城市公交一卡通系统
解决方案

成都易科士信息产业有限公司

2012 年 08 月

目　录

引言

交通状况是一个国家和城市发达程度的重要标志，城市交通运输成为人们越来越关注的热点问题。公共交通是一个大型的服务性行业，涉及公交（大巴/中巴/小巴）、出租小汽车、地铁、轻轨、轮渡等，它担负着市民日常出行的任务，与城市广大市民的生活息息相关，而以电子支付和身份标识为主要应用目标的智能卡在各领域得到了相当规模的应用，尤其在城市内公共交通费用支付方面得到了相当规模的应用，成为推动中国城市公共交通收费、管理和城市基础设施服务事业发展的重要高技术手段。

目前我国城市公交系统的发展尚存在着不少问题。由于公共交通运营公司隶属不同部门，各自建设自己的公交系统，制定自己的收费标准、收费方式和管理体制，独立发行仅限于本运营公司范围内使用的 IC 卡，市民外出必须携带各式各样的票卡，极不方便；没有遵循统一的技术标准，根据本身局部需求编制的收费和管理软件，采用的硬件设备、组网模式、通信方式、操作系统、接口协议以及网管软件五花八门。不断出现的重复投资、重复建设的局面，了造成公共交通建设投资的惊人浪费，因此迫切需要一个城市级别公交一卡通系统来将城市的公交，地铁，出租，城市购物等以电子货币的交易形式的各种应用统一，规范起来。迄今为止，国内大型城市如上海、北京、广州、深圳、大连、武汉、南京、天津、沈阳等地均实施或正在实施城市公共交通一卡通系统，当然还有相当一批中小型城市正准备实施或已经实施城市一卡通系统；其中上海市城市一卡通系统以近 300 万张发卡使用量，全面覆盖城市的公交、地铁、出租和轮渡应用，具有典型的现实指导意义。

一、需求分析

1.1 建设的必要性

城市公交的“无人售票”经过多年的运作，在管理上已经日趋完善，但随之而来的问题又出现了，零钱不够，这是实行无人售票以来乘客和公交公司之间最大的矛盾，无人售票对车辆的承运速度和业务管理无疑是起到很大的促进作用，但是由于无人售票那就无法找补零钱，对身上没有足够零钱的乘客来讲就是个问题了，换零钱？哪儿换？不仅浪费了时间还可能换不到零钱。无人售票需要完善，随着经济环境的变化，IC 卡运用于城市公交为实现城市公交自动化收费提供了现代技术的支持。

1.2 香港“八达通”系统

香港八达通系统成为城市公共交通一卡通系统中最成功的应用和运营管理系统实例，目前系统发卡量在 800 万张，日交易金额超过 4000 万港币，广发应用与公交车支付、轨道交通、轮渡和小额消费，借助良好的运营管理机制，八达通卡已成为香港市民出行交通的主要支付手段，同时由于充值卡的大面积使用（在公共交通已占 70%以上），因此大大减少了纸质票的使用量，从而极大节约系统运营和管理费用。八达通卡为香港市民提供了越来越多的方便，其应用范围和发卡量必将不断扩展和增加。

1.3 系统效益分析

1.3.1 经济效益

- 实时掌握客流情况，科学合理调度车辆，避免不合理而浪费；
- 预收票款，增加企业的周转资金；
- 减少售票和点钞人员，节约人工费用；

- 加快乘客上车速度，减少车辆在站台的停车时间，加速车辆运行周期，减少线路的车辆数量；
- 广告效益，可以在卡面印刷不同企业的广告，收取广告费用；
- 收费及统计自动化管理，有效堵塞漏洞，杜绝可能发生的管理人员贪污及假票现象。

1.3.2 社会效益

- 提高公共交通的服务档次，符合建设国际城市的目标；
- 方便市民，减少社会现金流通量。因为现在市面缺少零钱，乘车购物很不方便，使用 IC 卡后，可以乘坐所有公共交通和一些小额消费，包括公交、大巴、中巴、小巴、出租车、地铁、轮渡、轻轨、商场购物、商店购物、加油等等；
- 提高车辆运行效率，节省乘车时间；
- 一卡在手，走遍全市，不用带那么多零钱、银行卡等。

1.4 建设目标

公交一卡通系统是以提高城市交通运转效率、方便市民、降低运营公司成本为目的而规划建设的系统，它以非接触智能（Contactless Smart Card，简称 CSC）为车票载体，以计算机及各种电子收费终端（地铁、公共汽车、出租车等运输工具上的自动收费终端）为核心，以局域网和远程网络作为支撑，实现集中发卡管理和密钥管理，实现计费、收费、统计、汇总、预测、决策、分析以及中央清算等业务，实现乘客持一张 CSC 乘坐各种交通工具、小额消费、车辆停车、过路桥自动收费等全过程的电子化、自动化、网络化综合管理，而本公交一卡通系统是为了实现城市级一卡通用的消费系统的一部分，本期主要实现公交发卡，充值，刷卡消费，公交线路，车辆管理等基础性功能，并实现自动清分结算及银行结转功能。

二、运营模式

2.1 业务实体

2.1.1 城市公交一卡通平台

城市公交一卡通平台负责整个系统的管理、运作，主要包括平台的数据中心维护、基础配置的设置、各大运营商管理、终端管理、管理员权限分配等一系列应用之前的基础管理工作，可以由第三方企业负责管理，也可直接由公交公司管理。平台包括以下几个子系统：

- 权限管理子系统：负责设置平台、应用、运营商等操作员角色、权限分配；
- 基础管理子系统：负责运营商、终端、公告以及其他一些基础的配置；
- 卡务管理子系统：负责系统卡片类型、卡片基本信息、应用、PSAM 卡、用户以及用户的开卡、挂失、解挂、退卡、退款、换卡、补卡、充值等一系列的操作与管理；
- 密钥管理子系统：负责系统 PSAM 卡、管理卡、用户卡的初始化、加密工作；
- 报表管理子系统：可查询相关个人报表、清分结算报表、出纳报表、营业报表。

2.1.2 结算银行

结算银行是“城市公交一卡通”系统中最重要的服务提供商，“城市公交一卡通”系统充分利用结算银行现有的营业网点和系统网络资源，为广大持卡用户和运营商提供方便周到的服务，包括：

- 结算，资金的划拨；
- 代理发卡；
- 代理充值；
- 代理挂失、解挂和销卡；

◆ 代理数据采集、下载黑名单以及其它运营参数。

2.1.3 结算中心

结算管理中心同平台在一起，由同一个公司负责管理，它是整个“城市公交一卡通”系统的核心，对整个系统实施管理监控，并负责采集、管理所有运营商的消费交易数据和充值、挂失等服务数据，通过与运营商、结算银行的接口完成结算。同时，结算管理中心还负责卡片的发行管理，运营商终端设备的发行管理以及运营参数的管理。

2.1.4 运营商

加入城市公交一卡通系统的个人或者单位，是直接与结算中心进行结算的独立核算单位，它包括公交公司以及下属的子公司、出租车公司、地铁公司、轮渡公司、路桥公司、石油公司等。

2.1.5 发卡、充值点

出售用户卡片，为用户卡片充值，同时提供挂失、解挂、销卡等服务。

2.1.6 数据采集点

采集 POS 终端上的消费交易记录，上传至结算中心；从系统平台下载黑名单和运营参数至 POS 终端。

2.1.7 POS 终端用户

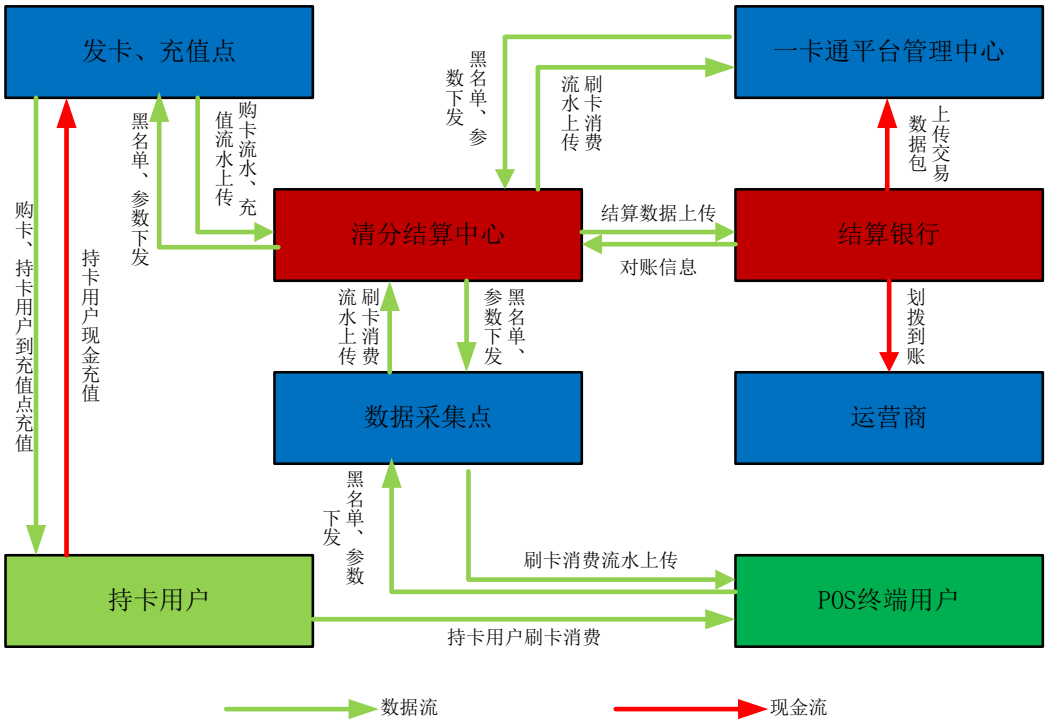
POS 终端用户，指能提供城市公交一卡通消费服务的业主。可能是独立的结算个体，如出租司机，也可能是隶属于某个运营商的经营个体，如大巴司机等。

2.1.8 持卡用户

是城市公交一卡通系统的服务对象和实际的消费者。在系统中，以卡 ID 作为其唯一标识。可分为记名卡、不记名卡。

2.2 业务流程

城市公交一卡通系统运营的业务流程如下图所示：



城市公交一卡通业务流程图

说明：

POS 终端用户，每天要将 POS 终端内的交易数据及时通过数据采集点上传至结算中心，系统通过数据采集点同时下载黑名单和运营参数；

清分结算中心对交易数据进行清算，向结算银行发出资金划拨指令，结算银行按指令向运营商结算帐户划拨资金；

各发卡充值点的发卡、充值记录上传至清分结算中心，清分结算中心与结算银行对帐，结算银行将相应收入划拨到清分结算中心结算帐户上；

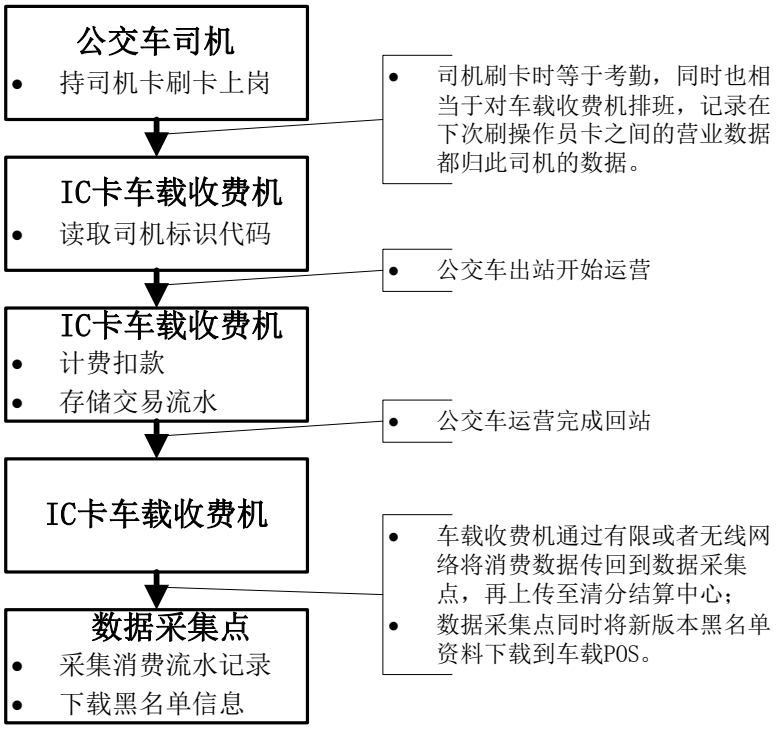
清分结算中心一切发卡、充值、交易等流水、统计报表均通过管理平台中的报表子系统体现账目。

2.3 公交运营模式

2.3.1. 现状分析

目前大多数公交都由公交公司统一管理，大部分由公交公司运营，有少部分承包给私人运营。同一个地区由于收费标准也存在差别，有统一票价、月票、分段计费等收费标准，

2.3.1. 运营流程



2.3.1.3 计费方式

公交车的计费方式主要有以下几种方式：

◆ **免费乘车**

针对公交集团或公司的职工可以免费乘坐所有公交车；上了一定年龄的老年人可以办理老年卡，乘车免费。

◆ **次数**

在充值的时候可以选择充值次数，充的次数在规定的时间内才能使用，超过时间则自动清除，使用次数刷卡可以设置优惠折扣，在充值的时候体现，比如设置的上交 10 块则充 20 次，可以根据不同卡类型设置不同的优惠比例。可设置刷卡次数限制。

- **单一票价**

车载消费机设置一个定值消费金额，每刷一次则扣除所设置的金额，可连续刷卡或者设置刷卡限制次数和两次刷卡的间隔时间。

- **分段计费**

改造现有语音报站设备，在语音报站的同时，向车载收费机内输入车站标识。乘客上车刷卡，IC 卡车载收费机在用户卡内特定区域记录上车站标识，乘客下车刷卡 ，IC 卡车载收费机从用户卡中读出上车站标识，再根据下车站标识以及运营参数计算出车费，扣费。

- **优惠规则**

可以设置一定的优惠规则，比如规定在一定时间段内同一张卡在不同的车载消费机上刷卡可以不再计费（次数）或者打折计费（金额），以提高市民对公交车的乘坐比例。

2.3.1.4 数据采集方式

车载消费机可以采用多种通讯方式：RS232 串口通讯、CAN 总线通讯、以太网通讯、GPRS/CDMA/3G、WIFI/ZIGBEE 等方式。

RS232 串口通讯

在数据采集点 PC 上连接 RS232 线，每个端口每次只能连接一台终端上传消费数据或者下载黑名单及参数。

CAN 总线通讯

在数据采集点 PC 连接一个 CAN 总线转换器，连接一根总线，此总线上连接 N 跟数据线，同时可以多台终端上传消费数据或者下载黑名单和参数。

以太网通讯

在数据采集点 PC 所在局域网中增加交换机，预留 N 根 RJ45 网线，每根网线可以连接一台终端上传消费数据或下载黑名单和参数。

GPRS/CDMA/3G

利用中国移动、中国电信或者中国联通现有的无线网络，实时传输终端的消费数据或者下载黑名单和参数，当然也可以设置为定时上传和下载。

WIFI/ZIGBEE

采用 WIFI/ZIGBEE 通讯方式，则需要在每辆公交车上安装无线移动站，无线移动站再通过 RS232 与车载终端连接，在公交总站建设无线基站，在公交车返回公交站的时，公交车离基站 1000 米范围内即可自动或者手动与系统联机，上传消费数据或下载黑名单和参数，这个过程在短时间内可以完成，无需人员参与。

