ICS 35.240.15

L 64

|  |
| --- |
| 备案号： |

DB**11**

北京市地方标准

DB11/T 159.2—20xx

|  |
| --- |
| 代替DB11/T 159.1—2015 |

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

|  |
| --- |
|  |
|  |

20XX - XX - XX发布

20XX - XX - XX实施

北京市市场监督管理局   发布

目  次

[前言 III](#_Toc322950093)

[1 范围 1](#_Toc1131037082)

[2 规范性引用文件 1](#_Toc1962477577)

[3 术语和定义 1](#_Toc159302366)

[4 缩略语 5](#_Toc249295988)

[5 系统构成 5](#_Toc177075019)

[6 系统功能 6](#_Toc1834993238)

[6.1 总中心计算机处理系统 6](#_Toc718696499)

[6.2 分中心或运营实体处理系统 7](#_Toc1684027965)

[6.3 移动支付系统 8](#_Toc1771023942)

[6.4 终端 8](#_Toc1476045774)

[6.5 客户端软件 9](#_Toc170233474)

[6.6 卡片 9](#_Toc665779714)

[6.7 安全单元（SE） 10](#_Toc1369852328)

[6.8 安全 11](#_Toc2083380856)

[6.9 检测 11](#_Toc661182457)

[7 性能指标 11](#_Toc1413165221)

[7.1 总中心计算机处理系统性能指标 11](#_Toc2046217174)

[7.2 分中心或运营实体处理系统 12](#_Toc968920360)

[7.3 终端技术指标 12](#_Toc275995319)

[7.4 卡片技术指标 12](#_Toc88648913)

[8 通信及传输要求 13](#_Toc1716113420)

[8.1 网络连接 13](#_Toc2012870730)

[8.2 网络协议 13](#_Toc1008467919)

[8.3 数据传输 13](#_Toc1379372509)

[8.4 数据组织结构 13](#_Toc1027789398)

[9 业务规范 14](#_Toc1845439365)

[9.1 业务类型 15](#_Toc193093934)

[9.2 应用领域 15](#_Toc481958121)

[9.3 交易模式 16](#_Toc2109306810)

[9.4 应用方式 16](#_Toc459510994)

[附录A（规范性 一卡通卡初始化流程 18](#_Toc650081546)

[附录B（规范性）卡号编码 19](#_Toc1671231333)

[附录C（规范性）交易类型编码 20](#_Toc1446394618)

[附录D（规范性）数据包类型 21](#_Toc39460686)

[附录E（规范性）数据包数据项 22](#_Toc1790786326)

[附录F（规范性）交易记录数据项 23](#_Toc762468377)

前  言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是DB11/T 159《市政交通一卡通技术规范》的第1部分。DB11/T 159已经发布了以下部分：

——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；

——第6部分：移动支付。

本文件代替DB11/T 159.1—2015《市政交通一卡通技术规范 第1部分：总则》，与DB11/T 159.1—2015相比，除结构调整和编辑性改动外，主要技术变化如下：

1. 在“系统构成”中增加了移动支付、安全、检测的构成（见5）；
2. 在“系统功能”中增加了对移动支付、检测的新要求（见6）；
3. 更改了“性能指标”中终端技术指标黑名单数据存储等要求（见7，2015年版的7）；
4. 更改了“通信及传输要求”中网络连接、交易类型及数据包结构要求（见8，2015年版的8）；
5. 更改了“安全要求”，将安全要求描述调整到“系统功能”中（见6，2015年版的9）；
6. 在“业务规范”中增加了发卡类应用、其他类应用（见9）；
7. 删除了“应用领域”中自行车租赁应用要求（见2015版的10.2.1.7）；
8. 更改了“附录”中数据包类型、数据包数据项、交易记录数据项（见附录D、附录E、附录F，2015年版的附录B、附录D、附录E、附录F），增加了新卡号编码要求（见附录B.2)。

