

DB

北 京 市 地 方 标 准

DB XX/ XXXXX—XXXX

市政交通一卡通技术规范

第 3 部分：终端规范

Municipal Administration & Communication Card Technology Standard

Part 3: Terminal Specifications

(征求意见稿)

XXXX - XX - XX 发布

XXXX - XX - XX 实施

北京市质量技术监督局 发布

目 次

前言..... 4

引言..... 5

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 1

4 缩略语..... 3

5 终端分类..... 3

6 终端要求..... 3

 6.1 基本物理配置..... 3

 6.2 卡片识别要求..... 4

 6.3 硬件要求..... 4

 6.4 软件要求..... 7

 6.5 管理功能要求..... 7

 6.6 业务功能要求..... 12

 6.7 数据要求..... 14

 6.8 接口..... 15

7 包装、运输、贮存要求..... 17

 7.1 包装储运..... 17

 7.2 运输..... 18

 7.3 贮存..... 18

附录 A（规范性附录） 刷卡标识图案 19

附录 B（规范性附录） 联机终端开机授权的处理流程图 20

附录 C（规范性附录） 充值的处理流程图 22

附录 D（规范性附录） 逻辑加密卡的恢复流程图 23

附录 E（规范性附录） 逻辑加密卡消费的处理流程图 24

附录 F（规范性附录） C类终端的业务处理流程图..... 25

前 言

DBxxxx-xxxx--《市政交通一卡通技术规范》分为五个部分：

- 第1部分：总则；
 - 第2部分：卡片规范；
 - 第3部分：终端规范；
 - 第4部分：安全规范；
 - 第5部分：检测规范；
- 本部分为规范的第 3 部分。

本部分按照GB/T 1.1-2009给出的规则起草

本部分代替了 DB11T159.3---2005《市政交通一卡通技术标准第2部分：终端》，除编辑性修改外主要技术变化如下：

- 对规范性引用文件，检查其标准的有效性，变更了10份已失效的标准文档，变更为最新实用的标准文档，增加两分标准文档《JR/T 0025.6-2013 中国金融集成电路(IC)卡规范 第6部分：借记/贷记应用终端规范》、《GB/T 2312-1980 信息交换用汉字编码字符集 基本集》。
- 对术语和定义部分增加六部分文档必要引用的说明，含前置机、PKI认证、终端机的业务授权、主机参数、交易流水号、响应码；并重新对终端进行了划分，以便随后对各类不同终端展开说明。
- 对终端分类，增加终端的认证要求，含强制认证、通讯方面的国家认证要求等。
- 对终端的基本物理配置，增加终端的API模块部分。
- 明确增加终端的卡片要求，含硬件部分的卡兼容性要求和软件部分的卡结构兼容性要求。
- 明确增加终端的软件要求，含系统软件、二次开发平台、安全加密部分要求。
- 明确增加终端的管理功能要求，含系统管理、操作员管理、应用管理、安全要求等。
- 规范终端API模块接口要求，通讯接口、硬件标准、天线标准等。
- 对各类安全要求和一些数字指标要求，结合实际，进行了重新的调整，如典型交易时间的要求，统一为不大于300ms等。
- 对一些实际不符的格式和流程进行调整，如交易数据格式要求、联机充值流程等。
- 将“试验方法”、“检验规则”章节移至本标准的第5部分“检测规范”中。

本部分由北京市交通委员会提出并归口。

本部分由北京市交通委员会组织实施。

本部分主要起草单位：北京市交通信息中心、一卡通公司。

本部分主要起草人员：

引 言

本部分为DBxxxx-xxxx的第3部分，与DBxxxx-xxxx的第1部分、第2部分、第4部分、和第5部分一起构成《市政交通一卡通技术规范》。

市政交通一卡通技术规范

第 3 部分：终端规范

1 范围

本部分规定了市政交通一卡通系统终端的通用技术要求。包括终端的电气机械特性、物理特性、逻辑接口、应用管理、参数管理、数据存储、安全存取模块及数据安全要求等。

本部分适用于市政交通一卡通系统终端的研制、生产、检验和验收。

2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

GB/T 191 包装储运图示标志（MOD ISO 780:1997）

GB/T 2312 信息交换用汉字编码字符集 基本集

GB 4943 信息技术设备的安全（eqv IEC 60950: 1999）

GB 9254 信息技术设备的无线电骚扰限值和测量方法（IDT IEC/CISPR 22:2006）

GB/T 13384 机电产品包装通用技术条件

GB/T 16649.3 识别卡 带触点的集成电路卡 第 3 部分:电信号和传输协议（IDT ISO/IEC 7816-3:1997）

GB/T 17618 信息技术设备抗扰度限值和测量方法（idt CISPR 24: 1997）

CJ/T 166 建设事业集成电路(IC)卡应用技术

JR/T 0025.6 中国金融集成电路(IC)卡规范 第 6 部分：借记/贷记应用终端规范

DBxxxx-xxxx.2 市政交通一卡通技术标准 第 2 部分：卡片

ISO/IEC 14443 识别卡 非接触集成电路卡

GSM 11.11 国际电信联盟插入式 SIM 卡标准

3 术语和定义

本部分采用了下列术语和定义。

3.1

一卡通卡Multi-application card

DBXX/ XXXXX—XXXX

由市政府授权、在国家IC卡注册中心注册的发卡机构统一发行，并符合DBxxxx-xxxx.2的IC卡。

3.2

终端 Terminal

指能完成一卡通卡应用的IC卡读写设备，从物理配置上分为A、B和C三类终端，三类终端都可以用来实现充值、消费或服务功能。

3.3

典型交易时间Currently Transcation Time

指终端完成一次正常消费交易的卡片处理时间，不包括处理意外、中断等附加时间。

3.4

API模块 API Module

指集成了市政交通一卡通核心应用的嵌入式组件。

3.5

A类终端 Type A Terminal

指安装有市政交通一卡通系统SAM模块或API模块、具有一卡通卡读写功能的专用设备。

3.6

B类终端 Type B Terminal

指安装有市政交通一卡通系统SAM模块或API模块、具有一卡通卡读写功能的非专用设备。

3.7

C类终端 Type C Terminal

不含市政交通一卡通系统SAM模块或API模块、通过远程控制，具有一卡通卡读写功能的装置。

3.8

前置机 Front Server

对终端进行远程授权认证的服务器。

3.9

业务授权 Business Authorization

终端机只有获得了获取工作密钥才能进行一卡通的相关业务，其必须由终端机通过通信线路向前置申请。

3.10

主机参数 Host Parameters

由主机系统维护的终端各类业务参数，下发到终端，终端执行业务时进行判断控制。

3.11

交易流水号 IC Number

由终端产生并维护，用于在终端唯一标识一笔IC卡类交易

3.12

响应码 Response Number
终端上送的交易经主机处理后，处理结果以代码形式返回。

4 缩略语

- API 应用程序接口 (Application Programming Interface)
- IC 集成电路 (Integrated Circuit)
- MTBF 平均故障间隔时间 (Mean Time Between Failure)
- PKI 公开密钥基础设施 (Public Key Infrastructure)
- SAM 安全存取模块 (Secure Access Module)
- TAC 交易验证码 (Transaction Authorization Code)

