随着各高校校园网的建成和投入使用，卡应用技术的日渐成熟为校园一卡通系统的建立提供了保障，校园内实现一卡通管理已成为校园管理发展的必然趋势。校园一卡通系统可以实现多种应用，给高校管理带来了方便。

基于数字化的校园一卡通平台研究

文/许 鑫 苏新宁 姚 瑶

随着高校信息化的推进，校园卡的应用也越来越广泛，由于大多校园应用系统互不相连，造成学生持有多张卡，给学生带来极大的不便。具体而言，学校的多种卡应用系统分别由学校内各部门根据自己的需求，独立引进并在本部门所辖范围内使用，各个部门采用系统的技术与规范也不统一，造成了各种卡应用系统无法兼容，资源不能合理配置和共享；同时学生手中的学生证卡、食堂饭卡、图书借阅卡、银行卡以及电话卡等等，除了使用不便以外，学校也难以统一管理，数据的一致性很差，造成不必要的混乱。

目前，随着各高校校园网的建成和投入使用，卡应用技术的日渐成熟为校园一卡通系统的建立提供了保障，校园内实现一卡通管理已成为校园管理发展的必然趋势。校园一卡通系统可以实现校园内的个人身份认证，体现以人为本的校园管理；校园一卡通系统还可以与学校管理信息系统连接，实现学生、教职员工的基本信息个人查询，领导与部门宏观管理的数据查询与综合分析等；校园一卡通系统与银行系统相衔接可以将银行存款自助圈存到校园卡，以实现校园内各类消费；校园一卡通的统一身份认证、统一信息查询及共享数据平台，最终将实现资源数字化、传输网络化，用户终端智能化，管理结算自动化的高校信息化目标。

新型的校园一卡通平台已经在诸多方面超越了传统的校园卡应用，具体而言，学生只需一张卡就可以在各个消费地点的POS机上刷卡付账，也可以在学校刷卡缴纳学费、转账缴纳学校的一切费用。校园一卡通亦可用作学生的身体档案，血型、体重、身高等基本资料及病历状况等均可记录在上面。校园一卡通还可代替学生证，把学籍基本信息记录在校园卡上，即有利于规范学籍管理，也可以为学校其他业务系统提供基础信息。

一卡通平台概述

一卡通平台与应用

计算机软硬件技术的发展，基于系统扩展性、安全性等方面的考虑，客观上要求实现平台层与应用层的分离，作为高校数字化校园建设中的重要组成部分，校园一卡通系统的建设也包含着一卡通平台的搭建和一卡通应用的完善两个方面的工作。

一卡通平台主要实现主干平台上的管理和服务，不少应用子系统的网络甚至是跨校区的，身份的控制和与银行电信的对接可以说是一卡通平台的关键。一卡通应用则是一个个的接收主干平台授权的管理信息系统，应用子系统主要通过驻留在底层的第三方接入程序与数据中心进行通讯以实现数据的共享，

这些应用子系统按照性质可以划分为：

商务消费类：如就餐、超市、饮水、复印、水控、电控等各类收费应用；

身份识别类：如考勤、门禁、通道机等各类验证身份的应用；

混合类：如图书、医疗、学籍教务等既要验证身份，又要进行收费结算的管理系统；

其他类：比如巡更管理系统，虽然也采用了射频卡和设备，但与一卡通平台系统没有直接的联系。

电子钱包

最早的一卡通平台是带有简单身份信息的消费一卡通。随着社会的进步与变革，各学校原有的消费和管理模式已不能适应新的发展要求，消费一卡通应运而生，消费一卡通即在学校内凡有现金、票证或需要识别身份的场合均采用卡来完成，此种管理模式代替了传统的消费管理模式，为学校管理带来了高效、方便与安全。学生可以在学校中一卡多用，一卡通用，在不同消费场合完成电子钱包的交易功能。

后来的消费一卡通完成了与银行系统的对接，通过自动圈存机，校园卡用户可以十分方便地将银行账户上的钱转存到校园卡账户上。其最大优势是电子支付手段和银行金融功能。电子支付手段可以实现在学校内的食堂吃饭、图书馆看书、电脑机房上网等消费支付；银行金融功能包括通存通兑、电话银行、网上银行、打折优惠、公交卡充值等。