本文件由北京市交通委员会提出并归口。

本文件由北京市交通委员会组织实施。

本文件主要起草单位：北京市智慧交通发展中心、北京市政交通一卡通有限公司。

本文件主要起草人员：

本文件及其所代替文件的历次版本发布情况为：

——2015年首次发布为DB11/T 159.1—2015《市政交通一卡通技术规范 第1部分：总则》，并入了DB11/T 159.3—2005《市政交通一卡通技术标准 第3部分：应用》的内容；

——本次为第一次修订。

市政交通一卡通技术规范

第1部分：总则

1. 范围

本文件规定了市政交通一卡通系统的系统结构、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。

本文件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。

1. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅所注日期对应的版本适用于本文件；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 22239 信息安全技术 网络安全等级保护基本要求

JR/T 0025 中国金融集成电路（IC）卡规范

JT/T 978 城市公共交通IC卡技术规范

JT/T 1059 交通一卡通移动支付技术规范

DB11/T 159.2 市政交通一卡通技术规范 第2部分：卡片

DB11/T 159.3 市政交通一卡通技术规范 第3部分：终端

DB11/T 159.4 市政交通一卡通技术规范 第4部分：安全

DB11/T 159.5 市政交通一卡通技术规范 第5部分：检测

DB11/T 159.6 市政交通一卡通技术规范 第6部分：移动支付

1. 术语和定义

下列术语和定义适用于本文件。



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。



发卡机构 card issuer

发行城市公共交通IC卡，并对清分结算的跨机构交易数据进行验证的机构。

[来源：JT/T 978.1—2015,2.17]



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、交通及其他服务行业应用，符合本规范的智能IC卡。简称一卡通卡。



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。



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。



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。



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。



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。



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。



读写器 reader

可以对IC卡进行数据交换的终端设备。



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。



安全单元 secure element （SE）

负责对具有安全认证的交易关键数据的安全存储和运算，且支持多应用管理及运行安全的移动支付安全载体。

[来源：JT/T 1059.1—2016,3.12]



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。



移动支付 mobile payment

用户使用移动支付终端对所消费的服务进行账务支付的一种方式。

[来源：JT/T 1059.1—2016,3.2，有修改]



支付平台 payment platform

为用户提供货币支付及资金清算等服务的第三方平台。



电子钱包 electronic purse(EP)

一种为方便持卡人进行小额消费而设计的IC卡应用，支持充值、消费等交易。



电子现金 electronic cash（EC）

采用借记/贷记技术设计和非对称和对称密钥结合体系的IC卡应用。

[来源：JT/T 978.1—2015,2.5]



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。

[来源：JT/T 978.2—2015,3.1]



余额 balance

电子钱包用于消费的可支付金额。



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。



明文 plaintext

没有加密的信息。



密文 ciphertext

通过密码系统产生的不可理解的文字或信号。



密钥 key

对数据进行加密时使用的秘密参数，可利用密钥对密文解密，使原数据文件恢复。



终端设备 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两类终端，两类终端都可以用来实现充值、消费或服务功能。



移动支付终端 mobile payment terminal

具有交通一卡通移动支付应用及移动通讯能力的终端设备。

[来源：JT/T 1059.1—2016,3.3]



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。



认证 authentication

确认一个实体所宣称的身份的措施。

[来源：JT/T 978.6—2015,3.7]



证书 certificate

由密钥管理系统使用其私钥对实体的公钥、身份信息以及其他相关信息进行签名，形成的不可伪造的电子数据。

[来源：JT/T 978.6—2015,3.8]



可信服务管理 trusted service management （TSM）

由可信第三方提供的安全载体生命周期管理、应用生命周期管理和应用管理等服务。

[来源：JT/T 1059.1—2016,3.18]



客户端 client

用于提供用户接口界面，与SE配合实现SE管理及应用管理功能的应用软件。

[来源：JT/T 1059.6—2016,3.1]

1. 缩略语

下列缩略语适用于本文件。

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）

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

CSN ：芯片序列号（Chip Serial Number）

ETC ：电子收费（Electronic Toll Collection）

IC：集成电路（Integrated Circuit）

IIN：发行机构注册识别码（Institution Identification Number）

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）

SAM：安全认证模块（Secure Authentication Module）

SE：安全单元 （Secure Element）

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)

