板	触发卡片进行自动充值的可用余额下限			M	

表 B.15(续)

数据名称	数据格式	标签	长度(字节)	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
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)	M			M
持卡人验证方法(CVM)列表	b	8E	10	0000 0000 0000 0000 1F03	按优先顺序列出卡片应用具备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	M			M
发卡机构行为代码(IAC)-拒绝	b	9F0E	5	00 10 80 00 00	指定交易不进行联机直接拒绝的条件	M			M
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	M			M
发卡机构行为代码(IAC)-缺省	b	9F0D	5	D8 60 3C A8 00	指定当交易请求联机但终端不能完成联机上送的交易拒绝的条件	M			M

B.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)宜设置为‘9F7A 01 9F02 06 5F2A 02 DF69 01’,见表 B.16。

表 B.16　处理选项数据对象列表(PDOL)

数据对象名称	标　　签	长度(字节)
电子现金终端具备指示器	9F7A	1
授权金额	9F02	6
交易货币代码	5F2A	2
SM2 算法具备指示器	DF69	1

B.1.2.3　持卡人验证方法(CVM)列表

持卡人验证方法(CVM)列表宜设置为‘0000 0000 0000 0000 1F03’,见表 B.17。

表 B.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	如果终端具备	CVM 处理过程失败

B.1.2.4　发卡机构行为代码 (IAC)(拒绝、联机和缺省)

发卡机构行为代码宜按如下设置:

a)　‘00 10 80 00 00’(发卡机构行为代码-拒绝);

b) ‘D8 68 3C F8 00’(发卡机构行为代码-联机);

c) ‘D8 60 3C A8 00’(发卡机构行为代码-缺省) 见表 B.18。

表 B.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
脱机静态数据认证(SDA)失败	0	1	1
卡片数据缺失	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
卡片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

B.1.3 非接触式应用数据

B.1.3.1 卡片数据对象

卡片数据对象见表 B.19。

表 B.19 卡片数据对象

数据名称	数据格式	标签	长度（字节）	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	说明此应用中卡片具备的功能	具备			
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）	M			M
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		M		
CAPP 交易指示位	b	DF60	1	初始设置为 00	如果卡片具备电子现金 CAPP 扩展应用交易，则需在 PDOL 中指明此数据： a）00-终端不具备电子现金扩展应用； b）01-选择或执行分时分段扣费交易； c）02-选择或执行脱机预授权交易； d）03-选择或执行脱机预授权完成交易				
分段扣费应用标识	b	DF61	1	01/02	如果卡片仅具备分段扣费交易时，发卡机构在 BF0C 中进行个人化 a）1-卡片仅具备分段扣费交易； b）2-卡片同时具备分段扣费交易和预授权交易功能				

表 B.19(续)

数据名称	数据格式	标签	长度(字节)	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
电子现金分时分段扣费抵扣限额	cn	DF62	6	初始设置为 0	如果卡片具备分时分段扣费抵扣功能,表示卡片在分时分段扣费交易中可抵扣的最大额度				
电子现金分时分段扣费已抵扣额	cn	DF63	6	初始设置为 0	如果卡片具备分时分段扣费抵扣功能,表示卡片当前已抵扣的额度				

B.1.3.2　应用交互特征(AIP)设置

应用交互特征(AIP)宜设置为‘7C00’,见表 B.20。

表 B.20　应用交互特征(AIP)

字　　节	位	值(二进制)	说　　明
1	8	0	RFU
1	7	1	具备 SDA
1	6	1	具备 fDDA
1	5	1	具备持卡人认证
1	4	1	具备终端风险管理
1	3	1	具备发卡机构认证
1	2	0	RFU
1	1	0	不具备 CDA
2	8～1	00000000	RFU

B.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)宜设置为‘9F66 04 9F02 06 9F37 04 5F2A 02 DF60 01(DF69 01)’,见表 B.21。

表 B.21　处理选项数据对象列表(PDOL)

数据对象名称	标　　签	长度(字节)
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
SM 算法具备指示器(可选数据)	DF69	1

B.1.3.4 卡片附加处理

卡片附加处理宜设置为‘81 40 00 00’,见表 B.22。

表 B.22 卡片附加处理

字节	位	值(二进制)	说 明
1	8	1	具备小额检查
1	7	0	不具备小额和 CTTA 检查
1	6	0	不具备小额或 CTTA 检查
1	5	0	不具备新卡检查
1	4	0	不具备 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
1	1	1	返回脱机消费可用额度
2	8	0	不具备预付
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具备脱机,不拒绝交易
2	5~1	00000	RFU
3	8	0	匹配货币的交易不具备联机 PIN
3	7	0	不匹配货币的交易不具备联机 PIN
3	6	0	对于不匹配货币交易,卡不要求 CVM
3	5	0	不具备签名
3	4~1	0000	RFU
4	8~1	00000000	RFU

B.1.3.5 卡片交易属性

卡片交易属性宜设置为‘00 00’,见表 B.23。

表 B.23 卡片交易属性

字节	位	值(二进制)	说 明
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具备接触式卡片应用,不终止
1	4~1	0000	RFU
2	8~1	00000000	RFU

B.1.3.6 发卡机构应用数据

发卡机构应用数据见表 B.24。

表 B.24 发卡机构应用数据

字节	位	值(十六进制)	条 件
1	8~1	07	长度(字节)
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
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		其他的发卡机构自定义数据

B.2 应用文件

B.2.1 电子现金专用文件

B.2.1.1 专用文件 1 (SFI=0x01)

电子现金专用文件 1 见表 B.25~表 B.27。

表 B.25 记录 1:应用基本数据

标 签	长度(字节)	值
57	Up~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 B.26 记录 2:数据认证数据 1

标 签	长度(字节)	值
90	128	发卡机构公钥证书

表 B.27 记录 3:数据认证数据 2

标 签	长度(字节)	值
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

B.2.1.2 专用文件2（SFI=0x02）

电子现金专用文件2见表B.28～表B.31。

表B.28 记录1:联机交易卡片风险管理数据

标 签	长度(字节)	值
5F25	3	应用生效日期
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B.29 记录2:数据认证数据

标 签	长度(字节)	值
93	128	签名的静态认证数据

表B.30 记录3:签名的静态认证数据

标 签	长度(字节)	值
9F46	128	ICC公钥证书

表B.31 记录4:ICC公钥数据

标 签	长度(字节)	值
9F47	1/3	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)

B.2.1.3 专用文件3（SFI=0x03）

电子现金专用文件3见表B.32～表B.35。

表B.32 记录1:脱机交易卡片风险管理数据

标 签	长度(字节)	值
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

表 B.32(续)

标　签	长度(字节)	值
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
5F28	2	发卡机构国家代码
9F0E	5	发卡机构行为码(IAC)拒绝
9F0F	5	发卡机构行为码(IAC)联机

表 B.33　记录 1:数据认证数据

标　签	长度(字节)	值
93	128	签名的静态认证数据

表 B.34　记录 2:签名的静态认证数据

标　签	长度(字节)	值
9F46	128	ICC 公钥证书

表 B.35　记录 3:ICC 公钥数据

标　签	长度(字节)	值
9F47	1/3	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)

B.2.1.4　专用文件 4 (SFI = 0x04)

电子现金专用文件 4 见表 B.36。

表 B.36　记录 1:电子现金相关数据

标　签	长度(字节)	值
9F74	6	电子现金发卡机构授权码

B.2.2　电子钱包专用文件

B.2.2.1　公共应用信息文件

电子钱包公共应用信息文件见表 B.37。

表 B.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

表 B.37(续)

文件标识(FID)		0x15
文件存取控制		读 = 自由
字节	数据元	长度(字节)
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

B.2.2.2 持卡人基本信息文件

持卡人基本信息文件见表 B.38。

表 B.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(字节)
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

B.2.2.3 管理信息文件

管理信息文件见表 B.39。

表 B.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(字节)
1～4	国际代码	4
5～6	省级代码	2

表 B.39(续)

文件标识(FID)		0x17
字节	数据元	长度(字节)
7～8	城市代码	2
9～10	互通卡种	2
11	卡种类型	1
12～60	预留	49
注:卡种类型见表 A.1 发卡机构特殊数据元(标签“DF11”)。		

B.2.2.4 交易明细文件

交易明细文件见表 B.40。

表 B.40 交易明细文件

文件标识(FID)		0x18
文件类型		循环文件
文件大小		10×23
文件存取控制		读=自由
字节	数据元	长度(字节)
1～2	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

B.2.3 金额数据

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

B.2.4 公共交通过程信息变长记录文件

B.2.4.1 公共交通过程信息变长记录文件结构

公共交通过程信息变长记录文件是变长记录结构,用于保存相应的换乘记录等信息。每条记录应有一定的预留字节,若发卡机构需要使用预留字节,则应按如下格式组织预留字节的内容:城市代码(2字节)、预留信息长度(1 字节)和预留信息内容(N 字节)。

公共交通过程信息变长记录文件见表 B.41。

表 B.41　公共交通过程信息变长记录文件

文件名称	公共交通过程信息变长记录文件——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)	2190		
文件权限	读取	自由	
	更新	保护	
记录号	记录描述		长度(字节)
1	城市轨道应用信息记录		128
2	公共汽电车应用信息记录		128
3	城市水上客运应用信息记录		128
4	出租汽车应用信息记录		128
5	租赁汽车应用信息记录		128
6	公共自行车应用信息记录		128
7	停车收费应用信息记录		112
8	长途客运应用信息记录		128
9	轮渡应用信息记录		128
10	城际铁路应用信息记录		128
11	民航应用信息记录		128
12	高速公路收费应用信息记录		128
13	优惠信息记录		30
14	本规范预留记录1		128
15	本规范预留记录2		128
16	本规范预留记录3		128
17	本规范预留记录4		128
18	本规范预留记录5		128

B.2.4.2　城市轨道应用信息记录

城市轨道应用信息记录的记录格式见表 B.42。

表 B.42　城市轨道应用信息记录

字节	数　据　元	长度(字节)	数 据 格 式
1~2	记录 ID 标识	2	2701
3	记录长度	1	固定为 0x7D
4	应用有效标识	1	固定为 0x01
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用没有锁定;1-应用锁定)	1	BCD

表 B.42(续)

字节	数 据 元	长度(字节)	数 据 格 式
7～14	交易流水号	8	BCD
15	交易状态	1	BCD
16～17	进闸城市代码	2	BCD
18～19	出闸城市代码	2	BCD
20～27	进闸机构标识	8	BCD
28～35	出闸机构标识	8	BCD
36～43	进闸站点	8	BCD
44～51	出闸站点	8	BCD
52～59	进闸终端编号	8	BCD
60～67	出闸终端编号	8	BCD
68～74	进闸时间	7	YYYYMMDDhhmmss
75～81	出闸时间	7	YYYYMMDDhhmmss
82～85	最大消费金额	4	HEX(高字节在前)
86～128	本规范预留	43	初始为 00

B.2.4.3 公共汽电车应用信息记录

公共汽电车应用信息记录的记录格式见表 B.43。

表 B.43 公共汽电车应用信息记录

字节	数 据 元	长度(字节)	数 据 格 式
1～2	记录 ID 标识	2	2702
3	记录长度	1	固定为 0x7D
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用没有锁定;1-应用锁定)	1	BCD
7～14	交易流水号	8	BCD
15	交易状态	1	BCD
16～17	上车城市代码	2	BCD
18～19	下车城市代码	2	BCD
20～27	上车机构标识	8	BCD
28～35	下车机构标识	8	BCD
36～43	上车站点	8	BCD
44～51	下车站点	8	BCD
52～59	上车终端编号	8	BCD
60～67	下车终端编号	8	BCD

表 B.43(续)

字节	数 据 元	长度(字节)	数 据 格 式
68～74	上车时间	7	YYYYMMDDhhmmss
75～81	下车时间	7	YYYYMMDDhhmmss
82～85	最大消费金额	4	HEX(高字节在前)
86	方向标识	1	HEX
87～88	线路号	2	HEX(高字节在前)
89～94	车辆号	6	ASCII
95～128	本规范预留	34	初始为 00

B.2.4.4 城市水上客运应用信息记录

城市水上客运应用信息记录的记录格式见表 B.44。

表 B.44 城市水上客运应用信息记录

字节	数 据 元	长度(字节)	数 据 格 式
1～2	记录 ID 标识	2	2703
3	记录长度	1	固定为 0x7D
4	应用有效标识	1	固定为 0x01
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用没有锁定;1-应用锁定)	1	BCD
7～128	本规范预留	122	初始为 00

B.2.4.5 出租汽车应用信息记录

出租汽车应用信息记录的记录格式见表 B.45。

表 B.45 出租汽车应用信息记录

字节	数 据 元	长度(字节)	数 据 格 式
1～2	记录 ID 标识	2	2704
3	记录长度	1	固定为 0x7D
4	应用有效标识	1	固定为 0x01
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用没有锁定;1-应用锁定)	1	BCD
7～128	本规范预留	122	初始为 00