三、总体设计方案

3.1 系统概述

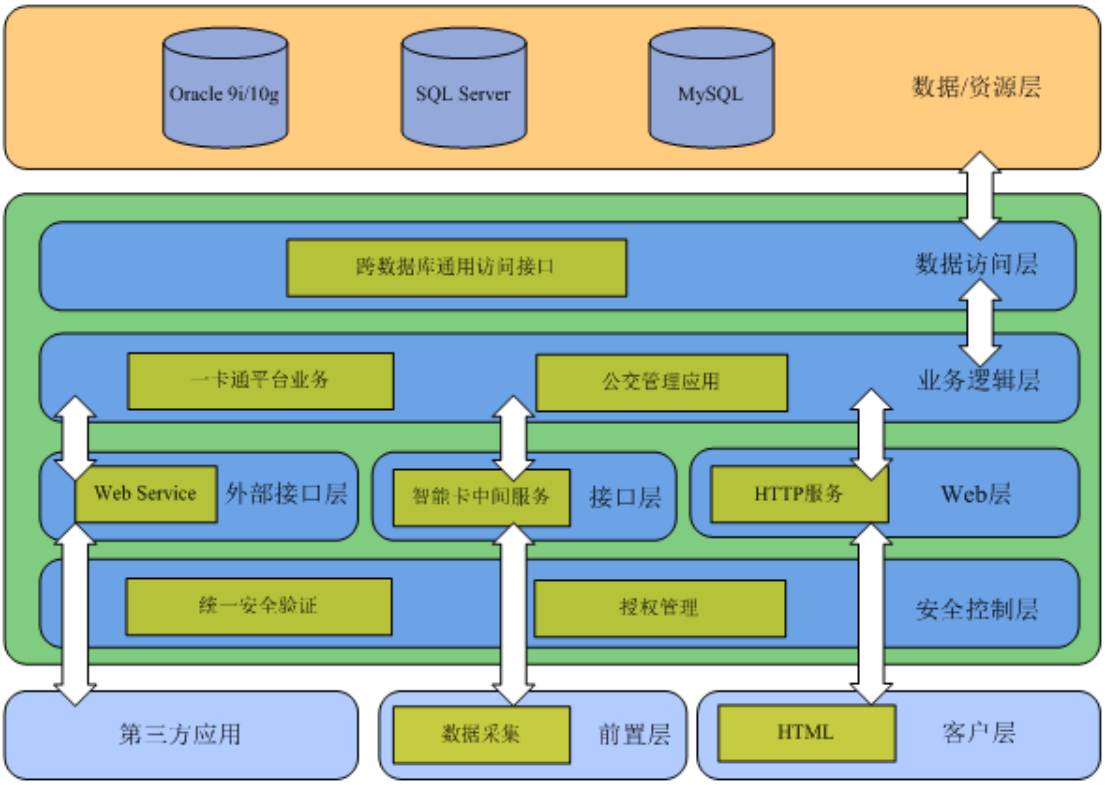
城市公交一卡通系统管理平台分为城市一卡通管理中心平台和公交应用管理平台两部分，包括权限管理，系统管理、公交管理、清分结算管理、卡务管理、银行结转及自助查询等模块应用。**统一的登录入口，自动识别操作员身份、权限。**

一卡通管理中心平台是一卡通系统建设的核心平台，它包含对一卡通中心主机系统的管理和维护，数据交换、交易及同步，用户及设备的管理、系统参数的和环境的设定，系统各模块的工作状态监控和工作模式的设定，密钥管理等功能。

基于“公交一卡通系统”骨干平台，建立商务管理、银行转账、身份识别管理、金融消费管理等各子系统，定义统一的接口标准和接入规范，随公交公司规模的扩大、卡片功能的增加可随时增加子系统应用，为公交公司以后的发展提供良好的数据接口，便于以后公交卡的功能向城市一卡通“市民卡”的扩展应用。持卡人的基本信息资料和电子钱包都作为统一的公用数据在全网上实时共享，经过中央集控中心的统一授权和管理，由数据交换中心、数据共享中心的统一发布，所有数据的变更都做到全网立即生效，做到整体系统数据的同步。

3.2 系统业务架构

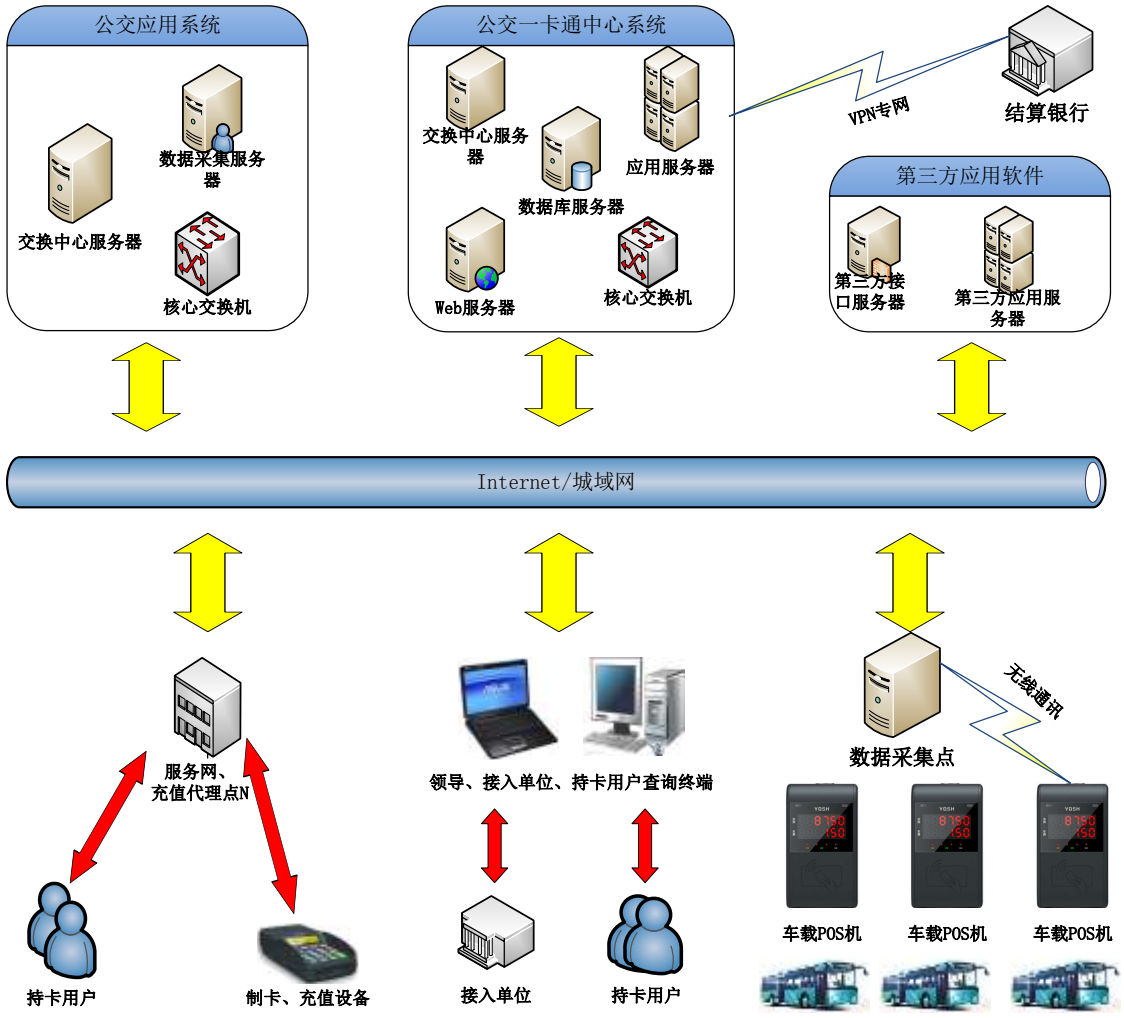
公交一卡通系统作为城市一卡通的应用，接入第三方小范围运营系统应用，又要兼顾作为单一的公交一卡通应用接入已部署的城市级一卡通应用，所以整个架构的设计尤为重要，系统设计分为以下几个层次，以适应复杂的市场需求。



- 数据资源层：数据中心采用大型数据库，Oracle10g 及以上版本，兼容 SQL Server2008 及以上版本，前置采集端采用 MySQL5.1 及以上版本数据库。方便的数据库移植，可以采用数据库集群和双机热备份功能。
- 数据访问层：封装数据库访问，为业务逻辑层提供一致的数据库访问接口，支持多种数据库；面向接口开发，为不同数据库开发对应的访问层实现，采用 Hibernate 持久层。
- 业务逻辑层：封装各子系统业务逻辑，为内外接口层及 Web 层提供一致的调用，可重用、松耦合、高扩展性，每个子系统就是一个插件，采用 Hibernate、Spring 框架。
- WEB 层：实现 Web 程序，易用，有较高的交互性，采用 Spring MVC、Exts 框架，使用 AJAX 增加交互性。
- 安全控制层：为系统提供一致的安全验证和授权，对接入设备及前置机进行合法性验证，支持多种验证方式并可扩展。采用 Spring Security、MD5 加密。
- 中间接口层：为制卡/采集提供服务接口，支持多平台调用，具有稳定高效、负载平衡之特性，采用 Web Server。

- 外部接口层：封装第三方应用接口，提供基本的通用功能，为特殊应用扩展接口，具有平台通用和扩展性的特性，采用 Web Server。
- 客户层：实现卡务管理的用户界面，与终端通讯、与接口层进行数据交换。具有高效率的数据交换和自定义传输协议，采用 C++前置接受系统，采集/监控通讯可实现为一个 Windows Service。

3.3 系统拓扑图



3.4 系统优势及特点

3.4.1 真正的电子钱包

非接触的读写特性、更快的读写速度。支持真正的离线运行。计费 POS 在离线运行时自身可以判定卡内是否有余额，该卡是否是已挂失或已注销的卡而不依赖于主控计算机中的数据库，有效验证卡的有效性和合法性。

3.4.2 强大的黑名单管理功能

系统中对挂失卡和注销卡，采用批次号黑名单和零散黑名单两级管理方式：将卡发行时设置有效期，如果使用时间超出有效期，不管该卡是否挂失或者注销，均拒绝使用。终端联机后主动请求验证黑名单版本信息，最大化保证卡片使用交易安全性。

3.4.3 高效、安全的管理

身份认证登录：系统管理软件可以为不同身份的管理人员划分不同的权限，灵活的权限设置可控制到具体功能点。

3.4.4 灵活的卡种类管理

卡片可由管理方自定义 255 种特征类别，并可分别针对每类卡种类设定不同的管理费，报表统计可以分类体现出各种类型卡片的账目数据；提高管理的科学性。

3.4.5 支持 M1 与 CPU 系列

非接触逻辑加密卡技术的不足之处也日益暴露[参考工信部《关于做好应对部分 IC 卡出现严重安全漏洞工作的通知》]，难以满足更高的安全性和更复杂的多应用的需求。因此，非接触 CPU 卡技术正成为一种技术上更新换代的选择。非接触 CPU 卡与非接触逻辑加密卡相比，拥有独立的 CPU 处理器和芯片操作系

统，所以可以更灵活的支持各种不同的应用需求，更安全的设计交易流程。但同时，与非接触逻辑加密卡（M1 卡）系统相比，非接触 CPU 卡采用更为安全的动态加密方式，系统建设也更为复杂，需要进行更多的系统改造，比如密钥管理、交易流程、PSAM 卡以及卡片个人化等。

非接触 CPU 卡可以通过内外部认证的机制，以及像建设部定义的电子钱包的交易流程，高可靠的满足不同的业务流程对安全和密钥管理的需求。对电子钱包圈存可以使用圈存密钥，消费可以使用消费密钥，清算可以使用 TAC 密钥，更新数据可以使用卡片应用维护密钥，卡片个人化过程中可以使用卡片传输密钥、卡片主控密钥、应用主控密钥等，真正做到一钥一用。由于非接触逻辑加密卡的交易流程比较简单，通过认证 KEYA 或者 KEYB，达到操作的安全权限，然后就直接进行交易操作，增加或者减少钱包金额。所以，在进行 CPU 卡的方案设计中，基于传统系统的平滑升级过渡和保护原有投资的角度考虑，可以达到兼容 Mifare 系统卡片使用的结果。

本系统采用先进而又成熟的技术、基于前瞻性的远期规划设计；在各种设备选型上按照合理超前、理性投资、避免重复投资、性能稳定、运行可靠、开放性和扩展性的原则进行设计的原则开发设计，系统类型为真正支持 CPU 卡的设计架构，而同时又兼容支持 Mifare 系列。

3.4.6 各种查询更加方便

针对持卡人可登录平台查询他的消费、纠错、存取款 次数消费等历史记录，以及消费情况曲线图。对于出纳员、管理员，可以方便地查询到详细操作记录和营业报表。系统提供各类报表查询（营业报表、出纳报表、个人存取款报表、流水明细表、清分清算报表、结算报表、车队营业报表、终端营业报表、卡种类营业统计报表等等），支持用户在线下载、打印、生成 WOED/EXCEL/PowerPoint 等多种报表导出方式。

3.4.7 系统特性

◆ **可靠性**

测试覆盖系统的面达 100%、审查覆盖达 80%以上。当软件或其组成部分遇到非法数据、异常操作、相关软件或硬件出现缺陷、超出规定性能要求等情况时，不能影响系统的正常服务的运行。建立健全的异常处理机制，包括操作异常，数据异常，流水异常处理等。

◆ **安全性**

阻止非法用户进入系统，对不同的用户授予不通的权限，并对操作日志进行详细记录。卡安全采用一卡多密，多种密钥管理，保证卡片的安全性，卡和终端进行 PSAM 验证，交易数据进行 TAC 密钥验证，保证每条流水的安全性。

◆ **可维护性**

软件应具有抗干扰能力。软件发生异常后，错误应不扩散，且应在最短的时间内上报维护系统；软件模块的相关性应尽可能少；对于公用函数尽可能放在公用模块中；输入数据有一致性检查，并且有数据的保护功能。

◆ **可移植性**

软硬件独立，易安装升级，可重用；清分结算中心和银行转账功能独立部署运行，一卡通管理平台和公交系统要考虑独立运行环境。服务部署要兼容在 Windows Server 2003,2008 的 64 位版及全移植到 Redhat Linux 5.0 以上版本操作系统。

◆ **扩展性**

在设计的时候，考虑终端机具等固定资产管理功能及公交管理功能的扩展。能最简化的对接第三方系统。

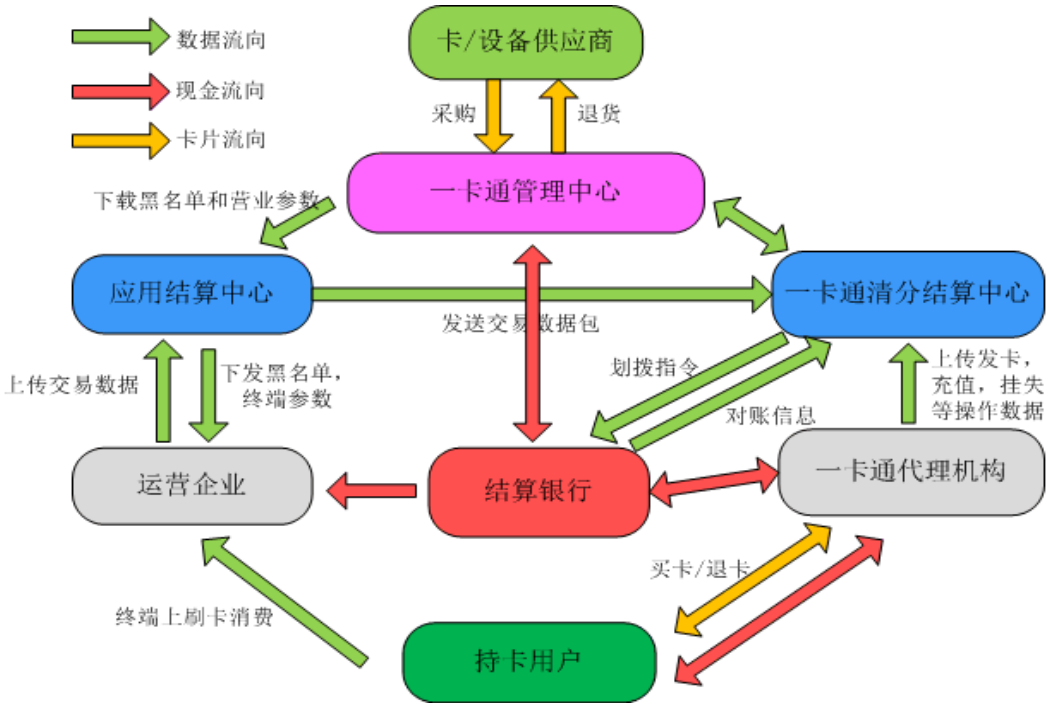
◆ **外部接口需求**

外部接口根据实际项目部署环境需求而定。

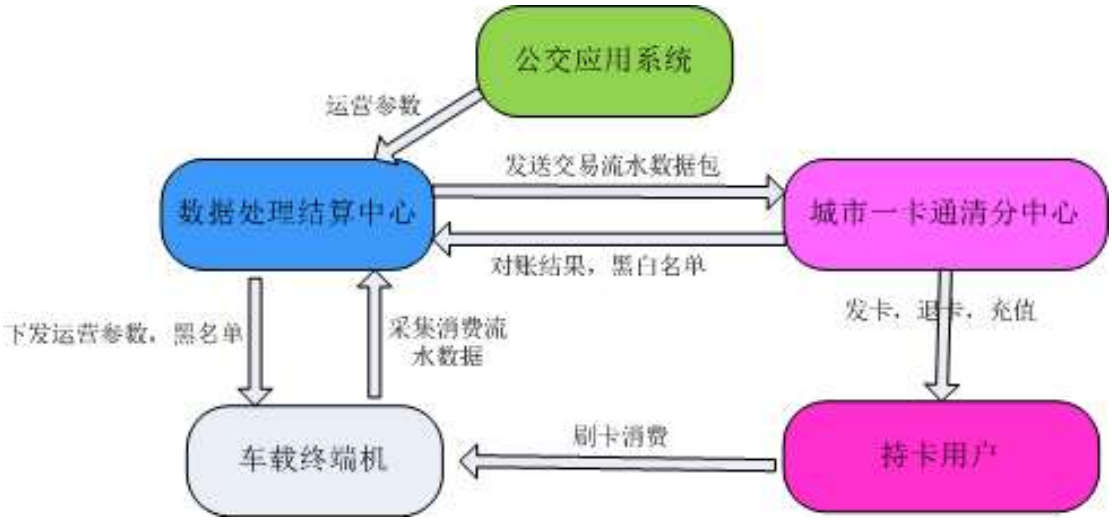
3.5 系统运营流程

城市公交一卡通适应两种复杂的市场需求环境：

◆ 一种是作为城市一卡通系统独立使用，兼容其他第三方消费应用系统。运营流程如下：



◆ 另一种是作为单一的公交应用系统对接现有的城市一卡通系统。



3.6 用户类型及要求

城市公交一卡通系统角色大致由以下部分组成：

序号	名称	说明
1	系统管理方	政府或企业担当，关注系统的稳定性，可靠性及实用性，清分结算的准确性,完善的账户平衡机制。
2	系统运营商	卡片发行或增值等其他业务代理，关注于代理业务数据准确性。
3	代理接入方	公交业务代理（发卡、充值），其他业务接入
4	应用管理方	公交公司、出租车公司、其他公司或个人，关注系统的终端稳定性，采集数据的便捷。实用的车辆，线路，司机管理功能，实时的黑名单下发及银行结转。
5	系统操作人员	管理上面各方业务，关注界面的可操作性，操作简单方便，错误能回滚，有详细的操作日志。
6	持卡用户	使用简单，一卡多用，使用场合广，充值方便

