ICS 35.240.15

L 64

|  |
| --- |
| 备案号： |

DB11

北京市地方标准

DB11/T 159.3—20xx

|  |
| --- |
| 代替DB11/T 159.3—2015 |

市政交通一卡通技术规范

第3部分：终端

Municipal administration & communication card technology specifications—Part 3:Terminal

|  |
| --- |
|  |
|  |

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 IV](#_Toc118471025)

[1 范围 1](#_Toc118471026)

[2 规范性引用文件 1](#_Toc118471027)

[3 术语和定义 1](#_Toc118471028)

[4 缩略语 2](#_Toc118471035)

[5 终端分类 2](#_Toc118471036)

[6 终端要求 2](#_Toc118471037)

[6.1 识别要求 2](#_Toc118471038)

[6.1.1 非接触式卡兼容要求 2](#_Toc118471039)

[6.1.2 接触式卡兼容要求 2](#_Toc118471040)

[6.1.3 卡结构兼容要求 2](#_Toc118471041)

[6.1.4 扫码兼容要求 3](#_Toc118471042)

[6.1.5 识别兼容要求 3](#_Toc118471043)

[6.2 基本物理配置 3](#_Toc118471044)

[6.3 硬件要求 3](#_Toc118471045)

[6.3.1 基本硬件 3](#_Toc118471046)

[6.3.2 供电 4](#_Toc118471047)

[6.3.3 外观和结构 4](#_Toc118471048)

[6.3.3.1 外观 4](#_Toc118471049)

[6.3.3.2 结构 4](#_Toc118471050)

[6.3.4 环境适应性 4](#_Toc118471051)

[6.3.4.1 机械条件 4](#_Toc118471052)

[6.3.4.2 气候条件 5](#_Toc118471053)

[6.3.5 电磁兼容性 5](#_Toc118471054)

[6.3.5.1 无线电骚扰 5](#_Toc118471055)

[6.3.5.2 抗扰度 6](#_Toc118471056)

[6.3.6 安全 6](#_Toc118471057)

[6.3.7 可靠性 6](#_Toc118471058)

[6.4 软件要求 6](#_Toc118471059)

[6.4.1 系统软件 6](#_Toc118471060)

[6.4.2 二次开发平台 6](#_Toc118471061)

[6.4.3 安全加密 6](#_Toc118471062)

[6.5 管理功能要求 6](#_Toc118471063)

[6.5.1 功能概述 6](#_Toc118471064)

[6.5.2 系统管理 6](#_Toc118471065)

[6.5.2.1 自检 6](#_Toc118471066)

[6.5.2.2 程序管理 7](#_Toc118471067)

[6.5.2.3 参数管理 7](#_Toc118471068)

[6.5.2.4 终端状态管理 8](#_Toc118471069)

[6.5.3 操作人员管理 8](#_Toc118471070)

[6.5.3.1 系统管理员 8](#_Toc118471071)

[6.5.3.2 操作员管理 8](#_Toc118471072)

[6.5.4 应用管理 9](#_Toc118471073)

[6.5.4.1 签到管理 9](#_Toc118471074)

[6.5.4.2 签到交易 9](#_Toc118471075)

[6.5.4.3 批上送 9](#_Toc118471076)

[6.5.4.4 签退管理 9](#_Toc118471077)

[6.5.4.5 参数查询 9](#_Toc118471078)

[6.5.4.6 终端状态上送 10](#_Toc118471079)

[6.5.4.7 交易查阅功能 10](#_Toc118471080)

[6.5.4.8 重打印功能 10](#_Toc118471081)

[6.5.4.9 锁定功能 10](#_Toc118471082)

[6.5.5 安全管理 10](#_Toc118471083)

[6.5.5.1 操作员密码 10](#_Toc118471084)

[6.5.5.2 终端密钥管理 10](#_Toc118471085)

[6.6 业务功能要求 10](#_Toc118471086)

[6.6.1 人机界面 10](#_Toc118471087)