5 终端分类

市政交通一卡通系统终端分为 A 类终端、B 类终端和 C 类终端。
A 类终端在本部分第 6、7 章中规定，B 类终端和 C 类终端分别参照 6、7 章中规定。
终端应满足以下认证：
a) 强制性产品认证（简称 3C 认证）。
b) 电信进网许可证，终端通讯采用 MODEM（电话口、电话线通讯）方式的使用认证。
c) 无委认证（无线电发射设备型号核准证），终端通讯采用 GPRS/CDMA 方式的使用认证。

6 终端要求

6.1 基本物理配置

终端应配置以下部件：显示器，数据通讯接口，非易失性存储器，电源，实时时钟，配置安装 SAM 时应配置读写器，至少 2 个安全模块（SAM）座。
根据应用需要，终端也可配置键盘、打印机等组件。

表1 终端部件配置

部件	型式			
	手持式	台式	车载式	固定式
显示器	M	M	M	M

安装 SAM 终端	读写器	M	M	M	M
	至少 2 个 SAM 座	M	M	M	M
安装 API 模块终端	API 模块	M	M	M	M
数据通信接口		M	M	M	M
非易失性存储器		M	M	M	M
电源		M	M	M	M
实时时钟		M	M	M	M
键盘		M	M	O	M
打印机		O	M	O	O
注：M-必备，O-可选。					

6.2 卡片识别要求

6.2.1 卡类型兼容性

终端应具有良好的读卡兼容性，能够正确识别符合 DBxxxx-xxxx.2 标准的卡片，处理非接触式 IC 卡和智能卡。

6.2.2 卡结构兼容性

终端应兼容不同的卡结构、格式，为兼容保留必要的扩展或升级能力。

6.3 硬件要求

6.3.1 基本硬件要求

在通讯等条件允许的情况下，终端应配置 API 模块。

终端根据配置要求，应满足以下一般性要求：

表2 终端的硬件要求

项 目		要 求
硬件要求		符合 JR/T 0025.6-2013 标准
显示屏		应显示ASCII可视字符。汉字显示应符合国家标准GB/T 2312汉字。
键盘		必须有 10 个数字键，若干功能键，必须能够输入字母。键盘使用寿命应达到每键可敲击 500,000 次以上
安 装 SAM 终端	IC 卡读卡器	符合 ISO/IEC 14443 标准
	SAM 接口	符合 CJ/T 166-2006 要求，同时支持不少于 2 个 SAM

项 目		要 求	
安 装 API 模块终端	API 模块	符合 ISO/IEC 14443 标准	
读写距离		100mm 以内有效、无盲区	
数据存储		交易记录	存储容量≥512Kb
		参数记录	存储容量≥256Kb
		数据保存时间	≥10 年
实时时钟		误差	±5 分钟
通讯方式		通讯端口应支持以下全部或部分类型的通讯方式： 串口通讯；MODEM 通讯；红外通讯；无线通讯；网络通讯；其它	
打印机		打印机可选用点阵击打式或热敏纸记录式打印机。能够打印可显示的 ASC II 字符或汉字。	
电源		要求在输入交流电压 220V±15%，工作频率 50Hz±1%的条件下能正常工作 车辆供电直流电压 12V±10%或 24V±10%（车载机）	
电池		容量 2000mAh 标称电压 3.7~7.5V（移动终端） 车载机：有时钟保护电池，工作供电电池依靠车辆电池供给，标准电压 24V。	
可靠性		除非特殊部件另有规定，平均无故障工作时间不低于10,000小时。	

6.3.2 电源

由直流电源供电时，当电压在标称值+10%、-20%范围内时，终端应正常工作。当经交流变换器供电时，交流电压在标称值±10%范围内时，终端应正常工作。终端应有掉电、过流、过压、短路、极性反接等保护措施，当电压恢复正常时，能自动恢复正常工作状态。

6.3.3 外观和结构

表面涂覆层应均匀，不应起泡、龟裂、脱落和磨损。表面不应有明显的凹痕、划伤、裂缝、变形和污染等。金属零部件不应有锈蚀及其他机械损伤。零部件应紧固无松动，按键、开关及其他活动部件的操作应灵活可靠及防止误触摸等设计。电路板的布线要合理，不能有临时接线。

终端的标志、铭牌和说明功能的文字及符号应简明、清晰、端正，并符合相关国家标准的要求。其中铭牌上要标出终端的名称、商标、产地、型号、制造单位及机器编号。

刷卡标识图形见附录 A。

6.3.4 环境适应性

1.1.1.1 机械条件

机械条件见表 3 和表 4。

表3 振动适应性

初始和最后振动响应检查	频率范围	5-55 Hz
	扫描速度	≤1 OCT/min

	驱动振幅	0.15mm
定频耐久试验	驱动振幅	0.75mm(5-25Hz) 0.15mm(25-55Hz)
	持续时间	20±1 min
扫频耐久实验	频率范围	5-55-5 Hz
	扫描速度	≤1 OCT/min
	驱动振幅	0.15mm
	循环次数	5
注：表中驱动振幅为峰值		

表4 冲击适应性

峰值加速度	300 米/秒^2
脉冲持续时间	11 ms
冲击波形	半正弦波形或后峰锯齿波或梯形波
注：终端标准中规定具体的冲击波形	

1.1.1.2 气候条件

终端设备的气候条件按使用环境分为室内和室外两种情况，具体要求见表 5。

表5 终端气候条件

设备使用环境	温度		相对湿度	
	工作	贮存运输	工作	贮存运输
室内	0℃～50℃	-40℃～70℃	20%～95%	10%～98%
室外	-20℃～90℃	-40℃～70℃	10%～90%	10%～98%

