

DB

北京市地方标准

DB XX/ XXXXX—XXXX

市政交通一卡通技术规范
第 1 部分：总则

Municipal Administration & Communication Card Technology Standard

Part 1: General 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..... 5

引言..... 6

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 1

4 缩略语..... 2

5 系统概述..... 2

6 系统构成..... 3

7 系统功能..... 3

 7.1 中心计算机处理系统..... 3

 7.2 运营实体计算机处理系统..... 5

 7.3 终端..... 5

 7.4 卡片..... 7

8 性能指标..... 7

 8.1 中心计算机处理系统业务指标..... 7

 8.2 终端技术指标..... 8

 8.3 卡片技术指标..... 9

9 通信及传输要求..... 10

 9.1 网络连接..... 10

 9.2 网络协议..... 10

 9.3 数据传输..... 10

 9.4 数据组织结构..... 11

10 安全要求..... 12

11 业务规范..... 13

 11.1 业务类型..... 13

 11.2 应用领域..... 13

 11.3 交易模式..... 14

 11.4 应用方式..... 15

附录 A（规范性附录） 一卡通卡初始化流程图..... 16

附录 B（规范性附录） 卡号编码..... 17

附录 C（规范性附录） 交易类型编码..... 18

附录 D（规范性附录） 数据包类型..... 19

附录 E（规范性附录） 数据包数据项..... 20

附录 F（规范性附录） 交易记录数据项..... 21

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1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3部分：应用》，以DB11T159.3---2005《市政交通一卡通技术标准第3部分：应用》为主，整合了DB11T159.1---2002《市政交通一卡通技术标准第1部分：卡片》、DB11T159.2---2005《市政交通一卡通技术标准第2部分：终端》的部分内容，除编辑性修改外主要技术变化如下：

- 更新了规范性引用文件中部分已过期标准的日期；
- 在规范性引用文件中增加了“GB/T 22239-2008 信息系统安全等级保护基本要求”、“GB 50174-2008 电子信息系统机房设计规范”；
- 删除了规范性引用文件中的“DB11/T 171-2002党政机关信息系统安全评测规范”；
- 增加了信息系统安全等级保护的要求；
- 对“5、应用分类”进行结构调整，从：业务类型、应用领域、交易模式和应用方式四个方面进行分类和描述，并对业务类型、应用领域、交易模式和应用方式进行了补充；
- 要求充值类、退卡类交易采用联机方式以提升交易的安全性，涉及“5、应用分类”、“8、终端应用要求”、“11、系统应用安全要求”等章节，对联机交易方式进行了定义并规定了应采取的安全措施；
- 对“9、中心计算机处理系统的应用要求”章节进行结构调整，将功能要求整合为7大类；
- 原标准中的“8、终端应用要求”章节描述比较简单，本部分中，按照终端应用通用要求和终端业务功能要求两方面进行了描述，终端业务功能要求中，将终端分为：充值类终端、消费类终端、退卡类终端、服务类终端四类，分别进行描述，根据系统实际情况，主要需增加的要求有：（1）、终端对各类参数下载、维护、业务判断的功能；（2）、终端在线升级功能；（3）、充值类、退卡类终端在线下载菜单功能；（4）、充值类、退卡类终端需采用联机交易模式的要求；（5）、安全性要求较高的消费行业及应用，应采用联机交易模式的要求；（6）、充值类、退卡类终端对操作员层级划分和管理的要求；
- 增加了系统业务连续性要求；增加“同城异地备份系统”的建设要求；
- 删掉原标准中部分编码规则及系统详细数据格式表格中的“字节数”“编码字段”改为中文说明；

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1部分，与DBxxxx-xxxx的第2部分、第3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》。

本部分对市政交通一卡通系统进行了总体的规范和定义，包括系统概述、系统构成、系统功能、性能指标、通信及传输要求、安全总体要求、业务规范等。详细的规范和要求请参见DBxxxx-xxxx的其他部分。

市政交通一卡通技术规范

第 1 部分：总则

1 范围

本部分对市政交通一卡通系统的构成、系统功能、业务流程及应用范围进行了规定和要求。

本部分适用于市政交通一卡通系统工程的设计、开发、实施、验收、运营与管理。

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，鼓励根据本标准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 2260 中华人民共和国行政区划代码
- GB/T 14916 识别卡 物理特性
- GB/T 22239 信息系统安全等级保护基本要求
- GB 50174 电子信息系统机房设计规范
- CJ/T 166 建设事业 IC 卡应用技术
- JR/T 0025 中国金融集成电路（IC）卡规范
- DBxxxx-xxxx.2 市政交通一卡通技术标准第 2 部分：卡片规范
- DBxxxx-xxxx.3 市政交通一卡通技术标准第 3 部分：终端规范
- DBxxxx-xxxx.4 市政交通一卡通技术规范第 4 部分：安全规范