[6.6.2 联机业务终端 10](#_Toc118471088)

[6.6.2.1 基本要求 10](#_Toc118471089)

[6.6.2.2 一般要求 11](#_Toc118471090)

[6.6.2.3 安全要求 11](#_Toc118471091)

[6.6.2.4 核心处理流程 11](#_Toc118471092)

[6.6.3 脱机业务终端 11](#_Toc118471093)

[6.6.3.1 基本要求 11](#_Toc118471094)

[6.6.3.2 一般要求 11](#_Toc118471095)

[6.6.3.3 安全要求 11](#_Toc118471096)

[6.6.3.4 核心处理流程 12](#_Toc118471097)

[6.6.4 互联网终端 12](#_Toc118471098)

[6.6.4.1 基本要求 12](#_Toc118471099)

[6.6.4.2 功能要求 12](#_Toc118471100)

[6.6.4.3 安全要求 12](#_Toc118471101)

[6.6.4.4 核心处理流程 12](#_Toc118471102)

[6.7 数据要求 12](#_Toc118471103)

[6.7.1 安全要求 12](#_Toc118471104)

[6.7.1.1 应用程序下载要求 12](#_Toc118471105)

[6.7.1.2 数据存储要求 12](#_Toc118471106)

[6.7.1.3 安全数据要求 12](#_Toc118471107)

[6.7.2 数据元要求 13](#_Toc118471108)

[6.7.3 异常中断恢复机制 13](#_Toc118471109)

[6.7.3.1 异常中断 13](#_Toc118471110)

[6.7.3.2 终端处理要求 13](#_Toc118471111)

[6.7.4 交易数据存储 14](#_Toc118471112)

[6.8 接口 14](#_Toc118471113)

[6.8.1 通信接口方式 14](#_Toc118471114)

[6.8.2 界面接口要求 14](#_Toc118471115)

[6.8.3 与IC卡的非接触接口 14](#_Toc118471116)

[6.8.4 与SAM接口 14](#_Toc118471117)

[7 包装、运输、贮存要求 14](#_Toc118471118)

[7.1 包装 14](#_Toc118471119)

[7.2 运输 15](#_Toc118471120)

[7.3 贮存 15](#_Toc118471121)

[附录A（规范性）联机终端开机授权处理流程 16](#_Toc118471122)

[附录B（规范性）充值处理流程 17](#_Toc118471123)

[附录C（规范性）脱机消费处理流程 18](#_Toc118471124)

[附录D（规范性）B类终端业务处理流程 19](#_Toc118471125)

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3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 159.3—2015《市政交通一卡通技术标准第3部分：终端》，与DB11/T 159.3—2015相比，除结构调整和编辑性改动外，主要技术变化如下：：

1. 更改了了终端分类（见5，2015年版的3 ）；
2. 增加了接触式卡、扫码等兼容识别要求（见6.1）；
3. 增加了摄像头配置要求（见6.2）；
4. 删除了API模块硬件要求（见2015年版的4.3.1）；
5. 增加了摄像头指标要求（见6.3.1）；
6. 更改了数据存储指标（见6.3.1，2015年版的4.3.1）；
7. 增加了整机可靠性要求（见6.3.7）；
8. 增加了国产密码算法支持要求（见6.4.3）；
9. 增加了外接设备自检要求（见6.5.2.1）；
10. 增加了互通卡类型、扫码数据等交易数据元项（见6.7.2）；
11. 删除了终端侧典型交易时间、交通行业交易时间的内容（见2015年版的4.8.3）；
12. 删除了API模块接口（见2015年版的4.8.5）；
13. 删除了刷卡标识图案（见2015年版的附录A）。

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：北京市政交通一卡通有限公司、北京市智慧交通发展中心。

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：

——2005年首次发布DB11/T 159.2—2005《市政交通一卡通技术标准 第2部分：终端》;  
——2015年第一次修订时，将本文件改名为DB11/T 159.3—2015《市政交通一卡通技术规范 第3部分：终端》；  
——本次为第二次修订。