对于校园卡和银行卡的结合，不仅仅是学校方面的业务需要，也是各家银行所大力追求的，其中的原因是多方面的。以中等规模的高校为例，从近期效益来看，每个学生一年的平均支出为6000元，1.5万名学生一年的银行平均沉淀资金就有近亿元。从远期效益看，经过几年的一卡通生活，大学生们肯定会对发卡银行产生良好的认同感，这种认同感将伴随他们走向社会，并促使他们继续成为该银行的银行卡的使用者。更重要的是高校对银行而言具有“低风险，高回报”的优势，高校是信誉最好的用户之一，而且随着教育产业的发展，科研经费、各种贷款也在不断增加，银行如果拿下了高校的金融一卡通项目，就等于拉近了与高校之间的关系，从而也更有机会获得各种金融服务的机会。

电子身份

电子钱包里的学生信息只是一些个人的简单信息，但是卡片做为一种很好的身份认证载体，其电子身份的功能变得越来越显著，通过校园统一身份认证平台与校园一卡通平台的结合完成各类身份与学校内各种各样管理信息系统的对接和扩展，以这样的方式同步身份信息，组织个人信息数据也可以比较好的维护数据的一致性，维护校园身份的唯一性。

不少学校已经考虑用校园卡取代学生证，改变管理形式。就以学生证为例，以前学生证都是手写或者打印的，学生从入学到毕业，经常需要到不同的部门办理各种手续，而每次填写的不外乎姓名、学号、性别、出生日期等信息。用校园一卡通系统之后，学生的身份信息都被存储在统一的身份服务器上，各个部门都可以共享，学生在办理手续时，只要一刷卡就可以了，这样不仅提高了学校的办事效率，还将彻底改变学校的管理方式。

电子档案

随着卡片容量的日益增大，卡片上能存储的信息也越来越多了，一是内容上，不仅仅是姓名学号等常规信息，甚至包括血型，或者一些应用子系统内的权限信息；二是格式上，可以是数字签名、各类证书或者图像信息，这样一些如指纹、虹膜类的个人生物信息也可以加入。这样一来，一张卡片其实就是一个人的个人档案了。

再有，随着CPU卡的应用，卡片中还可以包含一些简单的业务逻辑处理，在相关嵌入式程序的支持下，在卡片与读卡器的接触时甚至可以完成部分以前由终端计算机完成的业务逻辑处理。当然，这一步还远远没有达到。

常见一卡通平台分析

下面就以一个常见一卡通平台为例，分析其中核心的电子支付服务，包括电子支付应用服务器、电子支付平台应用系统、主要业务流程等。

电子支付应用服务器

一卡通数据库统一存放在数据中心，由于金额数据的重要性，在服务器中单独占用一个域。基于安全性问题，电子支付应用服务器一般采用Unix/Solaris平台，其上部署电子支付应用服务程序，然后通过各类前置机完成一卡通平台的使

用。

（1）综合前置机

综合前置机在技术构架中属于应用系统程序，在校园一卡通系统的逻辑构架中属于系统管理层，是一卡通系统的控制中心、安全中心和同步中心。综合前置机的运行环境可以采用Windows操作系统，但一般要求本机安装加密卡，配置通用读卡器。

综合前置机的主要功能包括：

负责控制后台状态。对后台自动或者手动发出日结、开工指令，以控制后台的正常交易、正在日结和日结完成状态。

负责同步白名单。从UNIX后台服务接收最新增加、变动或删除的白名单，并把它们实时准确地同步到各个在线处理机。

负责全系统的安全管理，是系统的安全中心。负责全系统各个接入子系统的安全性控制、密钥的产生与更新管理。

综合前置机一般具有同步白名单，实时、准确、迅速；具有多种调试方式，便于对出现的错误快速发现和解决；全天候24小时无人职守运行；可以灵活设置各种参数以提高综合前置机系统的性能；日志记录详细等特点。图1是一个综合前置机的程序结构。

（2）转账前置机

转账前置机为与银行通讯的专用前置机、自助转账终端形成银行转账系统。银行实时转账系统是利用计算机网络和终端设备实现持卡人银行账户资金向校园一卡通账户划转的系统，它将校园一卡通系统原有手工现金存款方式转变为持卡人自助操作的银行卡与校园一卡通之间资金转账，减少现金流动，延长服务时间，方便了持卡人，同时也是银行拓展业务、以低成本带来高效益的有效手段。主要功能为实时响应自助转账终端的转账请求，通过DDN/ISDN专线连接到银行网络，完成持卡人实时自助转账任务；转账前置机需要安装加密卡。

