南京理工大学紫金学院智慧校园建设项目需求及技术参数

# 项目内容

|  |  |
| --- | --- |
| **序号** | **项目内容** |
| 一 | 学校统一身份认证管理平台 |
| 二 | 虚拟校园卡平台 |
| 三 | 聚合支付系统建设 |
| 除具备基础功能外，还需完成与现有系统的对接：  1、与汇文图书管理系统对接，实现虚拟卡借还功能；  2、与图书馆苏亚星机房管理系统对接；  3、与教务处系统对接  4、与财务收缴系统（杭州银行缴费平台）对接  5、与总务水电缴费系统对接  6、全校食堂、商铺聚合支付平台及配套消费POS硬件。 |
| 四 | 校园人脸识别管理平台 |
| 1、南大门1组人脸识别双向双通道闸机、西门1组人脸识别双向单通道闸机；6套人脸识别门禁，校外人员读身份证登记进出（访客系统）  2、图书馆1组单进向三通道闸机改造（3套人脸识别门禁）  3、实验楼（A、B、C、D）4个门；（4套人脸识别门禁） |
| 五 | 泛门禁管理平台（具备宿舍管理系统功能） |
| 宿舍区域12个门（A区1个、B区4个、C、D区7个）、34栋宿舍楼（A区7栋、B区9栋、C区9栋、D区8栋、教师公寓1栋）；（46套虚拟卡门禁） |
| 六 | 学校移动端应用平台对接（钉钉、微信公众号） |

# 设备清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备属性 | 产品名称 | 数量 | 单位 |
| 1 | 软件 | 学校统一身份认证平台 | 1 | 套 |
| 2 | 软件 | 校园虚拟卡管理平台 | 1 | 套 |
| 3 | 软件 | 聚合支付系统建设 | 1 | 套 |
| 4 | 软件 | 校园人脸管理平台 | 1 | 套 |
| 5 | 软件 | 泛门禁管理系统 | 1 | 套 |
| 6 | 软件 | 移动端应用平台对接 | 1 | 项 |
| 7 | 软件 | 第三方对接 | 1 | 项 |
| 8 | 硬件 | 加密机 | 1 | 台 |
| 9 | 硬件 | 系统U-KEY | 1 | 块 |
| 10 | 硬件 | 虚拟校园卡读写卡器 | 6 | 台 |
| 11 | 硬件 | 智能POS终端 | 160 | 台 |
| 12 | 硬件 | 门禁控制器 | 46 | 台 |
| 13 | 硬件 | 虚拟卡门禁读卡器 | 46 | 台 |
| 14 | 硬件 | 电磁锁 | 50 | 台 |
| 15 | 硬件 | 翼闸单机芯通道 | 6 | 台 |
| 16 | 硬件 | 翼闸双机芯通道 | 3 | 台 |
| 17 | 硬件 | 人脸识别平板 | 13 | 台 |
| 18 | 硬件 | 身份证读卡器 | 6 | 台 |
| 19 | 硬件 | 线材、辅材 | 1 | 项 |
| 20 | 软件 | 项目实施及调试 | 1 | 项 |

# 项目建设要求

## 学校统一身份认证管理平台

### 用户中心

用户中心解决了用户账号统一管理的问题，采取从分散到集中的管理思路，将过去分散到各个业务系统中的用户进行集中管理，并提供接口使业务系统和用户中心系统的信息保持同步。