B.2.4.6 租赁汽车应用信息记录

租赁汽车应用信息记录的记录格式见表 B.46。

表 B.46　租赁汽车应用信息记录

字节	数　据　元	长度(字节)	数 据 格 式
1～2	记录 ID 标识	2	2705
3	记录长度	1	固定为 0x7D
4	应用有效标识	1	固定为 0x01
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用没有锁定;1-应用锁定)	1	BCD
7～14	交易流水号	8	BCD
15	交易状态	1	BCD
16～17	借车城市代码	2	BCD
18～19	还车城市代码	2	BCD
20～27	借车受理机构标识	8	BCD
28～35	还车受理机构标识	8	BCD
36～43	借车终端编号	8	BCD
44～51	还车终端编号	8	BCD
52～59	车辆信息	8	BCD
60～66	租车时间	7	YYYYMMDDhhmmss
67～73	还车时间	7	YYYYMMDDhhmmss
74～77	预授权金额	4	HEX(高字节在前)
78～128	本规范预留	51	初始为 00

B.2.4.7　公共自行车应用信息记录

公共自行车应用信息记录的记录格式见表 B.47。

表 B.47　公共自行车应用信息记录

字节	数　据　元	长度(字节)	数 据 格 式
1～2	记录 ID 标识	2	2706
3	记录长度	1	固定为 0x7D
4	应用有效标识	1	固定为 0x01
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用没有锁定;1-应用锁定)	1	BCD
7～128	本规范预留	122	初始为 00

B.2.4.8　停车收费应用信息记录

停车收费应用信息记录的记录格式见表 B.48。

表 B.48 停车收费应用信息记录

字节	数 据 元	长度(字节)	数 据 格 式
1～2	记录 ID 标识	2	2707
3	记录长度	1	固定为 0x6D
4	应用有效标识	1	固定为 0x01
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用没有锁定;1-应用锁定)	1	BCD
7～14	交易流水号	8	BCD
15	交易状态	1	BCD
16～17	城市代码	2	BCD
18～25	末次受理机构标识	8	BCD
26～33	入场终端编号	8	BCD
34～41	出场终端编号	8	BCD
42～49	车辆信息	8	BCD
50～56	入场时间	7	YYYYMMDDhhmmss
57～63	出场时间	7	YYYYMMDDhhmmss
64～67	最大消费金额	4	HEX(高字节在前)
68～112	本规范预留	45	初始为 00

B.2.4.9 长途客运信息记录

长途客运信息记录的记录格式见表 B.49。

表 B.49 长途客运信息记录

字节	数 据 元	长度(字节)	数 据 格 式
1～2	记录 ID 标识	2	2708
3	记录长度	1	固定为 0x7D
4	应用有效标识	1	固定为 0x01
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用没有锁定;1-应用锁定)	1	BCD
7～14	交易流水号	8	BCD
15	交易状态	1	BCD
16～17	上车城市代码	2	BCD
18～19	下车城市代码	2	BCD
20～27	上车机构标识	8	BCD
28～35	下车机构标识	8	BCD
36～43	上车站点	8	BCD

表 B.49(续)

字节	数 据 元	长度(字节)	数 据 格 式
44～51	下车站点	8	BCD
52～59	上车终端编号	8	BCD
60～67	下车终端编号	8	BCD
68～74	上车时间	7	YYYYMMDDhhmmss
75～81	下车时间	7	YYYYMMDDhhmmss
82～85	最大消费金额	4	HEX(高字节在前)
86～128	本规范预留	43	初始为 00

B.2.4.10 轮渡应用信息记录

轮渡应用信息记录的记录格式见表 B.50。

表 B.50 轮渡应用信息记录

字节	数 据 元	长度(字节)	数 据 格 式
1～2	记录 ID 标识	2	2709
3	记录长度	1	固定为 0x7D
4	应用有效标识	1	固定为 0x01
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用没有锁定;1-应用锁定)	1	BCD
7～128	本规范预留	122	初始为 00

B.2.4.11 城际铁路应用信息记录

城际铁路应用信息记录的记录格式见表 B.51。

表 B.51 城际铁路应用信息记录

字节	数 据 元	长度(字节)	数 据 格 式
1～2	记录 ID 标识	2	270A
3	记录长度	1	固定为 0x7D
4	应用有效标识	1	固定为 0x01
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用未锁定;1-应用锁定)	1	BCD
7～14	交易流水号	8	BCD
15	交易状态	1	BCD
16～17	进闸城市代码	2	BCD
18～19	出闸城市代码	2	BCD

表 B.51(续)

字节	数 据 元	长度(字节)	数 据 格 式
20～27	进闸机构标识	8	BCD
28～35	出闸机构标识	8	BCD
36～43	进闸站点	8	BCD
44～51	出闸站点	8	BCD
52～59	进闸终端编号	8	BCD
60～67	出闸终端编号	8	BCD
68～74	进闸时间	7	YYYYMMDDhhmmss
75～81	出闸时间	7	YYYYMMDDhhmmss
82～85	最大消费金额	4	HEX(高字节在前)
86～128	本规范预留	43	初始为 00

B.2.4.12 民航应用信息记录

民航应用信息记录的记录格式见表 B.52。

表 B.52 民航应用信息记录

字节	数 据 元	长度(字节)	数 据 格 式
1～2	记录 ID 标识	2	270B
3	记录长度	1	固定为 0x7D
4	应用有效标识	1	固定为 0x01
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用没有锁定;1-应用锁定)	1	BCD
7～128	本规范预留	122	初始为 00

B.2.4.13 高速公路收费应用信息记录

高速公路收费应用信息记录的记录格式见表 B.53。

表 B.53 高速公路收费应用信息记录

字节	数 据 元	长度(字节)	数 据 格 式
1～2	记录 ID 标识	2	270C
3	记录长度	1	固定为 0x7D
4	应用有效标识	1	固定为 0x01
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用没有锁定;1-应用锁定)	1	BCD
7～128	本规范预留	122	初始为 00

B.2.4.14 优惠信息记录

优惠信息记录的记录格式见表 B.54。

表 B.54 优惠信息记录

字节	数 据 元	长度(字节)	数 据 格 式
1～2	记录 ID 标识	2	270D
3	记录长度	1	固定为 0x1B
4	应用有效标识	1	固定为 0x01
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用没有锁定;1-应用锁定)	1	BCD
7	优惠类型	1	BCD
8～11	优惠开始时间	4	YYYYMMDD
12～15	优惠截止时间	4	YYYYMMDD
16	优惠计次	1	BCD
17～30	本规范预留	14	初始为 00

B.2.4.15 预留信息记录

本规范预留信息记录的记录格式见表 B.55～表 B.59。

表 B.55 本规范预留记录 1

字节	数 据 元	长度(字节)	数 据 格 式
1～2	记录 ID 标识	2	270E
3	记录长度	1	固定为 0x7D
4	应用有效标识	1	固定为 0x01
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用没有锁定;1-应用锁定)	1	BCD
7～128	本规范预留	122	初始为 00

表 B.56 本规范预留记录 2

字节	数 据 元	长度(字节)	数 据 格 式
1～2	记录 ID 标识	2	270F
3	记录长度	1	固定为 0x7D
4	应用有效标识	1	固定为 0x01
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用没有锁定;1-应用锁定)	1	BCD
7～128	本规范预留	122	初始为 00

表 B.57　本规范预留记录 3

字节	数　据　元	长度(字节)	数 据 格 式
1～2	记录 ID 标识	2	2710
3	记录长度	1	固定为 0x7D
4	应用有效标识	1	固定为 0x01
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用没有锁定;1-应用锁定)	1	BCD
7～128	本规范预留	122	初始为 00

表 B.58　本规范预留记录 4

字节	数　据　元	长度(字节)	数 据 格 式
1～2	记录 ID 标识	2	2711
3	记录长度	1	固定为 0x7D
4	应用有效标识	1	固定为 0x01
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用没有锁定;1-应用锁定)	1	BCD
7～128	本规范预留	122	初始为 00

表 B.59　本规范预留记录 5

字节	数　据　元	长度(字节)	数 据 格 式
1～2	记录 ID 标识	2	2712
3	记录长度	1	固定为 0x7D
4	应用有效标识	1	固定为 0x01
5	互联互通交易标识	1	1-采用分时分段扣费/复合消费 2-采用预授权消费
6	应用锁定标志(0-应用没有锁定;1-应用锁定)	1	BCD
7～128	本规范预留	122	初始为 00

B.2.5　公共交通过程信息循环记录文件

公共交通过程信息循环记录文件为循环记录结构,见表 B.60。

具备换乘优惠的应用应将本次交易明细记录在公共交通过程信息循环记录文件中。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。

本部分也可用于行业的其他自定义应用。

表 B.60　公共交通过程信息循环记录文件

文件名称	公共交通过程信息循环记录文件——交易信息记录文件			
文件类型	循环记录文件		文件标识	SFI=0x1E
文件大小(bytes)	48×30			
文件权限	读取	自由		
	更新	保护		
字节	数据元		长度(字节)	数据格式
1	交易类型		1	BCD
2~9	终端编号		8	BCD
10~17	交易流水号		8	BCD
18~21	交易金额		4	HEX(高字节在前)
22~25	交易后余额		4	HEX(高字节在前)
26~32	交易日期时间		7	YYYYMMDDhhmmss
33~34	受理方城市代码		2	BCD
35~42	受理方机构标识		8	BCD
43~48	本规范预留		6	初始为 00

附 录 C
（规范性附录）
应用指令

C.1 通用指令

C.1.1 选择命令

C.1.1.1 范围

选择(SELECT)命令通过文件名或 AID 来选择卡片中的 PPSE 或 ADF。

成功执行该命令设定 PPSE 或 ADF 的路径。后续命令作用于用 SFI 选定的 PPSE 或 ADF 相联系的 AEF。

从卡片返回的响应报文包含回送 FCI。

C.1.1.2 命令报文

SELECT 命令的报文编码见表 C.1。

表 C.1 SELECT 命令的报文编码

编 码	值(十六进制)
CLA	‘00’
INS	‘A4’
P1	‘04’
P2	‘00’
Lc	‘05’～‘10’
Data	文件名
Le	‘00’

C.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。

C.1.1.4 响应报文数据域

C.1.1.4.1 PPSE 的响应报文数据域

成功选择 PPSE 的响应报文(FCI)见表 C.2。

表 C.2 成功选择 PPSE 的响应报文 (FCI)

标 签	值(十六进制)			长度(字节)	条 件
6F	FCI 模板			变长	M
	84	“2PAY. SYS. DDF01”		变长	M
	A5	FCI 专用模板		变长	M
		BF0C	FCI 发卡机构自定义数据	变长	M

表 C.2(续)

标　签	值(十六进制)			长度(字节)	条　件
		61	目录入口	变长	M
			4F　DF 名(AID)	08～16	M
			50　应用标签	04～10	O
			87　应用优先指示器[a]	01	C
			9F2A　内核识别号[b]	8	O
		61	目录入口	变长	C
			4F　DF 名(AID)	08～16	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)	08～16	C
			50　应用标签	04～10	C
			87　应用优先指示器	01	C
[a] 若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'。 [b] 9F2A 的第一个字节[b8:b7]为'00',[b6:b1]从 1 到 7 对应 7 个内核识别号。					
注:本表及之后表格中的数据元对象定义说明见附录 A。					

C.1.1.4.2　电子现金的响应报文数据域

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。选择电子现金应用的响应报文见表 C.3。

表 C.3　选择电子现金应用的响应报文(FCI)

标　签	值(十六进制)			条　件
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
		DF11 (本部分规定的标签)	来自从应用提供商、发卡机构或交通卡片供应商的 1 个或多个附加(专用)数据元	O
		9F4D	交易日志入口	O

C.1.1.4.3 电子钱包的响应报文数据域

选择电子钱包应用的响应报文见表 C.4。其中,发卡机构自定义数据(FCI)见表 C.5。

表 C.4 选择电子钱包应用的响应报文(FCI)

标 签	值(十六进制)			条 件
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 C.5	O

表 C.5 发卡机构自定义数据(FCI)

数据字段的描述	长度(字节)
发卡机构代码	8
应用类型标识	1
发卡机构应用版本号	1
应用主账号	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

C.1.1.5 响应报文的状态字

SELECT 命令的响应报文状态字见表 C.6。

表 C.6 SELECT 命令的响应报文状态字

SW1	SW2	说 明
'64'	'00'	标志状态未改变
'67'	'00'	P1、P2 与 Lc 不一致
'6A'	'81'	不具备此功能
'6A'	'82'	未找到文件
'6A'	'86'	P1 和 P2 错误
'6D'	'00'	INS 不具备或错误
'6E'	'00'	CLA 不具备或错误
'62'	'83'	选择文件无效,应用已锁定,通过 APPLICATION BLOCK 指令锁定
'62'	'84'	选择文件无效,应用已锁定,由于安全报文 MAC 验证错误次数超限锁定
'93'	'03'	应用永久锁定