6.3.5 电磁兼容性

1.1.1.3 无线电骚扰

应符合 GB 9254 中 A 级的规定。

1.1.1.4 抗扰度

应符合 GB/T 17618 中的规定。

6.3.6 安全

终端安全要求应符合 GB 4943 中的有关规定。

6.3.7 可靠性

- a) 整机平均无故障工作时间（MTBF）的 m1（MTBF 的不可接近值）值应不低于 10000 小时（卡座、键盘除外）；
- b) 接触式卡座使用寿命应不低于 $1 \times (10^5)$ 次；
- c) 键盘使用寿命应不低于 $5 \times (10^5)$ 次。

6.4 软件要求

6.4.1 系统软件

应具有系统初始化，对软件、硬件的自检及报警功能，具备断电保护功能，并方便应用程序的加载和参数设定。

6.4.2 二次开发平台

提供高级语言（如 VC、Java、C 语言等）开发环境，并提供应用模块，具备应用程序的调试和测试环境。

6.4.3 安全加密

能根据软硬件加密 API，获取安全、可靠的加密算法，保证终端交易数据的完整性和隐私性。

6.5 管理功能要求

6.5.1 系统管理

6.5.1.1 自检

开机后对硬件状态进行检测和报警。

终端开机后，先进行自检，自检结束后自动进入工作状态。在工作状态中，操作员也可以通过选择功能设置对终端进行自检。自检完毕返回工作状态。

测试的内容如下：

表6 开机自检内容

序号	参数名称	序号	参数名称
01	打印机测试	02	读卡器测试
03	通信端口测试	04	键盘测试
05	显示屏测试		

6.5.1.2 程序下载管理

程序管理是指对终端使用的一些应用程序进行管理。

终端应支持串行口程序下载、双机对拷、远程在线应用程序下载等方式。

6.5.1.3 参数管理

根据初始和变更的方式，终端参数可分为出厂参数、业务参数、可设定参数和联机可更改参数四类。

- a) 出厂参数

出厂参数主要是与硬件相关的、影响硬件设备使用和运作的基本参数。

表7 出厂参数

参数名称	用途	设置时间	关联内容
硬件版本号	标识当前设备硬件版本	出厂	与硬件设备相关的其他参数
硬件序列号	当前设备唯一标识	出厂	设备管理数据库
操作系统版本号	标识当前设备操作系统	出厂或升级时	硬件版本、应用软件版本
内存状态	标识内存使用状况	程序下装后	应用软件使用
通讯端口类型	识别可用的通讯端口种类	出厂	操作系统、应用软件使用
通讯端口参数	根据具体应用更改设置	出厂或应用时	操作系统、应用软件使用
MODEM 类型	识别可用的 MODEM 种类	出厂	操作系统、应用软件使用
MODEM 参数	根据具体应用更改设置	出厂或应用时	操作系统、应用软件使用
GPRS/CDMA 类型	识别可用的 GPRS/CDMA 种类	出厂	操作系统、应用软件使用
GPRS/CDMA 参数	根据具体应用更改设置	出厂或应用时	操作系统、应用软件使用
打印机类型	识别可用的打印机种类	出厂	操作系统、应用软件使用
打印机参数	根据具体应用更改设置	出厂或应用时	操作系统、应用软件使用
IC 卡读写器参数	根据具体设备、应用更改	出厂或升级时	操作系统、应用软件版本

注：根据具体设备的差异，通讯端口参数、MODEM 参数、GPRS/CDMA 参数、打印机参数等项目可以包括多个子项目。

b) 业务参数

业务参数主要是用于设备自身管理和配置的参数。

表8 业务参数

参数名称	用途	设置时间	关联内容
终端编号	标识当前设备逻辑编号	安装或调整时	设备管理数据库、交易应用
商户编号	标识使用设备的商户编号	安装或调整时	设备管理数据库、交易应用
商户名称	标识商户的中文或英文名	安装或调整时	设备管理数据库、交易应用
超时时间	通讯响应超时时间	安装或调整时	交易应用
重试次数	通讯失败重试次数	安装或调整时	交易应用
运营	标识使用设备运营上需要的参数	安装或调整时	交易应用
通讯	标识使用设备通讯上需要的参数	安装或调整时	交易应用
卡类型	标识使用设备 IC 卡充值类交易需要识别的卡类	安装或调整时	交易应用
充值卡类型	标识使用设备 IC 卡充值类交易需要认证的卡类	安装或调整时	交易应用
消费卡类型	标识使用设备 IC 卡消费类交易需要认证的卡类	安装或调整时	交易应用
退卡类型	标识使用设备 IC 卡退卡类交易需要认证的卡类	安装或调整时	交易应用

