ICS 35.240.15
L64

DB11

北 京 市 地 方 标 准

DB 11/T 159.1—2015
代替 DB11/T 159.1—2002

市政交通一卡通技术规范
第 1 部分：总则

Municipal administration & communication card technology specifications—Part 1:General specifications

2015 - 01-28 发布　　2015 - 08-01 实施

北京市质量技术监督局　发布

目　　次

前　言

本部分按照GB/T 1.1-2009给出的规则起草。

DB11/T 159《市政交通一卡通技术规范》分为5个部分：

---- 第1部分：总则；

---- 第2部分：卡片；

---- 第3部分：终端；

---- 第4部分：安全；

---- 第5部分：检测。

本部分为DB11/T 159的第1部分。

本部分代替了DB11/T 159.3-2005《市政交通一卡通技术标准第3部分：应用》。

本部分与DB11/T 159.3-2005相比主要变化如下：

——修改了前言的描述（见前言，2005年版的前言）；

——删除了引言（见2005年版的引言）；

——修改了规范性引用文件清单所列标准中标示与引用文件的对应关系，只有正在起草的与引用文件存在一致性程度的标准，才需标示（见2，2005年版的2）；

——对“术语和定义”及“符号和缩略语”在正文中的出现情况做了核对，删除了没有出现的，修改了出现的，并同步将术语定义和缩略语统一在本标准第1部分“总则”中定义（见3和4，2005年版的3和4）；

——修改了“系统组成”，调整为“系统构成”（见5，2005年版的6）；

——根据当前先进技术的发展趋势及主流标准的应用情况，增加了对系统、终端、卡片的新要求（见6，7，8，9）；

——删除了“一卡通卡应用要求”、“终端应用要求”、“中心计算机处理系统的应用要求”，将其合并为“系统功能”，增加了系统业务连续性要求，增加了同城异地备份系统的建设要求（见6，2005年版的7、8和9）；

——增加了第7章“性能指标”（见7）；

——删除了“系统应用的安全要求”，将其调整为“安全要求”，增加了信息系统安全等级保护的要求（见9，2005年版的11）。

——删除了“主要应用方式”，将其调整为“业务规范”，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了补充（见10，2005年版的5）。

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、北京市政交通一卡通有限公司。

本部分主要起草人员： 葛昱、邹迎、俞宏熙、白洪波、陈文革、刘敬光、周湘鹏、蒋金煜、邢钊、曾正喜、卢明、李倩、陈智宏、刘浩、隋莉颖、王立勋、李伟。

市政交通一卡通技术规范

第 1 部分：总则

1 范围

本部分规定了市政交通一卡通的系统结构、系统功能、性能指标、通信及传输要求、安全要求、业务规范要求。

本部分适用于市政交通一卡通系统的设计、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，仅所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 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

CJ/T 304 建设事业 CPU 卡操作系统技术要求

JR/T 0025 中国金融集成电路（IC）卡规范

DB11/T 159.2-2014 市政交通一卡通技术规范 第 2 部分：卡片

DB11/T 159.3-2014 市政交通一卡通技术规范 第 3 部分：终端

DB11/T 159.4-2014 市政交通一卡通技术规范 第 4 部分：安全

ISO/IEC 14443-2 识别卡-无触点集成电路卡-邻近卡 第 2 部分：射频功率及信号接口

3 术语和定义

下列术语和定义适用于本标准。

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，持卡人使用一卡通卡，通过终端设备刷卡方式，在交易现场购买商品与服务，进行支付的行为。

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，交易数据保存在终端内部，定时批量上传至后台系统，交易处理全部在终端本地完成的交易。

3.5

联机交易 online transaction

在交易过程中，终端须与后台实时通讯，交易数据实时上传到后台系统，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。

3.6

公开密钥基础设施 public key infrastructure

提供鉴别、加密、完整性和不可否认性服务的支持公钥管理体制的基础设施。

3.7

数字签名 digital signature

对数据的一种非对称加密变换。该变换可以使数据接收方确认数据的来源和完整性，保护数据发送方发出和接收方收到的数据不被第三方篡改，也保护数据发送方发出的数据不被接收方篡改。