转账前置机完成的任务包括：银行卡向校园卡单向转账功能、银行卡账户余额查询、校园卡账户余额查询、校园卡挂失解挂功能、更改校园卡账户密码功能、更改校园卡消费密码和查询密码、校园卡代收代缴功能、自助转账终端（圈存机）的接入认证等。

转账前置机与银行联接的方式采用专线方式，同时考虑银行网端应与校方网端分开，在银行前置机上加装两块网卡，分别对应校内和银行两个IP地址，通过双网卡及关闭非安全端口等方式，可以屏蔽银行端和校园端的随意互访，保证了双方各自的安全性。

（3）身份前置机

身份前置机系统完成统一身份认证中心与一卡通身份信息的同步，同时也负责一卡通自身身份数据的维护。可以用来监视各个身份客户端操作的记录，显示后台服务和第三方代理的运行状态是否正常。

身份前置系统为一卡通金融系统及其他子系统提供提供基础数据。身份前置系统的功能和特点包括：

快捷的安装配置，真正实现“傻瓜化”；

系统升级简单，维护方便；

具有广泛、统一的接口支持，大部分基础信息均采用国标/教育信息标准；

能根据用户自定义进行数据的导入/导出，完全不受格式的限制；

相片采集方式灵活，可以支持摄像头、扫描仪等采集的照片，并能进行二次编辑；

安全方便的照片存取方式，能根据用户的习惯进行个性设置；

系统具有较强的适应性，能根据用户需要进行卡样设计，并具有科学合理的开户流程；

具有全局唯一性的基本配置信

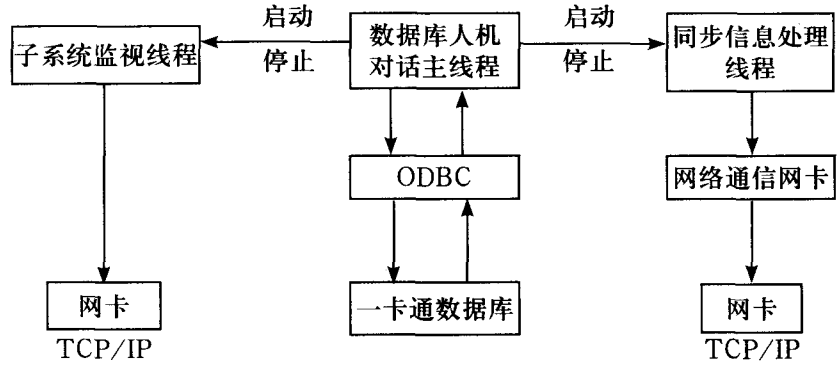


图1 综合前置机的程序结构

息，并能实时同步到各个子系统；

能根据不同的组合进行全方位的数据查询，并实现所见即所得的打印效果；

具有科学、具体、全面的操作员权限划分，对数据维护更安全；

具有全局性、及时性身份功能启用/禁用功能，更能体现一卡通身份的门户地位。

电子支付平台应用系统

（1）综合业务子系统

综合业务子系统作为一卡通系统的必要系统之一，部署在各校区的人工网点内，数量不受限制。相当于银行的人工网点的电子柜员系统，使用者是一卡通业务的运营部门。其功能一方面主要是面向持卡人的账户、卡片进行管理和服务，另一方面是面向商户账户进行管理和服务。可以完成开户处理（对经过审核的身份信息进行开户），普通账户处理（包括对普通持卡人账户进行查询、冻结、解冻、挂失、解挂、销户、充值、取款、变更、换卡、打印、修改查询密码、修改卡内密码、转账等），持卡人账户的补助、扣款（包括个别、批量、零散等方式），商户账户的维护和管理（包括开户、销户、冻结、解冻、信息变更、换卡、流水查询等），商户存取款及两个商户之间的转账，账户分析（包括国家统计、民族统计、部门统计、身份统计、总体情况统计分析等），账户管理参数设置（各种补助的发放设置、手续费设置、押金设置等），设置操作员的权限（不同等级的操作员只能根据设置的功能权限来使用部分功能），其他诸如系统锁定、操作员修改密码、系统设置、帮助文档等功能。