从建设内容与功能来说，用户中心应至少包括以下主要内容：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 功能模块 | 详细功能 | 描述 |
| 1 | 登录激活 | 用户登录 | 用户登录提供给用户多种方式登录用户中心系统，用户可以输入基本信息登录，例如:账号，安全手机，安全邮箱，证件号码，动态口令，除此之外，还可使用绑定成功的联合账号进行登录，联合账号登录支持：钉钉，微信等。 |
| 用户激活 | 用户激活是操作了系统中账号信息的状态,使账号处于开放正常状态,获得系统使用权，成为系统的合法用户。在用户中心的登录界面中，设置了用户激活的操作，用于激活用户状态。 |
| 找回密码 | 当用户在登录系统时忘记了密码或者输入密码有误的情况下，可以使用系统登录界面提供找回密码来完成对新密码的重置操作。  找回密码的前提条件是系统中已经有该用户账号且账号状态正常，找回密码的流程：用户首先输入账号，系统进行身份信息验证（输入账号是否与系统中账号一致，状态是否激活等），如果账号信息一致，则进入用户身份安全验证，安全验证成功后输入新密码，完成新密码设置，系统自动记录找回密码的操作日志。 |
| 2 | 个人中心 | 个人信息 | 应包括3个层面的含义：1.用户基础信息，包括姓名、性别、证件类型、证件号码等等，这些信息不涉及安全登录，可以作为用户登录帐号信息的生成来源。2.用户的联系信息，包括安全手机，安全邮箱和家庭地址，这些信息涉及到用户的安全身份验证；3.用户的帐号信息，包括登录帐号、密码、账号有效期、账号状态等，这些信息涉及用户安全登录，在进行用户认证时，构成校验信息的主体。 |
| 安全设置 | 为了更好的保护账号信息，系统用户登陆后，需要给用户提供一个个人安全设置中心，包括密码修改，安全手机、安全邮箱等相关设置，加强对账号的安全性 |
| 联合登录设置 | 为了提升用户体验，令登录操作省时高效，系统为用户提供社区账号登录的方式：微信、钉钉等，用户的社区账号通过在联合登录设置模块进行绑定或解绑操作。 |
| 3 | 系统管理 | 字典管理 | 包含性别类型、证件类型、部门类型等通用字典，由系统管理员在后台进行数据字典维护，如果用户需要增加或变更配置项，只需修改数据字典表的记录即可，不需要修改程序代码 |
| 用户登录方式管理 | 为了方便用户登录方式可维护性及可扩展性，提供给管理员多种用户登录方式的配置，用户登录方式管理模块包括基本信息和联合账号登录管理，其中，基础信息登录包括帐号登录、安全手机、安全邮箱、证件号码、动态口令；联合帐号登录方式支持微信、钉钉等。 |
| 用户激活方式管理 | 系统管理模块提供给系统管理员选择用户激活方式的操作，在用户账号的激活过程中，指定实名认证的激活方式，保障了激活账号身份的真实性和完整性。 |
| 身份类型管理 | 身份类型是作为用户账号的重要属性，用于区分用户的身份信息，对于不同用户身份有不同的定义，身份类型分两级，即身份大类和身份小类。通过定义身份类型，提升了系统的可扩展性和易用性 |
| 组织机构管理 | 对于用户所在的组织机构信息进行维护管理，为了保证数据的一致性和完整性，该模块针对于临时的组织机构进行维护管理，通常根据实际需求用于维护临时增加的组织机构。 |
| 人员管理 | 为了保证数据的一致性和完整性，人员管理仅针对于临时的组织机构管理下的人员信息进行维护管理。系统管理员可根据需求对临时组织机构大类下的人员信息进行增、删、改、查等操作。账号信息的状态有：正常，未激活，冻结，注销。 |
| 标签管理 | 为用户设计不同的标签，将用户账号按标签分类，实现对用户进行快速检索，通过访问不同的标签，快速检索查找和定位用户。 |

### 认证中心

以认证服务为基础的统一身份认证体系，将组织信息、用户信息统一存储，进行分级授权和集中身份认证，规范应用系统的用户认证方式。提高应用系统的安全性和用户使用的方便性，实现全部应用的单点登录。从建设内容与功能来说，认证中心应至少包括以下主要内容：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 功能模块 | 详细功能 | 描述 |
| 1 | 认证基础服务 | 认证服务 | 提供认证平台的认证基础服务，主要实现如下业务功能要求：  1.支持多种设备的认证，包括PC设备、移动设备、多媒体设备等  2.能够实现对用户身份的识别，及单点登录，提供对多账号的选择切换 |
| 传输安全协议 | 支持SSL安全传输协议，保证用户登录信息在传输过程中的安全性 |
| 用户账号同步 | 认证服务中用户数据采用访问和调用用户管理提供的API方式，从用户管理服务中获取，从而确保用户数据的一致性 |
| 2 | 集成接口 | | 为外部应用实现统一认证和单点登录提供接口和通道，能将各类应用纳入认证范围，实现集中统一的认证。主要实现如下业务功能需求：  1.支持跨平台和多语言（DOTNET、JAVA、PHP）的外部应用  2.将集成接口注入到开放平台的基础能力中，通过开放平台的基础能力方式对外提供服务  3.提供跨平台和多语言的对接文档规范，并提供demo和下载功能 |
| 3 | 登录 | | 支持多种方式登录系统：  1.用户可以通过填写登录账号、密码、手机验证码的方式登录认证系统，验证码可以是数字，图片或其他形式；  2.根据二维码进行扫码登录  3.提供联合登录，用户可以通过微信、钉钉等方式，通过二维码扫描登录系统。  4.支持手机动态验证码登录 |
| 4 | 登录方式配置 | | 配置可允许的登录方式，包括普通登录和联合登录：  1.联合登录：对微信、钉钉进行启用或停用。  2.普通登录：账号(默认必须)、手机号码、证件号码、邮箱等进行启用或停用。  3.扫码登录配置  4.手机动态验证登录配置 |
| 5 | 安全策略配置 | | 配置安全认证访问策略，包括登录频数设置和账号冻结设置：  1.登录频数设置包括冻结账号、锁定IP；冻结账号指访问认证服务次数超过已设定最小临界值（非闭区间）。锁定IP规则是指在设定时间内，访问认证服务次数超过已设定的最小临界值（非闭区间）。  2.账号冻结是指用户在认证登录界面输入密码次数超过已设定的临界值（非闭区间） |
| 6 | 日志管理 | 登录日志 | 记录用户登录、登出系统的行为记录 |
| 操作日志 | 记录用户的操作行为信息 |
| 警告日志 | 记录系统使用过程中，发生的系统警告异常信息 |
| 错误日志 | 记录系统使用过程中发生的系统异常错误的详细信息 |
| 日志归档 | 定期手动或自动归档日志 |
| 7 | 认证统计分析 | | 统计系统的访问情况，给学校管理者提供不同维度的数据分析；包括：  1.当前在线用户  2.异常登录用户数【可钻取名单】  3.当日访问人数【按用户计算，1个用户当日访问系统算1次】  4.当日访问人次【按用户计算，1个用户当日每登陆访问系统1次算1次】、  5.活跃用户人数【近7天内登陆的用户数】  6.用户访问人数和人次的曲线图【分为近24小时、7天、近30天】  7.人员活跃度统计：近7天访问人次的top50排行【按人员身份统计】 |