TSM：可信服务管理（Trusted Service Management）

UDP：用户数据报协议（User Dataprogram Protocol）

1. 系统构成

市政交通一卡通系统逻辑结构如图1所示：



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包括：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、移动支付系统、终端、客户端软件、卡片及SE等组成，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。通过密钥安全机制和加密算法，保障系统的卡片、终端或移动支付终端、交易、清分结算各环节整体安全性。通过各环节的检测机制建立系统质量保证体系。

1. 系统功能
   1. 总中心计算机处理系统
      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：

1. 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）、清算银行及其他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；
2. 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交易数据、终端状态信息和日志数据；
3. 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。
   * 1. 业务处理

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：

1. 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市政交通一卡通系统中使用。卡片初始化流程应符合附录A要求；
2. 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；
3. 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；
4. 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；
5. 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：开卡、发售充值、退卡退资、消费、激活、查询、卡片迁卡等联机类交易；
6. 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。
   * 1. 结算清分

具体功能要求如下：

1. 结算对帐：应能完成总中心计算机处理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；
2. 查询统计：具备交易数据分类查询统计的功能；
3. 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；
4. 数据审计：具备对交易数据及结算数据完整性的审核功能。
   * 1. 综合管理

具体功能要求如下：

1. 操作员管理：应能设置、管理和维护总中心计算机处理系统的操作员及权限的管理功能；
2. 授权额度管理：应能对具有发售充值功能的终端、商户、运营单位实现后台交易额度的控制和管理；
3. 报表功能：应提供查询、分析、统计数据的报表功能；
4. 对账功能：应提供总中心计算机处理系统与分中心或运营实体处理系统资金的对帐、划账功能。
   * 1. 基础数据管理

具体功能要求如下：

1. 卡帐户管理：应具备一卡通卡账户管理及维护的功能；
2. 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；
3. 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；
4. 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；
5. 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。
   * 1. 其他功能

具体功能要求如下：

1. 风险管理：可对联机交易、脱机交易进行风险控制；
2. 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；
3. 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；
4. 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。
   * 1. 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。

* 1. 分中心或运营实体处理系统
     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。

* + 1. 数据传输

应能将各类交易数据发送到总中心计算机处理系统，并具备重传功能。

应能接收总中心计算机处理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。

* + 1. 数据接口

应按总中心计算机处理系统的数据编码、数据格式、数据组织形式要求实现数据接口。

* + 1. 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。

应能实现与总中心计算机处理系统结算数据的对帐和异常数据处理。

应能实现对行业内交易数据及统计数据完整性的审核功能。

* + 1. 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。

* 1. 移动支付系统

移动支付系统主要由安全单元（SE）、客户端软件、可信服务管理系统组成。以SE为载体，客户端软件为入口，依靠安全、可靠的网络，通过统一的数据接口，实现开卡、充值、消费等功能。

* 1. 终端
     1. 终端应用通用要求

具体功能要求如下：

1. 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；
2. 终端应支持对一卡通总中心计算机处理系统各类参数的下载，包括通讯类参数、业务类参数、管理类参数等；
3. 终端应支持对一卡通总中心计算机处理系统黑名单参数实时下载；
4. 终端应依据一卡通总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；
5. 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；
6. 终端应保证一卡通卡内的数据完整性；
7. 终端应保证一卡通卡内机密数据的安全性；
8. 同一终端的不同应用之间不应互相影响；
9. 终端支持在线升级功能；
10. 终端支持交易数据查询、数据采集上传功能；
11. 终端应符合DB11/T 159.3的规定。
    * 1. 终端业务功能要求
         1. 充值类终端

终端应实现基本功能如下：

1. 终端应具有发售、充值、激活功能；
2. 终端应支持在线配置业务功能；
3. 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；
4. 终端的发售、充值、激活交易应采用联机方式进行；
5. 交易数据应实时上传总中心计算机处理系统；
6. 根据业务需求，应可与其他业务功能进行组合应用。
   * + 1. 消费类终端