3 术语和定义

本部分采用以下术语和定义。

3.1

运营实体 Operation Entity
参与市政交通一卡通系统运营的行业、公司、单位或其联合体。

3.2

近场支付 Near Field Pay
在交易过程中，持卡人使用智能卡，通过终端设备刷卡方式，在交易现场购买商品与服务，进行的支付行为。

3.3

远程支付 Remote Field Pay

在支付过程中，消费者使用手机或个人电脑，基于移动通信或互联网技术，以远程在线的方式完成支付的行为。

3.4

脱机交易 Offline Transaction

在交易过程中，终端无需与后台实时通讯，交易处理全部在终端本地完成的交易，交易数据保存在终端内部，定时批量上传至后台系统。

3.5

联机交易 Online Transaction

在交易过程中，终端须与后台实时通讯，与后台系统共同完成认证、传输、业务判断及交易处理的交易，交易数据实时上传到后台系统。

3.6

公开密钥基础设施（PKI, Public Key Infrastructure）

公开密钥基础设施是支持公钥管理体制的基础设施，提供鉴别、加密、完整性和不可否认性服务。

3.7

数字签名 Digital Signature

一种非对称加密数据变换，他使得接收方能够验证数据的原始性和完整性，保护发送和接受的数据不被第三方伪造，同时对于发送方来说，还可以防止接收方的伪造。

4 缩略语

ACC 轨道交通 AFC 清算管理中心（AFC Clearing Center）

AFC 自动售检票系统（Automatic Fare Collection）

API 应用程序接口（Application Programming Interface）

ETC 电子收费（Electronic Toll Collection）

MAC 报文验证码（Message Authorization Code ）

MTC 人工收费（Manual Toll Collection）

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）

TCP/IP 传输控制协议/网际协议(Transfer Control Protocol/ Internet Protocol)

UDP 用户数据报协议（User DataProgram Protocol）

5 系统概述

北京市政交通一卡通系统工程是按照北京信息化整体规划的要求，以建设数字北京，促进北京信息技术和信息产业的发展为目标，根据国家金卡办提出的“统一规划、统一标准、统一制造、统一发卡、统一管理”和住房和城乡建设部提出的“一卡多用、统一发卡”的原则，在市政府及有关部门的统一领导、规划和指挥下进行建设。

6 系统构成

市政交通一卡通系统逻辑结构如下图所示：

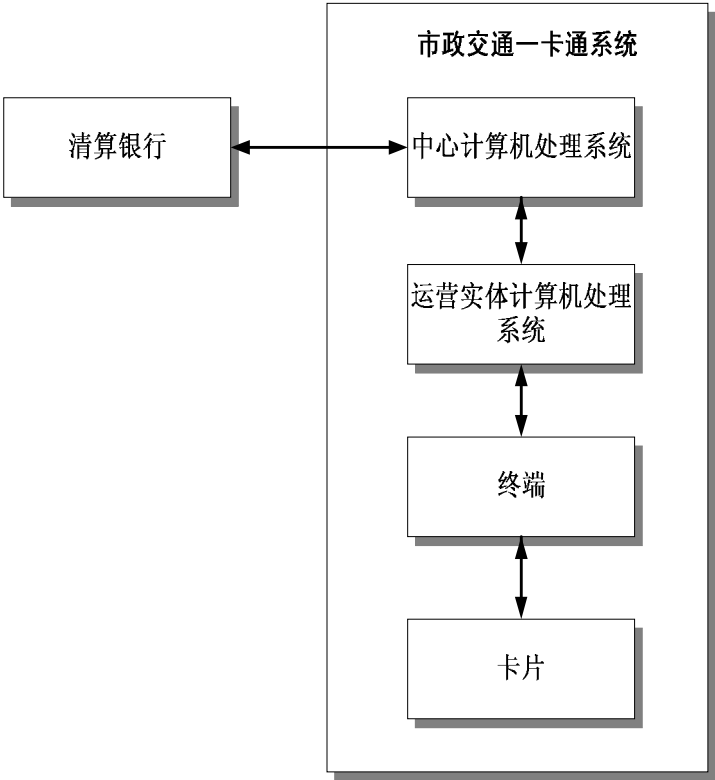


图1 市政交通一卡通系统逻辑结构图

市政交通一卡通系统是指以一卡通中心计算机处理系统为中心枢纽，利用计算机网络技术、通信技术、信息安全技术和IC卡技术，连接一卡通应用运营实体计算机系统以及持卡人和银行，实现发卡、充值、支付、退卡、结算、划帐及管理的应用系统。

市政交通一卡通系统由一卡中心计算机处理系统、运营实体计算机处理系统、终端、卡片共同组成。

7 系统功能

7.1 中心计算机处理系统

中心计算机处理系统是一卡通中心运营管理平台，实现一卡通系统相互之间的互连、互通、互操作，以及和外部系统的数据交换和处理。

为了保障一卡通系统的运行，保证一卡通卡在相关行业的应用，同时满足运营实体计算机处理系统和终端接入的要求，一卡通中心计算机系统应具备如下七类基本功能及辅助功能：接入和传输、业务处理、结算对账、综合管理、基础信息管理、辅助系统、备份与恢复。