（2）银行转账子系统

银行转账子系统是利用计算机网络和终端设备实现持卡人银行账户资金向校园卡账户划转的系统，它将校园卡系统原有手工现金存款方式转变为持卡人自助操作的银行卡与校园卡之间资金转账，减少现金流动，延长服务时间，方便了持卡人，同时也是银行拓展业务、以低成本带来高效益的有效手段。银行转账子系统的应用会给银行、一卡通用户、持卡人三方带来很多益处。

银行转账系统由分别放置在学校和银行的前置机和散布在校园内的转账终端（又叫圈存机）以及通讯网络组成。前置机是连接银行与一卡通系统的关键枢纽。数据对比的工作流程图如图2。

可以在学校端和银行端各设一台前置机，两台前置机之间采用DDN专线或拨号方式进行短连接，采用TCP/IP协议，通过应用层的报文交换实现转账交易。每台前置机均设两块网卡，一块网卡接内部网络，另一块网卡接专线的路由器。通过两块网卡的设置在逻辑上隔离内部网络和外部网络，提高了系统的安全性。

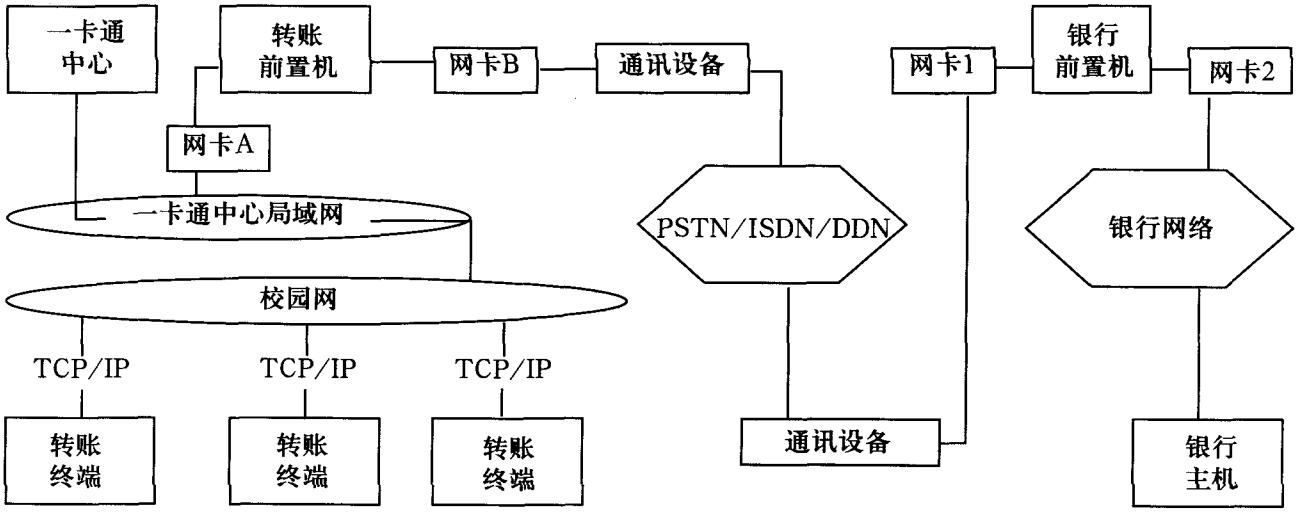


图2　数据对比的工作流程

(3) 人工充值系统

人工充值是银行转账和圈存系统的重要补充手段，系统提供在综合业务子系统或在单独的以太网POS机上的手工充值功能，将持卡人的现金存入卡片。

充值是综合业务子系统中的一个基本功能，在此不进行详细介绍，下面仅介绍一下以太网POS的充值方法。以太网POS是为零散型消费点制作的一款终端设备，它既可以用来消费又可以进行充值，而且可以在网络出现故障的情况下独立工作，脱机流水至少可达5000笔以上，它的特点是方便、灵活、可靠。以太网POS中内置微型打印机，可打印销售收据和统计报表。它的组成结构包括网卡模块、读卡模块和主体部分，其中主体部分又包含主程序模块和打印、显示、键盘等。它的存款流程如图3所示。