### 权限中心

权限服务的权限体系以角色为核心，角色的定义由各应用或服务开发时定义，可以通过授权服务提供的API，将各应用的角色信息，同步到本授权平台。通过本平台实现对应用的统一授权和监控。从建设内容与功能来说，权限中心应至少包括以下主要内容：

|  |  |  |
| --- | --- | --- |
| 序号 | 功能模块 | 描述 |
| 1 | 应用角色管理 | 提供对应用角色的统一查询和授权管理 |
| 2 | 角色组管理 | 为了提高授权的便捷性，将不同应用的具有相同岗位特性的一类角色进行分组，提高授权的便捷性。主要功能包括角色组的创建、修改以及角色组包含的角色、授权的成员名单管理等。 |
| 3 | 分级授权管理 | 鉴于授权服务支持对全校所有应用的统一授权，为了提高授权的效率，降低执行的难度，对授权服务提供分级管理功能，设置分级管理员，可以根据实际情况，支持多层级的分级管理。  分级授权主要功能包括分级授权的人员管理、各人员的授权权限设置和管理权限设置等。 |
| 4 | 用户授权管理 | 提供面向多种方式的授权方式，包括按角色授权、按角色组授权；并且支持批量授权和批量导入授权等 |
| 5 | 账号授权审计 | 以账号为审计对象，对账号的权限进行审计，包括账号拥有的权限（角色、角色组）、账号拥有的管理权限（授权权限、管理权限）、账号的授权历史信息和操作日志等。 |
| 6 | 角色/角色组授权审计 | 以角色和角色组为审计对象，对角色的授权用户清单、角色授权日志，归属角色组信息进行审计；对角色组的授权用户情况、授权日志情况、拥有的角色情况等信息进行审计 |
| 7 | 操作日志审计 | 对授权的操作日志进行查询，可以按授权人、被授权人、授权时间段、授权的权限以及授权应用等多个维度进行日志的审计查询 |
| 8 | 认证授权日志 | 为确保对用户的授予权限和实际访问过程中通过认证获取的权限一致，提供了认证授权日志的审计查询功能 |
| 9 | 授权监控统计 | 对授权结果进行监控和统计，包括当前授权接入的应用数、角色数、角色组数以及未授权的角色和角色组信息；能够统计各应用的授权情况、角色的授权情况和近30日的授权变更操作情况等信息 |

### 日程服务

为学校各应用提供统一的个人日程、部门日程、系统日程的维护和管理。从建设内容与功能来说，日程服务应至少包括以下主要内容：

|  |  |  |
| --- | --- | --- |
| 序号 | 功能模块 | 描述 |
| 1 | 个人日程 | 个人日程的管理维护功能，提供用户创建新的日程、订阅公共日程、按天、周、月、年查看所创建和订阅的日程信息 |
| 2 | 部门日程 | 管理员注入的部门公共日历、日程的维护编辑功能，如部门的周工作计划等，相应的部门普通用户可以选择订阅部门公共日历 |
| 3 | 系统日程 | 管理员注入的系统公共日历、日程的维护编辑功能，如：校历等，相应的全校师生用户可以选择订阅系统日历 |