市政交通一卡通技术规范

第3部分：终端

1. 范围

本文件规定了市政交通一卡通系统终端的通用技术要求，包括终端分类、终端要求、包装、运输及贮存的要求。

本文件适用于市政交通一卡通系统终端的研制、生产、检验和验收。

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 191包装储运图示标志

GB/T 2423.10 环境试验 第2部分：试验方法 试验Fc：振动(正弦)

GB 4943.1 信息技术设备 安全 第1部分：通用要求

[GB/T 9254.2 信息技术设备、多媒体设备和接收机 电磁兼容 第2部分：抗扰度要求](https://std.samr.gov.cn/gb/search/gbDetailed?id=D4BEFFF4EA31B241E05397BE0A0AF581" \t "_blank)

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

GB 18030 信息技术 中文编码字符集

[JT/T 978.3 城市公共交通IC卡技术规范 第3部分:读写终端](https://std.samr.gov.cn/hb/search/stdHBDetailed?id=8B1827F250AEBB19E05397BE0A0AB44A" \t "_blank)

[JT/T 1179 交通一卡通二维码支付技术规范](https://std.samr.gov.cn/hb/search/stdHBDetailed?id=8B1827F24C40BB19E05397BE0A0AB44A" \t "_blank)

DB11/T 159.2 市政交通一卡通技术规范 第2部分：卡片

ISO/IEC 14443 个人识别卡和安全装置—非接触邻近物体—物理特性

1. 术语和定义

DB11/T 159.1界定的以及下列术语和定义适用于本文件。



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。



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。



A类终端 type A terminal

安装市政交通一卡通系统SAM卡，具有一卡通卡读写功能的设备。



B类终端 type B terminal

无须安装市政交通一卡通系统SAM卡，通过远程控制实现一卡通卡读写功能的装置。



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。



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。

1. 缩略语

DB11/T 159.1界定的以及下列缩略语适用于本文件。

MTBF：平均无故障工作时间（Mean Time Between Failure）

1. 终端分类

市政交通一卡通系统终端分为A类终端和B类终端。

A类终端应满足以下认证：

1. 强制性产品认证（简称3C认证）；
2. 电信进网许可证；
3. 无委认证（简称SRRC，无线电发射设备型号核准认证）。
4. 终端要求
   1. 识别要求
      1. 非接触式卡兼容要求

终端应具有良好的读写卡兼容性，能够正确识别和处理符合DB11/T 159.2标准的卡片。

非接触式卡片识别应优先选择交通应用。

* + 1. 接触式卡兼容要求

终端的SAM卡读写功能，应满足GB/T16649要求，包括机械、电气和逻辑协议等。

* + 1. 卡结构兼容要求

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。

* + 1. 扫码兼容要求

能够支持识别常用码制，并支持识别旋转、倾斜、偏转的二维码。

* + 1. 识别兼容要求

根据业务应用场景需要，交通行业应用终端应按照非接触式卡识别、扫码识别、其他类型识别的顺序执行识别兼容，并通过接口把数据提交给业务系统开展应用。

* 1. 基本物理配置

终端应至少配置显示屏、数据通信接口、非易失性存储器、电源、实时时钟、SAM、无线通讯模块、摄像头、蜂鸣器。根据应用需要，终端可配置键盘、打印机、语音模块等组件。

终端部件配置要求见表1。

1. 终端部件配置要求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 部件 | 型式 | | | |
| 手持式 | 桌面式 | 车载式 | 固定式 |
| 显示屏 | 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 |
| 支持SAM | M | M | M | M |
| 无线通讯模块 | O | O | M | O |
| 摄像头 | M | M | M | O |
| 蜂鸣器 | M | M | M | M |
| 键盘 | M | M | O | M |
| 打印机 | O | M | O | M |
| 语音模块 | O | O | O | O |
| **注**：M-必备，O-可选。 | | | | |