四、系统功能介绍

为了提高系统的兼容及扩充，方便与第三方系统对接，**易科士城市公交一卡通系统**分为五大部分：一卡通管理中心平台，一卡通清分结算中心，数据处理结算中心，公交应用管理平台和前置服务器数据采集。

易科士城市公交一卡通系统在中心管理平台、公交应用平台和用户查询平台均是**统一的登录入口**，在登录时自动识别登录账户的身份和权限，进入对应的平台界面，如下图：

4. 1 一卡通管理中心平台

易科士城市公交一卡通系统中心管理平台负责整个中心平台的管理，包括系统密钥管理系统，权限管理系统，基础管理系统，卡务管理系统和报表管理系统等五大子系统。主界面中有登陆人员的基本信息，显示站内的一些公告信息。

4.1.1 密钥管理系统

密钥管理系统是提供给用户卡片初始化和查询使用。卡片初始化包括 CPU 卡的初始化、M1 卡的初始化、PSAM 卡的初始化和 ISAM 卡的初始化，另外提供卡片初始化的流水记录的查询。

4.1.2 权限管理系统

4.1.2.1 URL 信息管理

权限管理系统提供对用户访问的 URL 配置管理功能，包括增加、删除、查询和修改功能。操作对象为配置管理人员，此功能不对平台操作用户开放。URL 的 ID 编码方式 00010001，第一级为页面 URL，第二级为页面内 URL。

4.1.2.2 模块管理

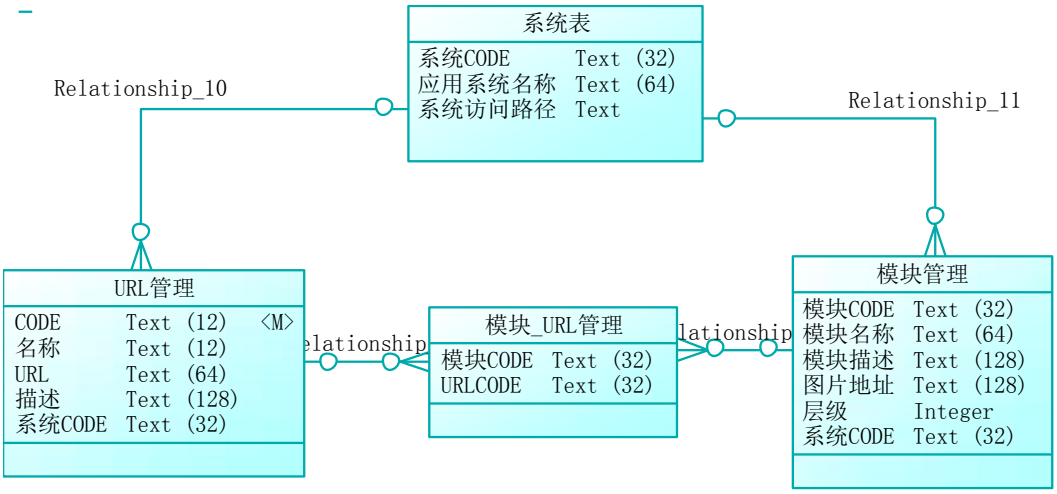
模块管理主要是提供系统对功能进行模块化划分及管理,便于用户使用以及系统的管理，该模块提供模块增加、修改、删除、查询的功能。可以将选定的 UR 划分到不同的模块中进行管理。此功能不对平台操作用户开放。moduleID 编

码方式 00010001 目前定义为 3 级。

子系统　0001

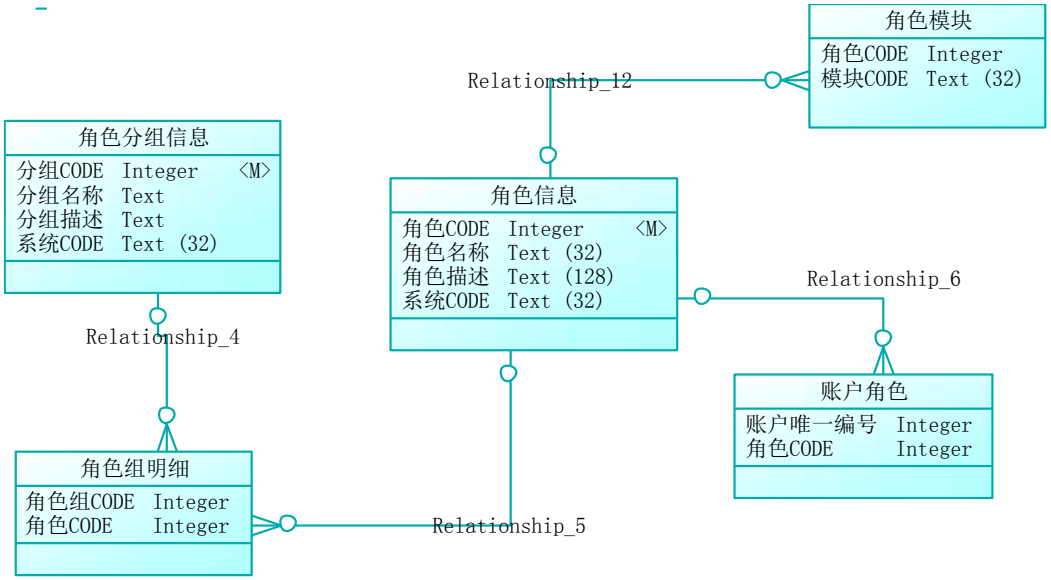
二级模块　00010001

菜单项目　000100010001



4.1.2.3 角色管理

角色管理主要提供系统使用过程中对不同人员能自由控制访问的页面，该模块提供角色的增加、修改、删除、查询和分组的功能。该角色在已经和用户绑定时将不允许用户删除。



在角色管理中，可以针对不同的角色设置功能资源，可具体到每个子系统中模块及模块中的单个功能项，如下图：

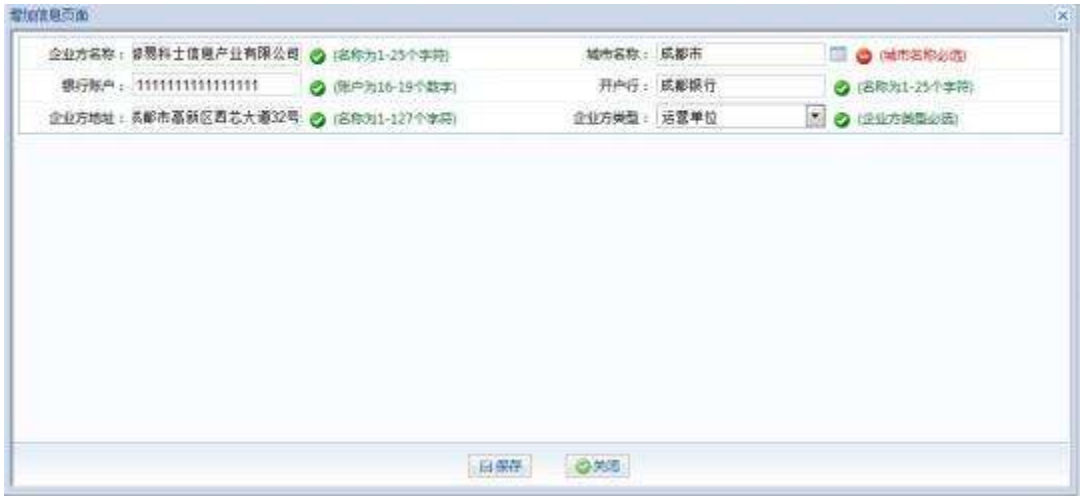
4.1.2.4 权限日志记录

负责记录登录到系统的用户日志信息，以备信息审计，提供查询功能。

4.1.3 基础管理系统

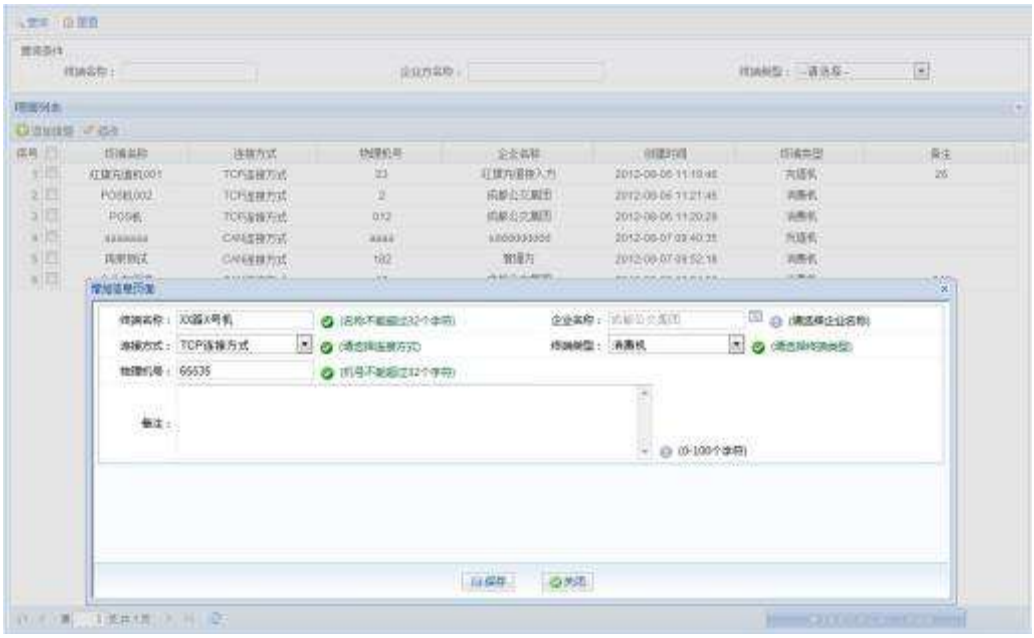
4.1.3.1 企业管理

基础管理系统维护下属接入方信息以方便为应用方分配卡片、终端及银行结算，基础管理系统提供接入方信息，包括增加、修改删除和查询功能。接入方信息包括企业名称、开户行及帐号、企业类型等信息。



4.1.3.2 终端管理

平台统一管理系统中的终端信息，初期为信息维护，后期为各企业的终端绑定。终端管理模块具有增加、修改、查询的功能。终端信息主要包括自动生成的终端号，通过列表获取的终端类型，终端的名称，物理机号，终端通讯方式等信息。



4.1.3.3 操作员管理

操作员管理模块提供操作员的增加、修改、启用和停用功能。操作员是属于接入企业的系统维护人员、管理人员或者一般操作员，他们分别有不同的权限做相对应的工作，每个操作员信息包括所属企业（用于管理企业单独的一些应用信息和充值结算）、角色（角色中赋予了各种不同的权限）、登录账号、登录密码、姓名等必要信息和手机号码、身份证号码、电子邮箱、QQ 号码、家庭住址等一系列的辅助信息。

4.1.3.4 字典管理

系统数据字典在系统初始化的时候自动建立，包括性别、企业类型、城市名称及代码、名族等信息。可供查询使用。

4.1.3.5 登录日志

登录日志可以查询所有操作员的登录记录，包括操作员用户名、登陆时间、登录地址和登录类型等信息。

4.1.3.6 黑名单管理

黑名单管理提供黑名单的明细包括产生黑名单的原因、黑名单生成的时间、黑名单卡卡号等信息。

4.1.3.7 卡片日志管理

卡片日志管理提供系统中卡片的操作明细记录查询，可通过卡片物理类型、卡种类、操作时间、操作员、操作类型等条件进行查询。

4.1.3.8 公告信息管理

提供公告信息管理功能，可以在系统中编辑公告、通知，包括公告的标题、内容和创建人，公告显示在登录后的主界面上，点击标题即可查询整个通知内容。

4.1.3.9 密码修改

密码修改提供登录的操作员修改自己的登录密码，只能修改当前登录操作员的密码，在修改的时候需要输入原密码。

4.1.4 卡务管理系统

卡务管理系统是城市公交一卡通系统的用户接待中心，是面向用户服务的综合接待窗口，负责接待和处理用户的各种服务请求，负责持卡人的综合业务。

4.1.4.1 基础管理

卡务基础管理包括卡类型管理、卡应用管理、卡种类管理、次数计价管理以及卡片基本信息管理。其中卡类型包括 M1 卡、CPU 卡，应用目前为公交应用，这两种属于系统内嵌的信息，提供查询功能，不提供增加、修改和删除的操作。

卡种类管理定义人员持有卡片的身份类型，例如：普通卡、老年卡、学生卡、员工卡等身份种类，可以根据不同的身份类型进行优惠的设置。卡类型管理模块提供卡类型的增加、修改、删除和查询功能，可设置每种类型的有效期限。

次数计价管理提供根据身份类型定义每种身份类型人员在充值次数的时候充值一次代表多少金额（单位元），例如普通卡类型 1 次代表 5 毛钱，则在普通卡充值的时候充值 20 元，则系统换算成次数就是 40 次；学生卡类型 1 次代表 2 毛钱，则在学生卡充值的时候充值 20 元，则系统换算成次数就是 100 次。整个系统中根据身份的次数换算金额都是通用的，每一种身份类型只能有一种次数计价方式。

卡片基本信息管理提供对卡片明细的查询功能，包括卡片类型、卡种类、是否记名、开卡时间、卡片状态等信息，可以根据多种条件组合进行查询。

4.1.4.2 卡务管理

卡务管理提供开卡、挂失、退卡、退款、换卡、补卡、充值、取款、解挂、废卡退卡等日常操作。

城市公交一卡通系统的卡片开卡是将白卡中写入相应的信息并能正常使用的一个操作，卡通卡片包括两种方式，一种是不记名，只定义卡片类型，卡片种类，根据卡片种类定义卡片的押金及手续费用等，不记名卡不挂失、不补卡；另一种是记名卡，除了定义卡片类型、卡片种类外，还增加了持卡用户的详细资料，包括姓名、身份证号、联系方式等，记名卡可以通过开户时登记的资料，持相应证件挂失、补卡等。

挂失操作提供根据用户唯一号、用户卡号、客户姓名和身份证号等条件来精确和模糊查询出需要挂失的用户信息，进行挂失操作，挂失的卡片立即作为黑名单下发到联机的终端机中。解挂是与挂失相对的，解挂操作只对处于挂失状态的账户进行操作，将挂失的卡片放在发卡器上，读卡、解挂，此时系统将更新黑名单版本，将之前挂失的卡号从黑名单中清除。

退卡操作分为有卡退卡和无卡退卡。有卡退卡操作在退卡的时候需要先读取卡片信息，再将卡片中的所有内容清除。无卡退卡方式和挂失操作类似，根据用户唯一号、用户卡号、客户姓名和身份证号等条件来精确和模糊查询出需要退卡的用户信息，进行退卡操作，在退卡的时候系统将此卡的卡号列入到黑名单中，下发到联机的终端机中。