计次卡类型	标识使用设备 IC 卡计次卡类交易需要认证的卡类	安装或调整时	交易应用
黑名单列表	标识使用设备 IC 卡需要锁卡的卡表	安装或调整时	交易应用

注：根据具体设备的差异，具体功能的差异，对应实际的参数。

c) 可设定参数

可设定参数主要是与交易内容直接相关并需要长期存放在终端中使用的应用参数，包括以下几类：

当前重要编号：当前通讯流水号、IC 流水号、当前操作员号。

最大日志笔数：允许当批交易保存的最大交易笔数。

操作员管理表：操作员号、操作员密码、操作员属性。

日期与时间表：实时时钟的日期和时间，在每次签到交易成功后调整。

终端支持的交易类型：终端支持哪些交易（不支持的交易被屏蔽掉）。

是否打印故障报告单：当冲正交易不成功或脱机类交易上送不成功大于规定次数（即：消息重发次数）时，系统根据该参数的值确定是否需要打印“故障报告单”。

状态上传的时间间隔点：终端状态上传的时间间隔点

d) 联机可更改参数

通讯参数，终端应用类型，商户号、单位代码、消费额度等，终端支持的交易类型（不支持的交易被屏蔽掉）等。

6.5.1.4 终端状态管理

终端可以有以下三种状态：工作状态、已签退状态、锁定状态。

a) 工作状态

是指终端签到后终端所处的工作状态。此时终端可以实现规定的交易功能。终端自动签退（如终端参数设置不允许自动签退，则按功能键签退），处于已签退状态。

b) 已签退

是指终端签到之前或指终端签退之后的状态。此时终端应显示签到提示。

c) 锁定

操作员可以将终端设为锁定状态。此时终端将不接受任何操作，并提示输入操作员密码（特定情况下可为主管操作员密码）。解除锁定后，终端返回工作状态。

6.5.2 操作员管理

终端根据不同场合使用，最大可以将操作员分为二级：系统管理员和操作员。

6.5.2.1 系统管理员

系统管理员负责对终端系统进行管理，包括软件下载、参数设置。

系统管理员对终端操作前需通过安全认证。

系统管理员可以修改自身密码，并可设置主管操作员的代码和初始密码。

6.5.2.2 操作员管理

终端必须具有操作员管理功能，可以修改操作员密码等。操作员使用操作员代码和密码进行身份认证。终端应至少能够存储和管理 10 个操作员的有关数据。

终端操作必须由指定的操作员进行。

终端操作员分主管操作员和一般操作员。

a) 主管操作员

主管操作员的职责是管理终端和其他操作员，包括查询一般操作员等，本身不能做终端签到和进行交易。

主管操作员密码的修改和验证在终端上进行。

b) 一般操作员

一般操作员只能完成交易功能。

一般操作员的密码存放在终端内，密码修改和验证在终端上进行。

6.5.3 应用管理

根据业务要求，具有一卡通前置授权认证的终端，做以下应用管理：

6.5.3.1 签到管理

签到管理分为操作员签到和终端签到两种。

a) 操作员签到

操作员开机后，键入操作员代码和密码，终端验证操作员的合法性。签到成功后操作员可对终端进行操作。

b) 终端签到

终端签到采用联机方式。终端向前置主机上送终端号、商户号、操作员代码，主机验证商户和终端的有效性后，产生终端工作密钥、提取交易批次号、主机的交易日期和时间，将这些数据下传到终端。终端只有签到成功后才可以进行交易。终端可以根据签到应答消息中主机的时间设置终端的时间。

签到交易有以下四个作用：

a) 终端与主机的批次号同步。批次号必须以主机的批次号为准。

b) 终端从主机获取新的终端工作密钥。如果终端连续收到加密出错的消息，则需要重新发送签到消息，以与主机进行密钥同步；或由主机在应答消息中提示终端重新签到。

c) 终端从主机获取主机的日期和时间。

- d) 终端上送交易流水号、IC 流水号，和主机进行比对，从主机获取最新的流水号或判定数据是否丢失。

注：如终端在使用过程中掉电，重新开机后操作员需要重新签到。

6.5.3.2 批上送

终端在进行联机交易时，通过联机报文将交易信息发送给清算中心。交易完成后，交易记录将在终端本地也进行存放作为备份。终端需要将这些交易记录批量上传到清算中心。

查询、管理类交易，其它不成功的联机类交易不做批上送。

6.5.3.3 签退管理

终端在开机签到时，如果后台反馈终端已签到，需签退提示后，终端向主机发送签退通知，收到签退应答后，终端进入签到提示状态，直到下一次成功签到后，方可处理其它交易。

操作员也可选择“签退”功能，在签退之前，必须进行批上送交易。

终端中存储的流水达到一定笔数（内存已满）后，终端要提示“存储满，请先签退”。

6.5.3.4 参数查询

在终端签到之后的每次联机时，如有必要，由主机引发向终端下载某些参数的操作。终端收到主机的参数传递要求后，立刻向主机发送参数查询请求报文，并接收应答；并根据查询信息，来决定下载哪类参数。

6.5.3.5 终端状态上送

终端根据设定的时间段，将终端的各部件的运行状况及其它信息上送给主机，以便于主机对终端的运行状况进行远程监控。

上送内容包括：硬件状态：模块状态，键盘状态，打印机状态，显示器状态

6.5.3.6 交易查阅功能

查阅终端上存储的签到以来的交易情况和统计情况。

a) 查询交易记录

在终端上从最近一笔交易开始，逐笔查询签到以来的交易明细。只有未签退的交易方可查询。

b) 根据卡号查询交易记录

根据卡号，在查询签到以来的本卡号所作的交易明细。只有未签退的交易方可查询。

c) 查询交易总额

查询当签到以来所做交易的总金额和总笔数，按照交易类型分开统计。

6.5.3.7 重打印功能

a) 重打上笔交易

交易成功但由于某种原因而没有完成打印签购单的情况下，用此功能补打最后一笔交易的签购单。

DBXX/ XXXXX—XXXX

重打印的签购单上必须有补打标志字样。

b) 重打指定交易

交易成功但由于某种原因而没有完成打印签购单的情况下,用此功能补打未签退之前的某笔交易的签购单。重打印的签购单上必须有补打标志字样。

c) 重打结算单

交易成功但由于某种原因而没有完成打印结算单的情况下,用此功能补打最新一次结算单。重打印的结算单上必须有补打标志字样。

6.5.3.8 锁定功能

终端需要暂停工作时,用此项功能可以暂时锁定终端,恢复操作时需要重新输入操作员密码。

6.5.4 安全要求

6.5.4.1 操作员密码

终端应具备操作员密码校验功能,校验失败时禁止交易。

终端的每个操作员都必须有独立的密码和一个代码。

6.5.4.2 终端密钥管理

按照联机业务的要求,对交易部分报文实现加密。掉电后可自动清除密钥。

6.6 业务功能要求

以下按照联机业务功能、脱机业务功能的不同,分别描述一般要求、安全要求和核心处理流程。A类、B类、C类终端均按照本要求执行。

6.6.1 人机界面

终端设备应能显示交易信息,有提示音或提示语音。

终端的界面应通过固定界面或主机下载菜单页面显示。

6.6.2 联机业务终端

联机业务需由终端获取一卡通前置授权后,才允许开通的业务,该类业务主要包括卡类的售卡、充值、退卡、退资、消费等业务。

6.6.2.1 一般要求

- a) 采用联机业务模式,并采用内置 API 模式;
- b) 应具备自检、参数管理、参数下载等功能;
- c) 应验证一卡通卡的合法性,能识别列入黑名单的一卡通卡并进行锁定;
- d) 根据业务参数,进行终端本地信息判断;
- e) 应支持通过外部接口实现应用程序的升级;

- f) 应能存储刷卡交易数据；
- g) 应能将存储的交易数据输出到外部设备或系统；
- h) 对一卡通卡操作的交易顺序号累计不清零；
- i) 应具有打印接口，根据市政交通一卡通系统要求，安装打印机，并按市政交通一卡通系统打印格式要求打印票据。