* 1. 硬件要求
     1. 基本硬件

基本硬件要求见表2。

1. 终端的硬件要求

| 项 目 | 要 求 |
| --- | --- |
| 硬件要求 | 符合JT/T 978.3的要求 |
| 显示屏 | 应显示ASCII可视字符。汉字显示应符合国家标准GB/T 18030汉字 |
| 摄像头 | 扫码识别摄像头应符合JT/T 1179—2018标准  人脸特征采集摄像头（可选）应采用3D结构光摄像头或者像素数不低于200万的专用宽动态摄像头。 |
| 键盘 | 必须有10个数字键，若干功能键，必须能够输入字母。 |
| SAM | 选用安装SAM的终端，则需配置符合ISO/IEC 14443标准的读写器SAM接口符合JT/T 978.3的要求，同时支持不少于4个SAM卡，其中不少于2个须使用卡座支持。 |
| 读写距离 | (0~60)mm以内有效、无盲区 |
| 数据存储 | 交易数据存储容量 ≥8Mbyte |
| 黑名单容量 ≥5Mbyte |
| 运营参数存储容量 ≥1Mbyte |
| 存储器寿命 ≥10年 |
| 实时时钟 | 支持时钟同步,误差±2秒钟/日 |
| 通信方式 | 通信端口应支持串口通信、4G及以上标准网络通信、无线通信；  还可选择支持以下类型的通信方式：蓝牙通信；红外通信；其他 |
| 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ASCⅡ字符或汉字 |
| 蜂鸣器 | 声音提示，可用于交易成功或失败提示 |
| 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±5%或24V±5%（车载机） |
| 电池 | 移动终端要求出厂电池具有24小时待机能力，具备二次充电能力；  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 |

* + 1. 供电

由直流电源供电，当电压在标称值±5%范围内时，终端应正常工作。

由交流变换器供电，交流电压在标称值15%范围内时，终端应正常工作。

终端应有断电、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。

终端瞬间断电的情况下，应有延时保护功能，保证数据存储不丢失。

* + 1. 外观和结构
       1. 外观

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。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。

* + - 1. 结构

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并采用防止误触摸设计。电路板的布线要合理，不能有临时接线。

* + 1. 环境适应性
       1. 机械条件

应满足如下要求：

（a）机械条件的振动适应性见表3。

1. 振动适应性

|  |  |  |
| --- | --- | --- |
| 项 目 | | 参 数 |
| 初始和最后振动响应检查 | 频率范围 | (10-55)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(10Hz-25Hz)  0.15mm(25Hz-55Hz) |
| 持续时间 | 20±1 min |
| 扫频耐久实验 | 频率范围 | (10-55-10) 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 | | |

（b）机械条件的冲击适应性见表4。

1. 冲击适应性

|  |  |
| --- | --- |
| 项 目 | 参 数 |
| 峰值加速度 | 300 m/s² |
| 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. 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。

1. 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%  （非凝露） | 10%～98%  （非凝露） |
| 室外 | -20℃～70℃ | -40℃～70℃ | 10%～90%  （非凝露） | 10%～98%  （非凝露） |

* + 1. 电磁兼容性
       1. 无线电骚扰

应符合GB 9254中A级的要求。

* + - 1. 抗扰度

应符合GB/T 17618中的相关要求。

* + 1. 安全

应符合GB 4943.1中的相关要求。

* + 1. 可靠性

应满足以下要求：

1. 整机平均无故障工作时间（MTBF）的m1值（不可接近值）应不低于10000小时（卡座、键盘除外）；
2. 整机使用寿命应不低于5年；
3. 接触式卡座使用寿命应不低于100000次；
4. 键盘使用寿命应不低于500000次。
   1. 软件要求
      1. 系统软件