退款操作提供根据用户唯一号、用户卡号、客户姓名和身份证号等条件来精确和模糊查询出需要退款的用户信息，然后进行卡片中余额的扣除功能，同时生成报表。

换卡操作提供根据用户唯一号、用户卡号、客户姓名和身份证号等条件来精确和模糊查询出需要换卡的用户信息，然后进行换卡操作。进行换卡操作的账户卡片状态必须为正常状态，换卡会根据身份类型的设置收取一定的卡费、手续费等，直接从账户余额中扣除，并生成报表。

补卡操作提供根据用户唯一号、用户卡号、客户姓名和身份证号等条件来精确和模糊查询出需要补卡的用户信息，然后进行补卡操作。进行补卡操作的账户卡片状态必须为挂失状态，补卡会根据身份类型的设置收取一定的卡费、手续费等，直接从账户余额中扣除，并且生成报表，补卡后账户自动从挂失状态变成正常状态。

系统中提供通过通过发卡器充值和取款的操作，将卡片直接放在发卡器上，然后在充值或取款功能模块中读卡，直接在键盘上输入要充值或者取款的金额，确定即完成操作。

废卡退卡操作和之前提到的退卡有所区别，此处的废卡退卡是将不用的卡片初始化处理。

4.1.4.3 PSAM 卡管理

PSAM 卡管理提供 PSAM 的开卡，与终端的绑定、解绑，PSAM 卡的退卡操作。

PSAM 卡开卡是指将空白的 PSAM 卡写入系统的密钥、机号文件、基本信息文件等的过程，类似于用户卡开卡，只是 PSAM 卡是给机器用的，每张 PSAM 卡都有唯一的标识号，在使用过程中只认 PSAM 卡而不认终端机器，这样就为维护和更换终端机具提供了便利，在终端机具出现问题的情况下只需要将 PSAM 卡取下安装到另外一台正常的终端即可马上使用。

PSAM 卡绑定是将已开卡的 PSAM 卡卡号与终端机的机号进行绑定操作，即每一张 PSAM 卡的卡号只能对应一台终端设备的机号，这两个号码相互绑定。也可以解除 PSAM 卡与终端机号的绑定。

4.1.4.4 ISAM 卡管理

ISAM 卡是用于提供给接入方二次加密使用的加密卡，操作方式和 PSAM 卡一样，ISAM 卡管理提供 ISAM 的开卡，与终端的绑定、解绑，ISAM 卡的退卡操作。

4.1.4.5 用户管理

用户管理提供通过用户唯一号、用户姓名或身份证号等条件查询出人员列表，以供修改和完善人员基本信息。

4.1.5 报表管理系统

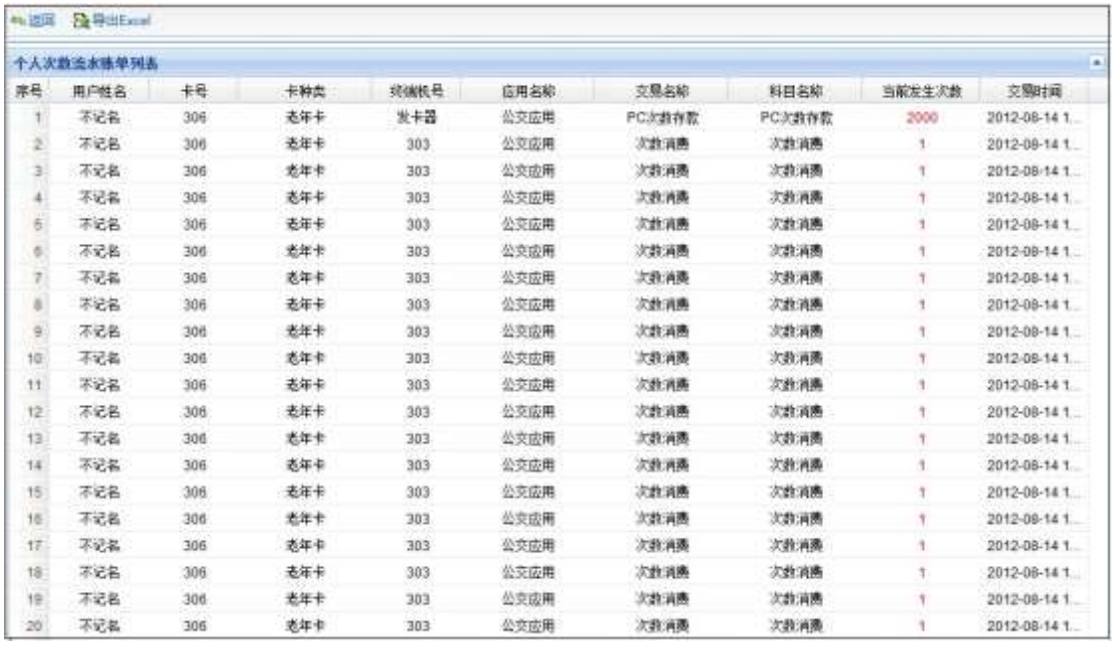
4.1.5.1 个人报表查询

◆ **个人现金消费流水账单**

个人现金消费流水账单提供多种条件查询，包括单个用户、多个用户、不记名卡、记名卡、账单日期、流水类型等条件进行查询，查询的结果为钱包应用产生的流水记录。查询出的流水明细可以导出到 Excel 表格。

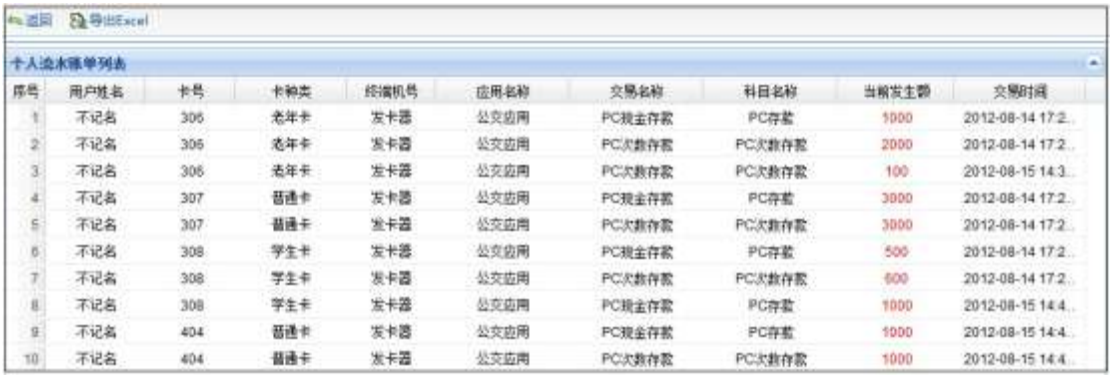
◆ 个人次数消费流水账单

个人次数消费流水账单提供多种条件查询，包括单个用户、多个用户、不记名卡、记名卡、账单日期、流水类型等条件进行查询，查询的结果为公交次数应用产生的流水记录。查询出的流水明细可以导出到 Excel 表格。



◆ 个人存取款流水账单

个人次数消费流水账单提供多种条件查询，包括单个用户、多个用户、不记名卡、记名卡、账单日期、流水类型等条件进行查询，查询的结果为包括现金充值、取款，次数充值所产生的流水记录，次数不能被取款操作。查询出的流水明细可以导出到 Excel 表格。



4.1.5.2 清分结算报表查询

◆ 管理方清算阶段报表

管理方清算阶段报表查询提供所有接入方、代理商的结算报表，包括终端刷卡营业情况和企业所属操作员的出纳情况。

◆ 代理商清算阶段报表

代理商的定义为城市公交一卡通系统的各个代理办卡点、充值点。代理商清算阶段报表是指专门针对代理商提供的结算报表，可以选择任何一段时间进行报表统计、查询。

◆ 接入方清算阶段报表

接入方清算阶段报表是针对所有接入城市公交一卡通系统的企业或个人提供的出纳、营业等所有业务的清算统计报表，管理方通过此报表与接入方结算，可以选择任何一段时间进行报表统计、查询。

4.1.5.3 出纳报表查询

◆ 出纳阶段报表查询

出纳阶段报表查询提供整个系统每个操作员在一段时间内的开卡、退卡、补卡、换卡、充值、取款等涉及到钱的汇总，且按照每一天统计。

◆ 出纳汇总报表查询

出纳汇总报表查询提供整个系统每个操作员在一段时间内的开卡、退卡、补卡、换卡、充值、取款等涉及到钱的汇总，按照所选时间段汇总统计。

4.1.5.4 营业报表查询

◆ 营业日报

营业日报表提供接入方企业任何一天的营业额的查询，可以选择查询所有终端总营业额，每个接入方企业生成一条数据，也可以选择查询每台终端的营业额，每台终端生成一条数据。

◆ 营业月报

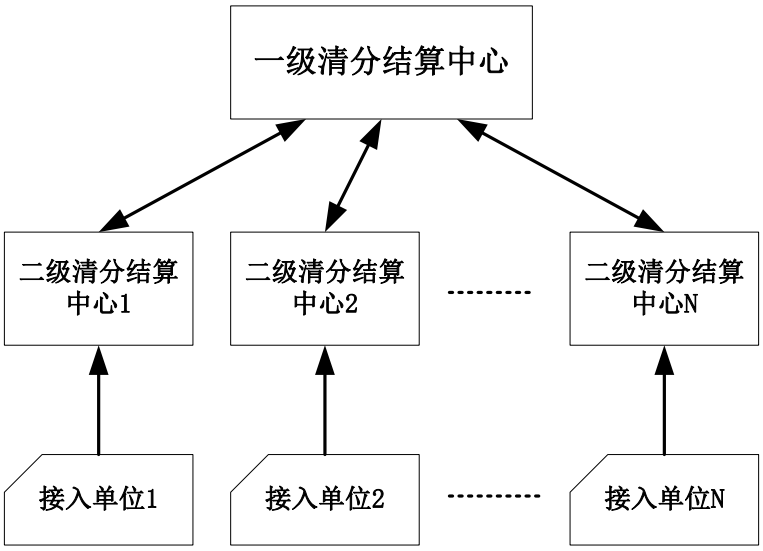
营业月报表提供接入方企业任何一个月的营业额的查询，可以选择查询所有终端总营业额，每个接入方企业生成一条数据，也可以选择查询每台终端的营业额，每台终端生成一条数据。

◆ 营业阶段报表

营业阶段报表提供接入方企业任何一段时间的营业额的查询，可以选择查询所有终端总营业额，每个接入方企业生成一条数据，也可以选择查询每台终端的营业额，每台终端生成一条数据。

4.2 一卡通清分结算中心

4.2.1 清分结算中心结构



清分结算中心结构图

4.2.2 清分结算中心功能

4.2.2.1 一级清分结算中心

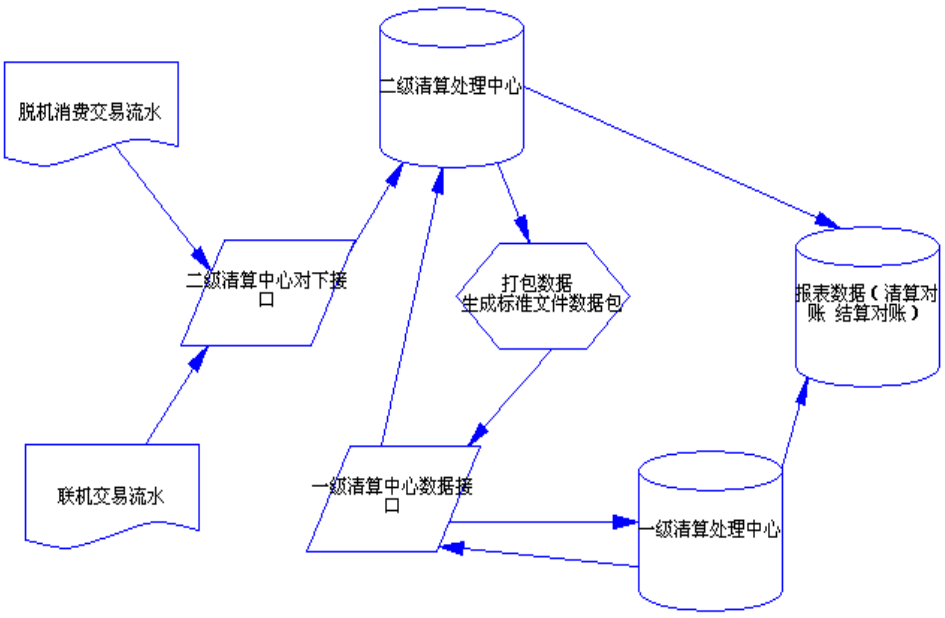
- 接收二级清分结算中心上传的交易数据包；
- 验证交易数据明细的完整性及正确性；
- 生成交易处理结果并将结果下发至对应的二级清分结算中心 生成交易日志及交易明细；
- 处理二级清分结算中心上报可疑数据文件；
- 进行根据 T+1 时间规则做日批处理工作 生成日批次处理清算汇总文件及明细文件 下发至二级清算中心（或对应的文件 报表服务器）；
- 以清算结果为准做清分操作 按照约定时间生成划账数据并对相应的结算银行做结算操作（或对应的文件 报表服务器）；
- 生成对应接入方的对账文件（或对应的文件 报表服务器）；
- 所有消费数据（次 金额）都需要收取。

4.2.2.2 二级（应用平台）清分结算中心

- 二级清分结算中心负责处理区域内的交易数据将交易数据登记入账并将消费记录打包上传到一级清算中心 ；二级清分中心可按照地域区分（市 区为 1+N 结构组合而成）；
- 接收经过上级清分结算中心验证后的交易处理结果 再次验证交易明细 并上报可疑数据；
- 依据一级清算平台的结账结果对下属结算单位在约定的结算周期做清分结算操作，并生成结算对账文件；
- 二级清算平台结算时间为一级清算中心对应用平台结算周期+N（约定时间）。

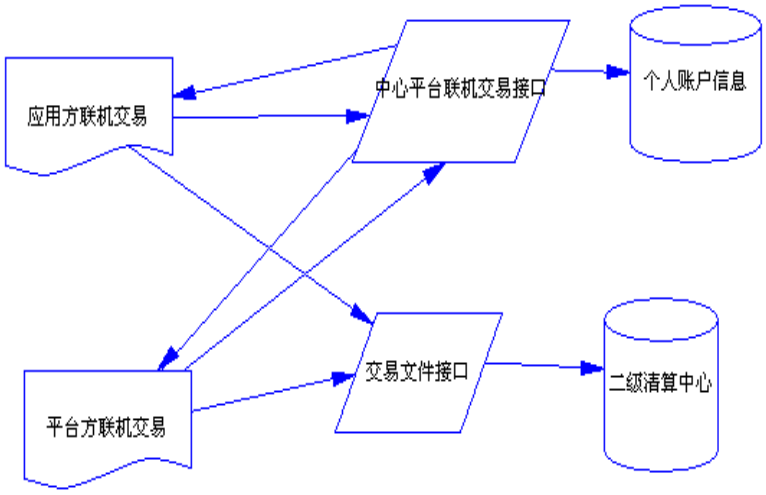
4.3 数据处理结算中心

数据流转过程



联机交易：根据 WEB 端卡片交易的实际情况，可能交易是分属在应用方也可能在中心平台提供的 WEB 服务上发生 所以上层平台需要提供消费接口（处理个人账

户数据）并在分属的二级清算中心发布流水数据 在一级清算中心接收到该数据后将不在更改其个人账户信息，只做数据统计。



脱机交易：各应用接入方将各采集点的数据收取到应用平台数据库中，按照约定的流水文件格式将数据发到所属的二级清算中心；二级清算中心将收取到的文件进行存储，然后按照约定的文件格式组合成交易数据包（联机交易 脱机交易黑名单 可疑文件确认……）对生成的交易日志和数据包明细做本地记录；将数据包上传到一级清算中心。