3.8

智能IC卡 Smart Card

带CPU的集成电路卡，用于执行处理和/或存储功能的电子器件，简称IC卡。

3.9

市政交通一卡通卡 multi-application card

国家IC卡注册中心注册，北京市指定的发卡机构统一发行，并在市政、交通及其它服务行业应用，符合本规范的智能IC卡。简称一卡通卡。

3.10

读写器 reader

可以对IC卡进行数据交换的终端设备。

3.11

初始化 initialization

在卡发行前，由卡的发行机构对IC卡进行格式化，并在卡中写入卡的发行信息的过程。

3.12

应用文件 application file

按照一定的数据格式产生的具有不同功能的数据文件，应用文件包括卡的应用目录文件、发行文件、电子钱包文件、交易记录文件和用户过程文件等。

3.13

电子钱包 electronic purse

一种为方便持卡人进行小额消费而设计的IC卡应用，支持圈存、消费等交易，除圈存交易外，其它交易均无须提交个人密码。

3.14

加密算法 cryptographic algorithm

为了隐藏或揭露信息内容而变换数据的算法。

3.15

明文 plaintext

没有加密的信息。

3.16

密文 ciphertext

通过密码系统产生的不可理解的文字或信号。

3.17

密钥 key

对数据进行加密时使用的秘密参数，密钥对密文解密，使原数据文件恢复。

3.18

终端 terminal

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。

3.19

典型交易时间 currently transaction time

终端完成一次正常消费交易的卡片处理时间，这个时间是从终端寻卡成功，到终端接收到卡片返回的最后一条指令为止，不包括处理意外、中断等附加时间。

3.20

API模块 API module

集成了市政交通一卡通核心应用的嵌入式组件。

3.21

授权 authorization

终端机需通过通信线路向前置系统申请，只有获得了系统认证通过后，才能进行一卡通卡的相关业务。

3.22

充值机 add-value machine

可以对IC卡中电子钱包进行充值的终端设备。

3.23

对称加密技术 symmetric cryptographic technique

发送方和接收方使用相同保密密钥进行数据变换的加密技术。在不掌握保密密钥的情况下，不可能推导出发送方或者接收方的数据交换。

3.24

非对称加密技术 asymmetric cryptographic technique

采用两种相关变换进行的加密技术，一种是公开变换（由公共密钥定义），另一种是私有变换（由私有密钥定义）。这两种变换具有以下属性，即私有变换不能通过给定的公开变换导出。