应具有系统初始化功能，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。

* + 1. 二次开发平台

可提供高级语言（如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。

* + 1. 安全加密

应能根据软件加密要求，获取安全、可靠的加密方法，支持国际密码算法、国产密码算法，保证终端交易数据的存储机密性、完整性。

* 1. 管理功能要求
     1. 功能概述

管理功能包括系统管理、操作人员管理、应用管理、安全管理。终端应具有系统管理功能，宜具有操作人员管理、应用管理、安全管理功能。

* + 1. 系统管理
       1. 自检

终端开机后，应先进行自检，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。自检发现异常应报警。

自检项目见表6。

1. 开机自检项目

| 序号 | 项目名称 |
| --- | --- |
| 01 | 打印机测试 |
| 02 | 通信端口测试 |
| 03 | 读卡器测试 |
| 04 | 键盘测试 |
| 05 | 显示屏测试 |
| 06 | 外接设备测试 |

* + - 1. 程序管理

程序管理应对终端使用的应用程序进行管理。

终端应支持串行口下载、USB下载、远程在线下载等应用程序下载方式。

* + - 1. 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，具体要求如下：

1. 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，具体要求见表7；
2. 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 |
| 通信端口类型 | 识别可用的通信端口种类 | 出厂 | 操作系统、应用软件使用 |
| 通信端口参数 | 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 |
| 通讯类型 | 识别可用的通讯种类 | 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 |

1. 业务参数：主要是用于设备自身管理和配置的参数，根据设备具体功能的差异对应实际的参数，具体要求见表8；
2. 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 | 通信响应超时时间 | 安装或调整时 | 交易应用 |
| 重试次数 | 通信失败重试次数 | 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卡指定交易需要识别和认证的卡类 | 安装或调整时 | 交易应用 |
| 运营参数 | 标识使用设备IC卡指定交易需要遵照执行的业务指标 | 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 |
| 白名单列表 | 标识使用设备IC卡允许交易的机构或卡表 | 安装或调整时 | 交易应用 |

1. 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：
2. 重要编号：通信流水号、交易顺序号；
3. 最大日志笔数：允许当批交易保存的最大交易笔数；
4. 操作员管理表：操作员号、操作员密码、操作员属性；
5. 日期与时间表：实时时钟的日期和时间，在每次签到交易或信息采集成功后调整；
6. 交易类型：设定终端支持的交易，不支持的交易被屏蔽掉；
7. 打印设置： 支持打印的设备，可设置是否打印、打印联数
8. 时间间隔点：终端状态上传的时间间隔。
9. 联机可更改参数：包括业务参数，通信参数，终端应用类型，商户号，单位代码，消费额度，终端支持的交易类型（不支持的交易被屏蔽掉）等。
   * + 1. 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。具体要求如下：

1. 工作状态：终端自检并获取业务授权后终端所处的状态。此时终端可以实现规定的交易功能；
2. 已签退状态：终端业务授权失效之后的状态。此时终端不允许实现除获取授权以外的任何交易功能；
3. 锁定状态：操作员可以将终端设为锁定状态。此时终端应不接受任何操作，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。
   * 1. 操作人员管理
        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应通过安全认证。

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。

系统管理员不能做终端授权和进行交易。

* + - 1. 操作员管理

终端具有操作员管理功能，可以设置并修改操作员密码。

操作员使用操作员代码和密码，或认证卡等方式进行身份认证。终端应至少能够存储和管理10个操作员的有关数据。

终端操作应由指定的操作员进行。

终端操作员可分主管操作员和一般操作员：

1. 主管操作员的职责是管理终端和一般操作员，及设置一般操作员权限，本身不能做终端授权和进行交易。
2. 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。
   * 1. 应用管理
        1. 签到管理

签到管理分为操作员签到和终端签到两种。

1. 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；
2. 终端签到：终端签到应采用联机方式。终端向一卡通总中心计算机处理系统上送终端号、商户号、操作员代码，一卡通总中心计算机处理系统验证商户和终端信息有效性，产生终端工作密钥、提取交易批次号、主机交易日期和时间，将这些数据及参数下传到终端。终端只有签到成功后才可以进行交易。终端可根据签到应答消息中一卡通总中心计算机处理系统的时间设置终端的时间。
   * + 1. 签到交易