6.6.2.2 安全要求

- a) 应取得一卡通安全系统对 API 模块的授权，才能进行联机业务交易；
- b) 应具有密文加校验传送的功能；
- c) 生成的交易记录应含有 TAC；
- d) 应具有掉电 API 模块工作权限丧失功能；
- e) 应具有时效性设置功能。

6.6.2.3 核心处理流程

联机类终端在联机时的核心处理是对业务的处理需要后台的授权，并及时上传处理结果。为了保证在市政交通一卡通系统内一卡通卡的通用性和各类终端处理的一致性，本部分规定了联机类终端在交易处理时的处理流程。

a) 开机授权流程

联机终端开机授权的处理流程图见附件 B

b) 典型充值业务流程（其它联机业务类同）

充值的交易处理流程图见附件 C

6.6.3 脱机业务终端

指终端使用 SAM 或 API 模块，完成对一卡通卡进行脱机类扣款、查询等操作的功能。

6.6.3.1 一般要求

- a) 应具备自检、参数管理、参数下载等功能。
- b) 应验证一卡通卡的合法性，能识别列入黑名单的一卡通卡并进行锁定。
- c) 根据业务参数，进行终端本地信息判断。
- d) 应能支持应用软件升级。
- e) 应能存储刷卡交易数据，并能输出到外部设备。

6.6.3.2 安全要求

- a) 应使用市政交通一卡通系统专用的 SAM 或 API 模块；
- b) 生成的交易记录应有 TAC。

6.6.3.3 核心处理流程

为了保证在市政交通一卡通系统内一卡通卡的通用性和各类终端处理的一致性,本部分规定了收费类终端在消费交易处理时的核心处理流程,包括钱包消费及交易计数处理顺序、钱包及卡交易计数恢复处理流程。

a) 智能卡核心交易流程

应符合 CJ/T166《建设事业 IC 卡应用技术》基本要求。

b) 逻辑加密卡核心交易流程

逻辑加密卡的核心交易流程图见附录 D。

c) 恢复流程

逻辑加密卡的恢复流程图见附录 E。

C 类终端的业务处理流程, 参见附录 F。

6.7 数据要求

A 类、B 类、C 类终端均按照本要求执行。

6.7.1 安全要求

内部应用参数及交易记录的访问或修改应有安全控制。

6.7.1.1 应用程序下载要求

应用程序下载应取得相应授权并通过验证。终端应能保证下载应用程序的完整性。

6.7.1.2 数据存储要求

终端中的交易数据以记录的形式保存在存储器中, 终端应能保证存储数据的完整性、可用性和保密性。

6.7.1.3 安全数据要求

终端应能保证与 SAM 之间交互的数据不改变、不泄漏。

6.7.2 交易数据要求

终端交易记录中至少应包括表 9 中的数据项。

表9 交易数据要求

序号	数据项	说明
1	SAM 卡号	存储在 SAM 卡中的终端机编号
2	交易日期	格式为“YYYYMMDD”
3	交易时间	格式为“HHMMSS”
4	城市编码	北京市城市编码
5	行业编码	市政交通行业编码

6	卡发行号	卡发行顺序号
7	卡类型	一卡通卡的卡类型，如非记名成人卡、福利卡、学生卡等
8	卡物理类型	定义卡片的物理特征，如逻辑加密卡、双界面 CPU 卡等
9	交易顺序号	对一卡通卡钱包具有加款权限的终端机具，应保证对一卡通卡操作的交易顺序号连续，且交易顺序号累计不清 0
10	交易类型	表示交易的应用形式特征，如一卡通卡充值、消费等交易
11	交易金额	交易金额，计次卡时为次数
12	卡内余额	交易后一卡通卡内余额，计次卡时为次数
13	卡序列号	一卡通卡内部序列号 CSN；
14	卡交易计数	一卡通卡中的累计交易计数，充值与消费共用同一计数
15	TAC	由 SAM 卡对相关数据项计算得出的交易验证码
16	交易前余额	一卡通卡交易前卡内余额，计次卡时为次数
17	交易状态	交易的业务状态

6.7.3 异常中断恢复机制

6.7.3.1 异常中断

终端在读写一卡通卡时，异常中断分为以下几种情况：

- a) 一卡通卡离开感应区；
- b) 终端停止操作。

6.7.3.2 终端处理要求

- a) 交易异常中断时，终端应在一卡通卡重新进入感应区后，从断点开始继续处理。
- b) 终端瞬间掉电恢复正常工作后，应从断点开始继续处理。
- c) 在以下情况下，终端可退出异常中断恢复处理状态：
 - 1) 有一卡通卡进入感应区时；
 - 2) 超时；
 - 3) 人工干预。

6.7.4 交易数据存储

终端应至少保存 7 天的交易记录。交易记录存储接近最大容量时，终端应及时提示。

6.8 接口

终端应具备与其他外部设备通信的能力。

6.8.1 数据接口方式

通讯端口应支持以下全部或部分类型的通讯方式：

串口通讯；MODEM 通讯；红外通讯；无线通讯；网络通讯；其它

对主机多个通讯地址，具备自动切换功能；

6.8.2 接口要求

- a) 时钟：误差精度不超过 ± 5 分钟。
- b) 显示：显示器字符应清晰完整，易于辨认。
- c) 声音：应具备声音提示功能，音量可调。

6.8.3 与一卡通卡的非接触接口

A 类、B 类终端均按照本要求执行。

- a) 应符合 ISO/IEC14443TYPE A 和/或 TYPE B 的要求；
- b) 频率：13.56 MHz $\pm$ 7kHz；
- c) 在读写有效区域内的最小场强：1.5A/m rms；
- d) 在读写有效区域内的最大场强：7.5A/m rms；
- e) 通信波特率：106~424kHz；
- f) 调制方式：ASK 100%（TYPE A）和/或 ASK 10%（TYPE B）；
- g) 通信距离：
 - 1) 天线读写距离 0~100mm
 - 2) 短距终端：0~30mm 能正常刷卡；
 - 3) 长距终端：0~80mm 能正常刷卡。