7.1.1 接入与传输

为终端设备、运营实体系统提供业务接入及数据通讯服务。包括：

- a) 应能为各业务终端、运营实体计算机处理系统（采集点、分中心、清算银行及其它外部相关系统）提供脱机或联机业务的功能及通讯接入，具备终端或接入平台进行合法性检查功能。
- b) 应能接收业务终端、运营实体计算机处理系统的各类 IC 卡交易数据、终端状态信息和日志数据。
- c) 应能将结算统计数据、业务对帐数据、系统运行参数数据、运行管理数据发送到运营实体计算机处理系统。

7.1.2 业务处理

具备一卡通系统中的各类业务处理功能，包括卡片初始化、业务数据处理、交易合法性检查、联机交易认证及交易处理、异常业务处理等：

- a) 卡初始化：具备一卡通卡初始化功能，包括创建一卡通卡应用文件、写入密钥和发行商标识及卡片发行相关信息，只有经过初始化的卡才可在一卡通系统中使用；卡片初始化流程参见附录 A。
- b) 交易合法性验证：具备交易记录合法性检查功能，包括：数据格式检查、重复性检查、逾期检查、卡帐户及黑名单检查等，验证原始交易记录的交易认证码 TAC。
- c) 包级合法性检查：包含：包接收单位有效性检查，包类型有效性检查，包重复性检查，包格式有效性检查，包完整性检查，包版本有效性检查等。
- d) 终端管理：具备为终端提供联机授权认证、参数下载功能。
- e) 联机交易服务：具备为联机交易提供交易认证、后台合法性检查及交易处理，包括：发卡充值、退卡退资、消费、查询等联机类交易。
- f) 异常业务处理：具备终端、卡帐户、交易记录等异常数据处理的功能。

7.1.3 结算对账

具备结算、对账、划账、统计、分析功能：

- a) 结算对帐：应能及时完成一卡通中心计算机系统收到的各类交易数据的结算，并产生资金清分的数据和报表，完成与各运营实体的数据对帐，并生成划账信息。
- b) 查询统计：具备交易数据分类查询统计功能。
- c) 数据分析：具备对交易数据、历史数据和各类统计数据的功能。

7.1.4 综合管理

具备用户及权限管理、额度管理、报表导出等综合管理功能：

- a) 操作员管理：具备设置、管理和维护一卡通中心计算机处理系统的操作员及终端操作员权限的管理功能。
- b) 授权额度管理：具备对具有发卡充值功能的终端、商户、运营单位实现后台交易额度的控制和管理。
- c) 报表功能：具备查询、分析、统计数据的报表功能。

7.1.5 基础数据管理

具备对一卡通系统中的基础数据进行管理和维护功能：

- a) 卡帐户管理：具备一卡通卡账户管理及维护功能。
- b) 终端信息管理：具备终端基础信息管理及维护功能，包括终端基本信息管理、参数维护、状态监控、额度控制等。
- c) 运营实体管理：具备运营实体基础信息管理及维护功能，包括：行业、单位、商户、网点结算手续费率等。
- d) 参数管理：具备中心计算机处理系统的运行参数的管理和维护功能；具备运营实体运营参数的管理和维护功能。
- e) 黑名单管理：具备黑名单的收集、生成、跟踪、下发及维护功能。

7.1.6 辅助系统

- a) 数据审计系统：对交易数据进行审计，用以及时发现异常的交易数据或交易行为。
- b) 客户服务系统：面向用户提供卡账户及交易信息查询、信息发布等功能。
- c) 监控系统：具备网络状态、设备运行状态、物理环境及数据传输状态监控等功能。
- d) 数据挖掘系统：对历史累计数据进行统计分析，深度挖掘潜在信息。

7.1.7 备份与恢复

具有各类交易数据、结算统计数据、系统运行参数、管理数据等存储、备份及恢复功能。

7.2 运营实体计算机处理系统

为实现接入一卡通中心计算机系统，应具备以下基本功能。运营实体的相关业务要求本标准不作规定。

7.2.1 数据采集

应能及时、完整采集所属范围内终端的各类原始交易数据。

7.2.2 数据传输

应能将各类交易数据发送到一卡通中心计算机系统，并具备重传功能。

应能接收一卡通中心计算机系统的结算统计数据、业务对帐数据、系统运行参数数据、运行管理数据，并能将黑名单、相关参数及时发送到分中心系统及系统内的所有终端。

7.2.3 数据接口

应按一卡通中心计算机系统的数据编码、数据格式、数据组织形式要求实现数据接口。

7.2.4 数据结算及对帐

应能实现行业内交易数据的结算，并能完成行业内资金清分。

应能实现与一卡通中心计算机系统结算数据的对帐和异常处理。

7.2.5 数据存储

应具备各类原始交易数据、结算统计数据、系统运行参数数据、运行管理数据的存储、备份和恢复功能。

7.3 终端

市政交通一卡通系统的终端设备或系统应符合 DBxxxx-xxxx.3 规定。

7.3.1 终端应用通用要求

- a) 终端须经一卡通系统授权后方可使用。
- d) 终端应满足市政交通一卡通系统的使用要求，功能具有可扩展性。
- e) 终端应支持对一卡通中心计算机处理系统各类参数的及时下载，参数包括：通讯类参数、业务类参数、管理类参数、及黑名单等。
- f) 终端应依据一卡通中心计算机处理系统下载的各类参数进行准确的业务判断，对黑名单卡须进行锁卡。
- g) 终端应依据一卡通各类业务处理标准对卡片进行交易处理，交易成功后应生成符合一卡通格式标准的交易数据。
- h) 终端不应损坏一卡通卡内的数据。
- i) 终端不应泄露一卡通卡内的机密数据。
- j) 同一终端的不同应用之间不应互相影响。
- k) 终端支持在线升级功能。
- l) 终端支持交易数据查询、数据采集上传功能。