### 消息中心

从建设内容与功能来说，消息中心应至少包括以下主要内容：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 功能模块 | 详细功能 | 描述 |
| 1 | 消息消费管理 | 消息接收设置 | 消息消费者可以根据消息的接收方式，设置消息接收策略。包括：  1、微信消息的免打扰时间设置。  2、短信消息的免打扰时间设置  3、针对不同的消息类型，勾选不同的消息接收方式。 |
| 消息接收管理 | 消息消费者可以查阅各类消息内容，对各类消息进行处理，包括删除等。 |
| 2 | 消息生产管理 | 通讯录管理 | 消息发送人员，可以根据自身的需要，定义个人的通讯录，设置各类群组和成员，在发送消息时，可以按群组进行发送 |
| 短信流量申请 | 当需要使用短信进行消息发送时，相关的发送部门，必须以部门为单位，首先进行短信流量的使用申请，填写流量申请数量，审核通过后方可使用 |
| 消息发送/审核管理 | 填写并起草需要发布的信息内容，设置消息的发送方式、消息的接受者等；如果消息需要审核，则必须指定消息的审核人，待消息审核通过后，对外进行发布 |
| 3 | 消息通讯平台 | 发送方式配置 | 通讯平台提供了多种消息发送配置，学校可以根据自身的实际情况，进行设置，开通相关消息发送方式。提供消息发送方式包括：  1、短信发送发送  2、微信发送方式  3、邮件发送方式  4、站内信发送方式等 |
| 短信流量管理 | 对各部门提交的短信流量申请进行审核和分配，对短信流量的使用情况进行监控。可对异常部门的流量使用进行处置，包括冻结流量使用、取消流量使用资格和关闭短信通道等多种手段。 |
| 消息来源管理 | 消息服务中的消息既涵盖了内部消息，也包含了第三方集成和对接的消息，对第三方集成和对接的消息，需要对消息的来源进行注册和维护。主要方式包括：  1、数据交换方式：通过数据交换工具，将第三方需要集成的消息同步到本平台。  2、API接口方式：通过消息服务平台提供的API，第三方将消息内容写入到通讯平台。 |
| 消息类型管理 | 对各源头的消息进行消息类型的维护和管理。 |
| 消息发送设置 | 对消息的发送方式（支持短信、邮件、微信等，站内信为系统默认自带，不需要设置）进行配置和管理，既可以按部门设置各类消息的发送方式，也可以按消息类型、消息来源设置各各类消息的发送方式，如果涉及短信发送，则可以设置方式的条目数量等。 |
| 发送策略管理 | 在消息发送过程中，为了确保消息发送的安全可靠，提供了消息重发策略的配置：当消息发送失败后，消息的重发机制设置 |
| 消息日志审计 | 对消息发送日志和内容进行审计查询，提供基于发送时间段、发送方式【短信、微信、邮件等】、发送内容关键字、消息来源应用或系统、消息接收部门、消息接收人、消息发布人等多维度的消息发送日志的审计功能。 |

## 虚拟校园卡平台

### 管理中心模块

1. 具有首页信息概览功能，展示常用重要数据；
2. 支持应用子系统的授权开通及维护；
3. 支持多校区管理；
4. 支持交易类型管理；
5. 支持结算部门管理；
6. 支持餐别管理；
7. 支持设备管理；支持终端设备使用设备码进行注册；支持PSAM卡管理；
8. 支持职员管理，包括身份、权限、登录限制等；
9. 支持功能插件管理与升级；
10. 支持基于角色的权限管理；支持对功能和数据进行分权设置；
11. 具有系统日志记录，包括操作日志、登录日志和异常日志等。

**餐饮消费管理：**

1. 支持金额、定额、快捷菜单等扣费模式；
2. 可指定卡类别和终端定向消费；
3. 支持自定义设置餐次及时间段；
4. 可根据身份类别进行优惠打折；
5. 可根据商户类型进行管理费用收取；
6. 支持设置终端机最大脱机时间，超时禁止消费，联网后自动恢复；
7. 支持设置餐次消费限额和日消费限额，超额须密码验证。

### 客户中心模块

1. 支持卡类型和挂失类型管理；
2. 支持客户批次和客户身份管理；
3. 支持客户部门管理；
4. 支持客户信息管理；
5. 客户信息数据支持自定义扩展字段；
6. 支持过期黑名单管理。

### 制卡中心模块

1. 支持各类卡务操作，包括制卡、挂失/解挂、补卡、注销等；
2. 支持基本用户信息管理，支持从三方系统同步、文件导入或手工操作；信息维护支持批量操作；
3. 支持副卡管理；
4. 支持用户照片批量导入或实时联机证照拍摄采集；
5. 支持智能拍照：自动人脸捕获，自动提醒姿态调整，自动智能调节光圈，自动快门；
6. 支持证卡打印版面设置；支持批量发卡，自动批量一次完成发卡和证卡打印；
7. 支持各类功能卡的发放、挂失、补卡等操作；功能卡包括系统卡、参数卡、定价卡等；
8. 支持存款、取款、领款、消费纠错、暂存款领取、修改卡失效期、修改消费密码、退卡等持卡人操作；
9. 支持批量/批次挂失和批量/批次注销；
10. 支持指纹采集及管理。