主要业务流程

(1) 身份信息同步

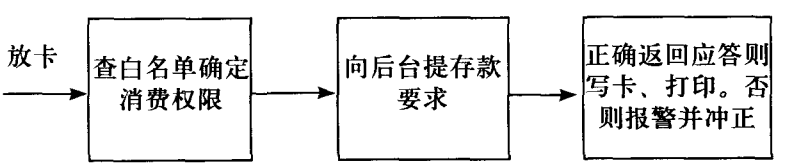


图3 以太网POS存款流程

身份信息同步是由统一身份认证中心发起，一卡通系统通过WebServices获得变更的身份数据。一卡通系统需要判断此身份信息的变更是否影响黑、白名单的变更，如果是，则产生黑、白名单的同步任务并发送到综合前置机上。

(2) 黑白名单同步

综合前置机收到黑白名单的任务后，会根据当前各应用系统在线的情况产生同步通知。对于离线的应用系统会自动保存一个未达任务，待应用上线后，再进行同步。网关收到来自综合前置机的黑白名单的同步后，更新本机的黑白名单库，并下发至各POS机。同步服务器收到黑白名单的同步后，会检查它所管辖的区域内的应用系统的运行状态，如果是在线的，则立即同步给应用系统，如果是脱网的，则生成一个未达任务，待应用联线时，再行同步。

(3) 交易业务流水

首先是各消费终端点产生交易流水；各终端点向其上位机发送交易流水，如果是网关下的终端设备则向网关汇集，如果是应用子系统，则根据配置可能向代理服务器或是同步服务器汇集，也可能直接向后台服务发送；网关或是代理服务器将交易流水汇集后，集中向后台服务进行传送。可以选定一定的汇集策略，比如在5秒内满1K数据，则立即上传，超出5秒后，不论有多少数据都立即上传。对于现金充值交易，不合并，必须实时在线交易，并且保证每笔交易完成后，才能进行下一笔交易。

(4) 银行自动转账

银行自动转账是对自助转账的一种补充，在技术上实现上一般有两种方式。

第一种方式：定时自动转账。这种方式的实质是，系统在设定的时刻检查所有账户，并且对低于某个数值的账户产生一个转账请求，转账请求通过批量的方式传给银行业务系统进行处理，处理成功的账户按补助方式进行处理，并且在下一次卡片消费的同时，写入到卡片中。

第二种方式：触发式自动转账。这种方式的理论是，只有卡片消费，它的余额才可能低于某个限额。那么在卡片每次消费后，系统应该检查该账户的余额是否低于限额，如果是，则触发自动转账服务进行银行转账，在卡片下一次的消费时，钱额就会写入到卡片中。

两种方式的比较是：第一种方式实现简单，对银行服务的响应不敏感，缺点是时间跨度大；第二种方式实现复杂，对银行服务的实时性要求高，优点是真正做到了自动转账。图4是银行转账业务的一个示意图。

(5) 圈存流程

自助实时转账业务：持卡人利用自助转账终端完成银行卡向校园卡的资金划转。自助实时转账业务流程如图5。

一卡通平台接入方案

目前学校在管理方面已经应用了较为成熟且专业的应用管理系统，如：图书管理系统、教务管理系统等，并且一些专业的生产厂家在某些方面已经开发出了较为成熟的应用系统，为了保护学校前期的投资和系统平滑升级，一卡通平台还应为所有一卡通的应用开发商提供通用接口。通过该接口，第三应