C.1.2 取数据命令

C.1.2.1 范围

当 APDU 不能用现有协议传输时,取数据(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。

C.1.2.2 命令报文

GET RESPONSE 命令的报文编码见表 C.7。

表 C.7 GET RESPONSE 命令的报文编码

编 码	值(十六进制)
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

C.1.2.3 命令报文数据域

命令报文数据域不存在。

C.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。

若 Le 的值为零,在附加数据有效时,卡片应回送状态字'6CXX',否则回送状态字'6F00'。

C.1.2.5 响应报文状态字

此命令执行成功的状态字是'9000'。GET RESPONSE 正常状态情况见表 C.8;卡片可能回送的警告状态见表 C.9;卡片可能回送的错误状态字见表 C.10。

表 C.8 GET RESPONSE 正常状态

SW1	SW2	说 明
'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

表 C.9 GET RESPONSE 警告状态

SW1	SW2	说 明
'62'	'81'	回送的数据可能有错

表 C.10 GET RESPONSE 错误状态字

SW1	SW2	说 明
'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)

表 C.10(续)

SW1	SW2	说　明
'6D'	'00'	INS 不具备或错误
'6E'	'00'	CLA 不具备或错误
'6F'	'00'	数据无效

C.1.3　读记录命令

C.1.3.1　范围

读记录(READ RECORD)命令从一个线性文件中读一条文件记录。从卡片返回的响应中将包含这条被读出的记录。

C.1.3.2　命令报文

READ RECORD 命令的报文编码见表 C.11;命令报文的引用控制参数见表 C.12。

表 C.11　READ RECORD 命令的报文编码

编　码	值(十六进制)
CLA	'00'
INS	'B2'
P1	记录号
P2	引用控制参数,见表 C.12
Lc	不存在
Data	不存在

表 C.12　命令报文的引用控制参数

编　码		值(十六进制)						
Le		'00'						
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

C.1.3.3　命令报文的数据域

命令报文的数据域不存在。

C.1.3.4　响应报文的数据域

针对电子现金应用:成功的 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 0x01 ~0x0A 范围内的 SFI,这个记录是一个标签为'70'的 BER-TLV 结构数据对象。

C.1.3.5　响应报文的状态字

'9000'编码表示命令成功执行。

C.1.4　修改记录命令

C.1.4.1　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。

C.1.4.2 命令报文

UPDATE RECORD 命令的报文编码见表 C.13;UPDATE RECORD 命令报文的引用控制参数见表 C.14。

表 C.13 UPDATE RECORD 命令的报文编码

编　码	值(十六进制)
CLA	'00'或'04'
INS	'DC'
P1	记录号
P2	引用控制参数,见表 C.14
Lc	后续数据域的长度
Data	更新原有记录的新记录加报文鉴别码(MAC)数据元(4 字节)
Le	不存在

说明:

a) CLA = '00'不需要安全报文;

b) CLA = '04'需要安全报文;电子现金应用使用安全报文更新方式更新。

表 C.14 UPDATE RECORD 命令报文的引用控制参数

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

C.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。若需要安全报文,则 MAC 长度为 4 字节。算法见 JT/T 978.6。

C.1.4.4 响应报文的数据域

响应报文的数据域不存在。

C.1.4.5 响应报文的状态字

'9000'编码表示命令成功执行。命令可能返回的警告信息见表 C.15;表 C.16 列出了命令可能返回的错误信息。

表 C.15 UPDATE RECORD 命令的警告响应码

SW1	SW2	说　明
'62'	'00'	没有信息返回
'62'	'81'	数据可能被破坏

表 C.16 UPDATE RECORD 命令的错误响应码

SW1	SW2	说　明
'64'	'00'	没有准确诊断
'65'	'81'	内存失败

表 C.16(续)

SW1	SW2	说　明
'67'	'00'	长度错误
'68'	'82'	不具备安全报文
'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'	'80'	数据域不正确
'6A'	'81'	功能不具备
'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

C.2　电子现金应用指令

C.2.1　应用锁定命令

C.2.1.1　范围

应用锁定(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:

a)　对选择(SELECT)命令,无效的应用应返回状态字节"选择文件无效"(SW1 SW2 = '6283');

b)　对生成应用密文(GENERATE AC)命令,一个无效的应用应返回 AAC 代替 AC 作为响应;

c)　电子钱包应用切换成应用临时锁定的状态。

C.2.1.2　命令报文

APPLICATION BLOCK 命令的报文编码见表 C.17。

表 C.17　APPLICATION BLOCK 命令的报文编码

编　码	值(十六进制)
CLA	'84'
INS	'1E'
P1	'00';其他值保留
P2	'00';其他值保留
Lc	数据域字节长度
Data	4 字节 MAC 值
Le	不存在

C.2.1.3 命令报文的数据域

命令报文的数据域中包含了 JT/T 978.6 中安全报文格式编码的 MAC 数据。

C.2.1.4 响应报文的数据域

响应报文的数据域不存在。

C.2.1.5 响应报文的状态字

‘9000’表示命令成功执行。

C.2.2 应用解锁命令

C.2.2.1 范围

应用解锁(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卡片上的限制被解除。

C.2.2.2 命令报文

APPLICATION UNBLOCK 命令的报文编码见表 C.18。

表 C.18 APPLICATION UNBLOCK 命令的报文编码

编　码	值(十六进制)
CLA	‘84’
INS	‘18’
P1	‘00’;其他值保留
P2	‘00’;其他值保留
Lc	数据域字节长度
Data	4 字节 MAC 值
Le	不存在

C.2.2.3 命令报文的数据域

命令报文的数据域中包含了 JT/T 978.6 安全报文格式编码的 MAC 数据。

C.2.2.4 响应报文的数据域

响应报文中的数据域不存在。

C.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。

C.2.3 卡片锁定命令

C.2.3.1 范围

卡片锁定(CARD BLOCK)命令是一个发行后命令,用来永久地停止卡片中所有的应用。CARD BLOCK 命令停止卡片中所有的应用,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“功能不具备”(SW1 SW2 = ‘6A81’)的反馈,并且不执行任何其他动作。

C.2.3.2 命令报文

CARD BLOCK 命令的报文编码见表 C.19。

C.2.3.3 命令报文的数据域

命令报文的数据域中包含 JT/T 978.6 安全报文格式编码的 MAC 数据。

表 C.19　CARD BLOCK 命令的报文编码

编　　码	值(十六进制)
CLA	'84'
INS	'16'
P1	'00';其他值保留
Lc	'00';其他值保留
P2	数据域字节长度
Data	4 字节 MAC 值
Le	不存在

C.2.3.4　响应报文的数据域

响应报文的数据域不存在。

C.2.3.5　响应报文的状态字

不论卡片是否已经被锁,'9000'编码都表示命令成功执行。

C.2.4　外部认证命令

C.2.4.1　范围

外部认证(EXTERNAL AUTHENTICATE)命令要求卡片中的应用认证一个密文。卡片的响应应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。

C.2.4.2　命令报文

EXTERNAL AUTHENTICATE 命令的报文编码见表 C.20。

表 C.20　EXTERNAL AUTHENTICATE 命令的报文编码

编　　码	值(十六进制)
CLA	'00'
INS	'82'
P1	'00'
P2	'00'
Lc	8～16
Data	发卡机构认证数据
Le	不存在

在 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。

C.2.4.3　命令报文的数据域

C.2.4.3.1　本命令报文的数据域包含标签为'91'的值域,编码如下:

a)　前 8 个字节为必选的授权响应密文 ARPC;

b)　附加的 1～8 个可选字节是专有数据。

C.2.4.3.2 发卡机构认证数据包括下列两个数据元：

a) ARPC(8 字节)；

b) 授权响应码(2 字节)。

C.2.4.4 响应报文的数据域

响应报文的数据域不存在。

C.2.4.5 响应报文的状态字

‘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’。

C.2.5 生成应用密文命令

C.2.5.1 范围

生成应用密文(GENERATE AC)命令传送交易相关数据到卡片,卡片计算并且返回一个密文。由卡片返回的密文可能由于卡片的内部处理过程而与命令报文中要求的密文不一样。生成应用的密文类型见表表 C.21。

表 C.21 生成应用的密文类型

类 型	说 明
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

C.2.5.2 命令报文

GENERATE AC 命令的报文编码见表 C.22;GENERATE AC 命令中的引用控制参数见表 C.23。

表 C.22 GENERATE AC 命令的报文编码

编 码	值(十六进制)
CLA	‘80’
INS	‘AE’
P1	引用控制参数(见表 C.23)
P2	‘00’
Lc	变长
Data	交易相关数据
Le	‘00’

表 C.23 GENERATE AC 命令引用控制参数

b8	b7	B6	b5	b4	b3	b2	b1	说 明
0	0							AAC
0	1							TC
1	0							ARQC
1	1							保留

表 C.23(续)

b8	b7	B6	b5	b4	b3	b2	b1	说　明
			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

C.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 B 中描述。

C.2.5.4　响应报文的数据域

C.2.5.4.1　密文的生成算法见 JT/T 978.6,具备的密文版本见附录 H。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以下两种格式之一编码:

a)　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 C.24 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);

b)　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,应包括密文信息数据、应用交易序号和由卡片计算出的密文(可以是应用密文或专有密文)。

表 C.24　GENERATE AC 响应的报文数据域格式 1

值	条　件
密文信息数据	M
应用交易计数器(ATC)	M
应用密文(AC)	M
发卡机构应用数据	O

C.2.5.4.2　响应报文是 JT/T 978.6 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附录 A。如果卡片不执行 CDA,命令在响应报文数据域中的数据对象按格式 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格式 2 编码。

C.2.5.4.3　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信息数据编码见表 C.25。

表 C.25　密文信息数据编码

b8	b7	b6	b5	b4	b3	b2	b1	说　明
0	0							AAC
0	1							TC
1	0							ARQC

表 C.25(续)

b8	b7	b6	b5	b4	b3	b2	b1	说　明
1	1							RFU
		x	x					卡片系统密文
				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	其他值保留

C.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’。

C.2.6　取数据命令

C.2.6.1　范围

C.2.6.1.1　概述

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。

C.2.6.1.2　特殊设备

在表 C.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 GET DATA 命令访问。普通终端不能用取数据命令获得。

表 C.26　使用 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)

表 C.26(续)

数 据 元
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)
电子现金分时分段扣费抵扣限额(DF62)
电子现金分时分段扣费已抵扣额(DF63)

C.2.6.1.3 支付交易

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。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”)。

C.2.6.2 命令报文

GET DATA 命令的报文编码见表 C.27。

表 C.27 GET DATA 命令的报文编码

编 码	值(十六进制)
CLA	‘80’
INS	‘CA’
P1 P2	要访问数据的标签
Lc	不存在
Data	不存在
Le	‘00’

C.2.6.3 命令报文的数据域

命令报文的数据域不存在。

C.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)。

C.2.6.5 响应报文的状态字

‘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’。

C.2.7 获取处理选项命令

C.2.7.1 范围

获取处理选项(GET PROCESSING OPTIONS)命令用来启动卡片内的交易,卡片的响应报文中包含应用交互特征(AIP)和应用文件定位器(AFL)。

C.2.7.2 命令报文

GPO 命令的报文编码见表 C.28。

表 C.28 GPO 命令的报文编码

编　码	值(十六进制)
CLA	'80'
INS	'A8'
P1 P2	'00'
Lc	'00'
Data	PDOL 相关数据(如果存在)或 8300
Le	'00'

C.2.7.3 命令报文的数据域

命令报文的数据域根据卡片提供的处理选项数据对象列表(PDOL)编码。PDOL 通过标签"83"标记。当卡片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卡片的数据对象的值域的总长度。

C.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编码:

a) 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);

b) 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。数据域可包含多个 BER-TLV 编码的对象,但至少要包含应用交互特征(AIP)和应用文件定位器(AFL)。

应用交互特征定义了可以被卡片中的应用具备的功能;AFL 包括一个不含有分隔符的由文件与记录组成的列表。

C.2.7.5 响应报文的状态字

'9000'编码表示命令成功执行。

C.2.8 内部认证命令

C.2.8.1 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。

C.2.8.2 命令报文

INTERNAL AUTHENTICATE 命令的报文编码见表 C.29。

表 C.29 INTERNAL AUTHENTICATE 命令的报文编码

编　码	值(十六进制)
CLA	'00'
INS	'88'
P1	'00'
P2	'00'
Lc	认证相关数据长度
Data	认证相关数据
Le	'00'

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。

C.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 B 的动态数据认证数据对象列表(DDOL)规则来编码的。

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 格式编码的长度应限制在 JT/T 978.6 定义的范围内。

C.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。

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附录 B 中的规则。

C.2.8.5 响应报文的状态字

'9000'编码表示命令成功执行。

C.2.9 PIN 修改/解锁命令

C.2.9.1 范围

PIN 修改/解锁(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:

a) PIN 尝试记数器的值将复位到 PIN 尝试限制数(最大值);

b) 如果有请求,脱机 PIN 值将被设置为新的 PIN 值。

为保密,如果本命令包含有 PIN 数据,则该数据应加密。

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。

C.2.9.2 命令报文

PIN CHANGE/UNBLOCK 命令的报文编码见表 C.30。

表 C.30 PIN CHANGE/UNBLOCK 命令的报文编码

编 码	值(十六进制)
CLA	'84'
INS	'24'
P1	'00'
P2	'00'、'01'或'02'
Lc	数据字节数
Data	加密 PIN 数据成员(如果存在)和 MAC 数据
Le	不存在
注1:当 P2 为'00',PIN 尝试计数器复位。 注2: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。 注3:当 P2 为'02',PIN 尝试计数器复位同时 PIN 修改,PIN 修改时不使用当前的 PIN。	