7.3.2 终端业务功能要求

终端根据业务功能可分为：充值类终端、消费类终端、退卡类终端、服务类终端四类。

业务功能可以根据业务需要进行相应组合。

7.3.2.1 充值类终端

- a) 具有发卡、充值、延期、激活功能。
- b) 终端支持在线下载菜单功能。
- c) 终端操作权限应至少支持两级管理，实现操作员及系统管理员不同权限控制。
- d) 终端的发卡、充值、延期、激活交易应采用联机方式进行。
- e) 交易数据须实时上传一卡通中心计算机处理系统。

7.3.2.2 消费类终端

- a) 具有消费、缴费功能。
- b) 终端的消费交易可采用脱机方式进行，对于所需安全性较高的行业及应用，应采用联机方式进行。
- c) 交易数据须及实时上传一卡通中心计算机处理系统。

7.3.2.3 退卡类终端

- a) 具有退卡、退资功能。
- b) 终端支持在线下载菜单功能。
- c) 终端操作权限应至少支持两级管理，实现操作员及系统管理员不同权限控制。
- d) 终端的退卡、退资交易应采用联机方式进行。
- e) 交易数据须实时上传一卡通中心计算机处理系统。

7.3.2.4 服务类终端

- a) 具有查询、补票、修复功能。
- b) 交易数据须及实时上传一卡通中心计算机处理系统。

7.4 卡片

7.4.1 一卡通卡

一卡通卡应符合 DBxxxx-xxxx.2 的规定。

7.4.2 应用类型

应用类型编码, 最多可支持 256 种类型。

7.4.3 初始化

一卡通卡应进行初始化, 初始化是对 IC 卡创建一卡通卡应用文件, 写入密钥和发行商标识及卡片发行信息的过程。

7.4.4 发售

已初始化的一卡通卡, 可在经授权的终端上发售, 发售后方可使用。

7.4.5 充值

已发售的一卡通卡, 可在经授权的终端上充值, 使用过程中可多次充值。

7.4.6 消费

已充值的一卡通卡, 可在一卡通应用领域的终端设备上使用。

7.4.7 服务

在使用过程中, 若一卡通卡出现故障不能继续使用, 或持卡人终止使用一卡通卡, 可在经授权的终端设备上办理退卡或退资业务。

在使用过程中, 用户可在经授权的终端设备上办理查询、补票、修复、延期、激活等服务业务。
经授权的终端设备须对黑名单卡进行锁卡, 锁卡后的卡片将不能再使用。

7.4.8 回用

回用应由发卡机构负责。

对回收的一卡通卡, 在经授权的终端设备上分拣、并对符合回用标准的一卡通卡进行回用。
一卡通中心计算机处理系统对回收回用的一卡通卡后台信息进行核销, 并进入初始状态环节。

7.4.9 销毁

销毁应由发卡机构负责。

对回收的一卡通卡, 在经授权的终端设备或系统上进行分拣、并对符合销毁标准的一卡通卡进行销毁。

一卡通中心计算机处理系统对销毁的一卡通卡后台信息进行核销。

8 性能指标

8.1 中心计算机处理系统业务指标

中心计算机处理系统的处理性能要求如下表所示：

表1 中心计算机处理系统的处理性能要求

项目	指标
清算处理性能	≥每小时 1000 万笔交易
单笔交易后台处理速度（联机交易）	≤2 秒
最大并发交易处理数（联机交易）	≥20000 笔
结算准确率	≥99.9%
系统平均无故障时间	8751 小时
各类统计数据保存时间	5 年
原始数据保存时间	5 年

8.2 终端技术指标

终端的通用技术性能指标如下表所示：

表2 终端的通用技术性能指标

项目	指标
卡片识别要求	正确识别符合本规范卡片部分的卡片
终端硬件基本要求	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	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
SAM 接口	符合 CJ/T 166-2006 要求，不少于 2 个 SAM
IC 卡读卡模块--	应符合 ISO/IEC14443TYPE A 和/或 TYPE B 的要求； 频率：13.56 MHz±7kHz； 在读写有效区域内的最小场强：1.5A/m rms；最大场强：7.5A/m rms； 通信波特率：106～424kHz； 调制方式：ASK 100%（TYPE A）和/或 ASK 10%（TYPE