4. 4 公交应用管理平台

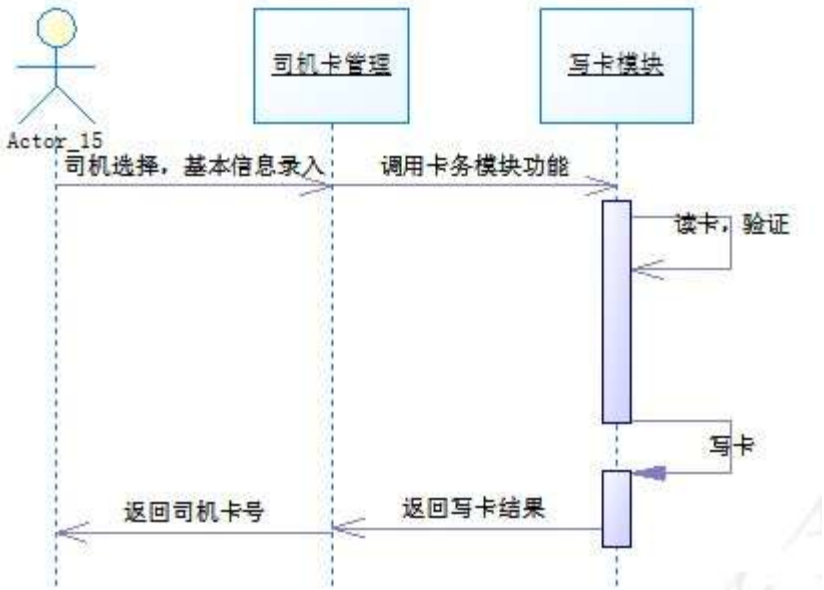
公交应用管理平台是整套城市公交一卡通系统的中间层系统管理，可作为独立的公交应用系统接入现有的城市一卡通项目，其功能主要包含公交应用的基础参数管理，公交车辆管理，公交线路管理，线路排班管理，公交司机卡管理，调度卡管理，配置卡管理以及相关运营报表管理功能。主要实现城市一卡通的公交应用部分，为公交公司提供一个智能的公交管理服务，收集分析终端采集上来的流水，并打包发送到城市一卡通清分结算中心，实现系统的对账及划账，并接收一卡通划账处理结果和黑名单数据，并将黑名单数据下发到相关终端。

4.4.1 公交应用管理系统

4.4.1.1 公交卡务管理

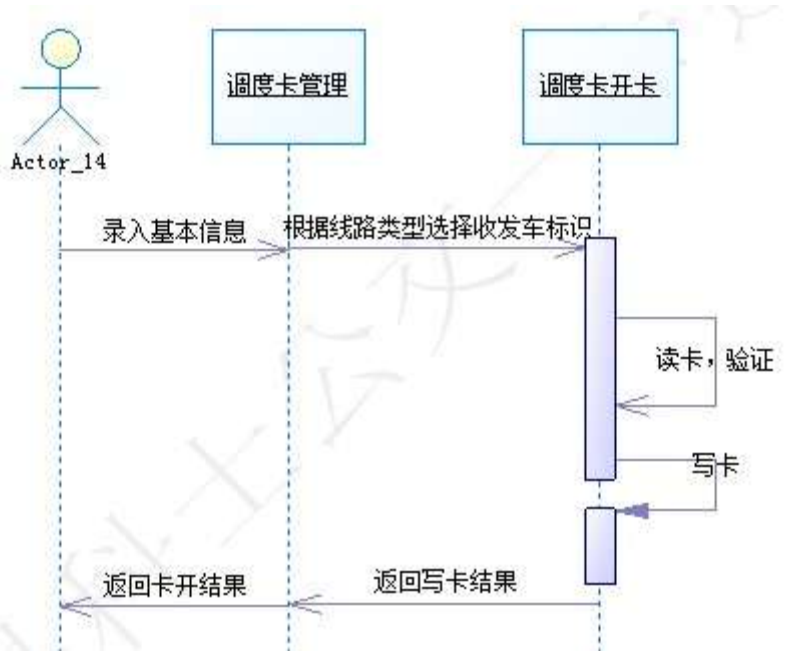
◆ 司机卡管理

司机卡主要是用于统计司机的上下班时间，在上班时，刷一次司机卡，记录该司机上班时间，下班交接时再刷一次司机卡，司机卡起到考勤的作用，同时也可以统计每个司机当班时候的营业情况。在司机刷卡签到后，所有刷卡收入都会统计在该司机的班次中，如果在交班时未签退，下个司机刷司机卡的时候前面一个自动签退，所有刷卡收入就会统计在第二个司机的班次中。



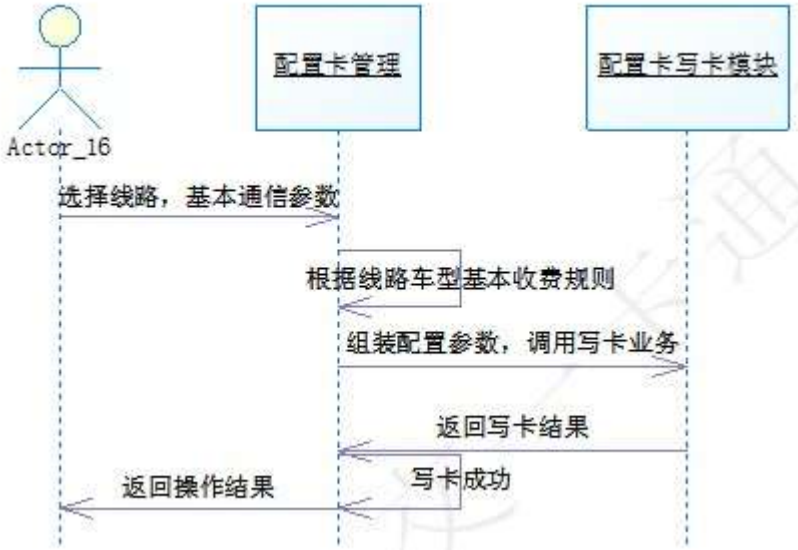
◆ 调度卡管理

调度卡也叫发车卡，调度卡和每条线路绑定，在每个班次发车之前需要刷调度卡，记录发车时间。



◆ **配置卡管理**

配置卡是用来设定费率等终端配置参数的卡片，网络参数、费率等需要通过配置卡来配置，包括采集服务器的地址、端口号，计费规则，刷卡时间间隔，扣费费率，线路编号，心跳间隔时间，应答超时时间等一系列参数。



4.4.1.2 公交配置管理

◆ **使用方管理**

使用方管理是指增加、修改使用方的基本信息资料，是系统组织机构的最顶级部门。包括使用方名称、单位负责人、地址、联系方式等信息。

◆ 组织机构管理

组织机构定义为使用方的组织层级，相当于是组织部门级别，可以增加超过10 级的部门，输出为树形结构，便于查询和管理。

◆ 车队管理

车队管理提供车队信息的增加、修改和删除操作。

◆ 员工管理

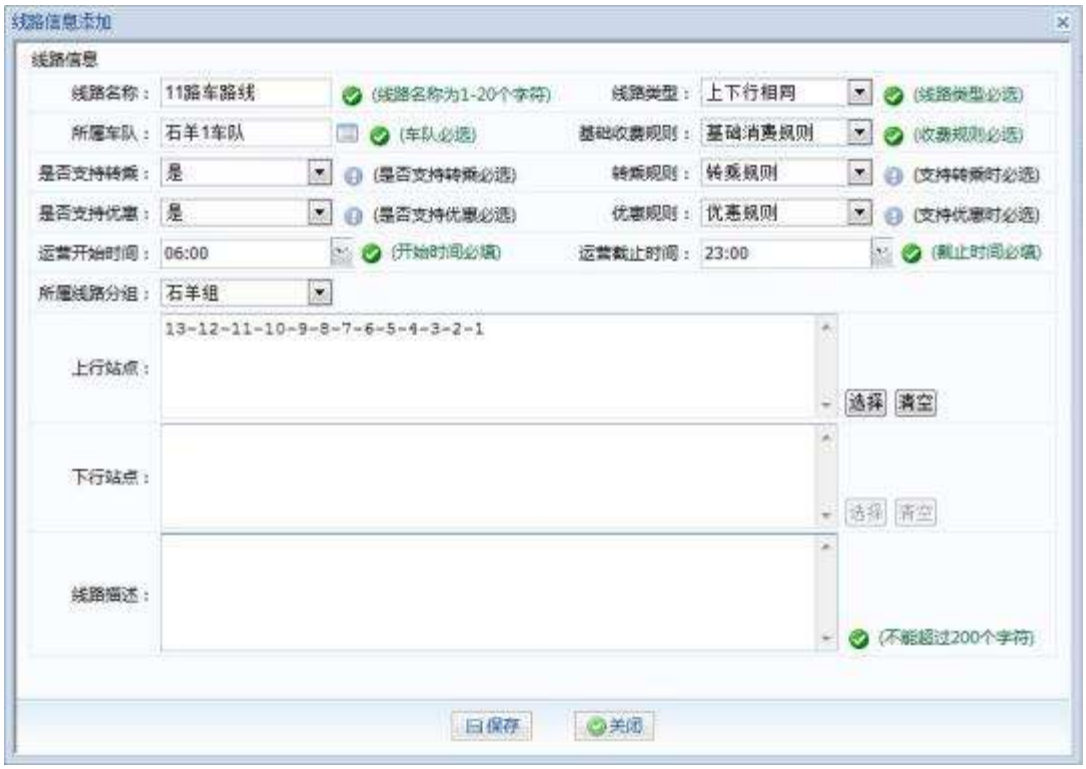
员工管理提供使用方内部人员信息的管理，包括增加、修改和删除人员信息。

◆ 站点管理

站点管理提供对全部站点的增加、修改和删除操作，每个站点都有名称，每个站点对应一个唯一的站点编号，每个站点都归属到某个片区，以备在进行路线管理的时候直接调用。

◆ 线路管理

路线管理提供路线的增加、修改、删除和路线的站点管理。路线的内容包括路线名称，该路线所属的车队和所属线路分组，路线的基础收费规则，路线的优惠规则以及转乘规则和营运时间的管理。站点的管理可供语音报站接入使用。



◆ 线路分组管理

线路分组管理提供分组组别的增加、修改和删除操作。

◆ 车辆管理

车辆管理提供对车辆基本资料的增加、修改和删除操作，车辆的基本信息包括车牌号、车辆类型（空调车、非空调车、大巴、中巴等）、所属路线、品牌、型号、座位数等资料。

◆ 线路特殊收费管理

线路特殊收费管理配置为特殊的规则设置，例如该路线在正常的时间内运行收费规则为普通基础规则，超过某时间点后收费规则在基础规则基础上增收多少钱每次。

4.4.2 系统参数管理系统

4.4.2.1 终端参数配置

终端参数配置是通过上层管理平台增加的终端，在公交应用系统中对分配到该使用方的终端进行参数的配置，包括初始化参数 ID 号，所属车辆，网络参数、采集服务器的地址、端口等，为联机设置必要的参数信息。最终把单独的每台终端绑定到每台车辆上。

4.4.2.2 优惠规则管理

优惠规则管理提供对各种身份种类的优惠折扣进行添加、修改和删除操作，在使用基础规则刷卡的情况下，每种身份类型的卡片实际扣款的折扣率可以不同。

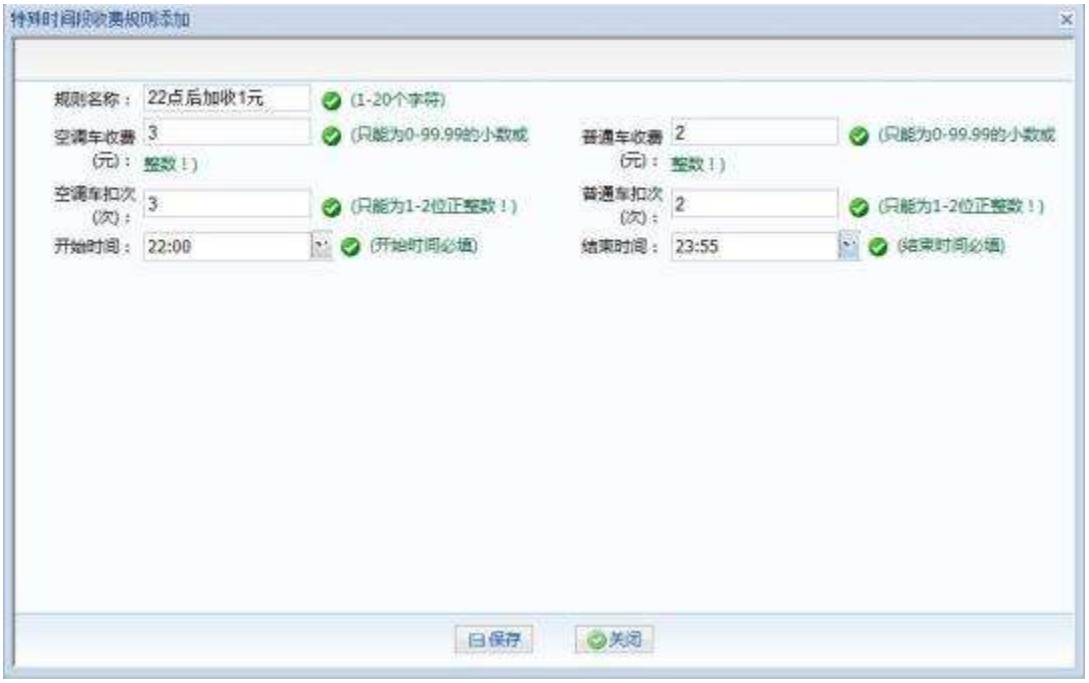
4.4.2.3 基础收费规则管理

基础收费规则管理提供对基础规则的添加、修改和删除操作。内容包括：

- **计费优先级**，在公交刷卡中有两种扣费方式，按金额扣费和按次数扣费，在实际的使用中，可能会有部分路线只允许扣除金额，部分路线允许扣除次数和金额，而在允许扣除次数和金额的计费中，有需要设置是先扣次数还是先扣金额。
- **连续刷卡计费**，在实际使用的过程中，不可能完全一人一卡，会有多人使用一张卡的情况，那么就会存在连续刷卡，在这个规则里面可以设置连续刷卡扣费的方式，允许连续扣除次数、金额，或者是在第一次刷卡扣除次数后，后面第二次以上刷卡均扣除金额。
- **连续刷卡时限**是设置在一定时间范围内刷卡均符合连续刷卡计费的方式，超过这个时限后则重新按照计费规则计费。
- **收费标准**，在实际的使用过程中，相同路线的车辆型号可能会不同，有的车收费贵（空调车），有的车收费相对便宜（非空调车），在同一个规则中可以设置不同类型的车辆的费率。

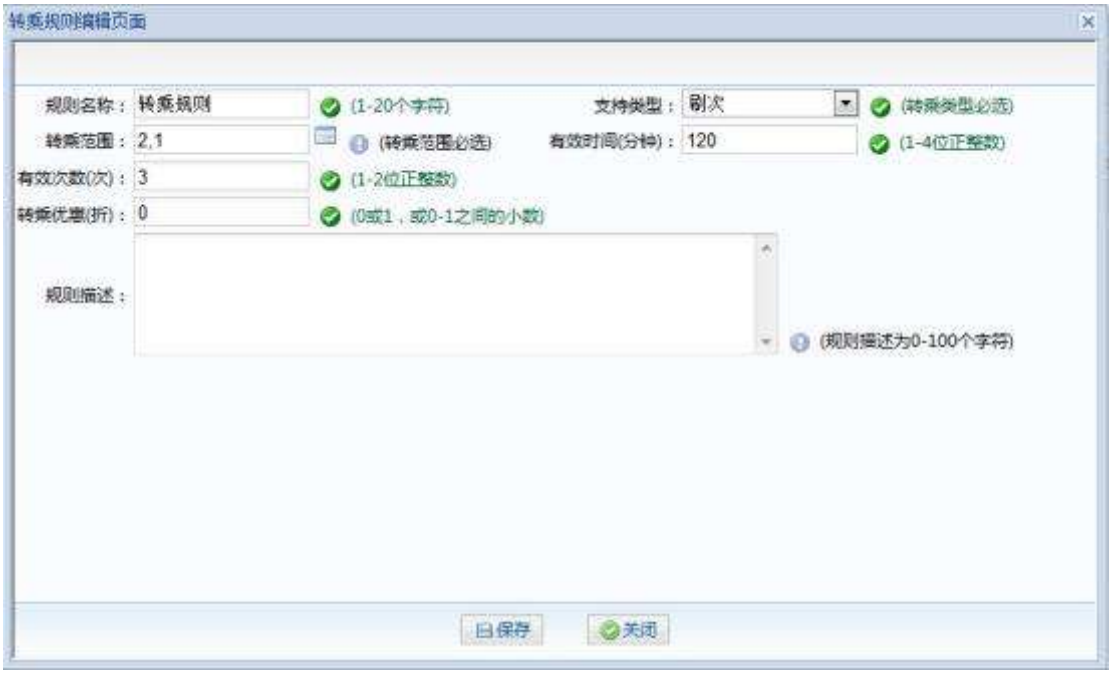
4.4.2.4 特殊收费规则管理

特殊收费规则是指在基础收费规则的条件下，由于其他一些因素如时间达到一定成都的情况下会多收费。



4.4.2.5 转乘规则管理

转乘规则是指在一定时间段内不止乘坐一辆车的情况，因为每条公交线路不可能能到达任何地点，往往乘客在去某个地点的时候会转乘多辆车，系统针对这种情况设计了转乘的优惠设置，可以设置在规定时间段内转乘部分车辆免费、折扣。支持转乘扣费类型设置（刷卡、刷金额）、转乘范围设置（部分设置的路线或车辆）、转乘有效时间、转乘次数和转乘折扣。