C.2.9.3 命令报文的数据域

C.2.9.3.1 一般要求

报文的数据域包括 PIN 加密数据,后面可以加上 4~8 字节的安全报文 MAC 数据,包括两种情况:

a) 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 PIN 修改/解锁命令中不包含新的 PIN 值,故 PIN 不会更新。

b) P2 等于‘01’或‘02’的值的处理步骤分别在附录 C.3.9.3.2 和附录 C.3.9.3.3 中描述。

C.2.9.3.2 使用当前 PIN 修改 PIN 值

C.3.9.3.2.1 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下列步骤进行,见表 C.31～表 C.33:

a) 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;

b) 生成过程密钥 Ks;

c) 生成 8 字节 PIN 数据块 D3;

表 C.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 C.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

注 1:N-新 PIN 的数字个数(16 进制)。

注 2:P-新 PIN 值,长度 4～12 个数字(2～6 字节),当无实际数据时用 F 填充。

注 3:D1 和 D2 执行异或得到 D3。

d) 使用当前 PIN 生成 8 字节数据块 D4;

表 C.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

e) 将数据块 D3 和 D4 执行异或得到 D;

f) 用 Ks 对 D 进行加密,得到 PIN 加密数据。

C.3.9.3.2.2 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下列步骤进行,见表 C.34、表 C.35:

a) 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;

b) 生成过程密钥 Ks;

c) 生成 8 字节 PIN 数据块 D3;

d) 用 Ks 对 D 进行加密,得到 PIN 加密数据。

表 C.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 C.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

注 1:N-新 PIN 的数字个数(16 进制)。
注 2:P-新 PIN 值,长度 4～12 个数字(2～6 字节),当无实际数据时用 F 填充。
注 3:D1 和 D2 执行异或得到 D。

C.2.9.4　响应报文的数据域

响应报文的数据域不存在。

C.2.9.5　响应报文的状态字

‘9000’编码表示命令成功执行。

C.2.10　设置数据命令

C.2.10.1　范围

C.2.10.1.1　概述

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。

C.2.10.1.2　可以用设置数据命令修改的数据

表 C.36 列出的数据可以使用此命令修改。

表 C.36　使用 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)
电子现金分时分段扣费抵扣限额(DF62)
发卡机构特殊数据元(DF11)

C.2.10.2　命令报文

PUT DATA 命令的报文编码见表 C.37。

表 C.37 PUT DATA 命令的报文编码

编　码	值(十六进制)
CLA	'04'
INS	'DA'
P1 P2	要修改的数据对象的标签
Lc	数据域字节数
Data	数据对象的新值(不包括标签和长度)和 MAC 数据
Le	不存在

C.2.10.3 命令报文的数据域

命令数据域中包括要修改的数据对象的值,后面加上 4 ~ 8 字节的 MAC。MAC 的计算见 JT/T 978.6。

C.2.10.4 响应报文的数据域

响应报文的数据域不存在。

C.2.10.5 响应报文的状态字

'9000'编码表示命令成功执行。表 C.38 列出了命令可能返回的警告信息;表 C.39 列出了命令可能返回的错误信息。

表 C.38 PUT DATA 命令警告信息响应码

SW1	SW2	说　明
'62'	'00'	没有信息返回
'62'	'81'	数据可能被破坏

表 C.39 PUT DATA 命令错误信息响应码

SW1	SW2	说　明
'64'	'00'	没有准确诊断
'65'	'81'	内存失败
'67'	'00'	长度错误
'68'	'82'	不具备安全报文
'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'	功能不具备
'6A'	'84'	文件中没有足够空间
'6A'	'85'	Lc 和 TLV 结构不一致

C.2.11 验证命令

C.2.11.1 范围

验证(VERIFY)命令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。验证方式由卡片中的应用自行决定。当从 CVM 列表中选择的持卡人验证方法(CVM)是脱机 PIN 时,使用 VERIFY 命令。

C.2.11.2 命令报文

VERIFY 命令的报文编码见表 C.40;参考数据(P2)的意义见表 C.41;卡片明文脱机 PIN 数据块见表 C.42;脱机 PIN 数据块含义见表 C.43。

表 C.40 VERIFY 命令的报文编码

编 码	值(十六进制)
CLA	'00'
INS	'20
P1	'00'
P2	参考数据定义
Lc	变长
Data	交易 PIN 数据
Le	不存在

表 C.41 VERIFY 命令参考数据定义 (P2)

b8	b7	b6	b5	b4	b3	b2	b1	说 明
0	0	0	0	0	0	0	0	ISO/IEC 7816-4 定义[a]
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	保留
1	0	0	1	x	x	x	x	发卡机构保留

注:P2-'00'表示没有使用特别的限定符。

[a] 未采用 P2 = '0'。

表 C.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

表 C.43 脱机 PIN 数据块含义

对 应 项	名 称	值
C	控制域	值为 0010 的四位二进制数(十六进制 2)
N	PIN 长度	值在 0100 到 1100 之间的 4 位二进制数(十六进制‘4’到‘C’)
P	PIN 数字	值在 0000 到 1001 之间的 4 位二进制数(十六进制‘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(十六进制‘F’)
注:卡片中处理验证命令的应用应明确地找到 PIN 数据。		

C.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。

C.2.11.4 响应报文的数据域

响应报文的数据域不存在。

C.2.11.5 响应报文的状态字

‘9000’编码表示命令成功执行。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,卡片会返回 SW2 = ‘Cx’,‘x’代表还可以重新验证的次数;如果卡片返回了‘C0’,不再验证,CVM 会被锁定。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’。

C.2.12 读取扩展应用数据命令

C.2.12.1 范围

C.2.12.1.1 读取扩展应用数据(READ CAPP DATA)命令用于扩展应用交易中,终端判断卡片是否具备相应行业应用,同时可获得上笔扩展应用交易信息。

C.2.12.1.2 终端通过扩展应用所属的 ID 号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。

C.2.12.1.3 卡片在接收 READ CAPP DATA 命令后将进行以下操作:

a) 根据 P2 指定的 SFI 选取相应的 EF 文件。若文件不存在,卡片回送状态字‘6A82’(未找到文件);

b) 若 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)。

C.2.12.2 命令报文

此命令的报文编码见表 C.44;此命令报文中的引用控制参数 P2 见表 C.45。

表 C.44 READ CAPP DATA 命令的报文编码

编 码	值(十六进制)
CLA	‘80’
INS	‘B4’
P1	‘00/01’
P2	见表 C.45
Lc	‘02’或‘0A’

表 C.44（续）

编　　码	值(十六进制)
Data	详见说明
Le	‘00’
注:此命令报文中的 P1 定义 R－MAC 算法(若卡片具备 R－MAC 保护),0x00 表示采用 JT/T 978.6 描述的 DES 算法,0x01 表示采用 JT/T 978.6 描述的 SM4 算法。	

表 C.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	说明
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
其他值								RFU

C.2.12.3　命令报文数据域

当卡片不具备扩展应用记录的 R-MAC 保护时,命令报文数据域包括 2 个字节的 ID 号;当卡片具备扩展应用记录的 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。

C.2.12.4　响应报文数据域

当卡片不具备扩展应用记录的 R-MAC 保护时,响应报文数据包括指定 ID 号的记录内容;当卡片具备扩展应用记录的 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 JT/T 978.6 中的报文鉴别码,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。

C.2.12.5　响应报文的状态字

命令执行成功的状态字是‘9000’。卡片可能回送的错误状态字见表 C.46。

表 C.46　READ CAPP DATA 错误状态字

SW1	SW2	说　　明
‘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’	不具备此功能
‘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

C.2.13 更新应用数据缓存命令

C.2.13.1 范围

更新应用数据缓存(UPDATE CAPP DATA CACHE)命令用于扩展应用交易中更新应用数据缓存,每次更新0x1E交易的UPDATE CAPP DATA CACHE命令只更新第一条记录。

C.2.13.2 卡片在收到UPDATE CAPP DATA CACHE命令后的操作

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

a) 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;

b) 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GPO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;

c) 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;

d) 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,则回送状态字'6A80'(数据域不正确),终端应终止此次扩展应用交易。

C.2.13.3 命令报文

此命令的报文编码见表C.47;此命令报文中的引用控制参数P2见表C.48。

表C.47 UPDATE CAPP DATA CACHE命令的报文编码

编　码	值(十六进制)
CLA	'84'
INS	'DE'
P1	'00'
P2	见表C.48
Lc	后续数据域的长度
Data	详见说明
Le	'00'

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

B8	B7	B6	B5	B4	B3	B2	B1	说　明
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)
其他值								RFU

C.2.13.4 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。

C.2.13.5 响应报文数据域

当卡片不具备扩展应用记录的 R-MAC 保护时,响应报文数据域不存在;当卡片具备扩展应用记录的 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 JT/T 978.6 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。

国密算法的卡片,在执行该命令时,命令报文 MAC、响应报文 R-MAC 的算法应和终端在 GPO 指令中指定的算法保持一致。

C.2.13.6 响应报文的状态字

此命令执行成功的状态字是'9000'。卡片可能回送的错误状态字见表 C.49。

表 C.49 UPDATE CAPP DATA CACHE 错误状态字

SW1	SW2	说 明
'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'	不具备此功能
'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

C.2.14 新增记录命令

C.2.14.1 范围

新增记录(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:

a) 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';

b) 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。

C.2.14.2 命令报文

APPEND RECORD 的命令的报文编码见表 C.50;此命令报文中的引用控制参数 P2 见表 C.51。

表 C.50　APPEND RECORD 命令的报文编码

编　　码	值(十六进制)
CLA	‘04’
INS	‘E2’
P1	‘00/01’
P2	见表 C.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) 加上新增的记录内容和 MAC
Le	不存在
注:此命令报文中的参数 P1 定义加密算法类型,0x00 表示采用 JT/T 978.6 的 DES 算法,0x01 表示采用 JT/T 978.6 的 SM4 算法。	

表 C.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	说　　明
0	0	0	0	0				RFU
x	x	x	x	x				SFI
1	1	1	1	1				RFU
					x	x	x	RFU
其他值								RFU

C.2.14.3　命令报文数据域

此命令报文数据域由加密后 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。

C.2.14.4　响应报文数据域

响应报文的数据域不存在。

C.2.14.5　响应报文的状态字

此命令执行成功的状态字是‘9000’。卡片可能回送的错误状态字见表 C.52。

表 C.52　APPEND RECORD 错误状态字

SW1	SW2	说　　明
‘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’	不具备此功能
‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到记录

表 C.52（续）

SW1	SW2	说　明
‘6A’	‘84’	文件中存储空间不够
‘94’	‘07’	应用禁止

C.2.15　取脱机交易应用密文命令

C.2.15.1　范围

取脱机交易应用密文(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 0。

C.2.15.2　命令报文

GET TRANS PROVE 的命令的报文编码见表 C.53。

表 C.53　GET TRANS PROVE 命令的报文编码

编　码	值(十六进制)
CLA	‘80’
INS	‘5A’
P1	‘00’
P2	‘00’
Lc	‘02’
Data	终端指定的交易 ATC
Le	‘08’

C.2.15.3　命令报文数据域

命令报文的数据域由终端指定的交易 ATC 组成。

C.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)。

C.2.15.5　响应报文的状态字

此命令执行成功的状态字是‘9000’。卡片可能回送的错误状态字见表 C.54。

表 C.54　GET TRANS PROVE 错误状态字

SW1	SW2	说　明
‘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

表 C.54（续）

SW1	SW2	说　明
‘6E’	‘00’	命令类型不具备
‘94’	‘06’	所需 TC 不可用

C.2.16　安全方式更新命令

C.2.16.1　范围

安全方式更新(SECURITY UPDATE)命令是使电子钱包应用无效的一个发卡机构脚本命令。指令执行之后,电子钱包应用永久锁定。

C.2.16.2　命令报文

此命令的报文编码见表 C.55。

表 C.55　SECURITY UPDATE 命令的报文编码

编　码	值(十六进制)
CLA	‘84’
INS	‘12’
P1	‘00’;其他值保留
P2	‘00’;其他值保留
Lc	数据域字节长度
Data	4 字节 MAC 值
Le	不存在

C.2.16.3　命令报文的数据域

命令报文的数据域由 JT/T 978.6 中的安全报文格式编码的 MAC 数据填充。

C.2.16.4　响应报文的数据域

响应报文的数据域不存在。

C.2.16.5　响应报文的状态字

不论电子钱包应用是否有效,‘9000’编码始终表示命令成功执行。

C.3　电子钱包应用指令

C.3.1　应用锁定命令

C.3.1.1　范围

C.3.1.1.1　应用锁定(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。

C.3.1.1.2　当 APPLICATION BLOCK 命令成功完成应用临时锁定后,用选择(SELECT)命令选择已临时锁定的应用(电子钱包、电子现金应用),将回送状态字“选择文件无效”(SW1 SW2 = ‘6283’)。同时回送 FCI。