	B); 通信距离: 100mm 以内有效、无盲区 典型交易时间: 非接触智能卡消费类终端不大于 300ms。
数据存储	交易记录 存储容量$\geq 512\text{Kb}$ 参数记录 存储容量$\geq 256\text{Kb}$ 数据保存时间 ≥ 10 年
时钟	误差 ± 5 分钟
通讯方式	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 $220\text{V} \pm 15\%$, 工作频率 $50\text{Hz} \pm 1\%$ 的条件下能正常工作 车辆供电直流电压 $12\text{V} \pm 10\%$ 或 $24\text{V} \pm 10\%$ (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	平均无故障工作时间不低于10,000小时。
温度	存储温度 $-40^{\circ}\text{C} \sim 70^{\circ}\text{C}$ 工作温度 $-20^{\circ}\text{C} \sim 90^{\circ}\text{C}$
湿度	存储湿度 10%~98% 工作湿度 10%~95%
使用寿命	≥ 5 年

8.3 卡片技术指标

卡片的技术性能指标如下表所示:

表3 卡片的技术性能指标

项目	指标
规范	符合：《市政交通一卡通技术规范—第二部分 卡片》 符合：GB/T 14916 标准和 ISO/IEC14443 TYPE A 系列标准
频率	13.56 MHz±7 KHz
通信距离	卡与读写器之间感应距离在 0mm~100mm 应能正常通信。
场强	当 PCD 组件的激励频率为 13.56 MHz，场强最小为 1.5A/m 最大为 7.5A/m 时，卡应能正常应答。
通信波特率	卡与读写器之间采用半双工通讯协议，其最低通信速率规定为 106k 波特率或 106k 波特率的倍频。
调制方式	ASK 100% (TYPE A)
数据存储容量	芯片内 NVM 的数据容量应不小于 8Kbyte,并应具有足够存储空间，保留用于应用扩展。
芯片使用寿命	芯片内 NVM 的擦写无故障次数应不少于 10 万次，数据存数保证 10 年不丢失。
卡片操作系统	卡片操作系统须符合 JR/T 0025-2013 和 CJ/T 166-2006 的相关规定。
卡片 ATQA 响应时间	卡片在进入天线感应区后，ATQA 响应的的时间须小于 3ms。

9 通信及传输要求

本部分规定一卡通中心计算机处理系统和运营实体计算机处理系统连接时通信和数据传输的要求。

9.1 网络连接

- 一卡通中心计算机处理系统和运营实体计算机处理系统之间主要通过公共电信网络实现。包括各种公共电信网络服务商提供的专线、拨号等方式。相互之间也可建立专用网络。
- 一卡通中心计算机处理系统和运营实体计算机处理系统之间的网络连接的带宽应满足数据传输的要求。
- 一卡通中心计算机处理系统和运营实体计算机处理系统之间的网络物理连接应有备份线路。
- 直接与一卡通中心计算机处理系统连接的设备 IP 地址应统一规划和分配。

9.2 网络协议

一卡通中心计算机系统和与其连接的计算机系统、终端之间的数据传输协议有：

- 基于 TCP/IP 协议
- 基于 UDP 协议

9.3 数据传输

- a) 计算机处理系统相互之间的数据传输应基于统一的应用层通信接口。
- b) 计算机处理系统相互之间的数据传输在应用层应以本标准规定格式的数据包进行。
- c) 数据包内最大原始交易记录的数量不应超过 65535 条记录。
- d) 发送到一卡通中心计算机处理系统的数据包的传输时间、间隔可通过参数设置。

9.4 数据组织结构

9.4.1 卡号编码

市政交通一卡通系统发行的每张一卡通卡应设置唯一的卡号，编码规则见附录 C。

9.4.2 应用单位编码

市政交通一卡通系统中的每个应用单位应设置唯一的编码，

9.4.3 交易类型编码

一卡通系统主要交易类型包括发卡、充值、消费、补票、锁卡、退卡、退资等，并可根据应用的需要进行扩展。

交易类型支持最多 256 种交易类型的应用。

已定义的主要交易类型编码见附录 C。

9.4.4 数据包结构要求

数据包包括交易文件数据包和联机交互报文两种包格式：

交易文件格式：

- a) 数据包结构包括包头、包体和三部分。
- b) 包头包括公共部分和个性部分。
- c) 包体包括若干条数据记录。

数据包结构如下所示：

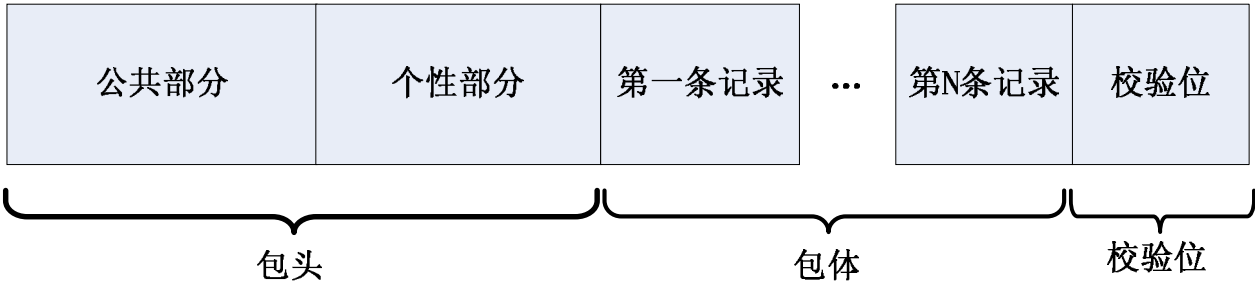


图2 数据包结构图

联机交互报文格式：

- a) 交互的消息报文由消息包头、消息包体、CRC 三部分组成。
- b) 消息包头又可划分为包长度、同步信息、压缩加密标志三个组成部分。
- c) 消息包体包含明文部分和密文部分