终端应实现基本功能如下：

1. 终端应具有消费、缴费功能；
2. 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；
3. 交易数据应及时上传一卡通总中心计算机处理系统；
4. 根据业务需求，应可与其他业务功能进行组合应用。
   * + 1. 退卡类终端

终端应实现基本功能如下：

1. 终端应具有退卡、退资功能；
2. 端应支持在线配置业务功能；
3. 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；
4. 终端的退卡、退资交易应采用联机方式进行；
5. 交易数据应实时上传总中心计算机处理系统；
6. 根据业务需求，应可与其他业务功能进行组合应用。
   * + 1. 服务类终端

终端应实现基本功能如下：

1. 终端应具有查询、补票、修复功能；
2. 交易数据应及时上传总中心计算机处理系统；
3. 根据业务需求，应可与其他业务功能进行组合应用。
   1. 客户端软件
      1. 客户端软件应用通用要求

具体功能要求如下：

1. 客户端软件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；
2. 客户端软件应能提供支付和TSM应用管理等功能；
3. 客户端软件应有规范的上线发布流程，并应提供安全可靠的客户端下载、发布和升级渠道；
4. 客户端软件应依据总中心计算机处理系统及移动支付系统的各类参数进行准确的业务判断，对黑名单卡进行提示；
5. 客户端软件应保证一卡通卡内的数据完整性；
6. 客户端软件应保证一卡通卡内机密数据的安全性；
7. 客户端软件应支持对SE中的应用进行余额查询，以及卡片参数设置等操作；
8. 客户端软件应符合DB11/T 159.6的规定。
   * 1. 客户端软件业务功能要求

客户端软件实现基本功能如下：

1. 客户端软件应能通过界面操作完成用户注册；
2. 客户端软件应具有开卡、消费、充值、退卡、迁卡、查询功能；
3. 所有交易应采用联机方式进行；
4. 交易数据应实时上传移动支付系统，移动支付系统应实时上传总中心计算机处理系统。
   1. 卡片
      1. 基本要求

卡片规范应符合DB11/T 159.2的相关规定。

* + 1. 应用类型

应用类型编码应支持256种类型。

* + 1. 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。

* + 1. 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。

* + 1. 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。

* + 1. 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，可在经授权的终端设备上办理查询、补票、修复、激活等服务业务。

锁卡后的黑名单卡不能再使用。

* + 1. 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、并对一卡通卡进行回用。

总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。

* + 1. 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、并对一卡通卡进行销毁。

总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。

* 1. 安全单元（SE）
     1. 基本要求

SE规范应符合DB11/T 159.6的相关规定。

* + 1. 开卡

通过移动支付终端发起开卡请求，完成SE应用创建的过程。

* + 1. 充值

通过已授权终端发起充值请求，完成SE应用充值的过程。

* + 1. 消费

通过移动支付终端与终端设备或支付平台交互进行支付，并在交易完成后将交易通知或文件转发至总中心计算机处理系统进行处理。

* + 1. 退卡

通过移动支付终端请求TSM平台删除SE应用并退还余额的过程。

* + 1. 迁卡

将移动支付终端上的一个SE应用迁移到另一台移动支付终端上的过程，迁移前后SE应用数据完全一致。

* 1. 安全

应符合网络安全等级保护基本要求，并通过密钥的安全机制和加密算法，保障卡片、终端、交易、清分结算各部分以及整体的安全性。

* + 1. 基本要求

系统安全基本要求如下：

1. 系统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，应不低于 GB/T 22239中第三级的要求；
2. 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；
3. 卡片交易验证应通过内置在终端的SAM卡或后台金融加密机完成；
4. 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。
   * 1. 详细要求

其他安全要求应符合DB11/T 159.4相关规定。

* 1. 检测

依据统一的技术标准、质量要求和业务流程，执行卡片、终端及应用系统的检测，实现系统规范性、稳定性及可靠性。

其他检测要求应符合DB11/T 159.5相关规定。

1. 性能指标
   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：

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） | ≥5000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 |