3.25

非平台卡 non platform card

智能卡COS与硬件平台紧密结合在一起，不具备二次开发能力的智能卡。

3.26

平台卡 platform card

具有安全防护性的方式来执行小型Java Applet的智能卡。

3.27

标准卡 standard card

卡片规格遵循 GB/T 14916-2006的 5.1.1的尺寸和公差的卡片。

3.28

异形卡 alien card

卡片外观和尺寸不符合标准卡要求的卡片。

3.29

Timing攻击 Timing attack

在加密过程中，由于各分支语句的执行、频率、RAM命中率等因素所造成时间不一致，利用这些漏洞进行的攻击活动。

3.30

SPA/DPA攻击 simple power analysis/differential power analysis attack

系统消耗功率的大小随微处理器执行的指令不同而不同，通过观察系统的功耗，来提取与密钥有关信息的攻击活动。

3.31

A类终端 type A terminal

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。

3.32

B类终端 type B terminal

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。

3.33

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，通过远程控制实现一卡通卡读写功能的装置。

3.34

私钥 private key

一个实体的非对称密钥对中仅供实体自身使用的密钥，在数字签名模式中，私钥用于签名功能。

3.35

公钥 public key

一个实体的非对称密钥对中可以公开的密钥，在数字签名模式中，公钥用于验证功能。

4 缩略语

下列缩略语适用于本标准。

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）

AQL：合格质量水平（Acceptable Quality Level）

ATQA：对 A 型卡请求的应答（Answer To Request，Type A）

COS：卡片操作系统（Chip Operating System）

CPU：中央处理单元（Central Process Unit）

CSN：芯片序列号（Chip Serial Number）

ETC：电子收费（Electronic Toll Collection）

IC：集成电路（Integrated Circuit）

MAC：报文验证码（Message Authorization Code）

MF：主文件（Master File）

MTBF：平均故障间隔时间（Mean Time Between Failure）

MTC：人工收费（Manual Toll Collection）

NVM：非挥发性存储器（Nonvolatile Memory）

PCD：接近耦合设备（Proximity Coupling Device）

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

RSA：一种非对称加密算法（Rivest,Shamir,Adleman）

SAM：安全存取模块（Secure Access Module）

SHA：安全哈希算法（Secure Hash Algorithm）

SN：序号（Serial Number）

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 系统构成

市政交通一卡通系统逻辑结构如图 1 所示：

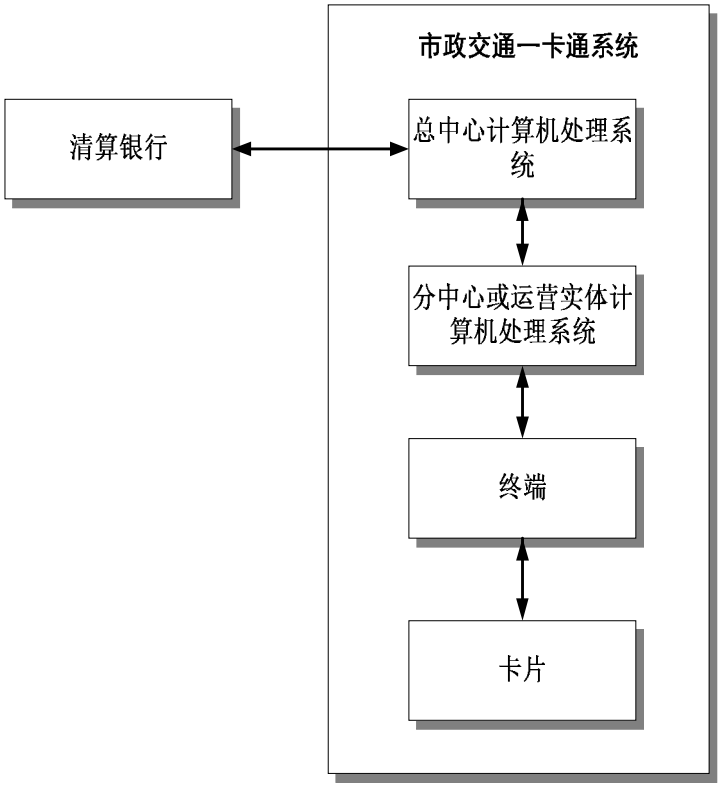


图1　市政交通一卡通系统逻辑结构图

市政交通一卡通系统架构分为四层，应由总中心计算机处理系统、分中心或运营实体计算机处理系统、终端、卡片等组成，由总中心计算机处理系统和清算银行进行系统连接，完成清分结算。

6 系统功能

6.1 总中心计算机处理系统

6.1.1 接入与传输

应能为终端、分中心或运营实体计算机处理系统提供业务接入及数据通讯服务，具体要求如下：

a) 应能为各业务终端、分中心/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、分中心或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分中心或运营实体计算机处理系统。

6.1.2 业务处理

一卡通系统中的业务处理功能应包括卡片初始化、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，具体要求如下：

a) 卡初始化：应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。卡片初始化流程见附录 A；
b) 包级合法性检查：系统应对上传的数据包进行合法性检查，主要包含：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；
c) 交易合法性验证：系统应对上传的交易记录进行合法性检查，主要包括：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验证码；
d) 终端管理：系统应对终端进行管理，包括为终端提供联机授权认证、参数下载功能；
e) 联机交易服务：应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的功能，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：应具备终端、卡帐户、交易记录等异常数据处理的功能。

6.1.3 结算清分

具体功能要求如下：

a) 结算对帐：应能完成一卡通总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的功能；
c) 数据分析：具备对交易数据、历史数据和各类统计数据分析的功能。

6.1.4 综合管理

具体功能要求如下：

a) 操作员管理：应能设置、管理和维护一卡通总中心计算机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：应能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：应提供查询、分析、统计数据的报表功能。