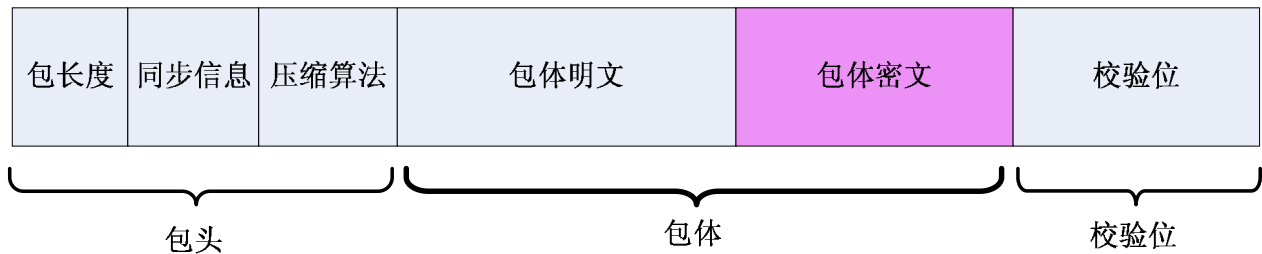


图3 联机交互报文格式

9.4.5 数据包类型

一卡通中心计算机处理系统接收及下发的数据包类型包括管理数据、黑名单数据、各类参数、原始交易数据、统计对帐数据等。数据包类型见附录D。

9.4.6 数据包数据项

数据包内的数据内容包含数据包的版本号、数据包编号、产生时间、发送及接收方编码、数据包内记录数量、数据包长度等，具体数据项见附录E。

9.4.7 交易记录数据项

交易记录的数据项包括公共数据项和个性数据项，至少应由附录F规定的的数据项组成。

10 安全要求

系统安全应包括：卡片安全、交易安全、鉴别及访问控制安全、操作审计、数据安全、网络与计算环境的安全几个要素，基本要求如下：

- a) 市政交通一卡通系统应用安全要求应符合 GB/T 22239-2008 《信息系统安全等级保护基本要求》不低于第三级的基本要求。
- b) 市政交通一卡通系统密钥管理要求应符合 CJ/T 166 的相关规定。
- c) 一卡通卡应采用一卡一密的密钥管理体系；对称密钥管理采用三级密钥管理体系，分别为部级主密钥，城市分散密钥，卡片分散密钥。
- d) 卡片交易验证应通过内置在终端的 SAM 卡、一卡通 API 模块或后台金融加密机完成，售卡充值类交易须采用联机方式进行。

- e) 互联网交易，须采用向用户颁发数字证书、交互报文附带数字签名的方式，加强交易的安全性和抗抵赖性。
- f) 终端应正确生成和完整保存交易数据，并将交易数据实时上传至一卡通中心计算机系统；交易数据包含交易验证码 TAC。
- g) 系统安全应包括鉴别及访问控制、操作审计、网络安全、计算环境安全等，应符合 GB/T 22239-2008 中应用安全的第三级要求。