* 1. 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。

* 1. 终端技术指标

终端的通用性能指标如表2所示：

1. 终端的通用性能指标

|  |  |
| --- | --- |
| 项目 | 指标 |
| 规范 | 应符合DB11/T 159.3的规定 |
| 卡片识别要求 | 应识别符合DB11/T 159.2的卡片 |
| SAM卡 | 支持不少于4个SAM卡，其中不少于2个须使用卡座支持 |
| IC卡读卡模块 | 通信距离：(0~60)mm、无盲区 |
| 数据存储 | 数据存储容量 ≥8Mbyte  黑名单容量 ≥5M  存储器寿命 ≥10年 |
| 时钟 | 支持时钟同步，误差±2秒钟/日 |
| 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%（非凝露）  工作湿度 10%～90%（非凝露） |
| 使用寿命 | ≥5 年 |

* 1. 卡片技术指标

卡片的性能指标如表3所示：

1. 卡片的性能指标

|  |  |
| --- | --- |
| 项目 | 指标 |
| 规范 | 应符合DB11/T 159.2的规定 |
| 频率 | 13.56 MHz±7 KHz |
| 通信距离 | 卡片与读写器之间感应距离在(0～100)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 |
| 通信速率 | 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 |
| 数据存储容量 | 芯片内NVM的数据容量支持电子钱包应用的数据空间不小于20K，支持电子现金应用的数据空间不小于10K，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 | 卡片操作系统符合JT/T 978的相关规定，当支持电子现金应用时，应符合JR/T 0025 |
| 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 |

1. 通信及传输要求
   1. 网络连接

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、移动支付系统网络连接具体要求如下：

1. 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之间应统一规划，采用安全、可靠的网络实现，包括各种电信运营商提供的专线，相互之间也可建立VPN专用网络；
2. 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之间的网络连接的带宽应满足数据传输的要求；
3. 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之间的网络物理连接应有冗余备份线路；
4. 总中心计算机处理系统和移动支付系统可通过局域网、专线实现；
5. 直接与总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，并支持IPV6。
   1. 网络协议

总中心计算机处理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。

* 1. 数据传输

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：

1. 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；
2. 计算机处理系统相互之间的数据传输在应用层应以本文件8.4格式的数据包进行；
3. 数据包内最大原始交易记录的数量不应超过65535条记录；
4. 发送到总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。
   1. 数据组织结构
      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，编码规则应符合附录B要求。

* + 1. 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。

* + 1. 交易类型编码

主要交易类型包括开卡、发售、充值、消费、补票、锁卡、退卡、退资、激活等，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应符合附录C要求。

* + 1. 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：

1. 数据包结构包括包头及包体两部分；
2. 包头包括公共部分和个性类型；
3. 包体包括若干条数据记录。

数据包结构如图2所示：



1. 数据包结构图

联机交互报文格式要求如下：

1. 交互的消息报文由消息包头、消息包体、签名数据三部分组成；
2. 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；
3. 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：



1. 联机交互报文格式
   * 1. 数据包类型

总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。数据包类型应符合附录D要求。

* + 1. 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，具体数据项应符合附录E要求。

* + 1. 交易记录数据项

交易记录的数据项至少应符合附录F要求规定的数据项组成。

1. 业务规范
   1. 业务类型
      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。

* + 1. 发卡类应用

在具有发卡功能的终端上应能对一卡通卡进行发售。

在具有开卡功能的移动支付终端上应能对一卡通卡进行开卡。

* + 1. 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充值。

* + 1. 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。

* + 1. 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。

* + 1. 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。

* + 1. 其他类应用

针对特定一卡通卡应用实现特定功能，包含但不限于迁卡等。

* 1. 应用领域
     1. 交通领域
        1. 公共电汽车应用

通过车载、壁挂或手持式等读写终端，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。

* + - 1. 轨道交通应用

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

* + - 1. 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。

* + - 1. 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。

* + - 1. 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。

* + - 1. 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。

* + 1. 市政领域
       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。

* + - 1. 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。

* + - 1. 文化体育场馆应用

应能实现文化体育场馆付费的要求。

* + - 1. 公共电话亭

应能实现拨打公共电话付费的要求。

* + 1. 商业应用领域

应能通过市政交通一卡通系统专用终端及与系统兼容的终端，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。