6.1.5 基础数据管理

具体功能要求如下：
a) 卡帐户管理：应具备一卡通卡账户管理及维护的功能；
b) 终端信息管理：应能对终端基础信息进行管理及维护，包括终端基本信息管理、参数维护、状态监控、额度控制等；
c) 分中心或运营实体管理：应能对运营实体基础信息进行管理及维护，包括：行业、单位、商户、网点结算手续费率等；
d) 参数管理：应能对中心计算机处理系统的运行参数进行管理和维护；应能对运营实体运营参数进行管理和维护；
e) 黑名单管理：应具备黑名单的收集、生成、跟踪、下发及维护的功能。

6.1.6 其它功能

具体功能要求如下：
a) 数据审计：可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：可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：应具备网络状态、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：可对历史累计数据进行统计分析，深度挖掘潜在信息。

6.1.7 备份与恢复

应满足各类交易数据、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。

应建设总中心计算机处理系统的容灾备份系统，保障灾难发生时的业务连续性和数据完整性。

6.2 分中心或运营实体处理系统

6.2.1 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。

6.2.2 数据传输

应能将各类交易数据发送到一卡通总中心计算机系统，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或运营实体系统及系统内的所有终端。

6.2.3 数据接口

应按一卡通总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。

6.2.4 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。

应能实现与一卡通总中心计算机系统结算数据的对帐和异常数据处理。

6.2.5 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。

6.3 终端

6.3.1 终端应用通用要求

具体功能要求如下：

a) 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；
b) 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；
c) 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；
d) 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；
e) 终端应保证一卡通卡内的数据完整性；
f) 终端应保证一卡通卡内机密数据的安全性；
g) 同一终端的不同应用之间不应互相影响；
h) 终端支持在线升级功能；
i) 终端支持交易数据查询、数据采集上传功能；
j) 终端应符合 DB11/T 159.3-2014 的规定。

6.3.2 终端业务功能要求

6.3.2.1 充值类终端

终端应实现基本功能如下：

a) 终端应具有发卡、充值、延期、激活功能；
b) 终端应支持在线配置业务功能；
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) 交易数据应实时上传一卡通中心计算机处理系统；
f) 根据业务需求，应可与其它业务功能进行组合应用。

6.3.2.2 消费类终端

终端应实现基本功能如下：

a) 终端应具有消费、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) 交易数据应及时上传一卡通中心计算机处理系统；
d) 根据业务需求，应可与其它业务功能进行组合应用。

6.3.2.3 退卡类终端

终端应实现基本功能如下：

a) 终端应具有退卡、退资功能；
b) 终端应支持在线配置业务功能；
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) 交易数据应实时上传一卡通中心计算机处理系统；
f) 根据业务需求，应可与其它业务功能进行组合应用。

6.3.2.4 服务类终端

终端应实现基本功能如下：
a) 终端应具有查询、补票、修复功能；
b) 交易数据应及时上传一卡通中心计算机处理系统；
c) 根据业务需求，应可与其它业务功能进行组合应用。

6.4 卡片

6.4.1 一卡通卡

一卡通卡应符合 DB11/T 159.2-2014 的规定。

6.4.2 应用类型

应用类型编码应支持 256 种类型。

6.4.3 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。

6.4.4 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。

6.4.5 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。

6.4.6 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。

锁卡后的黑名单卡不能再使用。

6.4.7 回用

对回收的一卡通卡，应在经授权的终端设备上进行分拣、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应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。

6.4.8 销毁

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应对销毁的一卡通卡后台信息进行核销。

7 性能指标

7.1 总中心计算机处理系统性能指标

总中心计算机处理系统的处理性能指标如表 1 所示：

表1 总中心计算机处理系统的处理性能指标

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	≥99.99%
系统平均无故障时间	≥8751 小时
各类统计数据保存时间	≥10 年
原始数据保存时间	在线保存≥2 年，离线永久保存