C.3.1.1.3　当 APPLICATION BLOCK 命令成功完成应用永久锁定后,电子钱包、电子现金应用执行所有命令,卡片将回送状态字“应用永久锁定”(SW1 SW2 = ‘9303’)。

C.3.1.1.4　对其他命令的影响根据不同应用而定。

C.3.1.2 命令报文

APPLICATION BLOCK 命令的报文编码见表 C.56。

表 C.56 APPLICATION BLOCK 命令的报文编码

编　码	值(十六进制)
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
注1: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。 注2:P2-'01',此命令执行成功后将永久锁定应用。	

C.3.1.3 命令报文数据域

报文鉴别码(MAC)数据元。根据 JT/T 978.6,由应用锁定密钥计算。

C.3.1.4 响应报文数据域

响应报文的数据域不存在。

C.3.1.5 响应报文状态字

此命令执行成功的状态字是'9000';卡片可能回送的状态字见表 C.57。

表 C.57 APPLICATION BLOCK 状态字

SW1	SW2	说　明
'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'	不具备此功能
'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

表 C.57（续）

SW1	SW2	说　明
‘6D’	‘00’	INS 不具备或错误
‘6E’	‘00’	CLA 不具备或错误

C.3.2　应用解锁命令

C.3.2.1　范围

应用解锁(APPLICATION UNBLOCK)命令用于恢复卡片应用,该指令只能在特殊终端上使用。

当 APPLICATION UNBLOCK 命令成功完成后,由 APPLICATION BLOCK 命令产生的对卡片应用命令响应的限制将被取消。

C.3.2.2　命令报文

APPLICATION UNBLOCK 命令的报文编码见表 C.58。

表 C.58　APPLICATION UNBLOCK 命令的报文编码

编　码	值(十六进制)
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

C.3.2.3　命令报文数据域

根据 JT/T 978.6,报文鉴别码(MAC)数据元由应用解锁密钥计算。

C.3.2.4　响应报文数据域

响应报文的数据域不存在。

C.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’)。

卡片可能回送的错误状态字见表 C.59。

表 C.59　APPLICATION UNBLOCK 错误状态

SW1	SW2	说　明
‘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

表 C.59（续）

SW1	SW2	说　明
‘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 不具备或错误
‘6E’	‘00’	CLA 不具备或错误
‘93’	‘03’	应用已被永久锁定

C.3.3　外部认证命令

C.3.3.1　范围

外部认证(EXTERNAL AUTHENTICATION)命令要求卡片中的应用认证一个密文,卡片的响应包括命令处理状态的回送。

C.3.3.2　命令报文

EXTERNAL AUTHENTICATION 命令的报文编码见表 C.60。

表 C.60　EXTERNAL AUTHENTICATION 命令的报文编码

编　码	值(十六进制)
CLA	‘00’
INS	‘82’
P1	‘00’
P2	‘00’
Lc	8～16
Data	发卡机构认证数据
Le	不存在

注 1: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。

注 2: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。

C.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:

a)　前 8 个必备型字节包含密码;

b)　可选的 1～8 个附加字节是专用的信息。

C.3.3.4　响应报文数据域

响应报文的数据域不存在。

C.3.3.5　响应报文状态字

此命令执行成功的状态字是‘9000’。卡片可能回送的警告状态字见表 C.61;卡片可能回送的错误状态字见表 C.62。

表 C.61 EXTERNAL AUTHENTICATION 警告状态

SW1	SW2	说 明
‘63’	‘Cx’	认证失败(x 代表剩余尝试次数)

表 C.62 EXTERNAL AUTHENTICATION 错误状态

SW1	SW2	说 明
‘67’	‘00’	Lc 不正确
‘69’	‘83’	认证方法锁定
‘6A’	‘86’	P1 和 P2 错误
‘6D’	‘00’	INS 不具备或错误
‘6E’	‘00’	CLA 不具备或错误

C.3.4 取随机数命令

C.3.4.1 范围

取随机数(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。

C.3.4.2 命令报文

GET CHALLENGE 命令的报文编码见表 C.63。

表 C.63 GET CHALLENGE 命令的报文编码

编 码	值(十六进制)
CLA	‘00’
INS	‘84’
P1	‘00’
P2	‘00’
Lc	不存在
Data	不存在
Le	‘04’或‘08’

C.3.4.3 命令报文数据域

命令报文的数据域不存在。

C.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。

C.3.4.5 响应报文状态字

此命令执行成功的状态字是‘9000’。卡片可能回送的错误状态字见表 C.64。

表 C.64　GET CHALLENGE 错误状态

SW1	SW2	说　明
‘6A’	‘81’	不具备此功能
‘6A’	‘86’	P1 和 P2 错误
‘6D’	‘00’	INS 不具备或错误
‘6E’	‘00’	CLA 不具备或错误

C.3.5　内部认证命令

C.3.5.1　范围

内部认证(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。

C.3.5.2　命令报文

INTERNAL AUTHENTICATION 命令的报文编码见表 C.65。

表 C.65　INTERNAL AUTHENTICATION 命令的报文编码

编　码	值(十六进制)
CLA	‘00’
INS	‘88’
P1	‘00’
P2	‘00’
Lc	认证数据的长度
Data	认证数据
Le	‘00’

注 1: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。

注 2: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。

C.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。

C.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,其格式和定义不在本标准的范围之内。

C.3.5.5　响应报文状态字

此命令执行成功的状态字是‘9000’。卡片可能回送的警告状态字见表 C.66;卡片可能回送的错误状态字见表 C.67。

表 C.66　INTERNAL AUTHENTICATION 警告状态

SW1	SW2	说　明
‘62’	‘81’	回送的数据可能有错

表 C.67 INTERNAL AUTHENTICATION 错误状态

SW1	SW2	说 明
'64'	'00'	标志状态位未变
'67'	'00'	Lc 域不存在
'68'	'82'	不具备安全报文
'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 不具备或错误

C.3.6 读二进制文件命令

C.3.6.1 范围

读二进制文件(READ BINARY)命令用于读取二进制文件的内容(或部分内容)。

C.3.6.2 命令报文

READ BINARY 命令的报文编码见表 C.68;命令报文中的引用控制参数见表 C.69。

表 C.68 READ BINARY 命令的报文编码

编 码	值(十六进制)
CLA	'00'或'04'
INS	'B0'
P1	见表 C.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 C.69 READ BINARY 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	说 明
x 1								读取模式: 用 SFI 方式
	0	0						RFU(如果 b8 = 1)
			x	x	x	x	x	SFI

C.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。

C.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 字节(短长度)或 65 536 字节(扩展长度)之内,则其

全部字节将被读出。

C.3.6.5 响应报文状态字

此命令执行成功的状态字是‘9000’。卡片可能回送的警告状态字见表 C.70;卡片可能回送的错误状态字见表 C.71。

表 C.70 READ BINARY 警告状态

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

表 C.71 READ BINARY 错误状态

SW1	SW2	说 明
‘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’	不具备此功能
‘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 不具备或错误
‘6E’	‘00’	CLA 不具备或错误

C.3.7 更新二进制文件命令

C.3.7.1 范围

更新二进制文件(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。

C.3.7.2 命令报文

UPDATE BINARY 命令的报文编码见表 C.72 ;UPDATE BINARY 命令报文中的引用控制参数见表 C.73。

表 C.72 UPDATE BINARY 命令的报文编码

编 码	值(十六进制)
CLA	‘00’或‘04’
INS	‘D6’
P1	见表 C.73

表 C.72（续）

编　码	值(十六进制)
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	修改用的数据加报文鉴别码(MAC)数据元(4 字节)
Le	不存在
注:CLA-‘00’不需要安全报文;CLA-‘04’需要安全报文。	

表 C.73　UPDATE BINARY 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	说　明
x 1								读取模式: 用 SFI 方式
	0	0						RFU(如果 b8 = 1)
			x	x	x	x	x	SFI(取值范围 21 ~ 30)

C.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。

C.3.7.4　响应报文数据域

响应报文的数据域不存在。

C.3.7.5　响应报文状态字

此命令执行成功的状态字是‘9000’;卡片可能回送的警告状态字见表 C.74;卡片可能回送的错误状态字见表 C.75。

表 C.74　UPDATE BINARY 警告状态

SW1	SW2	说　明
‘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。

表 C.75　UPDATE BINARY 错误状态

SW1	SW2	说　明
‘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)

表 C.75（续）

SW1	SW2	说　明
‘6A’	‘81’	不具备此功能
‘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 不具备或错误
‘6E’	‘00’	CLA 不具备或错误
‘93’	‘03’	应用永久锁定

C.3.8　圈存命令

C.3.8.1　范围

圈存(CREDIT FOR LOAD)命令用于圈存交易。

C.3.8.2　命令报文

CREDIT FOR LOAD 命令的报文编码见表 C.76。

表 C.76　CREDIT FOR LOAD 命令的报文编码

编　码	值(十六进制)
CLA	‘80’
INS	‘52’
P1	‘00’
P2	‘00’
Lc	‘0B’
Data	见表 C.77
Le	‘04’

C.3.8.3　命令报文数据域

CREDIT FOR LOAD 命令报文数据域见表 C.77。

表 C.77　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

C.3.8.4　响应报文数据域

CREDIT FOR LOAD 响应报文数据域见表 C.78;如果命令执行不成功,则只在响应报文中回送 SW1 和 SW2。

表 C.78 CREDIT FOR LOAD 响应报文数据域

说　明	长度(字节)
TAC	4

C.3.8.5 响应报文的状态字

此命令执行成功的状态字是‘9000’。卡片可能回送的错误状态见表 C.79。

表 C.79 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 不具备或错误
‘6E’	‘00’	CLA 不具备或错误
‘93’	‘02’	MAC 无效

C.3.9 消费命令

C.3.9.1 范围

消费(DEBIT FOR PURCHASE)命令用于消费交易。

C.3.9.2 命令报文

DEBIT FOR PURCHASE 命令的报文编码见表 C.80;执行 INITIALIZE FOR PURCHASE 后即选择消费交易。

表 C.80 DEBIT FOR PURCHASE 命令的报文编码

编　码	值(十六进制)
CLA	‘80’
INS	‘54’
P1	‘01’
P2	‘00’
Lc	‘0F’
Data	见表 C.81
Le	‘08’

C.3.9.3 命令报文数据域

命令报文数据域见表 C.81。

表 C.81 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

C.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 C.82;如果命令执行不成功,则只在响应报文中回送 SW1 和 SW2。

表 C.82 DEBIT FOR PURCHASE 响应报文数据域

说　明	长度(字节)
TAC	4
MAC2	4

C.3.9.5 响应报文的状态字

此命令执行成功的状态字是‘9000’。卡片可能回送的错误状态见表 C.83。

表 C.83 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 不具备或错误
‘6E’	‘00’	CLA 不具备或错误
‘93’	‘02’	MAC 无效

C.3.10 圈提命令

C.3.10.1 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。

C.3.10.2 命令报文

DEBIT FOR UNLOAD 命令的报文编码见表 C.84。

表 C.84 DEBIT FOR UNLOAD 命令的报文编码

编　码	值(十六进制)
CLA	‘80’
INS	‘54’

表 C.84（续）

编　码	值(十六进制)
P1	‘03’
P2	‘00’
Lc	‘0B’
Data	见表 C.85
Le	‘04’

C.3.10.3　命令报文数据域

命令报文数据域见表 C.85。

表 C.85　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

C.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 C.86;如果命令执行不成功,则只在响应报文中回送 SW1 和 SW2。

表 C.86　DEBIT FOR UNLOAD 响应报文数据域

说　明	长度(字节)
MAC3	4

C.3.10.5　响应报文的状态字

此命令执行成功的状态字是‘9000’。卡片可能回送的错误状态见表 C.87。

表 C.87　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 不具备或错误
‘6E’	‘00’	CLA 不具备或错误
‘93’	‘02’	MAC 无效

C.3.11　查询余额命令

C.3.11.1　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。

C.3.11.2 命令报文

GET BALANCE 命令的报文编码见表 C.88。

表 C.88 GET BALANCE 命令的报文编码

编　码	值(十六进制)
CLA	'80'
INS	'5C'
P1	'00'/'01'/'02'/'03'/'04'/'05'
P2	'02'
Lc	不存在
Data	不存在
Le	'04'/'10'

