湖北交通职业技术学院

校园密码应用服务系统采购合同

甲　　方：湖北交通职业技术学院

乙　　方：武汉明华旭日科技有限公司

签订地点：湖北●武汉

采 购 合 同

合同编号：JZYZC-2019091

甲方：湖北交通职业技术学院

乙方：武汉明华旭日科技有限公司

甲方为提高学校校园网信息安全防护及保障水平，特向乙方订购校园密码应用服务系统设备及配套对接学校统一身份认证系统，并实现学校现有办公自动化系统密码改造升级服务，包括系统登陆密码升级、电子公章升级、加密算法升级、登陆验证码升级等，以及功能模块优化，具体包括外出公务活动管理、因私出国（境）管理、会议室管理移动端、考勤管理、值班管理等。为了明确双方的权利义务，在平等自愿的基础上，根据《合同法》以及相关法律法规的规定，经双方协商一致，签订本合同。

一、项目明细

甲方向乙方订购校园密码应用服务系统设备，依托该设备配套对接学校统一身份认证系统，并实现学校现有办公自动化系统密码改造升级服务，包括系统登陆密码升级、电子公章升级、加密算法升级、登陆验证码升级等，以及功能模块优化，具体包括外出公务活动管理、因私出国（境）管理、会议室管理移动端、考勤管理、值班管理等，商品名称、型号、价格、数量以报价文件为依据详见附件（产品清单

及技术要求)。

二、到货时间、地点、运输、安装方式

1.乙方在合同签订后30天内完成交货。乙方送货到甲方指定地点(湖北交通职业技术学院院内)。

2.运输费用由乙方负责。

3.乙方负责所提供产品的安装及操作使用培训。

三、合同总价款与支付方式

1.合同总价款:总金额为:¥245,000.00元(人民币大写:贰拾肆万伍仟元整),包含运输、保险、税金、安装调试、OA改造、培训等费用;

2.支付方式:在乙方安装调试、配套软件开发、培训完毕并甲方验收合格,乙方向甲方支付合同金额5%的履约保证金:¥12,250.00元(人民币大写:壹万贰仟元贰百伍拾元整)后,甲方向乙方一次性支付合同总货款,并按政府采购程序履行支付手续。

3.若设备运行正常,履约保证金自验收合格之日起满1年后一次性无息退还。

四、**验收方式**

1.验收合格条件:设备到货、安装调试完毕,OA软件定制改造完成、运行正常,培训完毕。

2．不合格的产品乙方应尽快予以退换，如验收仍不合格，则甲方退货，乙方赔偿由此给甲方造成的全部损失。

3．货到后，甲方应在7个工作日内组织验收。任何一方对验收结果有异议的，应在3个工作日内提出异议，否则视为放弃提出异议的权利。

五、质量保证和售后服务

1．所投设备软硬件质保期三年。质保期从甲方验收合格之日开始计算。

2．乙方保证所提供的产品质量为合格。产品标准执行国家标准或行业标准。否则，乙方负责产品质量问题而产生的一切费用。

3. 乙方保证提供的产品拥有知识产权的合法使用权，否则，引起的任何法律责任均由乙方承担，并赔偿由此给甲方造成的全部损失。

4. 一个月内有质量问题包换，质保期内除耗材外配件免费更换，在甲方通知后的5日内进行无偿维修。其它根据国家三包法标准执行。

5. 关于售后服务，乙方承诺：

(1) 乙方对甲方操作人员免费培训，质保期内负责维护和升级服务；

(2) 乙方在收到甲方的故障通知之后，1小时作出响应，2小时达到现场，4～8小时内解决问题；

(3) 因甲方使用、操作或保管不当所造成的设备损坏或故障，以及非产品质量问题所产生的故障，乙方负责维修，甲方支付相关维修费和材料费。

六、违约责任

1. 甲方或者乙方不履行合同义务或者履行合同义务不符合约定的，应当承担继续履行、采取补救措施和赔偿损失等违约责任。

2. 甲方按照政府采购程序及时支付价款，未支付价款或者逾期支付价款的，乙方可以要求甲方支付价款和逾期利息并按日计算违约金，每逾期一日支付总价款 1‰的违约金。

3. 乙方不履行交货义务或者履行交货义务不符合约定的，甲方可以要求乙方赔偿损失。乙方逾期交货的，甲方可以要求乙方继续履行并承担违约金责任，违约金按日计算，每逾期一日支付总价款 1‰的违约金。乙方逾期交货因标的物质量不符合质量要求，甲方可以拒绝接受标的物或者解除合同。并可以根据标的的性质以及损失的大小，要求乙方承担赔偿损失、修理、更换、重作、退货、减少价款等违约责任。