* + 1. 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。

* 1. 交易模式
     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总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。

* + 1. 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、总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总中心计算机处理系统进行结算。

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：开卡、发售、充值、退卡、退资类交易，部分消费类交易等。

* 1. 应用方式
     1. 近场支付

近场支付应能支持脱机支付、联机支付。

* + 1. 远程支付

远程支付应为联机交易。

1. （规范性）  
   一卡通卡初始化流程

一卡通初始化流程见图A.1



* 1. 一卡通初始化流程图

1. （规范性）  
   卡号编码

卡号编码含义见表B.1、B.2。

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 |

表B.2卡号编码

|  |  |
| --- | --- |
| 数据项 | 说明 |
| 发卡机构识别码（IIN码） | 310517：北京市 |
| 扩展发卡机构识别码 | 有效范围：00-99 |
| 发行顺序号 | 有效范围：00000000000-99999999999 |

1. （规范性）  
   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 |

1. （规范性）  
   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 |
|  | 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 |
|  | 终端交易数据 | 消费终端原始消费数据，发售、充值、退卡、服务终端原始交易数据 |
|  | 统计对帐数据 | 发售、充值、消费、退卡、服务终端交易统计数据 |
|  | 测试数据 | 测试交易数据包数据、通信测试数据包数据 |
|  | 参数数据 | 运营参数、业务参数、黑名单参数、卡类型参数、优惠参数、白名单参数 |
|  | 其他数据 | 预留供系统扩展使用 |

1. （规范性）  
   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 |
|  | 包格式版本号 |  |
|  | 包编号 | 每个传输的数据包须有唯一代码 |
|  | 发送方代码 | 运营实体编码 |
|  | 接收方代码 | 运营实体编码 |
|  | 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 |
|  | 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 |
|  | 记录长度 | 如果包体不分记录，写包体长度 |
|  | 包中记录总数 | 记录总条数 |
|  | 数据包生成时间 | YYYYMMDDhhmmss（打包时间） |
|  | 包状态 | 表示不同数据包类型的个性化特征 |
|  | 其他 | 预留 |
|  | 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 |
|  | 记录1 |  |
|  | 记录2 |  |
| … | …… |  |
|  | 记录N |  |

1. （规范性）  
   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 |
|  | SAM卡号 | 存储在SAM卡中的编号 |
|  | 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 |
|  | 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 |
|  | 交易金额 | 交易金额，计次卡时为次数 |
|  | 卡内余额 | 交易后一卡通卡内余额，计次卡时为次数 |
|  | 交易日期 | 格式为“YYYYMMDD” |
|  | 交易时间 | 格式为“hhmmss” |
|  | 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 |
|  | 卡交易计数 | 一卡通卡中的累计交易计数 |
|  | 城市编码 | “城市编码”或“发卡机构识别码+扩展发卡机构识别码” |
|  | 发行顺序号 | 一卡通卡发行顺序号 |
|  | TAC | 由用户卡对相关数据项计算得出的交易验证码 |
|  | 交易前余额 | 一卡通卡交易前卡内余额，计次卡时为次数 |
|  | 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 |
|  | 卡物理类型 | 定义一卡通卡的物理特征，如智能卡等 |
|  | 互通卡类型 | 互联互通应用卡种类型 |
|  | 应收金额 |  |
|  | 交易状态 |  |
|  | 交易类型标识 | 交易类型标识，如：电子钱包脱机消费、电子钱包复合应用消费 |
|  | 发卡方机构代码 | 发卡方机构的编码，每个机构唯一 |
|  | 密钥版本 | 密钥版本号 |
|  | 密钥索引 |  |
|  | 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、受理方机构代码等 |
|  | 其他 | 预留 |