终端在使用过程中断电，重新开机后操作员应重新签到。签到交易有以下四个作用：

1. 终端与一卡通总中心计算机处理系统的批次号同步。批次号应以一卡通总中心计算机处理系统的批次号为准；
2. 终端从一卡通总中心计算机处理系统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，则应重新发送签到消息，以与一卡通总中心计算机处理系统进行密钥同步；或由一卡通总中心计算机处理系统在应答消息中提示终端重新签到；
3. 终端应从一卡通总中心计算机处理系统获取主机的日期和时间；
4. 终端上送通信流水号、交易顺序号，和主机进行比对，从一卡通总中心计算机处理系统获取最新的流水号或判定数据是否丢失。
   * + 1. 批上送

终端在进行联机交易时，通过联机报文将各类交易信息发送给清算中心。交易完成后，交易记录应在终端本地进行备份存储。终端应将这些交易记录、及汇总信息（成功、失败））批量上传到清算中心。

查询类交易、管理类交易及其他不成功的联机类交易不做批上送。

* + - 1. 签退管理

操作员可选择“签退”功能执行签退。在签退之前，应进行批上送交易。

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

终端在开机签到时，如果一卡通总中心计算机处理系统反馈终端已签到，应在签退提示后向一卡通总中心计算机处理系统发送签退通知，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，方可处理其他交易。

* + - 1. 参数查询

在终端签到之后的每次联机时，应根据业务需要，由一卡通总中心计算机处理系统引发向终端下载参数的操作。终端收到一卡通总中心计算机处理系统的参数传递要求后，应立刻向一卡通总中心计算机处理系统发送参数查询请求报文，并接收应答。根据查询信息，决定下载参数种类。

* + - 1. 终端状态上送

终端应根据设定的时间段，将终端的各部件的运行状况及其他信息上送给一卡通总中心计算机处理系统，以便于一卡通总中心计算机处理系统对终端的运行状况进行远程监控。

须上送内容包括： SAM状态，位置信息等。

可支持上送内容包括：硬件状态，键盘状态，打印机状态，显示器状态等。

* + - 1. 交易查阅功能

终端可支持查阅存储的签到以来的交易情况和统计情况。具体要求如下：

1. 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；
2. 根据卡号查询交易记录：根据卡号，查询签到以来的本卡号所作的交易明细；
3. 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。
   * + 1. 重打印功能

具体要求如下：

1. 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。重打印的签购单上应有补打标志字样；
2. 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。重打印的签购单上应有补打标志字样；
3. 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。重打印的结算单上应有补打标志字样。
   * + 1. 锁定功能

终端需要暂停工作时，用此项功能暂时锁定终端，恢复操作时应重新输入操作员密码。

* + 1. 安全管理
       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应有独立的密码和唯一代码。

* + - 1. 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。断电后应自动清除密钥。

* 1. 业务功能要求
     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一卡通总中心计算机处理系统下载菜单页面显示。

* + 1. 联机业务终端
       1. 基本要求

联机业务终端应在获取一卡通前置业务授权后，允许开通售卡、充值、退卡、退资、消费等业务。

* + - 1. 一般要求

联机业务终端一般要求如下：

1. 应采用联机业务模式，并采用授权模式；
2. 应具备自检、参数管理、参数下载等功能；
3. 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；
4. 可根据业务参数，进行终端本地信息判断；
5. 应支持通过外部接口实现应用软件的升级；
6. 应能存储刷卡交易数据；
7. 应能将存储的交易数据输出到外部设备或系统；
8. 对一卡通卡操作的交易顺序号应累计不清零；
9. 应具有打印接口，打印机安装和票据打印应符合市政交通一卡通要求。
   * + 1. 安全要求