4.4.3 应用报表管理系统

4.4.3.1 终端报表管理

◆ **终端现金流水明细报表**

终端现金流水明细报表提供各条路线的每台终端的金额刷卡流水，查询结果显示每台终端的查询时间段内的所有流水明细。报表提供导出到 Excel 中。

◆ 终端次数流水明晰报表

终端次数流水明细报表提供各条路线的每台终端的次数刷卡流水，查询结果显示每台终端的查询时间段内的所有流水明细。报表提供导出到 Excel 中。

◆ 终端营业日报表

终端营业日报表提供各条路线的每台终端每一天的刷卡消费合计，分为金额合计和次数合计。报表提供直接打印和导出到 Excel 中。

◆ 终端营业汇总报表

终端营业汇总报表提供各条路线的每台终端在一段时间段内的消费合计，分为金额合计和次数合计。报表提供直接打印和导出到 Excel 中。

4.4.3.2 车队报表管理

车队营业报表提供所有车队的某一时间段内的营业汇总情况查询，查询出的每个车队的营业报表中有卡种类的小计，每种卡种类同时分次数和现金消费两种，便于车队分析乘车人群的构成等情况。报表提供直接打印和导出到 Excel 中。

4.4.3.3 卡种类报表管理

卡种类营业报表的作用是提供给公交公司统计分析使用，可以查询每天线路的每种卡种类的刷卡情况，便于公交公司做出合理的车辆调度。报表提供直接打印和导出到 Excel 中。

4.4.3.4 班次报表管理

线路班次日报表是按天统计每条线路，每条线路的每个司机每个班次的营业情况。供公交公司统计分析每条线路的不同班次的营业情况，为合理调度安排车辆作依据。报表提供直接打印和导出到 Excel 中。


公交一卡通报表

显示页 1 / 1

转到页:

线路班次日报表

单位：易科士信息产业有限公司

时间段：2012-08-01至2012-08-31

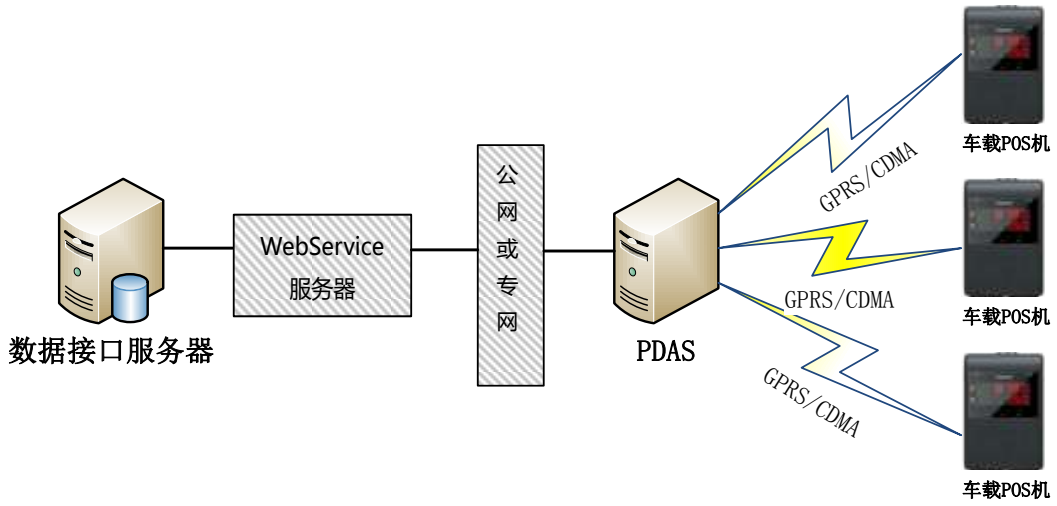
日期	线路名称	司机	终端号	发车卡	收发车标识	班次号	消费类型	现金消费	次数消费	次数对应金额	总笔数
2012-8-16	120	张三7	407	202	发车	0	次数消费	¥0.00	86	¥45.75	86
							现金消费	¥34.20	0	¥0.00	21
				终端班次总计				¥34.20	86	¥45.75	107
				司机班次总计				¥34.20	86	¥45.75	107
				线路班次总计				¥34.20	86	¥45.75	107

操作员：admin　　操作时间：2012-08-16 10:43:44

4.5 前置服务器数据采集

前置数据采集服务器（以下简称 PDAS：Prepositive Data Acquisition Server）主要与数据接口服务器通过 WebService 服务器进行数据间接通信，将数据接口服务器上保存的终端下发参数分发到相应的公交 POS 硬件设备上，同时也会将公交 POS 硬件设备上相应流水数据无差错转发至数据接口服务器。

4.5.1 网络结构



协议逻辑网络结构图

4.5.2 前置服务器功能

◆ POS 联机处理（PDAS->数据接口服务器）

1、POS 向 PDAS 发起 TCP 连接请求；

2、PDAS 收到 POS 连接请求后，根据其发送来的第一条签到消息进行合法性校验，通过验证后，同意连接的建立，并保持连接；

3、更新界面显示，记录日志，同时将其 POS 机号及消息内携带的参数版本号和黑名单版本号通过 WebService 接口发送至数据接口服务器；

4、数据接口服务器检查此 POS 的参数版本号和黑名单版本号是否为最新，不为最新时，回复 PDAS 有参数需要下发，否则回复无参数需要下发；

5、PDAS 回复 POS 签到消息，并通知其是否有需要更新参数或黑名单。

◆ POS 脱机处理(PDAS->数据接口服务器)

1、PDAS 检测到与 POS 的 TCP 连接中断或者在规定时间内未响应消息应答；

2、更新界面显示，记录日志。

◆ POS 联机状态定时维护(PDAS->POS)

1、POS 定时发送心跳包至的 PDAS；

2、PDAS 在收到心跳包后，将其 POS 机号及消息内携带的参数版本号和黑名单版本号通过 WebService 接口发送至数据接口服务器；

3、数据接口服务器检查此 POS 的参数版本号和黑名单版本号是否为最新，不为最新时，回复 PDAS 有参数需要下发，否则回复无参数需要下发；

4、PDAS 回复 POS 心跳包消息，并通知其是否有参数或黑名单需要下发。

◆ POS 脱机状态定时维护(PDAS->POS)

1、PDAS 在规定的间隔时间内未收到来自 POS 的心跳包；

2、PDAS 断开与此 POS 的 TCP 连接，更新界面显示，记录日志。

◆ POS 参数下载（PDAS->POS）

1、POS 向 PDAS 发送参数或黑名单更新请求消息；

2、PDAS 将其携带的参数版本号或黑名单号，通过 WebService 接口发送至数

据接口服务器，请求最新的参数或黑名单信息；

3、数据接口服务器检查此 POS 的参数版本号和黑名单版本号是否为最新，不为最新时，回复 PDAS 相应的参数或黑名单信息，否则回复无参数需要下发；

4、PDAS 根据数据接口服务器的回复消息，回复 POS。

◆ POS 流水采集(POS->PDAS)

1、POS 向 PDAS 发送流水消息；

2、PDAS 解码收到的流水消息：如成功后将流水消息、标志位、流水接收日期、流水号等信息组合，写入当日流水数据文件尾部；如解码失败，则将相应的错误原因记录至日志文件，中止执行后续流程；

3、存储成功后，回复终端流水收到确认消息（如不在规定时间内回复，终端将再次上传此流水数据）。

◆ 流水上载（PDAS->数据接口服务器）

1、PDAS 定时检查流水数据文件时，发现有未上传流水；

2、PDAS 向通过 WebService 接口向数据接口服务器发送流水消息；

3、发送成功后将数据文件中此流水的标志位修改为已发送，等待数据接口服务器应答；发送失败时，则等待下一时间重新发送；

4、PDAS 接收到来自数据接口服务器的应答后，将数据文件中此流水的标志位修改为发送成功，然后继续发送下一条未上传流水；

5、PDAS 在超时时间内未收到数据接口服务器的应答后，则等待下一时间重新发送。

五、公交车载 POS 机硬件

5.1 车载 POS 机图片

车载POS机正面图

车载POS机背面图

5.2 车载 POS 机参数特点

- 整机机构牢固、外形美观；外观表面采用耐用冲击材料上、下盖结合处无错位，间隙＜0.1mm；机壳色泽均匀、光鲜，无划伤、无污点；印刷字体清晰，标牌牢固端庄；紧固件结实牢固，无缺少、松动现象
- 显示界面友好，显示内容丰富，背面装有供司机了解刷卡情况的数码显示管；
- 车载机配有语音提示，语音清晰宏亮；容量大于 50 段；
- 车载机有控制按键，用于设置、查询、司售人员上下班等操作；
- 车载机安装方便可靠，提供多种安装方式和安装结构件，随机提供安装及使用说明书；
- 车载机可抗±4500V 以上的高频脉冲群干扰，能在恶劣环境（点火起动、制动、低温、加速、爬坡等）下正常工作；
- 车载机内电源能在+9V-+36V 的宽电压范围内正常工作，具有反接、过压过流自动保护自动恢复等功能；当电源发生故障或更换时，车载机所保存的刷卡数据应不受影响；电源维修方便快捷；
- 车载机工作温度为-20℃ - +70℃，储存温度为-40℃ - +80℃，工作湿度为 20% - 90%；
- 刷卡感应距离为 0~10cm；
- MTBF>10000 小时，产品寿命周期大于 5 年
- 刷卡交易迅速，典型的刷卡交易处理过程小于 0.3 秒（包括完成有效性检验、密码认证、黑名单查询和正常的消费交易）；
- 车载机内装有实时钟电路，时钟误差小于 30 秒/月，功耗低，精度高，能保证车载机的时钟准确；
- 保存的数据在断电后保持十年不变：
- 采用大容量存储器，可保存刷卡记录 50000 条以上和 20 万条以上黑名单，并可进行扩展；
- 机具标配 3 个密钥卡座，支持 PSAM、ESAM 和 ISAM 卡，以实现安装建设部 PSAM 卡安全模块的功能；地方安全模块密钥可通过 ESAM 支持；
- 机具配置 1 个通讯卡座，支持 GPRS 和 CDMA 无线传输功能，可扩充 WI-FI 接口，CAN 总线、USB 数据接口和 RS232 总线结构；

- 可以正常识别成都天府通现已公开发行的所有卡片（通过接入现有成都公交系统），交易和业务流程符合成都公交所有要求，数据可以接入现有系统进行清算，tac 验算通过；
- 数据的读写采用 3DES、RAS 安全算法，保证数据存放及传输的安全性；
- 预留一个 RS232 接口和外部设备进行数据交互；
- 采用多信息域记录存储方式，每条记录须包含卡类型、卡消费类型、卡物理号、卡发行流水号、卡消费数据（时间、消费额、原额、消费城市代码）、充值数据、TAC 验证码、前次消费数据（时间、消费额、消费 POS 机号）、校验字等近各种信息，记录长达 64 字节；
- 车载机在司机上下班过程中，可以向司机的签到卡内回写一些信息，例如所上班的车的车辆号，上班时间等，以便公交内部管理系统使用；
- 可方便地对漏采数据按车辆、按日期、按流水号进行补采集，保证刷卡记录的完整性；
- 机具具有双存储器，一块作为正常的流水记录，另一块为备份存储器，备份存储器数据满后采用覆盖的方式备份最新流水；
- 单车当天运营汇总功能,当班司机查询最近 10 笔交易明细功能，当班查询未上送交易明细笔数功能，管理卡支持功能；
- 采用工业级，主 CPU 采用 32 位 ARM 处理器；
- 硬件平台支持符合人民银行 PBOC2.0 规范及建设部规范的 13.56M 非接触 CPU 卡操作功能（符合 ISO14443）；
- 支持 ESAM 模块的装载与集成。

5.3 车载 POS 机功能模块介绍

5.3.1 显示屏幕

车载 POS 机屏幕分为两个部分：前端刷卡面显示和司机面显示。前端刷卡面显示屏为双排 LED 显示，每排 6 位显示；司机面显示为单排 6 位 LED 显示。具体显示内容如下表：

	操作类型	显示内容	备　注
前端刷卡面显示屏	开机	第一排显示“load..”； 第二排会顺序显示机器版本号、费率和机号。	开机自检过程
	正常待机	第一排显示时间，格式为“HH-mm”； 第二排显示基础扣费金额。	时间中间的“-”规律闪烁，每闪烁一次时间为 1s。
	用户卡正常刷卡	第一排显示卡内余额或者剩余次数，格式为“XXX.XX”或“XX”； 第二排显示当次扣款金额或者当次扣除次数。	在刷卡前屏幕显示基础扣费金额，当不同的身份卡刷卡时会根据规则扣除不同金额，显示的扣款金额是优惠后的金额。
	非法卡刷卡	第一排保持显示时间； 第二排显示不同非法类别的不同代码信息。	非法卡刷卡主要是两种：注销卡和挂失卡，注销卡在刷卡时的代码为 ER-00，挂失卡在刷卡时的代码为 ER-33。
	管理卡刷卡	第一排保持显示时间； 第二排：刷卡成功时显示“good”，刷卡失败时显示或“Err”。	
司机面显示屏	正常待机	不显示。	因为此面是供司机看扣款是否成功，又可能连续的卡扣的费用不同，所以不会一直显示。
	用户卡正常刷卡	显示扣款金额或者扣除次数。	每次刷卡显示 3 秒钟时间后自动返回。

5.3.2 卡感应区

卡感应区是供刷卡的区域，此区域在前端显示屏下方，有明显的刷卡提示标志。

5.3.3 键盘功能

车载 POS 机在司机面有一个薄膜小键盘，有两个方向键、一个确定键和一个取消键构成。按键支持单独使用和组合使用，具体功能如下表：

按键名称	功能描述	
上方向键	向上翻页	
下方向键	向下翻页	
确定键	确认所选择的内容	
取消键	取消选择并返回到上级	
上方向键和确定键组合	显示	对应内容
	F1	显示连接前置的配置端口号
	F2	显示流水条数
	F3	版本显示
	F4	显示机号
	F5	USB 配置参数
下方向键和确定键组合	手动发起网络连接（屏幕无任何显示）	

5.3.4 语音功能

车载 POS 机具有语音提示功能，在刷卡时根据卡的验证、卡的类型等会有不同的语音提示。具体提示信息如下：

语音提示内容	备　　注
嘟. .	普通卡刷卡成功提示声音，因为在实际使用环境中，持有普通卡的用户基本占全部持卡者的 90%以上，而且刷卡频率相对较快，刷卡成功就只提示一声单音。
“特殊身份提示”	根据项目的实际需求写入特殊身份类型卡片的提示音，如“老年卡”、“学生卡”、“员工卡”等。
请投币	卡内余额/次数不足以扣除当次乘车费用，刷卡失败。
请充值	卡内余额/次数低于设定的充值提示金额，每当卡内余额小于此金额的时候就会提示“请充值”，刷卡成功。

请重新刷卡	在刷卡时拿卡过快，导致交易未完成，刷卡不成功，此时提示请重新刷卡，必须用同一张卡再刷一次或者手动按键取消，否则其他卡不能刷。
挂失卡	在刷已经挂失的卡片的时候，系统会验证卡的合法性。
签到成功/签退成功	在刷司机卡的时候，系统会自动识别是签到或者签退并进行语音提示。

5.3.5 USB 数据接口

车载 POS 机配置一个 USB 接口，可以通过 USB 接口进行终端参数的配置、终端黑名单的更新、刷卡数据的采集，也可通过 USB 接口与其他第三方设备进行对接，实现一些个性化的功能。

5.3.6 电源及开关

车载 POS 机电源自适应 9-36V 的直流电压，具有反接、过压过流自动保护自动恢复的功能。

5.3.7 密钥卡座及通讯卡座

车载 POS 机支持 3 个 PSAM/ISAM/ESAM 卡卡座和 1 个用于无线通讯的卡座。

5.3.8 串口

车载 POS 机配置了一个 RS232 串口接口，通过这个接口可以进行终端设备的程序更新，可以使用总线方式来下发终端的参数、更新黑名单和采集刷卡数据。或者通过串口与其他第三方设备进行对接，实现一些个性化的功能。