注：1.根据具体使用环境，选用短距终端或长距终端；

2.通信距离 0~30mm 和 0~80mm 是指终端感应区机壳到一卡通卡之间的垂直距离。

- h) 典型交易时间：
 - 1) 非接触智能卡消费类终端不大于 300ms。
 - 2) 非接触逻辑加密卡消费类终端不大于 300ms。

注：对交易时间有严格要求的应用，应适当缩短交易时间。

6.8.4 与 SAM 接口

A 类、B 类终端均按照本要求执行。

- a) 通信接口应符合 GB/T 16649.3；
- b) 物理接口应符合 GSM11.11 规范；
- c) 应能兼容 5V 和/或 3V 直流电源的 SAM；
- d) 数据通信速率：应能支持 9600~115200 bit/s，支持 PPS 自适应，通信速率自动识别；

e) 当任意两个触点之间短路时，终端不应损坏。

6.8.5 与 API 模块接口

A 类、B 类终端均按照本要求执行。

- a) 数据通信接口，采用 TTL 电平串口或标准 RS232 接口。
- b) 物理接口应满足 ISO-7816 协议、ISO-14443 1/2/3 协议、CJ/T 166 规范；
- c) 天线接口，采用直联式或 50 欧姆同轴电缆式接口。
- d) 其它一些指标如下：

表10 API 模块指标

项目	指标	
工作电压	DC5V±5%	
功耗	小于 140 mA	
程序存储容量	128K Byte 可扩展 256K Byte	
数据存储容量	64K Byte，可扩展 2M Byte	
通讯速率	115200 bps	
温度	存储温度	-40℃～150℃
	工作温度	-20℃～70℃
相对湿度	存储湿度	10%～98%
	工作湿度	30%～95%
使用环境	防潮、防尘、防腐蚀	
使用寿命	≥ 5 年	
卡兼容性	非接触、兼容逻辑加密卡和 CPU 卡	
读写距离	最大感应距离不低于 60mm	
启动时间	小于 100 毫秒	

7 包装、运输、贮存要求

7.1 包装储运

终端包装应符合 GB/T 191 中的规定，并应符合 GB/T 13384-2008 中防潮、防霉的规定。

在包装箱上标志以下内容：

DBXX/ XXXXX—XXXX

- a) 终端名称、型号;
- b) 制造厂厂名、厂址;
- c) 标准号;
- d) 外形尺寸及毛重;
- e) “小心轻放”、“防潮”等字样及相应图案;
- f) 收货单位及地址;
- g) 生产许可证编号;
- h) 数量、重量及体积;
- i) 装箱日期(年、月)。

包装箱内应有下列文件:

- a) 装箱单;
- b) 说明书;
- c) 合格证;
- d) 随机所带附件。

7.2 运输

运输中应防止受到强烈冲击、雨淋及曝晒。

7.3 贮存

应在制造厂原包装条件下在室内保存(可堆放),其环境温度为 $-20^{\circ}\text{C}\sim+40^{\circ}\text{C}$,相对湿度为20%~95%,且空气中不应含有腐蚀性气体和有害物质。