联机业务终端安全要求如下：

1. 应取得一卡通总中心计算机处理系统的授权，才能进行联机业务交易；
2. 应具有密文加校验传送的功能；
3. 生成的交易记录应含有TAC；
4. 应具有掉电工作权限丧失功能；
5. 应具有时效性设置功能。
   * + 1. 核心处理流程

联机业务终端的核心处理流程包括开机授权流程（应符合附录A要求）和典型充值业务流程（应符合附录B要求，其他联机业务类同）。

* + 1. 脱机业务终端
       1. 基本要求

终端应配置SAM，完成对一卡通卡脱机类扣款、查询等操作。

* + - 1. 一般要求

脱机业务终端一般要求如下：

1. 应具备自检、参数管理、参数下载等功能；
2. 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；
3. 可根据业务参数，进行终端本地信息判断；
4. 应能支持应用软件升级；
5. 应能存储刷卡交易数据，并能输出到外部设备。
   * + 1. 安全要求

脱机业务终端安全要求如下：

1. 应使用市政交通一卡通系统专用的SAM；
2. 生成的交易记录应有TAC。
   * + 1. 核心处理流程

为了保证在市政交通一卡通系统内智能IC卡的通用性和各类终端处理的一致性，收费类终端在消费交易处理时应遵照业务流程规定执行（应符合附录C要求）。

* + 1. 互联网终端
       1. 基本要求

指B类终端，可联网完成对一卡通业务操作的功能。

* + - 1. 功能要求

互联网终端一般要求如下：

1. 具有RF控制模块，应符合ISO/IEC14443标准，支持TYPE A协议的智能卡；
2. 应具备PKI安全体系；
3. 应支持证书及非对称加密算法；
4. 存放定制的内置安全程序负责卡片指令的解析；
5. 应具有对后台下发的不同指令集自动处理并反馈的能力；
6. 应能支持应用软件在线远程升级。
7. 应支持实时交易消息通知功能。
   * + 1. 安全要求

互联网终端安全要求如下：

1. 应具备存放证书和公私钥的安全芯片，芯片中存储密钥不可泄露；
2. 应调用的WEB安全控件具有签名功能。
3. 应确保数据存储的机密性、完整性；数据传输的机密性、完整性
   * + 1. 核心处理流程

为了保证在市政交通一卡通系统内智能卡、扫码的通用性和终端处理的一致性，互联网终端在交易业务处理时应遵照业务流程规定执行（应符合附录D要求）。

* 1. 数据要求
     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。

* + - 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。

* + - 1. 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机密性、完整性。终端具备延时断电功能，保证在突发断电时，交易数据可正常完成生成保存。

* + - 1. 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。A类终端均应按照本要求执行。

* + 1. 数据元要求

终端中应存储表9中的数据元项。

1. 数据元

|  |  |  |
| --- | --- | --- |
| 序号 | 数据元项 | 说明 |
|  | SAM卡号 | 存储在SAM卡中的终端机编号 |
|  | 交易日期 | 格式为“YYYYMMDD” |
|  | 交易时间 | 格式为“hhmmss” |
|  | 城市编码 | 一卡通卡城市代码 |
|  | 发行顺序号 | 一卡通卡发行顺序号 |
|  | 互通卡类型 | 互联互通应用的卡种类型 |
|  | 本地卡类型 | 本地自定义的卡类型，如非记名成人卡、学生卡等 |
|  | 卡物理类型 | 定义卡片的物理特征，如智能IC卡等 |
|  | 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 |
|  | 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，计次卡为交易次数 |
|  | 卡内余额 | 交易后一卡通卡内余额，计次卡为剩余次数 |
|  | 卡序列号 | 一卡通卡内部序列号CSN |
|  | 卡交易计数 | 一卡通卡中的累计交易计数 |
|  | TAC | 由一卡通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，计次卡为交易前次数 |
|  | 交易状态 | 交易的业务状态 |
|  | 应收金额 | 交易应该收取的金额（优惠前金额） |
|  | 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 |
|  | 扫码数据 |  |