详细的安全要求请见DBxxxx-xxxx.4《市政交通一卡通技术规范第4部分：安全规范》。

11 业务规范

一卡通系统业务规范可按照：业务类型、应用领域、交易模式和应用方式四个方面进行分类描述。

11.1 业务类型

一卡通系统业务类型包括：消费类应用、充值类应用、退卡类应用、信息管理类应用四类。

11.1.1 消费类应用

消费类应用是指在具有一卡通卡消费功能的终端上刷一卡通卡，对卡片进行扣款，完成支付或缴费类交易的应用。

11.1.2 充值类应用

充值类应用是指在具有一卡通卡充值功能的终端上刷一卡通卡，对卡片进行加值的的应用。

11.1.3 退卡类应用

退卡类应用是指在具有一卡通卡退卡功能的终端上刷一卡通卡，将卡片余额清空，完成退卡、退资或移资的应用。

11.1.4 信息管理类应用

信息管理类应用是指在具有一卡通卡信息管理功能的终端或网站上，进行卡片识别、信息查询、分析及处理等应用。

11.2 应用领域

一卡通卡支持交通领域、市政领域、商业应用领域及其它业务领域的应用。

11.2.1 交通领域

11.2.1.1 公共电汽车应用

通过车载、壁挂或手持式等一卡通卡读写终端，实现公共交通电汽车单一票制、分段票制和计次票制等收费要求。

11.2.1.2 轨道交通应用

与轨道交通 ACC/AFC 结合，以储值票的方式，实现轨道交通计程、计时收费要求。

11.2.1.3 出租汽车应用

运营出租汽车应安装具有一卡通读写功能的计价器，通过该终端设备，实现出租汽车乘客持卡付费的要求。

11.2.1.4 高速公路应用

与高速公路的 MTC、ETC 系统结合，实现高速公路持卡付费的要求。

11.2.1.5 停车场应用

与封闭式停车场和路侧停车场的收费终端结合，实现停车场付费的要求。

11.2.1.6 铁路客运应用

与铁路客运收费终端结合，实现铁路客运交通收费要求。

11.2.1.7 自行车租赁应用

实现公共自行车租车、还车业务的付费要求。

11.2.2 市政领域

11.2.2.1 水、电、气缴费应用

实现供水、供电、供气和供热应用的缴费的要求。

11.2.2.2 公园及旅游景点应用

实现公园及旅游景点付费的要求。

11.2.2.3 文化体育场馆应用

实现文化体育场馆付费的要求。

11.2.2.4 公共电话亭

实现刷一卡通卡拨打公共电话付费的要求。

11.2.3 商业应用领域

通过一卡通系统专用终端及与一卡通系统兼容的终端，实现超市、商场、连锁店、书报亭、菜市场、或快餐店等商业消费应用。

利用网络便携式读写器，实现一卡通卡网络购物、付费的要求。

11.2.4 信息管理领域

与楼宇、酒店、校园、企业、园区等管理系统相结合，实现将一卡通卡作为身份识别及信息管理介质的要求。

11.3 交易模式

从交易模式划分，一卡通卡交易可分为脱机交易和联机交易两大类。

11.3.1 脱机交易

脱机交易是指在交易过程中，终端无需与后台进行通讯，终端和卡片之间的密钥认证、数据传输、业务判断和处理全部在终端本地完成，交易成功后产生的交易记录暂存在终端内部的数据存储区内，定时或定期上传至一卡通中心计算机处理系统进行结算的交易模式。

脱机交易交易模式较多用于网络实时通讯较为困难，且要求快速通行的交通领域，如公交、轨道、出租等。

11.3.2 联机交易

联机交易是指在交易过程中，终端须与后台进行实时通讯，密钥认证、数据传输、业务判断和处理由终端、一卡通中心计算机处理系统、卡片共同完成，交易成功后产生的交易记录实时上传至一卡通中心进行结算的交易模式。