贮存期超过一年,应重新检验并满足要求后方可使用。

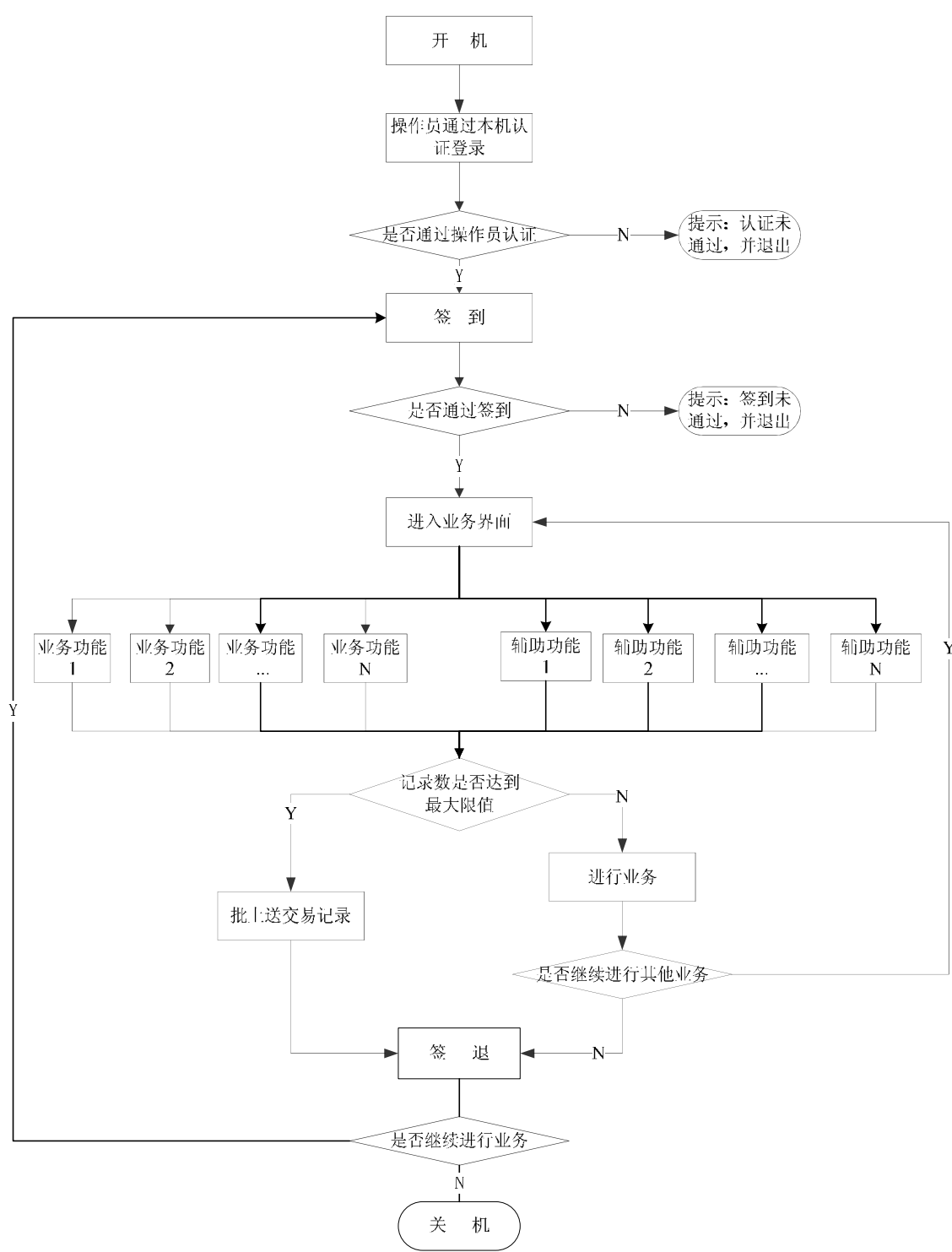
附 录 A
(规范性附录)
刷卡标识图案



基本图案为一卡通卡面图案。图形下方有“请刷卡”(宋体字)字样。

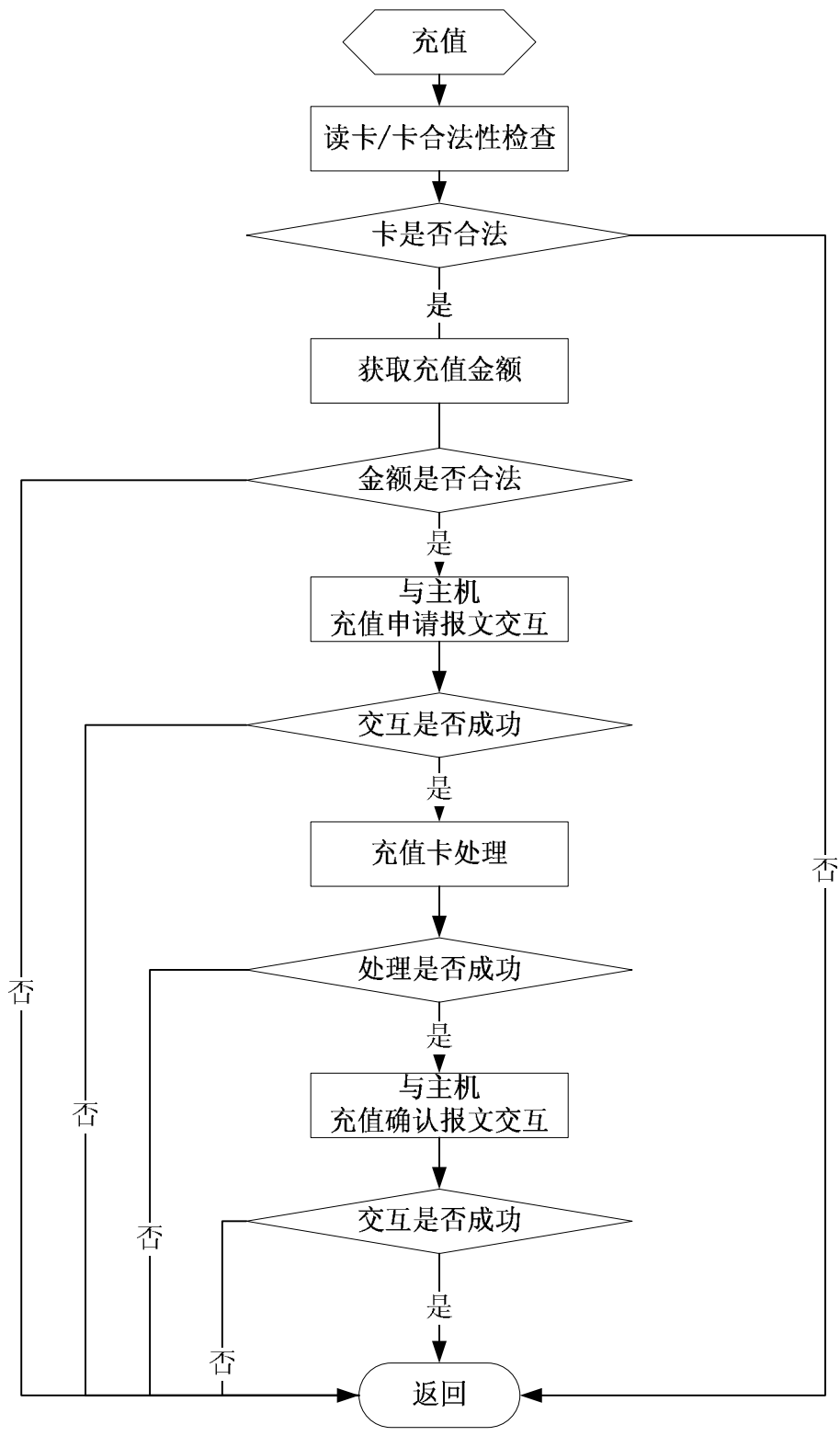
一卡通系统所有终端均应在刷卡区有此提示标识,提示标识应醒目,标示尺寸可根据终端外观尺寸大小按比例缩放。