C.3.11.3 响应报文数据域

响应报文的数据域如下：

a) 如果 P1 =00,则响应报文数据域为 4 字节电子钱包可用余额；

b) 如果 P1 =01,则响应报文数据域为 4 字节透支限额；

c) 如果 P1 =02,则响应报文数据域为 4 字节已透支金额；

d) 如果 P1 =03,则响应报文数据域为 4 字节电子钱包实际余额；

e) 如果 P1 =04,则响应报文数据域为 4 字节实际余额上限；

f) 如果 P1 =05,则响应报文数据域为 4 字节电子钱包实际余额加 4 字节实际余额上限加 4 字节已透支金额加 4 字节透支限额,总共 16 字节。

命令执行成功的响应报文数据域见表 C.89。如果命令执行不成功,则只在响应报文中回送 SW1 和 SW2。

表 C.89 GET BALANCE 响应报文数据域

说　明	长度(字节)
电子钱包余额、透支限额、已透支金额或实际余额上限	4/16

C.3.11.4 响应报文的状态字

此命令执行成功的状态字是'9000'。卡片可能回送的错误状态见表 C.90。

表 C.90 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 不具备或错误
'6E'	'00'	CLA 不具备或错误

C.3.12 取交易认证命令

C.3.12.1 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卡片离场并重新进场的恢复机制。

C.3.12.2 命令报文

GET TRANSACTION PROVE 命令的报文编码见表 C.91。

表 C.91 GET TRANSACTION PROVE 命令的报文编码

编 码	值(十六进制)
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 C.92
Le	'08'

C.3.12.3 命令报文数据域

GET TRANSACTION PROVE 命令报文数据域见表 C.92。

表 C.92 GET TRANSACTION PROVE 命令报文数据域

说 明	长度(字节)
要取的 MAC 或/和 TAC 所对应的联机或者脱机交易序号	2

如果命令中指定的交易类型标识和联机或者脱机交易序号对应的 MAC 或 TAC 可用,则响应报文数据域见表 C.93。

表 C.93 GET TRANSACTION PROVE 响应报文数据域

说 明	长度(字节)
MAC	4
TAC	4

C.3.12.4 响应报文的状态字

此命令执行成功的状态字是'9000'。卡片可能回送的错误状态见表 C.94。

表 C.94 GET TRANSACTION PROVE 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 不具备或错误

表 C.94（续）

SW1	SW2	说　明
‘6E’	‘00’	CLA 不具备或错误
‘94’	‘06’	所需 MAC 不可用

C.3.13　初始化圈存命令

C.3.13.1　范围

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

C.3.13.2　命令报文

INITIALIZE FOR LOAD 命令的报文编码见表 C.95。

表 C.95　INITIALIZE FOR LOAD 命令的报文编码

编　码	值(十六进制)
CLA	‘80’
INS	‘50’
P1	‘00’
P2	‘02’
Lc	‘0B’
Data	见表 C.96
Le	‘10’

C.3.13.3　命令报文数据域

INITIALIZE FOR LOAD 命令报文数据域见表 C.96。

表表 C.96　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

C.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 C.97;如果命令执行不成功,则只在响应报文中回送 SW1 和 SW2。

表 C.97　INITIALIZE FOR LOAD 响应报文

说　明	长度(字节)
电子钱包余额	4
联机交易序号	2
密钥版本号(DLK)	1

表 C.97（续）

说　明	长度(字节)
算法标识(DLK)	1
伪随机数(卡片)	4
MAC1	4

C.3.13.5　响应报文的状态字

此命令执行成功的状态字是‘9000’。卡片可能回送的错误状态见表 C.98。

表 C.98　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’	功能不具备
‘6A’	‘86’	P1 和 P2 参数不正确
‘6D’	‘00’	INS 不具备或错误
‘6E’	‘00’	CLA 不具备或错误
‘94’	‘03’	密钥索引不具备

C.3.14　初始化消费命令

C.3.14.1　范围

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

C.3.14.2　命令报文

INITIALIZE FOR PURCHASE 命令的报文编码见表 C.99。

表 C.99　INITIALIZE FOR PURCHASE 命令的报文编码

编　码	值(十六进制)
CLA	‘80’
INS	‘50’
P1	‘01’
P2	‘02’
Lc	‘0B’
Data	见表 C.100
Le	‘0F’

C.3.14.3　命令报文数据域

INITIALIZE FOR PURCHASE 命令报文的数据域见表 C.100。

表 C.100 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

C.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 C.101;如果命令执行不成功,则只在响应报文中回送 SW1 和 SW2。

表 C.101 INITIALIZE FOR PURCHASE 响应报文数据域

说　明	长度(字节)
电子钱包余额	4
脱机交易序号	2
透支限额	3
密钥版本号(DPK)	1
算法标识(DPK)	1
伪随机数(卡片)	4

C.3.14.5 响应报文的状态字

此命令执行成功的状态字是‘9000’。卡片可能回送的错误状态见表 C.102。

表 C.102 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 不具备或错误
‘6E’	‘00’	CLA 不具备或错误
‘94’	‘01’	金额不足
‘94’	‘03’	密钥索引不具备

C.3.15 初始化圈提命令

C.3.15.1 范围

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

C.3.15.2 命令报文

INITIALIZE FOR UNLOAD 命令的报文编码见表 C.103。

表 C.103 INITIALIZE FOR UNLOAD 命令的报文编码

编　码	值(十六进制)
CLA	'80'
INS	'50'
P1	'05'
P2	'02'
Lc	'0B'
Data	见表 C.104
Le	'10'

C.3.15.3 命令报文数据域

INITIALIZE FOR UNLOAD 命令报文的数据域见表 C.104。

表 C.104 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

C.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 C.105;如果命令执行不成功,则只在响应报文中回送 SW1 和 SW2。

表 C.105 INITIALIZE FOR UNLOAD 响应报文数据域

说　明	长度(字节)
电子钱包余额	4
联机交易序号	2
密钥版本号(DULK)	1
算法标识(DULK)	1
伪随机数(卡片)	4
MAC1	4

C.3.15.5 响应报文的状态字

此命令执行成功的状态字是'9000'。卡片可能回送的错误状态见表 C.106。

表 C.106 INITIALIZE FOR UNLOAD 错误状态

SW1	SW2	说　明
'65'	'81'	内存错误
'67'	'00'	长度错误

表 C.106（续）

SW1	SW2	说　明
‘69’	‘85’	使用条件不满足
‘6A’	‘86’	P1 和 P2 参数不正确
‘6D’	‘00’	INS 不具备或错误
‘6E’	‘00’	CLA 不具备或错误
‘94’	‘01’	金额不足
‘94’	‘03’	密钥索引不具备

C.3.16　修改初始化命令

C.3.16.1　范围

修改初始化(INITIALIZE FOR UPDATE)命令用于初始化修改透支限额交易。

C.3.16.2　命令报文

INITIALIZE FOR UPDATE 命令的报文编码见表 C.107。

表 C.107　INITIALIZE FOR UPDATE 命令的报文编码

编　码	值(十六进制)
CLA	‘80’
INS	‘50’
P1	‘04’
P2	‘01’
Lc	‘07’
Data	见表 C.108
Le	‘13’

C.3.16.3　命令报文数据域

INITIALIZE FOR UPDATE 命令报文的数据域见表 C.108。

表 C.108　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

C.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 C.109;如果命令执行不成功,则只在响应报文中回送 SW1 和 SW2。

表 C.109 INITIALIZE FOR UPDATE 响应报文数据域

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

C.3.16.5 响应报文的状态字

此命令执行成功的状态字是‘9000’。卡片可能回送的错误状态见表 C.110。

表 C.110 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 不具备或错误
‘6E’	‘00’	CLA 不具备或错误
‘94’	‘03’	密钥索引不具备

C.3.17 初始化复合应用消费命令

C.3.17.1 范围

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

C.3.17.2 命令报文

INITIALIZE FOR CAPP PURCHASE 命令的报文编码见表 C.111。

表 C.111 INITIALIZE FOR CAPP PURCHASE 命令的报文编码

编　码	值(十六进制)
CLA	‘80’
INS	‘50’
P1	‘03’
P2	‘02’
Lc	‘0B’
Data	见表 C.112
Le	‘0F’

C.3.17.3 命令报文数据域

此命令报文的数据域定义见表 C.112。

表 C.112 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

C.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 C.113;如果命令执行不成功,则只在响应报文中回送 SW1 和 SW2。

表 C.113 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
电子钱包脱机交易序号	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(卡片)	4

C.3.17.5 响应报文的状态字

此命令执行成功的状态字是‘9000’。卡片可能回送的错误状态见表 C.114。

表 C.114 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’	密钥索引不具备
‘94’	‘02’	交易计数器达到最大值
‘94’	‘08’	应用灰锁锁定

C.3.18 更新复合应用数据缓存命令

C.3.18.1 范围

更新复合应用数据缓存(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。

C.3.18.2 命令报文

命令的报文编码见表 C.115,命令报文中的引用控制参数 P2 见表 C.116。

表 C.115 UPDATE CAPP DATA CACHE 命令的报文编码

编　码	值(十六进制)
CLA	‘80’
INS	‘DC’
P1	复合应用类型标识符
P2	见表 C.116
Lc	后续数据域的长度
Data	记录内容
Le	不存在

表 C.116 UPDATE CAPP DATA CACHE 命令报文中的引用控制参数 P2

b8	b7	b6	b5	b4	b3	b2	b1	说　明
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
其他值								RFU

C.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。

C.3.18.4 响应报文数据域

响应报文的数据域不存在。

C.3.18.5 响应报文的状态字

此命令执行成功的状态字是‘9000’。卡片可能回送的错误状态字见表 C.117。

表 C.117 UPDATE CAPP DATA CACHE 可能回送的错误状态字

SW1	SW2	说　明
‘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’	‘80’	数据域不正确
‘6A’	‘81’	不具备此功能
‘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

C.3.19 复合应用消费命令

C.3.19.1 范围

复合应用消费(DEBIT FOR CAPP PURCHASE)命令用于复合应用消费交易。

C.3.19.2 命令报文

此命令的报文编码见表 C.118。

表 C.118 DEBIT FOR CAPP PURCHASE 命令的报文编码

编 码	值(十六进制)
CLA	'80'
INS	'54'
P1	'01'
P2	'00'
Lc	'0F'
Data	见表 C.119
Le	'08'

C.3.19.3 命令报文数据域

此命令报文的数据域定义见表 C.119。

表 C.119 DEBIT FOR CAPP PURCHASE 命令报文的数据域

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

C.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 C.120。

表 C.120 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。

C.3.19.5 响应报文的状态字

此命令执行成功的状态字是'9000'。卡片可能回送的错误状态见表 C.121。

表 C.121　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

C.3.20　增加记录命令

C.3.20.1　范围

增加记录(APPEND RECORD)命令用于对变长记录文件追加新记录。

C.3.20.2　命令报文

增加记录命名报文编码见表 C.122,命令报文中的引用控制参数见表 C.123。

表 C.122　APPEND RECORD 命令的报文编码

编　码	值(十六进制)
CLA	‘04’或‘00’
INS	‘E2’
P1	‘00’
P2	见表 C.123
Lc	后续数据域的长度
Data	追加的新记录加报文鉴别码(MAC)数据元(4 字节)
Le	不存在

表 C.123　APPEND RECORD 命令引用控制参数

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

C.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。

C.3.20.4　响应报文数据域

响应报文的数据域不存在。

C.3.20.5　响应报文状态字

此命令执行成功的状态字是‘9000’。卡片可能回送的错误状态字见表 C.124。

表 C.124 APPEND RECORD 错误状态

SW1	SW2	说 明
'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'	不具备此功能
'6A'	'82'	未找到文件
'6A'	'84'	文件中存储空间不够

C.3.21 修改透支限额命令

C.3.21.1 范围

修改透支限额(UPDATE OVERDRAW LIMIT)命令用于修改透支限额交易。

C.3.21.2 命令报文

UPDATE OVERDRAW LIMIT 命令的报文编码见表 C.125。

表 C.125 UPDATE OVERDRAW LIMIT 命令的报文编码

编 码	值(十六进制)
CLA	'80'
INS	'58'
P1	'00'
P2	'00'
Lc	'0E'
Data	见表 C.126
Le	'04'

C.3.21.3 命令报文数据域

命令报文的数据域见表 C.126。

表 C.126 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

C.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 C.127;如果命令执行不成功,则只在响应报文中回送 SW1 和 SW2。

表 C.127 UPDATE OVERDRAW LIMIT 响应报文数据域

说　明	长度(字节)
TAC	4

C.3.21.5 响应报文的状态字

此命令执行成功的状态字是‘9000’。卡片可能回送的错误状态见表 C.128。

表 C.128 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 不具备或错误
‘6E’	‘00’	CLA 不具备或错误
‘93’	‘02’	MAC 无效

C.3.22 国密/国际算法操作命令

C.3.22.1 范围

国密/国际算法操作(CRYPTOGRAPHIC OPERATION)命令用于当前卡片具备的国密算法和国际算法的读取、选择、设置默认密钥算法和锁定密钥算法。

C.3.22.2 命令报文

CRYPTOGRAPHIC OPERATION 命令的报文编码见表 C.129。

表 C.129 CRYPTOGRAPHIC OPERATION 命令的报文编码

编　码	值(十六进制)
CLA	‘80’/‘84’
INS	‘CD’
P1	‘00’:读取当前密钥组(当未选择密钥组时返回默认密钥组,否则为当前选择的密钥组,此时 P2 为 00); ‘01’:选择 P2 指定的密钥组别; ‘02’:设置 P2 指定的密钥组别为默认组别; ‘03’:锁定 P2 指定的密钥组别,此时 DATA 域为 4 字节 MAC 值
P2	密钥组别索引(01 DES/3DES、02 预留、03 SM4、04 预留),当 P1 =00 时 P2 =00
Lc	P1 =00/01/02 时 Lc = 00 P1 =03 时 Lc = 04