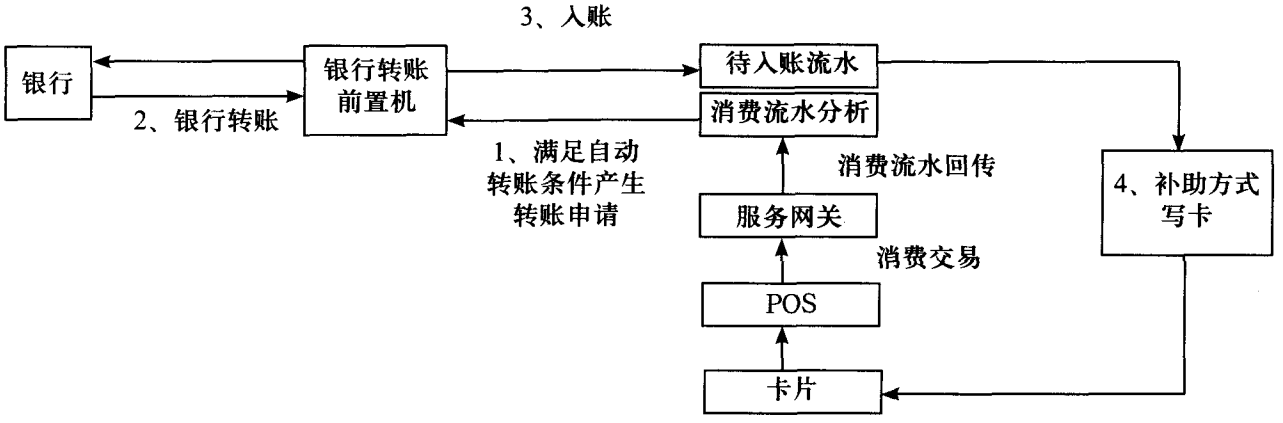


图4　银行转账业务示意图

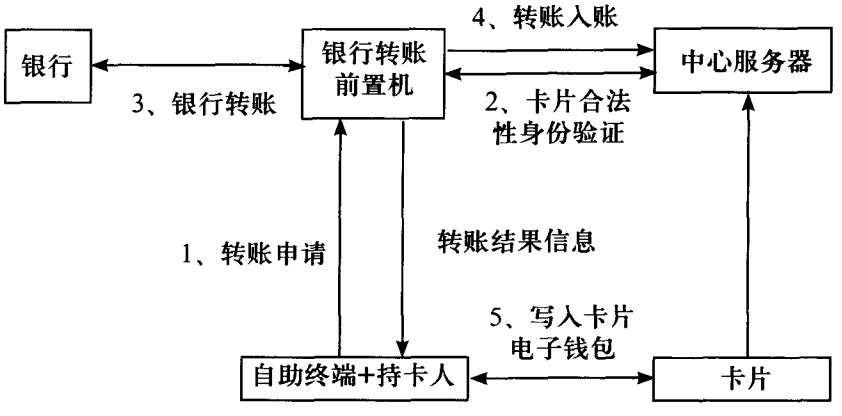


图5　自助实时转账业务流程

用程序可以使用一卡通的账户信息，读写校园卡，利用一卡通进行消费和结算，甚至接受一卡通的管理。

接口套件由PSAM卡、通用读卡器、服务驻留程序等组成，对于需要接入一卡通平台的系统，在计算机中插入PSAM加密卡，接入通用读卡器，安装服务驱动程序，在系统底层就驻留了连通一卡通中心数据库提取持卡人信息、回传消费流水账、自动维护白名单信息的程序。第三方子系统只要能够调用该服务程序就可以成为一卡通平台系统中的一个应用子系统。在一卡通系统中，第三方的接入是采用代理服务器机制来实现的。有以下模式：紧耦合、松耦合、不耦合模式，第三方子系统可以以三种耦合程序连接一卡通平台。

1、紧耦合模式

此方式完全符合一卡通系统的总体设计目标，由第三方产品提供商或客户根据一卡通平台提供的应用程序接口API进行原系统的改造。API接口形式可以根据第三方产品的实际情况进行调整，采用标准的Web Services或是自定义的基于TCP/IP的数据包交互。

第三方应用程序接口API主要包括：进行日间业务的函数、操作员签到/签退、操作员改密、操作员统计、开通/关闭（相对于开通操作的反操作）、查询、挂失/解挂、转账、改密、撤消操作、对流水账等。

2、松耦合模式

此方式不完全符合一卡通系统的总设计目标，但它对系统的改造要求相对较小，互联的实质是实现一卡多用。

互联的具体方法有两种：第一种方式，在卡片上提供应用区，供第三方读写使用；第二种方式，在卡片上提供一个应用区，供第三方只读使用。

3、不耦合模式

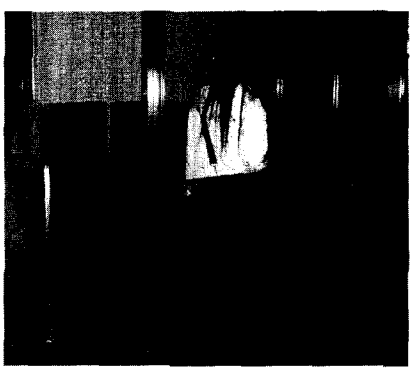
不耦合是指仅仅在形式上使用同一张卡片，应用子系统与一卡通平台不发生任何关系，卡片占用其中的独立扇区作为卡号或独立的小钱包，形成“一卡多用”、“小钱