7.2 分中心或运营实体处理系统

根据系统的应用规模和级别，可参照总中心计算机处理系统性能指标。

7.3 终端技术指标

终端的通用性能指标如表 2 所示：

表2 终端的通用性能指标

项目	指标
规范	应符合 DB11/T 159.3-2014 的规定
卡片识别要求	应识别符合 DB11/T 159.2-2014 的卡片
SAM 卡槽	不少于 4 个 SAM
IC 卡读卡模块	通信距离：(0~60)mm、无盲区 典型交易时间： 智能 IC 卡消费类终端不大于 300ms 交通行业交易时间：

表 2 终端的通用性能指标（续）

项目	指标
	入站（或上车）卡交易时间不大于 260ms，出站（或下车）卡交易时间不大于 300ms。
数据存储	数据存储容量 ≥8Mbyte 黑名单数据 ≥100000 条 存储器寿命 ≥10 年
时钟	支持时钟同步，误差±1 分钟
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℃～70℃ 工作温度 -20℃～70℃
湿度	存储湿度 10%～98% 工作湿度 10%～95%
使用寿命	≥5 年

7.4 卡片技术指标

卡片的性能指标如表 3 所示：

表3 卡片的性能指标

项目	指标
规范	应符合 DB11/T 159.2-2014 的规定
频率	13.56 MHz±7 KHz
通信距离	卡与读写器之间感应距离在(0～60)mm 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 106kbps 或 106kbps 的倍频
调制方式	ASK 100%，应符合 ISO/IEC14443-2

表 3 卡片的性能指标（续）

项目	指标
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，数据存储保证 10 年不丢失
卡片操作系统	卡片操作系统应符合 CJ/T 166-2006、CJ/T 304-2008 的相关规定，当支持电子现金应用时，应符合 JR/T 0025-2013
卡片 ATQA 响应时间	卡片在进入天线感应区后，ATQA 响应的时间应小于 3ms

8 通信及传输要求

8.1 网络连接

一卡通总中心计算机系统和分中心/运营实体计算机处理系统网络连接具体要求如下：

a) 一卡通总中心计算机系统和分中心/运营实体计算机处理系统之间宜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；
b) 一卡通总中心计算机系统和分中心/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；
c) 一卡通总中心计算机系统和分中心/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；
d) 直接与一卡通总中心计算机系统连接的设备 IP 地址应统一规划和分配。

8.2 网络协议

一卡通总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包括：基于TCP/IP协议、基于UDP协议。

8.3 数据传输

一卡通总中心计算机处理系统和分中心/运营实体计算机处理系统间数据传输要求如下：

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部分 8.4 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。

8.4 数据组织结构

8.4.1 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 B。

8.4.2 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。

8.4.3 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。

交易类型应支持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。

8.4.4 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。

交易文件格式要求如下：

a) 数据包结构包括包头、包体和校验位三部分；
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。

数据包结构如图2所示：

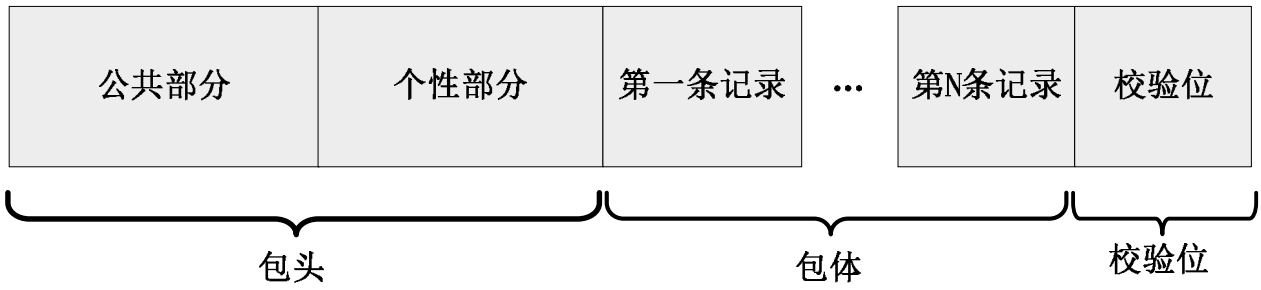


图2 数据包结构图

联机交互报文格式要求如下：

a) 交互的消息报文由消息包头、消息包体、校验位三部分组成；
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。