联机交易交易模式较多用于网络条件较好、交易所需的安全性较高的行业及应用，如：发卡、充值、退卡、退资类交易，部分消费类交易等。

11.4 应用方式

从应用方式划分，一卡通应用方式可分为近场支付和远程支付两大类

11.4.1 近场支付

是指在支付过程中，持卡人使用智能卡，通过终端设备刷卡，在交易现场购买商品或服务的支付方式。

根据终端设备是否需要联机进行支付处理，近场支付又可分为：脱机支付、联机支付两类。

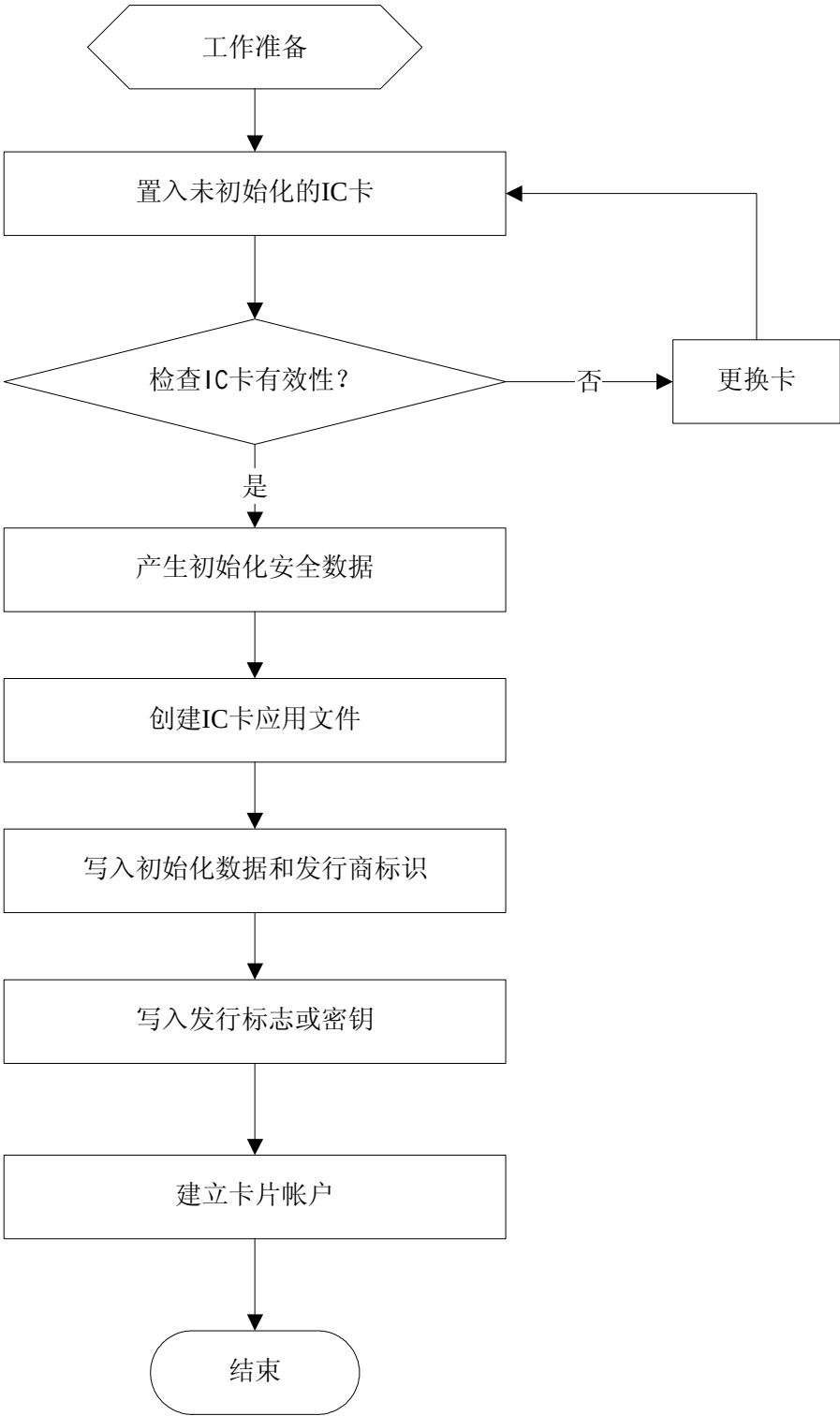
公共电汽车、轨道交通、出租车、停车场、超市便利店小额消费等应用均为近场交易。

11.4.2 远程支付

是指在支付过程中，消费者使用手机或个人电脑，基于移动通信或互联网技术，与后台服务器之间进行交互完成交易处理的支付方式。

远程支付均为联机交易。

附 录 A
(规范性附录)
一卡通卡初始化流程图



附 录 B
(规范性附录)
卡号编码

卡号编码含义见表 B.1。

表 B.1：卡号编码

数据项	说明
城市编码	1000：北京市
发行顺序号	有效范围：000000000000-999999999999

本节中城市编码规则引用 GB/T 2260。

附 录 C
(规范性附录)
交易类型编码

交易类型编码含义见表 C.1。

表 C.1：交易类型编码

交易类型编码	说明
0x00~0xDF	通用
0xE0~0xEF	预留
0xF0~0xFF	专用

附 录 D
(规范性附录)
数据包类型

数据包类型含义见表 D.1。

表 D.1：数据包类型

序号	数据包类型	数据包名称
1	管理数据	授权充值额度余额数据、交易费率表、结算清分参数表、交易模式数据、请求一卡通卡配送数据、一卡通卡回收配送数据、
2	终端交易数据	消费终端原始消费数据，售卡、充值、服务终端原始交易数据
3	统计对帐数据	售卡、充值、服务终端交易统计数据
4	测试数据	测试交易数据包数据、通信测试数据包数据
5	其它数据	预留供系统扩展使用

附 录 E
(规范性附录)
数据包数据项

数据包数据项含义见表 E.1。

表 E.1：数据包数据项

序号	数据项	说明
1	包格式版本号	
2	包编号	每个传输的数据包须有唯一代码
3	发送方代码	运营实体编码
4	接收方代码	运营实体编码
5	测试状态	标识此数据包是否为测试数据，标识是否参与清算划帐。0：非测试数据，1～255：测试数据
6	包中记录开始位置	本包的记录开始位置：相对文件开始位置的偏移量。
7	记录长度	如果包体不分记录，写包体长度
8	包中记录总数	记录总条数
9	数据包生成时间	YYYYMMDDHHMMSS（打包时间）
10	包状态	表示不同数据包类型的个性化特征
11	其它	预留
12	包头个性数据项	根据不同行业情况可分别设计定义。长度可变，个性区内部数据格式可根据需要定义。
13	记录 1	
14	记录 2	
...		
	记录 N	
	校验位	全为 FF 时表示无校验

附 录 F
(规范性附录)
交易记录数据项

交易记录数据项见表 F.1。

表 F.1：交易记录数据项

序号	数据项	说明
1	SAM 卡号	存储在 SAM 卡中的编号
2	交易顺序号	对一卡通卡钱包具有加款权限的终端，必须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
3	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
4	交易金额	交易金额，计次卡时为次数
5	卡内余额	交易后一卡通卡内余额，计次卡时为次数
6	交易日期	格式为“YYYYMMDD”
7	交易时间	格式为“HHMMSS”
8	卡序列号	一卡通卡内部序列号 CSN；CSN 超过 4 位时取低 4 位，没有 CSN 时，填写 FF
9	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
10	城市编码	
11	行业编码	
12	卡发行号	一卡通卡发行顺序号
13	TAC	由 SAM 卡对相关数据项计算得出的交易验证码
14	交易前余额	一卡通卡交易前卡内余额，计次卡时为次数
15	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
16	卡物理类型	定义一卡通卡的物理特征，如逻辑加密卡、智能卡等
17	锁定标记	未锁定为 0，锁定为 1，其它值为非法
18	月票标志	

DBXX/ XXXXX—XXXX

19	交易状态	
20	其它	预留
21	个性项数据	不同业务应用可使用不同的数据项