包”式应用。

采用小钱包的方式，包括自助复印机、校内公交车、自助洗衣机、饮水机等，这些设备只扣除小钱包中的金额，不回传流水，不联网，可以非常方便地布置在校区内不易布线的地方。

共享数据组织

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，做到一人一卡、一人一户，所有数据的变更都做到全网立即生效。在共享数据的组织上，除了实现消费一卡通和身份识别一卡通外，更主要的是实现与各子系统的挂接与捆绑，包括与传统售饭系统平稳过渡，减少投资；数字化校园建设中的其他MIS系统、OA系统，可以通过平台预留的扩展接口实现与校园卡系统的数据共享；取代各校区原有的各类借书证、卡，实现与图书馆管理系统、电子阅览室等系统的对接连通，做到系统软件直接扣除罚款的紧耦合连接；实现与教务管理系统的对接，实现学生按学期的学籍注册管理，实现教学资源、生活设施的使用控制；实现宿舍楼、学生公寓的用电控制管理、公共浴池的用水控制管理；



在不同操作系统、不同数据库基础上构建开发的公用机房上机收费管理、校医院挂号收费管理、宿舍楼出入门禁、教职工考勤管理、学籍管理、安全保卫的巡更管理等第三方子系统，都可以实现与一卡通系统的挂接与捆绑。

就以学生离校为例，该年度毕业学生的名单一经提交，一卡通身份相关的学生信息发生了变化，此时可以通过一卡通平台提供的数据的导入导出接口，利用已经变更后的数据为其它MIS系统提供系统相关数据并触发有关事务，如学校财务系统中的学生账户的结算、图书馆管理系统的借阅禁用、各类门禁的停用等等。利用前面提到的诸如身份同步、黑白名单等机制就可以保证数据的一致，再通过集中-分发模式就可以实现不同应用系统的相同数据集成，进而完成对共享数据的组织。

越来越多的学校开始建设和应用校园一卡通了，但是，不但建设有多种模式，而且其后续管理也是一项复杂的工程，需要注意解决一系列的问题。在建设模式中就包括开发模式、资金筹集模式、网络建设模式、用卡模式等，这些都是需要我们进行深入研究和比较的。比如在开发模式上，就有“银校合作”和“校银企”两种模式可供选择，前者一般首先对银行招标，再由中标银行选集成商开发；后者分别对银行和集成商招标，受银行限制不大。再比如网络建设模式和用卡模式，有的院校铺设了一卡通专网，有的则利用了校园网，这两种方案又是各有利弊，使用专用网可以使系统运行更可靠更安全，方便保证数据完整性，易操作易维护，但专用网络铺设成本相对较高；在用卡上又有些院校实现“两卡统一，物理分离”（即银行卡与校园卡物理上分开，但逻辑上统一、有机结合），有些实现“一卡”（银行金融卡和校园IC卡合二为一）。各种模式的选择都需要学校的斟酌，都需要和银行以及集成商之间做好沟通工作。

校园一卡通工程的建设和其他大型信息平台的建设一样，都要做到整体规划、分期实施、逐步完善、规范管理这几点。首先应在全面论证、做好需求分析的基础上，制定学校校园一卡通系统建设的技术方案和整体规划，考虑资金投入以及目前学校相关的管理子系统的现状，在具体实施上，实行分期实施、逐步到位。同时，考虑银行的投入，能够在前期实现的功能就应当尽早完成。要理顺全校内各项操作的规范要求，建立完善的系列执行制度，以促进学校管理的科学化、规范化建设。同时，要适当调整学校的原有政策和制度，适度考虑学校有关部门的利益，以减少校园一卡通建设过程中的阻力。

校园一卡通工程是数字化校园建设的基础工程，可以通过校园一卡通的建设，逐步形成全校范围的数字空间和共享环境。校园一卡通系统各项功能的实现，不但会为学校师生员工提供极大方便，同时也会极大地提升学校的管理水平和科学决策水平，成为学校实现现代化管理的标志。