附 录 B
(规范性附录)
联机终端开机授权的处理流程图

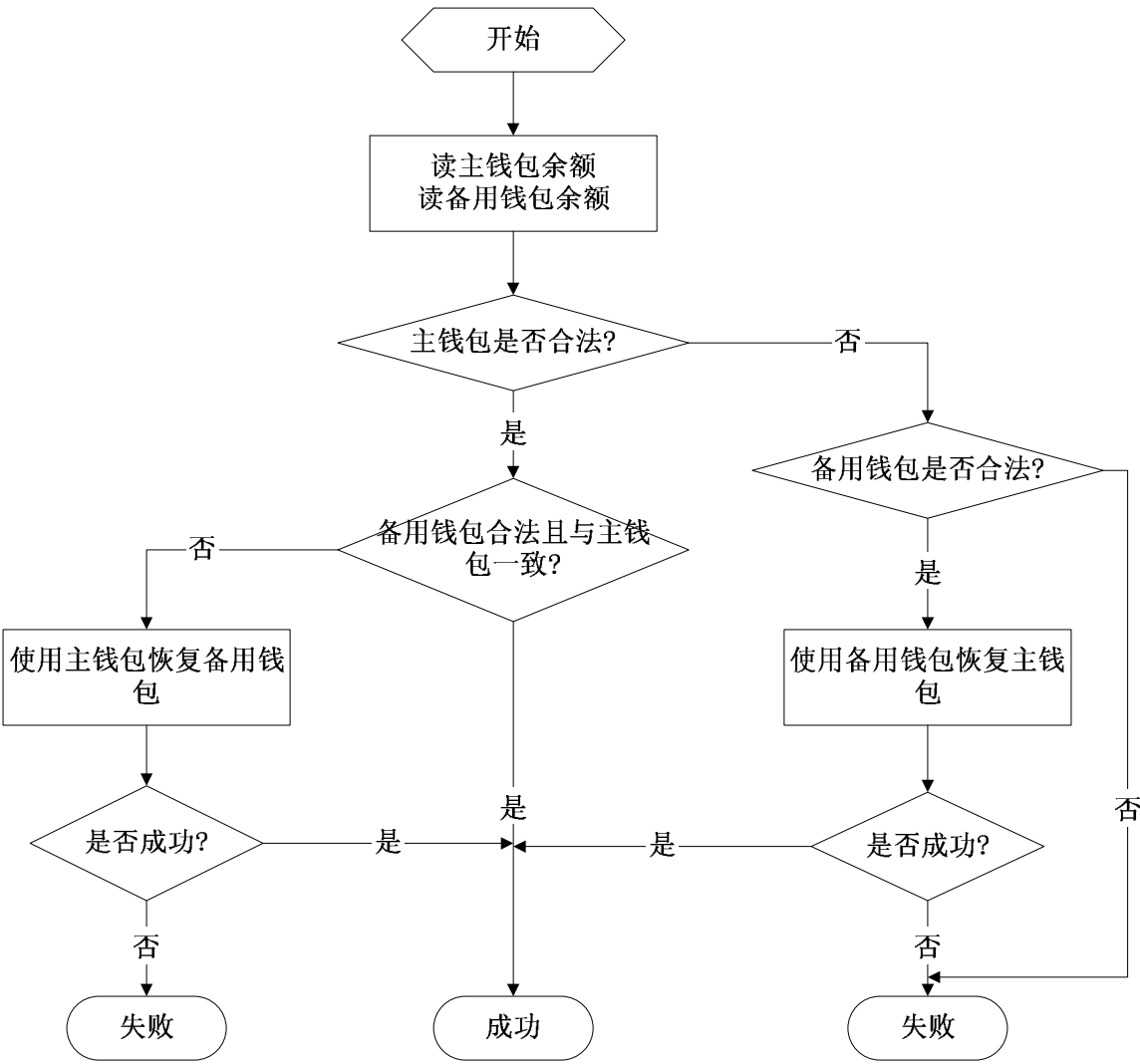


DBXX/ XXXXX—XXXX

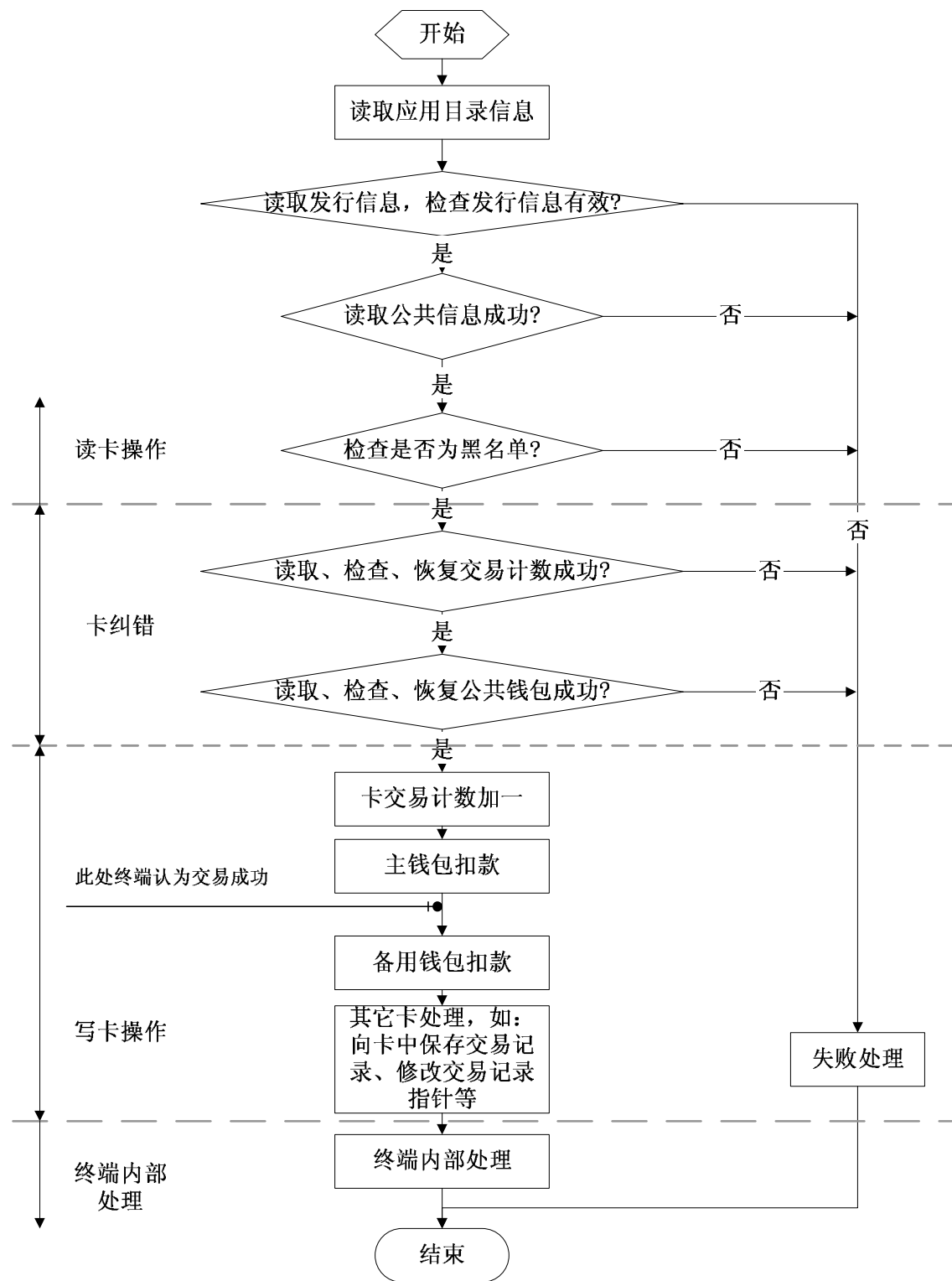
附 录 C
(规范性附录)
充值的处理流程图



附 录 D
(规范性附录)
逻辑加密卡的恢复流程图



附 录 E
(规范性附录)
逻辑加密卡消费的处理流程图



附 录 F
(规范性附录)
C 类终端的业务处理流程图