联机交互报文格式如图3所示：

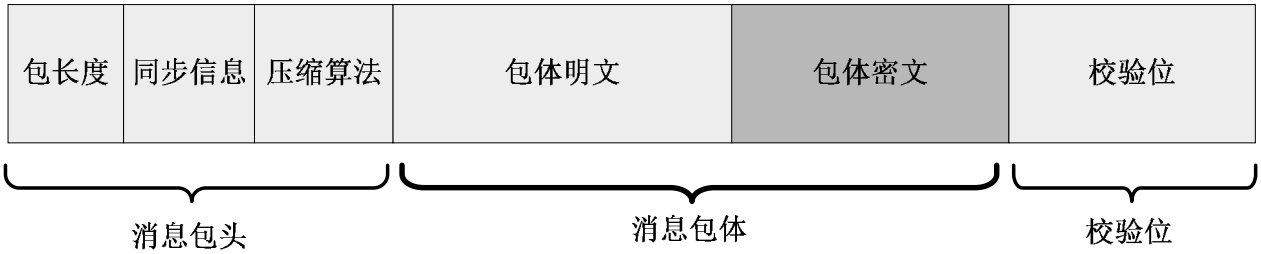


图3　联机交互报文格式

8.4.5　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。

8.4.6　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。

8.4.7　交易记录数据项

交易记录的数据项至少应由附录F规定的数据项组成。

9　安全要求

9.1　基本要求

系统安全基本要求如下：

a) 市政交通一卡通系统应用安全包括鉴别及访问控制、操作审计、网络安全、计算环境安全等，要求应不低于 GB/T 22239-2008 中第三级的基本要求；
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、API 模块或后台金融加密机完成，售卡充值类交易应采用联机方式进行；
e) 互联网交易，应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。

9.2　详细要求

其它安全要求见 DB11/T 159.4-2014。

10 业务规范

10.1 业务类型

10.1.1 消费类应用

在具有消费功能的终端上使用一卡通卡，应能对卡片进行扣款，完成支付或缴费类交易。

10.1.2 充值类应用

在具有充值功能的终端上应能对一卡通卡进行加值。

10.1.3 退卡类应用

在具有退卡功能的终端上使用一卡通卡，应能对卡片余额扣除，完成退卡、退资或移资。

10.1.4 信息管理类应用

在具有信息管理功能的终端或网站上使用一卡通卡，可对卡片识别、信息查询、分析、处理。

10.1.5 身份识别类应用

针对特定记名发行的一卡通卡，在具有身份识别功能的终端或网站上，可对记名卡信息进行识别、查询、分析的应用。

10.2 应用领域

10.2.1 交通领域

10.2.1.1 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，应能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。

10.2.1.2 轨道交通应用

应能与轨道交通 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。

10.2.1.3 出租汽车应用

应能通过具有一卡通读写功能的计价器，实现出租汽车乘客持卡付费的要求。

10.2.1.4 高速公路应用

应能与高速公路的 MTC、ETC 系统结合，实现高速公路持卡付费的要求。

10.2.1.5 停车场应用

应能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。

10.2.1.6 铁路客运应用

应能与铁路客运收费终端结合，实现铁路客运交通收费要求。

10.2.1.7 自行车租赁应用

应能实现公共自行车租车、还车业务的付费要求。

10.2.2 市政领域

10.2.2.1 水、电、气缴费应用

应能实现供水、供电、供气和供热应用缴费的要求。

10.2.2.2 公园及旅游景点应用

应能实现公园及旅游景点付费的要求。

10.2.2.3 文化体育场馆应用

应能实现文化体育场馆付费的要求。

10.2.2.4 公共电话亭

应能实现拨打公共电话付费的要求。

10.2.3 商业应用领域

应能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、菜市场及快餐店等应用的要求。

应能实现一卡通卡网络购物、付费的要求。

10.2.4 信息管理领域

应能与楼宇、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。

10.3 交易模式

10.3.1 脱机交易

在交易过程中，终端可不与后台进行实时通信，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。

脱机交易模式宜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。

10.3.2 联机交易

在交易过程中，终端应与后台进行实时通信，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应实时上传至一卡通总中心进行结算。