* + 1. 异常中断恢复机制
       1. 异常中断

终端在读写一卡通卡时，异常中断分为以下两种情况：

1. 一卡通卡离开感应区；
2. 终端停止操作。
   * + 1. 终端处理要求

出现异常中断情况，终端处理要求如下：

1. 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；
2. 终端瞬间断电恢复正常工作后，应从断点开始继续处理；
3. 在以下情况下，终端可退出异常中断恢复处理状态：
4. 有一卡通卡进入感应区时；
5. 超时；
6. 人工干预。
   * 1. 交易数据存储

终端应具备至少保存10天交易记录的容量。交易记录存储接近最大容量时，终端应及时提示。

终端应具备本地存储数据的补采集功能，可根据需求进行本地采集或数据自动上传处理。

* 1. 接口
     1. 通信接口方式

通信端口应支持串口通信、网络(4G及以上)通信/无线通信，还可选择支持以下类型的通信方式：蓝牙通信；红外通信；其他。

对一卡通总中心计算机处理系统多个通信地址，具备自动切换功能。

* + 1. 界面接口要求

界面接口应满足以下基本要求：

1. 时钟：误差±2秒钟；
2. 显示：显示器字符应清晰完整，易于辨认；
3. 声音：应具备声音提示功能，音量可调。
   * 1. 与IC卡的非接触接口

终端均按照本要求执行。

1. 应符合ISO/IEC14443；
2. 频率：13.56 MHz±7kHz；
3. 在读写有效区域内的最小场强：1.5A/m rms；
4. 在读写有效区域内的最大场强：7.5A/m rms；
5. 通信波特率：(106～424)kbps；
6. 调制方式：ASK 100%（TYPE A）；
7. 通信距离：
8. 天线读写距离(0～60)mm；
9. 短距终端：(0～30)mm能正常刷卡；
10. 长距终端：(0～60)mm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；

注2：通信距离(0～30)mm和(0～60)mm是指终端感应区机壳到一卡通卡之间的垂直距离。

* + 1. 与SAM接口

A类终端应按照本要求执行。

1. 通信接口应符合GB/T 16649.3的相关要求；
2. 物理接口应符合GSM11.11规范；
3. 应能兼容5V和/或3V直流电源的SAM；
4. 数据通信速率：支持(9600～223200) bit/s，支持PPS自适应，通信速率自动识别；
5. 当任意两个触点之间短路时，终端不应损坏。
6. 包装、运输、贮存要求
   1. 包装

终端包装应符合GB/T 191中的相关要求，并应符合GB/T 13384中防潮、防霉的规定。

在包装箱上应标志以下内容:

1. 终端名称、型号；
2. 制造厂厂名、厂址；
3. 标准号；
4. 外形尺寸及毛重；
5. “小心轻放”、“防潮”等字样及相应图案；
6. 收货单位及地址；
7. 生产许可证编号；
8. 数量、重量及体积；
9. 装箱日期（年、月）。

包装箱内应包括下列文件:

1. 装箱单；
2. 说明书；
3. 合格证；
4. 随机所带附件。
   1. 运输

运输中应防止受到强烈冲击、雨淋及曝晒。

* 1. 贮存

应在制造厂原包装条件下在室内保存（可堆放），环境温度为-20℃～40℃，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能使用。

1. （规范性）  
   联机终端开机授权处理流程

联机终端开机授权处理流程图，见图A.1。



图A.1 联机终端开机授权处理流程图

1. （规范性）  
   充值处理流程

充值处理流程见图B.1。



图B.1 充值处理流程图

1. （规范性）  
   脱机消费处理流程

脱机消费处理流程见图C.1。



图C.1 脱机消费处理流程图

1. （规范性）  
   B类终端业务处理流程

B类终端业务处理流程见图D.1。



图D.1 B类终端业务处理流程图