5.4 设备安装效果图

安装背面效果图

安装正面效果图

安装侧面效果图

六、第三方接口方案

6.1 标准接口方式

一卡通系统提供 WebService、EJB、COM+ 等多种接口包，供第三方产品通过无缝链接、有缝链接、不链接等多种方式进行接入扩展，具有很好的扩展性。

在数据层上，系统提供可定义的元数据（包含业务逻辑的数据视图）方式，供 WebService 接口调用，或以 XML、Excel 文件的方式供第三方调用。在功能层上，系统提供 EJB、COM+接口供第三方调用。在业务层上，系统提供 WebService、Socket 接口供第三方调用。

同时，系统可提供卡片、数据库、终端设备数据和动态链接库，方便用户二次开发和扩展应用。系统充分考虑了用户的现状和将来的升级需求，系统的开放性设计充分保证了用户投资的长期效益，避免资源重复浪费。

6.2 读卡助手方式

在一卡通系统中，我们开发了与第三方系统并接的驱动程序包，采取进程外接口服务方式，实现了在不进行现有第三方系统修改的情况下，原系统与一卡通系统的信息共享。

在一卡通系统中，用户卡上已经存放了各种基本信息和身份识别信息，第三方系统在多数情况下，正是使用这些信息中的某种信息进行用户身份识别的，我们开发的射频卡自动扫描助手程序，采用后台运行的方式，与第三方系统运行在同一个机器上，在主机安装射频卡读卡器，定时对读卡器进行扫描，一旦发现有用户卡放在读卡器上，根据用户识别类型，从卡上读出相应的信息进行解码，并采用键盘模拟输入的方式，将解码信息送入系统键盘中，直接送到第三方系统的用户识别码输入区中，完成用户识别信息的输入。

6.3 卡共享方式

除了接口的方式外，同时提供了卡共享方式，针对不同业务类型的系统，可以使用不同的卡操作方式。

对于消费类型的系统，也可以分为一本帐方式和两本帐方式：

- 对于一本帐方式，第三方系统使用与“一卡通”一致的帐目，这在驱动程序包中已提供了卡的操作方法。这种情况下，此系统的消费记录要传入到“一卡通”系统中，以维护“一卡通”系统的帐目平衡性和完整性；
- 对于两本帐的系统，系统可以在卡上为其另外分配一个存储区，用于存放其独立的帐目。

对于识别类的系统，系统开发有卡识别驱动程序包，此系统使用卡阅读器，即可以读取卡上的用户身份信息和卡状态信息，用于身份确认和卡有效性判别，同时，卡中心系统在制卡时，可以在卡上加入用于卡识别的个性信息，例如条码内部号码等。

七、系统安全方案

7.1 总体规划

安全体系的设计规划要求站在产品标准化的高度，卡片、终端、网络、软件产品的研发、测试、安装整个过程严格遵循 ISO9000 标准和国家相关标准进行。

安全体系的实施和维护规划要求做到服务标准化，向学校提供详细、标准、完整的售前，售中，售后各类文档。为学校各级操作人员提供良好培训，预防问题的发生，在系统出现性能抖动等异常情况时，能及时发现，使系统的安全事故和突发事件降到最低。

遵循“水桶”理论，从“城市公交一卡通”各组成部分进行安全性的设计。“一卡通”系统由卡片、终端设备、网络、软件、数据中心组成，通过密钥安全体系贯穿始终。

7.2 密钥管理体系设计

城市公交一卡通系统遵循安全设计的基本原则及国家相关标准的密钥体系，确保了从设计、开发、管理、使用和维护等各环节的安全性，达到七大目标：卡安全、终端安全、交易安全、网络安全、系统安全、数据安全和应用安全。

7.3 卡片安全体系设计

作为信息载体的基本单元，城市公交一卡通系统由 CPU 卡及逻辑加密卡，其卡片数据的写必须通过 PSAM 卡或加密机采用安全写的方式(CPU 卡)及通过 PSAM 卡计算登陆 KEY（逻辑加密卡）才能完成，操作时卡机数据校验采用 CRC 方式，需经双向三次论证，确保卡机在数据交换之前，两者进行互相身份合法性鉴别，从而对卡片的安全性做了保证。

为保证系统的密钥安全性，为保证系统的密钥安全性，系统所有的密钥均存在加密机中，同时所有得终端设备必须用主机联网授权获得授权才可正常使用。

联网授权:终端设备必须与主机联网，申请签到，并得到认可后，才可以操

作卡片大大提高了整个系统的安全性。

IC 卡安全管理 :对用户 IC 卡的制卡、发卡、挂失、补卡、销卡、黑（白）名单管理、制卡和领用等过程需制定一套严密完整的制度和实施方法，以保证"一卡通"系统的安全可靠性，保证结算中心、持卡人、运营商的利益。

7.4 终端设备安全体现设计

7.4.1 设备风险性分析

设备的授权——防止非法产品入网流通使用，所有终端设备须经授权才能在一卡通网络上使用。

设备的交易合法性

防止过期卡片使用

设备存储数据——应能做到防止数据泄露，断电后能够继续运行使用。

7.4.2 设备安全性规划及实施

注册／授权双向认证：产品具有特定的注册／授权双向互认功能，防止非法产品入网流通使用。

具有签到、签退功能：每台终端设备均具有签到、签退功能，保证交易的合法性。

使用权限及有效期识别：可设置 1—256 类卡，授予不同权限，满足不同消费对象或若干下属独立核算单位的类别管理。严密的有效期识别功能，能有效的防止过期卡片使用。

非法卡、黑卡报警功能：终端机广泛使用黑、白名单技术，对卡片进行合法性验证，并记录非法卡使用情况，有效防止非法卡片的流通。对黑卡以及各种非法卡使用状态，本机将自动识别并提示相应的报警代码，提示工作人员采取相应措施处理，防止的流通使用。

个人密码使用：可选使用，可设置消费与个人密码使用的对应关系。

逻辑开机锁：操作员可设置键盘锁定与开锁。

PSAM 卡接口：安全性达到金融级别要求。

终端设备子网采用星型拓扑结构：任何一台终端出现故障，都不影响其他设备及

整个系统。

存储数据：POS 机具中存放的消费明细是带消费交易认证码存放的，可以防止篡改。数据中心的数据加密存放，防止数据泄露。在终端设备比较集中的场所，如食堂等地方，均配置 UPS，在设备比较分散的地方，终端设备配置后备电池，以此保障终端设备在断电后能够继续运行使用。

7.4.3 消费交易的安全性

密钥管理：通过制定一套完整的密钥管理体系，来保证消费过程的安全性和终端机具使用的安全性。终端机具的密钥保存在 PSAM 卡中，无法读取，能够保障交易安全。

用户 IC 卡的合法性认证：当用户 IC 卡在 POS 终端上刷卡时，POS 终端首先需要验证 IC 卡的合法性。验证通过后,POS 终端需要进一步检查该 IC 卡是否在黑(白)名单中、是否为止付卡或过期卡等，若都不是，才确认该卡是合法的。

消费交易的安全性和完整性：用户 IC 卡 POS 终端之间进行双向身份认证，并且 IC 卡中每次消费额受到限制。

POS 终端使用的安全性：管理中心设置唯一的消费终端机具识别号。另外，为了防止伪造或非法使用 POS 终端，保证 POS 终端使用的安全感性，需要为每个合法操作员发放一张操作员卡，经过操作员卡后，POS 终端才能接受消费交易。

POS 中的消费数据的安全：POS 终端保存消费明细和该消费明细的消费交易认证码。进行数据采集时，将消费明细和消费交易认证码一起上传，结算中心可以对该消费交易认证码进行校验，以保证消费数据的真实性和完整性。

7.4.4 充值交易的安全性

IC 卡的联机合法性认证：充值交易采用联机交易。当 IC 卡在充值时，充值设备先进行初步认证，然后上传相应的卡信息和交易信息到管理中心，管理中心判断该 IC 卡是否在黑（白）名单中、是否为止付卡或过期卡等，若都不是，才确认该卡是合法的。

充值交易的安全性和完整性：用户 IC 卡和充值设备之间双向身份认证，并且 IC 卡中的余额设置上限。

7.5 网络安全体现设计

7.5.1 安全分析

根据"技术+实施+保证"的模式，从实体安全、平台安全、数据安全、通信安全、应用安全、运行安全、管理安全这七个层次对具有高等级安全要求的网络系统提出安全分析。

实体安全分析：实体安全是信息系统安全的基础。依据实体安全国家标准，将实施过程确定为以下检测与优化项目：机房安全、场地安全、机房环境/温度/湿度/电磁/噪声/防尘/静电/振动、建筑/防火/防雷/围墙/门禁、设施安全、设备可靠性、通信线路安全性、辐射控制与防泄露、动力、电源/空调、灾难预防与恢复等，检测优化实施过程按照国家相关标准和公安部的实体安全标准。

平台安全分析：平台安全泛指操作系统和通用基础服务安全，主要用于防范黑客攻击手段。目前市场上大多数安全产品均限于解决平台安全，我司以信息安全评估准则为依据，确定平台安全实施过程包括以下内容：操作系统漏洞检测与修复；Unix 系统、Windows 系统、网络协议、网络基础设施漏洞检测与修复；路由器、交换机、防火墙、通用基础应用程序漏洞检测与修复；数据库、Web/Ftp/Mail/DNS 等其他各种系统守护进程、网络安全产品部署。平台安全实施需要用到市场上常见的网络安全产品，主要包括防火墙、入侵检测、脆弱性扫描和防病毒产品、整体网络系统平台安全综合测试/模拟入侵与安全优化。

数据安全分析：为防止数据丢失、崩溃和被非法访问，我司以用户需求和数据安全实际威胁为依据，为保障数据安全提供如下实施内容：介质与载体安全保护、数据访问控制、系统数据访问控制检查、标识与鉴别、数据完整性、数据可用性、数据监控和审计、数据存储与备份安全。

通信安全分析：为防止系统之间通信的安全脆弱性威胁，我司以网络通信面临的实际威胁为依据，为保障系统之间通信的安全采取的措施有：通信线路和网络基础设施安全性测试与优化、安装网络加密设施、设置通信加密软件、设置身份鉴别机制、设置并测试安全通道、测试各项网络协议运行漏洞。

应用安全分析：应用安全可保障相关业务在计算机网络系统上安全运行，它的脆弱性可能给信息化系统带来致命威胁。我司以业务运行实际面临的威胁为依据，

为应用安全提供的评估措施有：业务软件的程序安全性测试(Bug 分析)、业务交往的防抵赖测试、业务资源的访问控制验证测试、业务实体的身份鉴别检测、业务现场的备份与恢复机制检查、业务数据的惟一性/一致性/防冲突检测、业务数据的保密性测试、业务系统的可靠性测试、业务系统的可用性测试。 测试实施后，可有针对性地为业务系统提供安全建议、修复方法、安全策略和安全管理规范。

运行安全分析：运行安全可保障系统的稳定性，较长时间内将网络系统的安全控制在一定范围内。我司为运行安全提供的实施措施有：应急处置机制和配套服务、网络系统安全性监测、网络安全产品运行监测、定期检查和评估、系统升级和补丁提供、跟踪最新安全漏洞、灾难恢复机制与预防、系统改造管理、网络安全专业技术咨询服务。运行安全是一项长期的服务，包含在网络安全系统工程的售后服务内。

管理安全分析：管理安全对以上各个层次的安全性提供管理机制，以网络系统的特点、实际条件和管理要求为依据，利用各种安全管理机制，为用户综合控制风险、降低损失和消耗，促进安全生产效益。我司为管理安全设置的机制有：人员管理、培训管理、应用系统管理、软件管理、设备管理、文档管理、数据管理、操作管理、运行管理、机房管理。

7.5.2 安全性规划

根据以上七个层次的安全分析，“城市公交一卡通系统”可从一卡通系统自身安全、一卡通网络与城域网安全、一卡通网络与银行网安全、一卡通与第三方接口安全性四方面进行安全规划。

7.5.2.1 一卡通系统自身安全

实体安全：机房建设的合理性及安全性是保障整个一卡通网络系统安全的前提。物理安全是保护计算机网络设备、设施以及其它媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏过程。我司将机房建设分为以下几个方面做为重点：防静电措施——静电引起的问题不仅硬件

人员很难查出，有时还会是软件人员误认为是软件故障，从而造成工作混乱。此外，静电通过人体对 计算机或其他设备放电时(即所谓的打火)当能量达到一定程度， 也会给人以触电的感觉，造成操作系统作维护人员的精神负担，影响工作效率。 对于计算机房的静电，我们采取以下措施：将计算机房内的所有设备的金属外壳统一接地（机房安全地），以防止计算机产生的静电累积；在计算机内安装高性能的防静电地板，地板贴面的阻率应在国家标准规定的 105－108 地板下的金属支架应进行多点有效接地(网状)最后接至大楼综合地或机房安全地；在机房区防静电地板下应铺设静电接地网（0.8×40 铜箔\镀锌钢板）间距为 600×600 方格，作良好的电气连接后接至大楼综合地或机房安全地。防雷措施——根据国际 GB50174—93《电子计算机房设计规范》，交流工作地、直流工作地、保护地、防雷地宜共用一组接地装置，其接地电阻按其中最小值要求确定。如果计算机系统直流地与其他地线分开接地，则两地极间应间隔 25 米；在动力室电源线总配电盘上安装并联式专用避雷器构成第一级衰减；在机房配电柜进线处，安装并联式电源避雷器构成第二级衰减； 机房布线不能延墙敷设，以防止雷击时墙内钢筋瞬间传导墙雷电流时,瞬间变化的磁场在机房内的线路上感应出瞬间的高脉冲浪涌电压把设备击坏。空气质量的控制——清新的新风提高机房的洁净度，使机房保证正压，并提供新鲜空气。新风应满足两个指标：其一，是每人每小时 40 立方米；其二，是应占空调系统总风量的 5~10%。本机房四周密封，新风极为重要。根据国家有关规范和标准规定，计算机房内应设排风系统，用以排可能出现的烟雾及灭火后出现的气体；电源的稳定性保证 ——建议在机房设置 UPS 电源，确保在断电情况下，UPS 能继续供电，保障系统的运行。

平台安全：操作系统漏洞检测与修复——对于我们选用的操作系统的安全防范可以采取如下策略：尽量采用安全性较高的网络操作系统并进行必要的安全配置、关闭一些起不常用却存在安全隐患的应用、对一些保存有用户信息及其口令的关键文件（如 UNIX 下：/.rhost、etc/host、passwd、shadow、group 等；Windows NT 下的 LMHOST、SAM 等）使用权限进行严格限制；加强口令字的使用（增加口令复杂程度、不要使用与用户身份有关的、容易猜测的信息作为口令），并及时给系统打补丁、系统内部的相互调用不对外公开。网络协议检测与修复——防止网络协议的脆弱性,保护所有可能的 Internet 相关威胁,扫描所有常用 Internet

协议，包括：HTTP，FTP，SMTP，POP3，IMAP，NNTP 及 SOCKS 等。各种系统守护进程的防护——在一卡通的应用系统安全上，应用服务器尽量不要开放一些没有经常用的协议及协议端口号。如文件服务等应用系统，可以关闭服务器上如 HTTP、FTP、TELNET、RLOGIN 等服务。还有就是加强登录身份认证。确保用户使用的合法性；并严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。充分利用操作系统和应用系统本身的日志功能，对用户所访问的信息做记录，为事后审查提供依据。交换机、防火墙漏洞检测与修复——将通过专业的检测软件对网络设备及系统进行漏洞检测。如防火墙回应 ICMP 时戳请求检测，防火墙回应 ICMP 子网掩码请求检测，防火墙接受 CONNECT 请求检测，防火墙接受 POST 请求检测等。

数据安全：数据访问控制措施——严格的管理制度，可制定的制度有：《用户授权实施细则》、《口令字及帐户管理规范》、《权限管理制度》、《安全责任制度》等。数据的机密性与完整性——病毒防护：网络系统中使用的操作系统一般均为 WINDOWS 系统，比较容易感染病毒。因此计算机病毒的防范也是网络安全建设中应该考虑的重要环节之一。软件保密：在传输协议上，采用金融报文交换格式 ISO 8583 标准，经过数字签名、DES、MD5 等加密措施，所有终端设备接入都采用动态密钥进行签到、签退。硬件保密：采用通过国家密码委认定的硬件产品—网络数据保护器（EPASS），内置多种加密算法，随机数生成器，三级权限安全文件系统。系统所有的业务进行前都必须通过 EPASS 的检验方可进行。达到应用环境的唯一性，从而加强系统的数据安全性。

通信安全：划分虚拟子网(VLAN)——一卡通的应用于将根据用户安全级别或者根据不同部门的安全需求，利用交换机来划分虚拟子网（VLAN），在没有配置路的情况下，不同虚拟子网间是不能够互相访问。配备防火墙——防火墙是实现网络安全最基本、最经济、最有效的安全措施之一。防火墙通过制定严格的安全策略实现内外网络或内部网络不同信任域之间的隔离与访问控制。并且防火墙可以实现单向或双向控制，对一些高层协议实现较细粒的访问控制。网络层加密——鉴于网络分布较广，网点较多，而且可能采用多种通讯线路。如果采用多种链路加密设备的设计方案则增加了系统投资费用，同时为系统维护、升级、扩展也带来了相应困难。因此在这种情况下我们建议采用网络层加密（VPN）。在“一卡通”