联机交易模式宜用于网络条件较好、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。

10.4 应用方式

10.4.1 近场支付

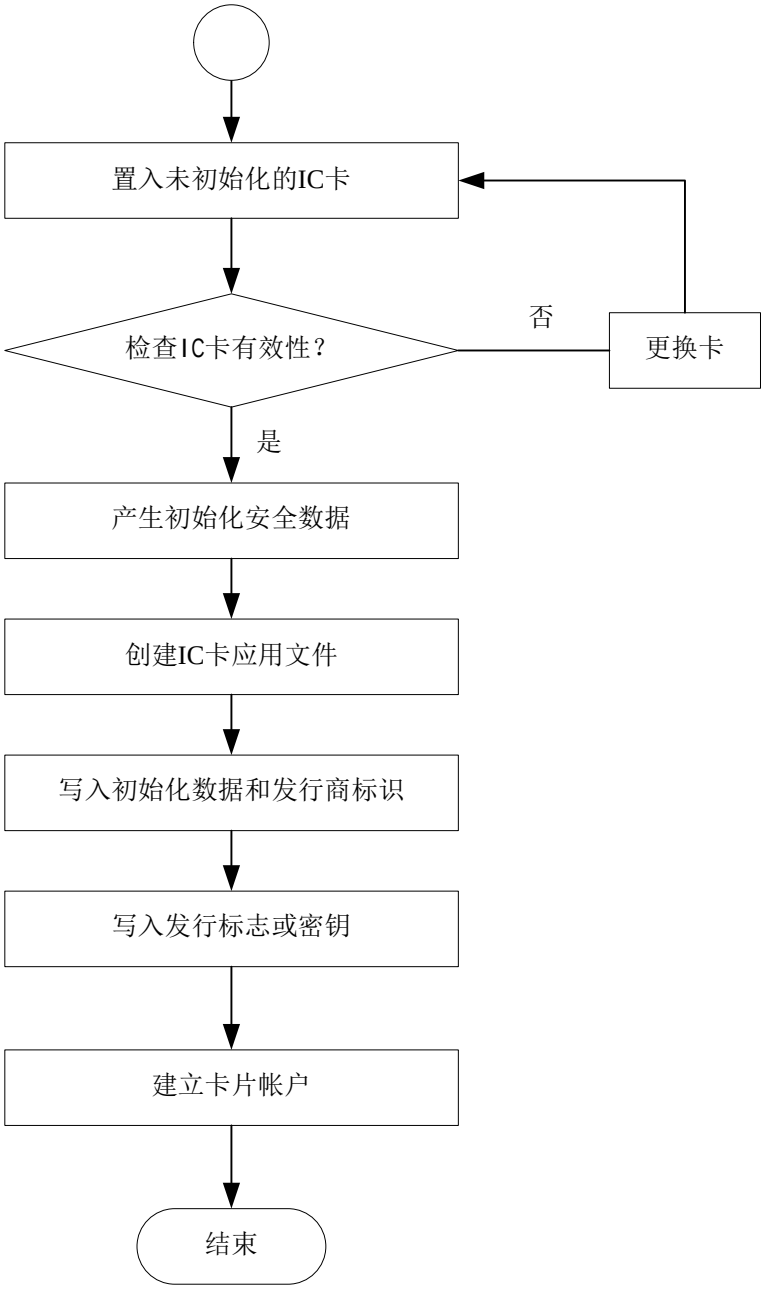
近场支付应能支持脱机支付、联机支付。

10.4.2 远程支付

远程支付应为联机交易。

附 录 A
（规范性附录）
一卡通卡初始化流程

一卡通初始化流程见图A.1



图A.1 一卡通初始化流程图

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

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值权限的终端，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 字节，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
10	城市编码	
11	发行顺序号	一卡通卡发行顺序号
12	TAC	由用户卡对相关数据项计算得出的交易验证码
13	交易前余额	一卡通卡交易前卡内余额，计次卡时为次数
14	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
15	卡物理类型	定义一卡通卡的物理特征，如智能卡等
16	应收金额	
17	交易状态	
18	其它	预留
19	个性项数据	不同业务应用可使用不同的数据项，如线路号、车辆号、上下车（进出站）站码等