### 结算中心模块

1. 支持对出纳账目和结算账目进行结转；
2. 支持交易未决管理，支持自动处理和手工处理；
3. 支持对批次注销客户的账户余额进行领取；
4. 支持卡务费、卡押金管理，其中，补卡费支持挂账；
5. 支持结算报表管理，作为商户、职员进行账目结算的凭证；
6. 支持平衡报表，体现收支汇总情况；
7. 支持各类客户信息查询，包括但不限于交易明细、交易统计、注销账户等；
8. 支持各类审计信息查询，包括但不限于存取款审计、终端机审计等；
9. 支持各类统计分析，包括但不限于管理费账目、出纳交易、终端交易、打折账目等；
10. 支持定制报表管理。

### 集控中心模块

1. 支持监控数据库、Windows服务和应用程序；
2. 支持监控终端设备的联机情况；
3. 支持拓扑图展示；
4. 支持监控权限管理。

### 补助管理模块

1. 支持补助计划的生成、审查、调整、提交生效和撤销；支持操作导航；
2. 支持自动生成和文件导入补助；支持按卡类型设置不同补助金额；
3. 支持文件导入开水补助、冻结金额、三方系统结转金额等代发款项；
4. 支持明细查询和统计报表。

### 代扣费系统模块

1. 支持代扣费科目管理；支持自定义代扣费科目；
2. 支持批量代扣（文件导入）、定额代扣、账单代扣和自定义代扣；
3. 支持通过自助终端设备进行代扣费操作；
4. 支持明细查询和统计报表。

### 密钥前置服务模块

1. 支持交易过程中的数据加/解密，采用硬件加/解密技术，适配金融级硬件加密机；
2. 支持交易数据的防篡改校验；
3. 支持加密设备和运行参数的自定义设置。

### 数据采集模块

1. 支持非智能设备接入，完成数据的上传下达；
2. 兼容交易类和身份识别类终端设备；兼容TCP/IP直连和网关/采集器级连；
3. 支持设备运行参数下发；
4. 支持黑/白名单下发；
5. 支持交易记录、身份识别记录和日志记录上传；
6. 支持业务处理相关的联机通信；
7. 支持设备运行状态上传。

### 虚拟卡管理

1. ▲虚拟校园卡以H5轻应用为载体，支持嵌入多种APP（微信、钉钉等）；
2. 虚拟卡二维码支持动态加密、自动更新，与后台通信支持加密传输；
3. 支持启用/关闭用户的虚拟卡功能；支持为临时人员开通虚拟卡功能的审批管理；
4. 支持按校园卡卡类型分别设置其虚拟卡功能的启用/关闭；

## 聚合支付系统建设

聚合支付系统须实现与各应用系统（自助打印系统、教务系统等）对接。以钉钉或微信平台为主要服务入口、聚合多种资金渠道（合作银行、银联云闪付、第三方支付机构包括微信、支付宝等）、以校方对公账户为资金归口，归拢资金流向，学校拥有完全自主权，可自主控制相应服务入口及资金渠道使用。系统所产生业务数据全部本地化存储，消费资金统一归集到学校对公账户，由校方集中管控与结算，实现入口多样化，出口唯一化，满足校内各类人群的使用需求。除具备基础功能外，还需完成与现有系统的对接：

1、与汇文图书管理系统对接，实现虚拟卡借还功能；

2、与图书馆苏亚星机房管理系统对接；

3、与教务处系统对接

4、与财务收缴系统（杭州银行缴费平台）对接

5、与总务水电缴费系统对接

6、全校食堂、商铺聚合支付平台及配套消费POS硬件。

## 校园人脸识别管理平台

### 校门人脸识别通道

在学校南门门口建设双向人脸识别双通道，西门门口建设双向人脸识别单通道支持校内人员人脸识别、虚拟卡进出。校外人员（访客）刷身份证进出，并能在平台上记录访客信息。

### 图书馆人脸识别通道

在学校图书馆建设单向人脸识别三通道通道，支持校内人员人脸识别、虚拟卡进出。

### 实验楼人脸识别通道

实验楼配备人脸识别门禁，支持师生通过人脸识别、虚拟卡进出。

校园人脸识别管理平台需实现以下功能：

1. ▲支持同时接入多种人脸识别算法，提供软件评测中心出具的测试报告（报告须明确响应此项功能指标）；
2. ▲支持按算法设置不同的参数组，提供软件评测中心出具的测试报告（报告须明确响应此项功能指标）；
3. 支持为应用系统接入提供规范接口，应用系统接入支持授权管控；
4. 支持接入多种类型的人脸识别终端；
5. 支持从三方系统同步用户照片；支持自助设备身份证比对后采集照片；支持WEB或H5应用自助上传照片；支持支付宝小程序内自助采集照片；
6. 支持用户照片采集后根据不同算法提取人脸特征；
7. 支持数据留底，自动持续完善人员生物特征；
8. 支持根据业务系统设置自动更新下发人员特征；
9. 支持向各业务系统推送人脸识别记录；
10. 支持活体检测，可有效防御纸质照片、电子照片、视频、面具等作弊方式；
11. 支持认证记录明细和汇总查询，支持多维度多形式可视化报表；
12. ▲要求投标人拥有完全自主知识产权，提供计算机软件著作权登记证书；
13. ▲要求软件产品成熟标准，提供软件评测中心出具的软件产品登记测试报告。