的设计中，网络服务器（LINE PORT）具有内置加密器，前置通信 PC 则安装硬件加密器（EPASS），所以两者在通信时会在形成网络层加密，保证数据的安全传输及防止黑客的入侵。IP 绑定——在“一卡通”系统里，对每个 IP 地址都进行与终端 MAC 地址的绑定，防止有恶意破坏者假冒 IP 入侵一卡通网络。入侵检测——防火墙虽然能抵御网络外部安全威胁，但对网络内部发起的攻击无能为力。动态地监测网络内部活动并做出及时的响应，就要依靠基于网络的实时入侵监测技术。监控网络上的数据流，从中检测出攻击的行为并给与响应和处理。实时入侵监测技术还能检测到绕过防火墙的攻击。

应用安全：内部资源共享——严格控制内部使用人员对网络共享资源的使用。在在一卡通内部子网中一般不要轻易开放共享目录，否则较容易因为疏忽而在交换信息时泄漏重要信息。对有经常交换信息需求的用户，在共享时也必须加上必要的口令认证机制，即只有通过口令的认证才允许访问数据。信息存储——对有涉及一卡通秘密信息的用户主机，使用者在应用过程中要做到尽量少开放一些不常用的网络服务。对数据库服务器中的数据库必须做安全备份。通过网络备份系统，可以对数据库进行备份存储。

运行安全：系统升级和补丁提供——定期对一卡通系统中的各种操作系统、应用程序进行升级和打补丁，避免 Bug 的出现。定期检查和评估——对一卡通的各种运行的程序进行定期的检查，及时发现问题及进行防治。

管理安全：制定健全的安全管理体制——制定健全的安全管理体制将是网络安全得以实现的重要保证。各使用部门可以根据自身的实际情况，制定如安全操作流程、安全事故的奖罚制度以及对任命安全管理人员的考查等。构建安全管理平台——构建安全管理平台将会降低很多因为无意的人为因素而造成的风险。构建安全管理平台从技术上如，组成安全管理子网，安装集中统一的安全管理软件，如病毒软件管理系统、网络设备管理系统以及网络安全设备统管理软件。通过安全管理平台实现全网的安全管理。增强人员的安全防范意识——一卡通管理机构应该经常对使用者进行网络安全防范意识的培训，全面提高使用者的整体网络安全防范意识。

7.5.2.2 一卡通网络与城域网的安全

网关防火墙的安全：防火墙既支持 Internet 网络的主要服务（如 WWW、E-mail、FTP、Telnet 等）和基于 TCP 协议的所有应用程序，又支持 UDP 一类的非连接协议的应用程序。而且，还支持数据库访问这样的商务应用程序和 Real Audio，VDOLive 和 Internet Phone 这样的多媒体应用程序。使用防火墙后不会出现服务失效的负作用。 采用透明防火墙技术，防火墙在网络中不可探测及访问，采用多级过滤措施，提供基于硬件地址、网络地址、TCP 端口和用户的鉴别和控制方式。 采用安全服务器网络技术，对用户的公开服务器实施保护。实时截获网络数据流，发现网络违规模式和未授权的网络访问尝试，根据安全设置做出反应，实时报警、事件日志。 作为网关型防火墙，对于应用层的支持是它的一大特色，对于常用高层应用（HTTP、FTP）做了更详细的控制，如 HTTP 命令级（GET、POST、HEAD）及 URL 级，FTP 级（GEI、PUT）及文件控制。作为一种安全防护，防火墙在网络中是众多攻击者的目标，必须有抗攻击能力，如 IP 地址假冒攻击，抗口令字探询攻击，抗网络安全性分析等。提供了较强的访问控制能力（如基于地址、协议、端口、用户、流量的访问控制），支持大量流行的应用和协议，对 IP 可以进行的包过滤包括：源 IP 地址、目的 IP 地址、协议类型（IP、ICMP、TCP、UDP）、源 TCP/UDP 端口、目的 TCP/UDP 端口、TCP 报文标志域、IP 分组分片标志等。NAT 在 IP 层上通过地址转换提供 IP 复用功能、解决 IP 地址不足问题，同时隐藏了内部网的结构，强化了内部网的安全。IP 映射功能，即反向 NAT 功能。是应用层网关的典型特点，如果希望内部网络中的服务器可以让 Internet 用户访问的话，可以利用反向 NAT 系统，为内部网络服务器作静态地址映射，这样 Internet 用户就可以通过防火墙系统直接访问服务器了。IP 与 MAC 地址绑定，防止 IP 假冒。IP 与 MAC 捆绑保护内部网某一台机器的 IP 地址不被另一台内部机器盗用。按照以往的经验，在网络的设计中，这是一个必不可少的需求。防止源 IP 地址欺骗，即防止通过修改 IP 地址方法对网络资源进行非授权访问。

端口的安全：端口就像一所房子（服务器）的几个门一样，不同的门通向不同的房间（服务器提供的不同服务）。我们常用的 FTP 默认端口为 21，而 WWW 网页一般默认端口是 80。但是有些马虎的网络管理员常常打开一些容易被侵入的端口服务，比如 139 等；还有一些木马程序，比如冰河、BO 等都是自动开辟一个不易

察觉的端口。所以我们建议在“一卡通”中把一些用不到的端口全部封锁起来，杜绝非法入侵。

一卡通网络与银行网的安全

一卡通系统与银行系统的应用将日益广泛。与此同时，网络的安全问题也越来越显得重要起来。在采用 PSTN/DDN 专线的基础上银行对接系统采用如下措施；

报文安全：关于涉及数据在公网或专网上传输，数据报文传输的安全，与银行前置机数据交换的安全主要由双向身份认证、加密和报文认证来保障。采用设立银行网关方式，双网卡隔离网段，杜绝校园网络对银行网络的访问，仅银行转账前置机可以访问银行网络。对传送的数据包加校验码（MAC 或 LRC）。对关键数据可进行加密处理。按银行要求将数据打包成 ISO8583 格式报文。

防火墙保护：在网络的对外出口处设置防火墙是理想的选择。防火墙在银行信息网中的安全防护原则：任何外部网络对银行信息网的内部情况"看不见"；外部非法入侵者及特殊信息"进不来"；机要敏感信息"拿不走"；任何的非法对外访问"出不去”

7.5.2.3 网络数据传输安全

系统中采用了 SSL 数字证书技术，SSL 证书通过在客户端和服务器之间建立一条 SSL 安全通道（Secure socket layer(SSL)安全协议，该安全协议主要用来提供对用户和服务器的认证，对传送的数据进行加密和隐藏，确保数据在传送中不被改变，即数据的完整性，实现数据信息在客户端和服务器之间的加密传输，可以防止数据信息的泄露，保证了双方传递信息的安全性。

7.5.2.4 第三方接口安全性

城市公交一卡通系统由多个子系统组成，接入并共享一卡通平台提供的资料，为了保证每一个子系统及终端设备接入的合法性与安全性，系统采取了严格的控制流程。每一个子系统都要通过系统授权、系统认证才能接入平台，使用一卡通资源。

系统授权：前置机为每一个子系统及终端设备建立授权注册信息，实现子系统授

权信息的安全传递与存储。信息包括：终端设备 ID 号、终端设备号。

交易：经过认证后的子系统及终端设备才能与中心数据库进行交易。如果不能进行认证进行交易申请，后台不会接受。

认证过程全部由一卡通统一接入接口自动完成，对子系统而言是透明的，没有因为流程的复杂增加了子系统接入的复杂度，但是通过以上措施却严格保证系统接入的安全。

7.6 软件安全体系设计

城市公交一卡通系统的应用程序软件安装在应用程序服务器上，在技术上是 J2EE 的三层结构，终端访问数据库服务器的时候，必须要经过应用程序软件这个中间层，所以应用程序软件与数据库的用户权限管理是不一样的。在用户管理、权限分级、程序资源、操作权限分配、登录控制、身份验证、密码控制、日志跟踪等方面设计了一套严密的机制。

系统操作权限：一卡通系统的典型应用涉及到十多个子系统的应用，往往系统的操作员涉及到数十甚至上百人。如此庞大数据的操作员的管理，需要很好的解决方案，才有可能达到系统安全、管理方便的目的。本系统采取设置分级管理。作为系统总管理员，只需管理各专业的分管理员即可，各级管理员可以在自己权限范围内进行权限的分配工作。例如，系统总管理员在系统中设置一个账务管理系统分管理员，同时赋与账务管理相关的系统操作权限，而不用关心账务系统的具体操作员；作为账务系统的分管理员，根据需要，设置领导、会计、出纳等操作员，同时将上级管理员所赋予的操作权限进行再次分配。在一卡通系统中，除了操作权限分级以外，同级操作员中，还存在数据的保护需求。对于金融交易数据，各营业商户之间的数据是互相保密的，采用部门隔离的处理办法，各商户只能查询到与该商户有关的交易数据。

敏感数据：在一卡通系统中涉及到很多的敏感数据，包括金融数据、单位密码、用户卡个人密码、系统操作员密码等，这些都需要严格保密的。在数据库的存储中，本系统采用密文形式进行保存。在数据加密方案中，本系统采用国际通用的 DES 算法。

软件运行：系统采用运行采用硬加密保护的主要目的是保证应用环境的唯一性，杜绝恶意的建立模拟的环境，尤其是数据环境，本系统采用 USB 接口的硬件加密器件 EPasss。Epass 是国家保密委认证通过、完全符合金融安全标准的产品。Epass 内置具有 MD5、哈希等多种国际标准算法，真随机数生成器，三级权限安全文件系统。在用户的系统运行开始，就自动将重要的保护参数写入 EPass 中；系统所有的业务进行前都必须通过 EPass 的检验方可进行。由于 Epass 不具有数据的复制功能，从而加强系统的数据安全性。

7.7 数据中心安全体现设计

7.7.1 数据库平台安全性规划及实施

数据库的安全性：Oracle 引入了虚拟数据库的概念大大简化了安全管理，这样可以使安全机制建立在数据之上而不是建立在每个访问数据库的应用程序之上。同时也提供了安全套接字层（SSL）和用户终端接入远程身份验证（RADIUS）协议适配器，所有这些都是为了保证校园间事务处理的安全性，包括了因特网上的事务处理。

数据加密与跟踪审查：数据库对重要数据、敏感数据进行加密，用密码存储数据，在存入时需加密，在查询时需要解密。跟踪审查是一种监视措施，它对保密数据，跟踪记录有关这些数据的访问活动。一旦发现潜在的窃密企图，DBMS 会自动发出警报，并把这些数据记录在日志文件中，供事后分析和调查。

访问控制安全性：数据库的访问控制：ORACLE 的访问控制共有三种：主机操作系统验证、网络验证、数据库验证。用户对数据库的访问权限控制。ORACLE 数据库多种数据备份方式，尤其是在线数据备份可保证系统 7*24 小时运行：可靠支持机制可实现数据库系统的快速灾难恢复，确保数据的绝对可靠

数据库模型安全性：设计数据库表时将重要数据同普通数据存放在不同的表中；重要的数据库表使用电子签名（防止有意篡该数据）；建立必要的视图，以隔离一些重要数据；设计必要的日志跟踪。

7.7.2 数据服务器安全性规划及实施

数据服务器，通过双机冗余软件实现 2 台数据服务器的冗余，确保 1 台数据服务器发生故障的时候，另一台服务器能取代，保障系统的安全运行。

磁盘阵列和磁带库作为数据存储和备份系统。备份可以实现高度自动化的热备份即实时备份，在遇到系统出现不稳定及灾难性崩溃时，能使“一卡通”里的各种数据及时恢复。服务器群里进行 VLAN 划分，应用服务器和数据服务器划分在同一 VLAN 段，应用服务器作为其中的中间层，又能和下面的终端划分为另外一个 VLAN 段，这样划分的目的，是保证下面的终端客户机不能直接访问数据服务器，只能通过应用服务器来访问，这样就确保了数据服务器里数据的。

7.7.3 数据备份设计

数据库运行有两种模式：非归档日志模式、归档日志模式，建议系统采用归档日志模式运行数据库。

建议一周做一次数据库完全备份，每天晚上或凌晨业务量较小的时候即数据库最闲的时候做一次差分备份，备份数据文件、归档日志到磁带中。这些备份数据可用磁带备份到远程的计算机系统中，请不要把已备份数据的磁带和当前数据库服务器放在同一个环境中。

7.7.3.1 物理备份设计

通过拷贝数据库文件的方式来备份数据库。系统中根据数据的重要性同时选用以下两种方法。

冷备份（脱机备份）：在正常的方式（shutdown normal /immediate）关闭数据库，在操作系统级的命令行上备份所有的数据文件（包括数据文件、联机重做日志文件和控制文件）；在归档日志模式下可以单独备份某个表空间。

热备份（联机备份）：只有数据库运行在归档模式下，才可以热备份表空间以及重做日志、控制文件。

7.7.3.2 逻辑备份设计

通过 Oracle 公司提供的工具（export）创建数据对象的逻辑拷贝，并将拷贝存入一个二进制文件。恢复时用 import 工具将导出的二进制文件导入到数据库中。解决了：

（1）当数据库文件的已分配的磁盘空间太大时，采用物理备份备份需要与当前数据库一样的磁盘空间，但是此时的数据并不多，采用物理备份并不合适，可能用 exp 工具导出的二进制数据文件，导出的文件就是数据记录占用的真正的空间，而不是已分配的空间。（有时数据库表空间可以在没有数据的情况下格式化一个区域出现存放数据，但是数据不一定填满，如果是物理备份，则在存放目的地要有与当前数据库相同的存储空间。而逻辑备份解决了这个问题。）同时我们还可以采用增量、差量备份手段提高备份的效率。

（2）不必担心数据文件所在的路径。

（3）经过全表数据扫描，可以检查出坏块。

遗留的问题主要有 2 个：A、不提供时间点恢复；B、只能恢复到自备份之前的数据，备份之后的数据将无法恢复。这些问题可以通过前面采用的归档日志模式来解决。

不管系统多么可靠，总会发生一些意想不到的事情，致使系统数据丢失。因此使用备份来保护数据不丢失是一种非常重要的手段，尤其在系统数据非常重要的时候。经常进行数据备份能够减少偶然破坏造成的损失，保证系统能够从错误中恢复正常运行。数据有备份后可以说是安全的，但这还是不够的，只有良好的备份策略才能确保数据的最终安全性，而且可以使整个数据备份工作变得合理而轻松。

在进行备份之前，首先要选择合适的备份策略，这将决定何时需要备份，以及出现故障时进行恢复的方式。通常使用的备份方式有三种：

完全备份(full backup)

每隔一定时间就对系统进行一次全面的备份，这样在备份间隔期间出现数据丢失等问题，可以使用上一次的备份数据恢复到前次备份时数据状况。

这种备份策略的好处是：当发生数据丢失的灾难时，只要用一盘磁带（即灾难发生最近的备份磁带），就可以恢复丢失的数据。然而它亦有不足之处，首先，

由于每天都对整个系统进行完全备份，造成备份的数据大量重复。这些重复的数据占用了大量的磁带空间，这对用户来说就意味着增加成本。其次，由于需要备份的数据量较大，因此备份所需的时间也就较长。如果业务繁忙、备份时间有限，选择这种备份策略是不明智的。

增量备份(incremental backup)

首先进行一次完全备份，然后每隔一个较短时间进行一次备份，但仅仅备份在这个期间更新或被修改的内容。这种备份策略的优点是节省了磁带空间，缩短了备份时间。但它的缺点在于，当灾难发生时，数据的恢复比较麻烦。例如，在系统崩溃时，需要拿出最近一次全备份作系统恢复；然后，按顺序依次对各个增量备份作恢复，如遇到某个增量备份磁带毁坏，则只能恢复到其上一个增量备份时的系统状态。

差分备份(differential backup)

在实际应用中，备份策略通常每天进行一次更新数据的备份。例如：管理员先在星期天进行一次系统完全备份，然后在接下来的几天里，管理员再将当天所有与星期天不同的数据（新的或修改过的）备份到磁带上。差分备份策略在避免了以上两种策略的缺陷的同时，又具有了它们的所有优点。首先，它无需每天都对系统做完全备份，因此备份所需时间短，并节省了磁带空间，其次，它的灾难恢复也很方便。系统管理员只需两盘磁带，即星期天磁带与灾难发生前一天的磁带，就可以将系统恢复。