表 C.129（续）

编　　码	值(十六进制)
Data	P1 =00/01/02 时 Data 不存在 P1 =03 时 Data = MAC(4 字节)
Le	P1 =00 时 Le = 01 P1 =01/02/03 时 Le 不存在

C.3.22.3　响应报文数据域

当 P1 =00 读取当前密钥组时,响应报文数据域为当前密钥组别;当 P1 非 00 时,响应报文数据域不存在。

C.3.22.4　响应报文的状态字

此命令执行成功的状态字是‘9000’。卡片可能回送的错误状态见表 C.130。

表 C.130　CRYPTOGRAPHIC OPERATION 错误状态

SW1	SW2	说　　明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘6A’	‘86’	P1 和 P2 参数错误
‘6D’	‘00’	INS 不具备或错误
‘6E’	‘00’	CLA 不具备或错误
‘69’	‘81’	密钥与运算方法(密钥组算法)不匹配
‘69’	‘82’	不满足安全状态
‘69’	‘83’	密钥(组别)已被锁定
‘69’	‘85’	不满足使用条件
‘6A’	‘82’	KEY 文件不存在
‘94’	‘03’	密钥(组别)不存在

附 录 D
（资料性附录）
电子现金快速动态数据认证

D.1 概述

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

D.2 卡片与终端交互过程

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（当卡片私钥的长度大于 1 024bits，用记录的方式）。

在 GPO 中返回的 AFL 指向的记录包含证书和相关 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信区域。终端认证 DDA 的动态签名数据。若认证失败，脱机交易被拒绝。

D.3 快速 DDA（fDDA）处理流程

D.3.1 fDDA 的处理流程如下：

a) 终端选择 PPSE；
b) 卡片返回唯一的电子现金应用 AID；
c) 终端选择电子现金应用 AID；
d) 卡片返回请求：
   1) 终端交易属性（标签“9F66”）；
   2) 随机数（标签“9F37”）；
   3) 其他和 fDDA 无关的标签；
e) 终端发出 GPO，提供：
   1) 标签“9F66”指明仅具备标准快速支付；
   2) 标签“9F37”随机数；
   3) 其他和 fDDA 无关的请求的数据；
f) 卡片响应如下数据：
   1) 交易证书（TC）；
   2) 动态签名；
   3) 同脱机数据认证（fDDA）相关的 AFL 列表记录；
   4) 其他和 fDDA 无关的数据；
g) 终端读取 AFL 指定的记录；
h) 卡片提供证书和数据，用来认证静态数据的哈希；
i) 终端认证动态签名；
j) 若 DDA 认证通过，终端提供如下清算消息：
   1) 交易证书（TC）；
   2) 相关数据。

D.3.2 若 fDDA 认证失败，交易被拒绝。

附 录 E
（规范性附录）
算法标识

E.1 公钥算法标识

公钥签名算法标识见表 E.1。

表 E.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

公钥加密算法标识见表 E.2。

表 E.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

E.2 哈希算法标识

哈希算法标识见表 E.3。

表 E.3 哈希算法标识

哈希算法标识	哈 希 算 法
‘01’	SHA-1
‘07’	SM3

E.3 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 E.4。

表 E.4 对称密钥算法标识

算 法	值(16 进制)
3DES	01
SM4	04

附 录 F
（资料性附录）
交易应用

F.1 电子现金扩展应用消费举例

F.1.1 出租汽车收费应用

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，然后选择电子现金支付应用，发送 GPO 指令，根据消费金额进行扣费。出租汽车收费交易流程见图 F.1。

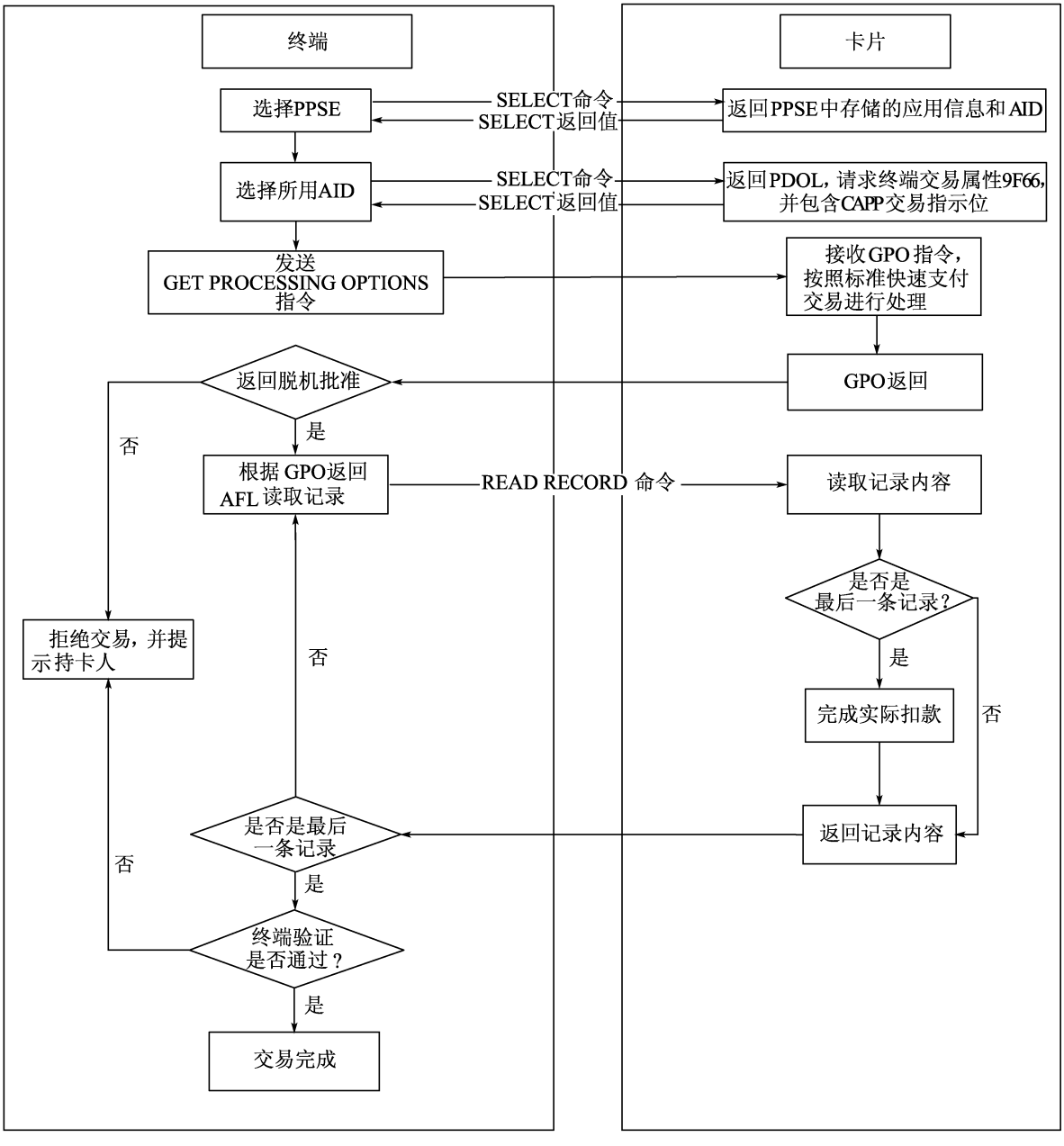


图 F.1 出租汽车收费应用交易流程

F.1.2 公共汽电车/城市轨道收费应用

F.1.2.1 进站交易流程

F.1.2.1.1 进站交易的基本流程为: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。

F.1.2.1.2 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。公共汽电车/城市轨道进站交易流程见图 F.2。

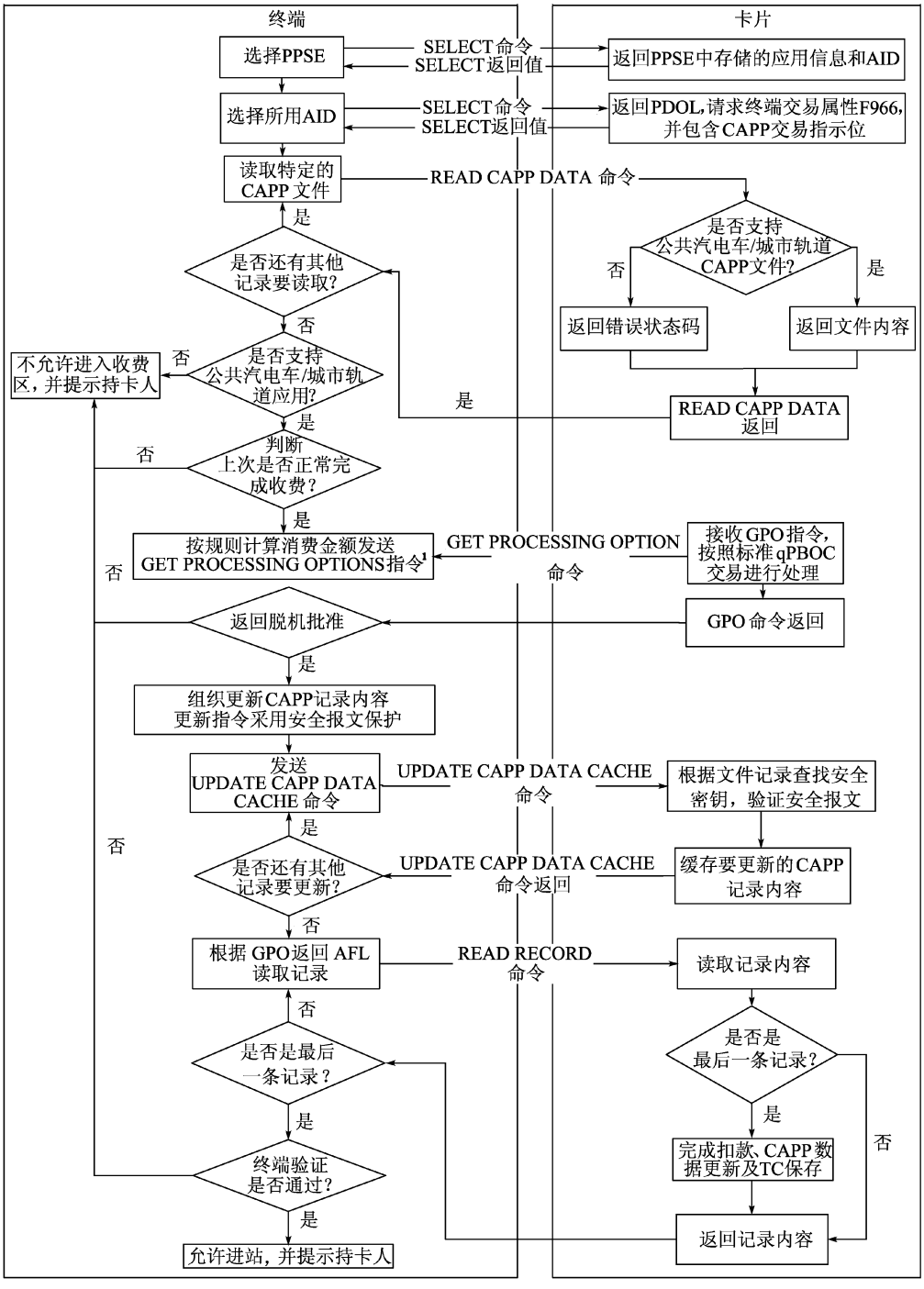


图 F.2 公共汽电车/城市轨道收费应用的进站交易流程

F.1.2.1.3 持卡人使用卡片在城市轨道收费应用环境中进行进站交易时,终端将作如下处理:

a) 终端首先选择和激活卡片,并通过 AID 选择判断卡片是否具备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,判断卡片是否具备城市轨道收费应用。如具备,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站交易,终端应提示持卡人。如处理结果允许进行进站交易,终端进行分时分段扣费交易,其中交易金额为0;

c) 终端根据其自身情况,在 UPDATE CAPP DATA CACHE 中更新城市轨道收费专用数据,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;

d) 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。

F.1.2.2 出站交易流程

F.1.2.2.1 出站交易的基本流程为: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,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。

F.1.2.2.2 公共汽电车/城市轨道出站交易见流程见图 F.3。

F.1.2.2.3 持卡人使用卡片在城市轨道收费应用环境中进行出站交易时,终端将作如下处理:

a) 终端首先选择和激活卡片,并通过 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;

b) 终端发出 READ CAPP RECORD 命令查询,判断卡片是否具备城市轨道收费应用功能。如具备,终端应读取城市轨道收费专用数据,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,终端进行分时分段扣费交易,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;

c) 终端根据其自身情况,在 UPDATE CAPP DATA CACHE 中更新城市轨道收费专用数据,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;

d) 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。

F.1.3 停车收费应用

停车收费应用的交易流程与城市轨道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,等同于进站交易和出站交易。但城市轨道收费应用是按旅客的乘坐路段收费,而停车收费应用是按顾客的停车时间收费。