## 泛门禁管理平台

门禁管理平台应具备宿舍管理系统功能，宿舍区域服务驿站及宿舍楼宇支持师生通过虚拟卡进出。

1. ▲多种终端集成管理：支持集中授权、统一管控，包括门禁终端、无线门锁、通道闸机等，提供软件评测中心出具的测试报告（报告须明确响应此项功能指标）；
2. 系统机制：支持按规则自动授权和授权时段自动下发；
3. ▲支持多种验证方式：包括校园卡、手机扫码（正扫和反扫）、HCE、蓝牙、动态密码、固定密码、指纹、人脸识别、身份证等；
4. 区域统一管理：终端设备归属到“区域”，进行统一授权管理，区域设置支持园区、楼栋、单元、楼层、房间等多种类型；
5. 职员分级管理：上级管理员可以创建下级职员，支持权限继承后自定义设置；
6. 授权时间段设置：支持授权有效时间段，到期自动生效，过期自动失效，支持按周期授权；
7. 自动授权授禁：支持设置指定部门或人员组与区域或设备组的权限绑定，支持人员或设备信息变化后自动授权/授禁；
8. 预约审批：支持用户提交预约申请经审批后自动下发授权；
9. ▲门禁地图监控：支持图形化展示设备开关状态、异常报警信息等，同时支持远程开门、实时视频查看等功能；
10. 视频监控联动：支持与视频监控设备进行联动，支持实时视频查看、历史视频回放、系统联动抓拍等功能；
11. 操作日志：支持完整记录授权信息的操作日志；
12. 匪警联动：提供硬件联动接口，在联动节点报警后，终端自动关闭，不允许普通用户出入；
13. 消防联动：提供硬件联动接口，在联动节点报警后，终端自动打开，取消报警后自动恢复；
14. 断电解锁功能：断电时自动将终端解锁成敞开状态；
15. 应用模式：支持常开模式、首卡开门、多卡开门、多门互锁、反潜回；
16. 高级功能：通道支持防尾随、验证记忆、语音提示；门禁支持胁迫码报警；
17. 非法闯入报警：受控通行时强行进入视为非法闯入，系统会自动报警；
18. 实时监控：支持图文并茂实时监控通行人员信息，包括姓名、学号、照片等；
19. 宿管联动：支持入住、调宿、退宿后授权自动更新；
20. ▲要求投标人拥有完全自主知识产权，提供计算机软件著作权登记证书；
21. ▲要求软件产品成熟标准，提供软件评测中心出具的软件产品登记测试报告。

## 学校移动端应用平台对接

上述人脸识别系统和虚拟卡功能需要与移动端应用平台（钉钉和微信）完成对接。

## 主要硬件设备参数要求

### 加密机

|  |  |
| --- | --- |
| **规格指标** | **指标参数** |
| 消息鉴别 | 支持消息鉴别码MAC/TAC的产生、验证等 数字签名/验证：支持1024～4096 bit RSA公钥密码算法； |
| 密码算法 | 对称算法支持DES/TDES, AES，非对称算法支持RSA（1024～4096比特），摘要算法支持MD5、SHA1等常用算法。 |
| CPU | Intel Atom D2550双核1.86G 1MB二级缓存（不低于上述参数） |
| DRAM | 板载DDR2 SDRAM 128MB（不低上述参数） |
| USB | ≥4个USB2.0 ⅹ2 A型接口 |
| LAN | ≥2个自适应10/100Mbps口（RJ45） |
| 串口标准 | ≥1个RS-232/422/485 |
| Console口 | RS485 |
| 波特率 | 1200bps~115200bps范围内标准波特率 |
| 系统平均无故障时间MTBF | ≥30000小时 |
| DES算法加解密速率 | ≤100Mbps |
| 金融专用算法加解密速率 | ≥30Mbps |
| 工作温度 | 不低于指标：-20︒C～65℃ |
| 工作湿度 | 不低于指标：0% - 90% 非凝结状态 |
| 输入电压 | AC110-240V TO DC12V |
| 电源功耗 | <12W |
| 报警工具 | 内建蜂鸣器和RTC（实时时钟） |

### 系统U-KEY

|  |  |
| --- | --- |
| **规格指标** | **指标参数** |
| 接口规范 | 免驱USB接口 |
| 其他要求 | 硬件加密，即插即用，内置加密狗程序 |

### 虚拟卡读写卡器

|  |  |
| --- | --- |
| **规格指标** | **指标参数** |
| 使用卡类 | 支持Mifare1卡/CPU卡/金融IC卡/ SWP-SIM卡/NFC预置卡 |
| 工作频率 | 13.56MHz |
| 安全性 | 数据加密和双向验证功能 |
| 读卡时间 | ≤500ms |
| 感应距离 | 0-10cm |
| PSAM卡槽 | 不少于2个 |
| 接口 | 免驱USB |
| 功耗 | ＜3W |
| 防雷防爆保护 | 支持 |
| 知识产权 | ▲要求投标人拥有完全自主知识产权，提供嵌入式软件的计算机软件著作权登记证书 |
| 产品认证 | 具有银行卡检测中心出具的PBOC3.0 非接触IC 卡支付终端通讯协议测试检测报告  具有国家电子计算机质量监督检验中心出具的生产许可证检验报告  具有CQC产品认证证书 |

### Psam卡

|  |  |
| --- | --- |
| **规格指标** | **指标参数** |
| 安全机制 | 存储计算、验证密钥，具有密钥销毁策略 |
| 故障时间 | 平均无故障时间大于7000小时 |
| 读卡成功率 | 读卡成功率百分之百 |
| 读取速度 | 读取PSAM卡数据速度大于1K |
| 加密速度 | 单DES数据加密不高于50ms/8字节 |
| PSAM规范 | 支持符合ISO-7816PSAM卡 |
| 电气标准 | PCI本地总线标准R2.1 |
| 总线主频 | 不低于 DC33MHz |
| I/O映射内存 | 采用内存映射的接口可以提供高效的数据块传输 |
| 地址/中断 | PCI BIOS可以提供地址和中断的自动配置（不需要跳线或选择开关） |
| 电压电流 | 电压5.0V 最大电流0.5A |
| 运行温度 | 0︒C～50︒C |
| 存放温度 | -20︒C～70︒C |
| 湿度 | 5%～80%，无冷凝 |
| 卡片质量 | 新卡无损坏或损坏免费更换，正常使用过程中卡片损坏率低于千分之一 |

### 智能POS终端

|  |  |
| --- | --- |
| **规格指标** | **指标参数** |
| 操作系统 | Android 6.0（含）以上 |
| 中央处理器 | 采用64位四核CPU架构，主频1.4GHz（含）以上 |
| 储存器 | 8G FLASH，1G DDR3 |
| 显示屏 | 前屏：7寸（含）以上彩屏，分辨率1024×600，多点触摸电容屏  后屏：3.5寸（含）以上彩屏，分辨率480×320 |
| 键盘 | 数字键/字母键+功能键 |
| SAM卡座 | 3个PSAM卡座，1个SIM卡座 |
| 非接读卡 | 支持Mifare1卡/CPU卡/金融IC卡/ SWP-SIM卡/NFC预置卡 |
| 二维码识别 | 内置扫码器，识别速度≤500ms |
| 外接接口 | ≥1个RJ45接口，≥1个RS232接口，≥1个USB2.0（OTG），≥1个USB Device接口 |
| 通讯方式 | TCP/IP或WiFi或4G全网通 |
| 声光提示 | 真人语音播报 |
| 电源 | AC220或DC12V |
| 电池 | 容量≥10000mAH锂电池 |
| 知识产权 | ★要求投标人拥有完全自主知识产权，提供终端应用软件的计算机软件著作权登记证书 |
| 产品认证 | ★具有银行卡检测中心出具的PBOC3.0 非接触IC 卡支付终端通讯协议测试检测报告 |

### 门禁控制器

|  |  |
| --- | --- |
| **规格指标** | **指标参数** |
| 通讯接口 | TCP/IP |
| 名单数量 | ≥10万/门 |
| 脱机记录 | ≥20万 |
| 读卡器 | 支持WG26/WG34 |
| 供电电压 | AC220V±10％ |
| 读头接口 | ≥2路韦根 |
| 门锁接口 | ≥2路 |
| 按键接口 | ≥2路 |
| 报警接口 | ≥2路 |
| 三方联动接口 | 支持消防、安防信号接入 |
| 数据保存时间 | ≥10年 |
| 知识产权 | ▲要求投标人拥有完全自主知识产权，提供嵌入式软件的计算机软件著作权登记证书 |
| 产品认证 | ▲具有CQC产品认证证书 |