F.1.4 电子现金公交日票/月票交易流程

F.1.4.1 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。

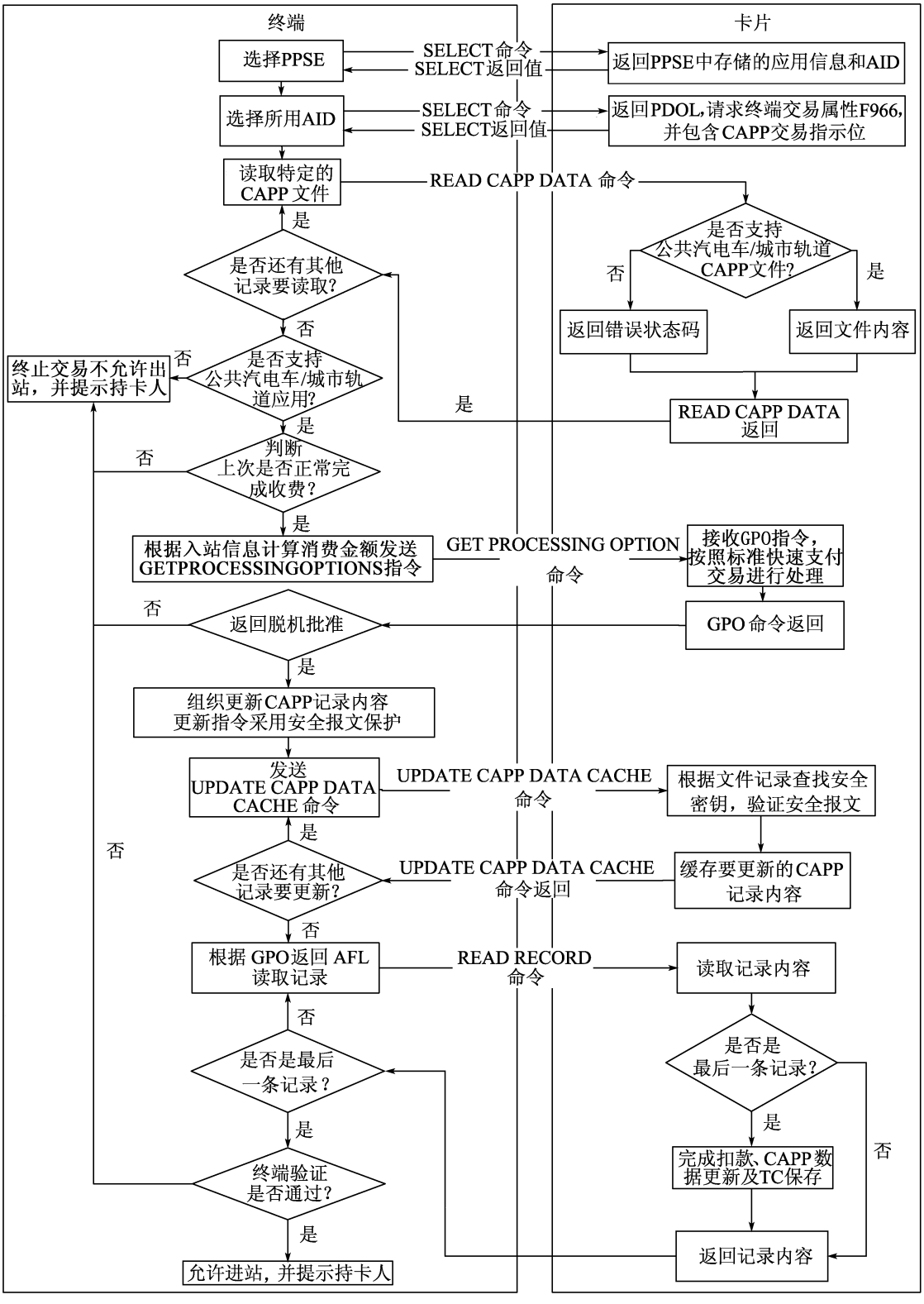


图 F.3　公共汽电车/城市轨道收费应用的出站交易流程

F.1.4.2　日/月票交易的基本流程为:读取扩展应用专用文件,判断卡片是否具备公交日/月票应用,若具备,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。

F.1.4.3　公交日票/月票消费交易流程见图 F.4。

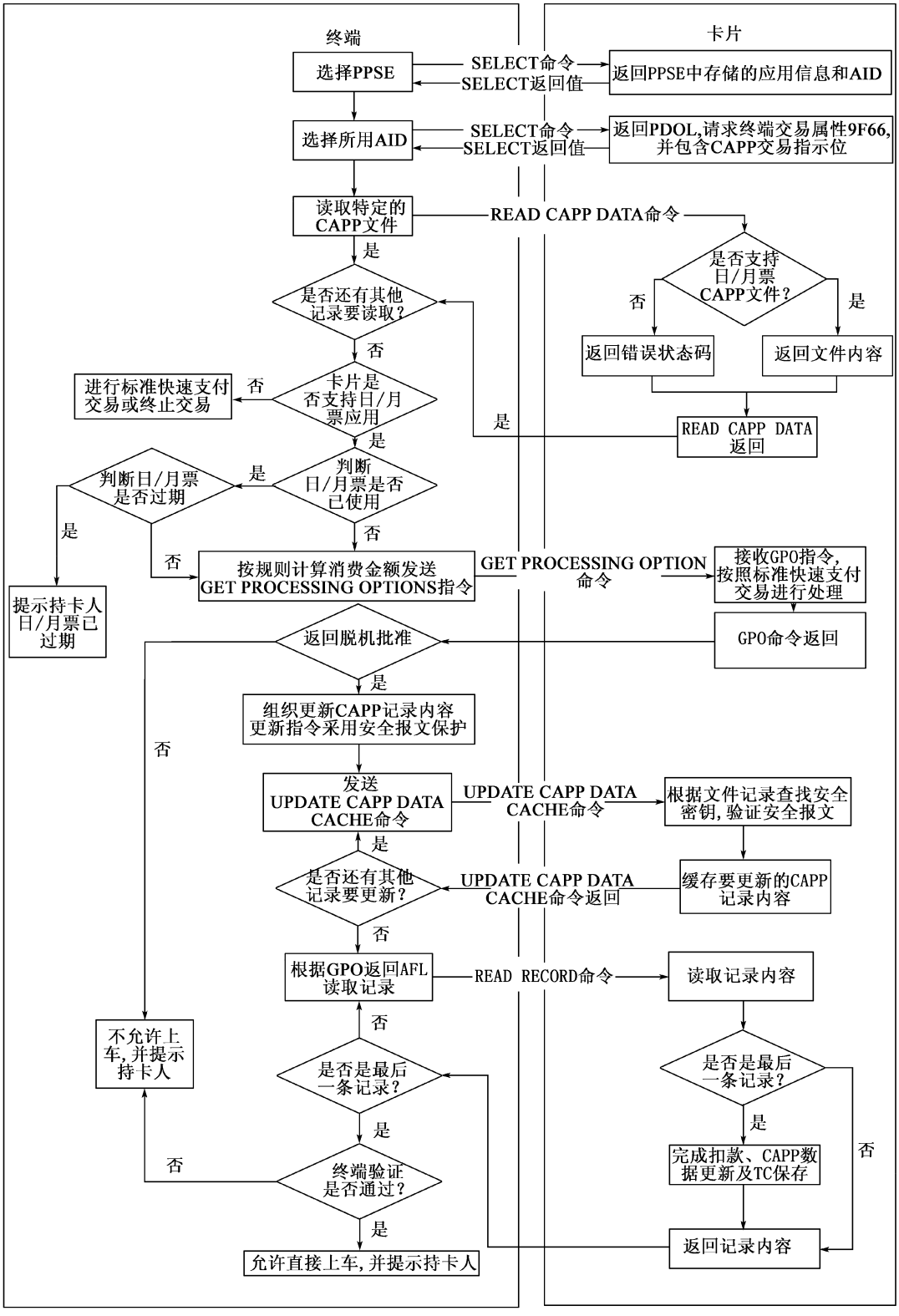


图 F.4　公交日/月票消费交易流程

F.1.4.4 持卡人使用卡片在日/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,判断卡片是否具备公交日/月票应用功能。如具备,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。过期则交易停止,并提示持卡人日/月票过期,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应记录日/月票的类型,日/月票的应用有效期,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/月票限定应在某日/月使用,则可以在充值/发卡时对 CAPP 文件进行更新。

F.2 电子钱包复合应用消费举例

F.2.1 概述

本附录以非接触式卡片电子钱包在一特定环境中的应用为示例,描述复合应用的一种实际应用模式。在这一特定环境中,空间被分割为收费区和非收费区。持卡人在进入收费区时,终端将在卡片中写入特定信息;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。

F.2.2 基础定义

此复合应用的类型标识符为'13'。复合应用记录格式见表 F.1。

表 F.1 复合应用专用文件

字 段 名	长度(字节)	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

F.2.3 交易流程

F.2.3.1 增加复合应用类型

持卡人如需使用非接触式卡片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。增加复合应用操作应在具备复合应用的终端上联机完成,具体处理流程为:

a) 终端在激活卡片后,由持卡人选择进入增加复合应用操作界面,终端向持卡人提示其具备的所有复合应用类型,其中包括此特定复合应用;

b) 当持卡人选择增加此特定复合应用后,终端使用 READ RECORD 命令查询卡片是否具备复合应用功能,是否具备此特定复合应用功能。如不具备复合应用功能,可联机创建复合应用专用文件。如卡片已具备此特定复合应用功能,终端应提示持卡人。如卡片具备复合应用,但不具备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。

F.2.3.2 进收费区交易流程

F.2.3.2.1 实现方式

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。

F.2.3.2.2 交易方式

持卡人使用非接触式卡片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:

a) 终端首先选择和激活卡片,判断卡片为非接触式卡片,并通过 AID 选择进入电子钱包应用目录;

b) 终端发出 READ RECORD 命令查询复合应用,判断卡片是否具备复合应用,是否具备此特定复合应用。如具备,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。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。

F.2.3.2.3 文件改写方式

持卡人使用非接触式卡片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:

a) 终端首先选择和激活卡片,判断卡片为非接触式卡片,并通过 AID 选择进入电子钱包应用目录;

b) 终端发出 READ RECORD 命令查询复合应用,判断卡片是否具备复合应用,是否具备此特定复合应用。如具备,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。

F.2.3.3 出收费区交易

F.2.3.3.1 持卡人使用非接触式卡片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:

a) 终端首先选择和激活卡片,判断卡片为非接触式卡片,并通过 AID 选择进入电子钱包应用目录;

b) 终端发出 READ RECORD 命令查询复合应用,判断卡片是否具备复合应用,是否具备此特定复合应用。如具备,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。

F.2.3.3.2 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。交易成功后,终端应允许持卡人出收费区。

附 录 G
（资料性附录）
行业应用开通指南

G.1 概述

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。卡片应用开通密钥的分散方法按 JT/T 978.6 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。

G.2 行业应用管理和开通的流程

行业应用管理和开通按以下步骤进行：

a) 发卡机构在其卡片密钥管理系统中产生行业应用开通主密钥；
b) 发卡机构在进行卡片数据准备时，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，得到卡片行业应用开通密钥；
c) 发卡机构在个人化时，预先创建扩展应用文件，预置相应的卡片行业应用开通密钥；
d) 持卡人在指定终端上，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。

G.3 行业应用开通的途径

行业应用开通的途径有以下方式：

a) 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，获得卡片行业应用开通密钥。终端在卡片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，通过卡片行业应用开通密钥加密后写入卡片）；
b) 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 H
（规范性附录）
电子现金具备的密文版本

H.1 概述

本部分定义的密文版本为01(0x01)和17(0x17)。密文版本01和密文版本17均使用JT/T 978.6中定义的对称密钥算法计算应用密文。

H.2 密文版本01的数据元

表H.1为密文版本01中生成TC/AAC和ARQC的数据元。

表H.1 密文版本01生成TC/AAC和ARQC的数据元

数 据 元	数 据 来 源
授权金额	终端
其他金额	终端
终端国家代码	终端
终端验证结果	终端
交易货币代码	终端
交易日期	终端
交易类型	终端
不可预知数	终端
应用交互特征(AIP)	卡片
应用交易计数器(ATC)	卡片
卡片验证结果(CVR)	卡片

H.3 密文版本17的数据元

表H.2为密文版本17中生成TC/AAC和ARQC的数据元和顺序。

表H.2 密文版本17生成TC/AAC和ARQC的数据元和顺序

数 据 元	数 据 来 源
授权金额	终端
不可预知数	终端
应用交易计数器(ATC)	卡片
发卡机构自定义数据	卡片

参 考 文 献

[1] JR/T 0025.6—2013 中国金融集成电路(IC)卡规范 第6部分:借贷记应用终端规范