### 虚拟卡门禁读卡器

|  |  |
| --- | --- |
| **规格指标** | **指标参数** |
| 供电 | DC9~15V |
| 处理器 | ARM-A7处理器 |
| 读卡类型 | 支持Mifare1卡/CPU卡/金融IC卡/ SWP-SIM卡/NFC预置卡 |
| 按键 | 12宫格电容触摸按键 |
| 声音 | 真人语音播报 |
| 显示 | 1、2.8吋IPS屏，可显示二维码供手机扫码开门； 2、刷卡标识LED呼吸灯 |
| 摄像头 | 广角高清摄像头，支持QR二维码 |
| 通讯方式 | 韦根 |
| 外部扩展 | 支持PSAM卡 |
| 产品外形尺寸 | 132mm×82mm×18mm |
| 工作环境 | 零下10摄氏度到50摄氏度 |
| 知识产权 | ▲要求投标人拥有完全自主知识产权，提供嵌入式软件的计算机软件著作权登记证书 |

### 电磁锁

|  |  |
| --- | --- |
| **规格指标** | **指标参数** |
| 工作电源 | 12VDC/0.53A |
| 工作方式 | 断电开锁 |
| 安装方式 | 挂装式 |
| 工作温度 | -40℃～50℃ |
| 工作状态 | 开门时红色指示灯亮，锁状态有指示灯指示，锁门时绿灯指示灯亮，带锁状态指示灯及联网信号指示 |
| 保护性 | 内置反向突波保护功能，有门侦测信号 |
| 绝缘性 | 绝缘电阻测试，DC500V（1分钟无击穿） |

### 翼闸通道机（单机芯/双机芯）

|  |  |
| --- | --- |
| **规格指标** | **指标参数** |
| 供电 | AC220V/50Hz |
| 功率 | <50W（单机芯），<100W（双机芯） |
| 材质厚度 | SUS304不锈钢，厚度1.5mm（含）以上 |
| 电机类型 | 长寿命直流无刷电机 |
| 电机寿命 | ▲MTBF≥800万次，提供权威第三方检测机构出具的检测报告 |
| 红外对数 | 6对长寿命对射红外 |
| 门翼材质 | 有机玻璃（带冷光源）或红色软翼 |
| 通道宽度 | 标准550mm |
| 机械特性 | 具备机械和红外电子双重防夹 |
| 电气安全 | 自带漏电保护器 |
| 声光指示 | LED通道指示和通行指示 |
| 敞开模式 | 支持设置敞开时段 |
| 消防联动 | 支持消防联动自动开闸和断电自动开闸 |
| 自检功能 | 具备自检测、自诊断、自动报警功能 |
| 报警功能 | 支持非法闯入、逆向通过、尾随等异常行为检测并报警 |
| 远程管理功能 | 支持远程配置 |
| 身份验证方式 | 扫码或人脸识别 |
| 通行速度 | 20-40人/分钟 |
| 尺寸 | 1400×950×280(mm) |
| 工作温度 | -20℃～70℃，支持扩展加热装置 |
| 使用环境 | 室内、外 |

### 人脸识别平板

|  |  |
| --- | --- |
| **规格指标** | **指标参数** |
| 供电 | DC12V/2A |
| 处理器 | 8核1.8GHz处理器 |
| 存储 | 2G RAM+16G Flash |
| 屏幕 | 8吋电容触控屏，分辨率1280×800 |
| 摄像头 | 500W像素双目摄像头（可见光+红外光） |
| 补光灯 | 自带红外和白色补光灯，支持灯光亮度调节 |
| 光感和测距 | 自带光感传感器和测距传感器 |
| 声音 | 真人语音 |
| 接口 | 以太网×1，继电器×1，USB×1，RS485×1，开门按钮×1，韦根×1，报警输入×2，报警输出×1 |
| 材质 | 钢化玻璃面板、CNC雕刻铝合金外壳 |
| 通讯方式 | 以太网、WIFI、蓝牙 |
| 安装方式 | 立柱安装 |
| 读卡 | 屏下读卡，支持M1、CPU、NFC、身份证 |
| 扫码 | 支持手机扫设备屏显二维码开门 |
| 人脸识别 | 内置算法，活体识别，不小于2万面部特征 |
| 在线升级 | 支持OTA软件升级，可升级固件和应用程序 |
| 防护等级 | ▲IP65，提供权威第三方检测机构出具的检测报告 |
| 产品厚度 | ≤22mm |
| 工作环境 | 零下20摄氏度到60摄氏度 |
| 知识产权 | ▲要求投标人拥有完全自主知识产权，提供终端应用软件的计算机软件著作权登记证书 |

# 售后及实施要求

## 项目实施要求

校园一卡通项目必须有详尽缜密的组织实施及设计方案。本部分将计入方案技术分。具体应包括以下几个方面：

1) 实施组织方案

2) 实施进度计划

3) 项目难点和要点分析

4) 风险与缓解措施

5) 质量控制管理

6) 项目验收方案

7) 培训方案等

## 售后服务保障与承诺

投标商应建立较为完善的售后服务体系，向用户提供充分考虑使用者利益的技术支持及售后服务模式。

具体应包括以下几个方面：

1) 本地运行保障机构

2) 售后服务流程

3) 质保期

4) 售后服务响应时间等