4. 乙方将合同义务全部或者部分转移给第三人的，甲方可以解除合同，要求乙方按照总价款 10% 承担违约责任并赔偿损失。

5. 因不可抗力不能履行合同的，根据不可抗力的影响，部分或者全部免除责任，但法律另有规定的除外。当事人迟延履行后发生不可抗力的，不能免除责任。

七、合同解除

1．双方协商一致可以解除合同；

2．如果乙方提供的产品不符合合同约定的质量标准、技术要求，要求乙方改正，而乙方拒绝改正的，甲方有权解除本合同，并要求乙方承担相应的损失；若甲方违反合同规定拒绝接货的，乙方有权解除合同，并要求甲方承担相应的损失。

八、其他

1．双方在合同履行过程中发生任何争议，应尽量协商解决，无法协商达成一致的，可向合同履行地人民法院起诉。

2．合同未尽事宜，须经双方共同协商，作出补充规定，补充规定与本合同具有同等法律效力。

3．本合同书一式陆份，甲方执肆份，乙方执贰份，自双方签字盖章起生效。合同执行期间，甲乙双方均不得随意变更或解除合同。

甲方：湖北交通职业技术学院

地址：武汉市洪山区雄楚大道 455 号

开户银行：工行科技支行

乙方：武汉明华旭日科技有限公司

地址：洪山区卓刀泉南路 108 号凯乐桂园 S-1 栋 A 单元 18 层 2 室 01 号

开户银行：招商银行武汉东湖支

行

账号：3202006909000056478

行号：826478

电话：027-87568987

法定代表人或

委托代理人：

日期：2019年7月23日

账号：275582870310001

行号：883368

电话：027-87665778

法定代表人或

委托代理人：

日期：2019年7月23日

附件 1：产品清单

序号	货物名称	明细	规格及型号	数量	交货期	质保期	单价（万元）	小计（万元）	备注
1	校园密码应用服务系统	校园密码应用服务系统	SJJ1517-A40 2U 千兆硬件平台，标配硬件加密卡（国产密码加密算法）；提供 1000 个 SSL VPN 接入授权 SSL 最大加密流量 360Mbps； SSL 理论并发用户数 5000 个； SSL 理论新建用户数 260 个/秒； IPSec 最大加密流量 540Mbps； IPSec 理论并发隧道数 6000； 防火墙理论吞吐量 1.5Gbps； 防火墙代理理论并发会话数目 1600000； 单电源；尺寸：2U；	1 台	同签订之日起 30 日内完成供货、安装、调试和培训等内容	3 年	21.408	24.50	

			接口:6 个千兆电口、2 个千兆光口（含模块）、2 个万兆光口（含模块）。						
		OA 系统配套密码改造服务	依托校园密码应用服务平台实现对学校现有办公自动化系统密码相关的改造服务，包括系统登陆密码改造、电子公章改造、加密算法改造、登陆验证码改造、外出公务活动管理改造、因私出国（境）管理改造、会议室管理移动端改造、考勤管理改造、值班管理改造等	1 套	同签订之日起 30 日内完成供货、安装、调试和培训等内容	无	3.092		
合计		大写：贰拾肆万伍仟元整（小写：245,000.00 元）							

附件 2 技术要求

1、总体要求

(1)要求本项目所涉及的所有加密算法为 SM1，SM2，SM3，SM4 等算法均可；

(2)要求与学校统一身份认证系统进行对接，实现登陆后直接访问校内信息化资源；

(2)要求以校园密码应用服务系统为基础，完成学校 OA 办公自动化系统相关加密功能的改造，使其符合国产密码相关要求；

(3) 要求以校园密码应用服务系统为基础，对学校现有 OA 办公自动化系统的登陆密码、电子公章、加密算法进行国产密码改造，同时完成登陆验证码功能升级和公务活动管理、因私出国（境）管理、会议室管理移动端、考勤管理、值班管理等功能模块定制开发。

2、校园密码应用服务系统技术参数

项目	功能指标要求
性能指标	专用 2U 千兆硬件平台，标配硬件加密卡（国产密码加密算法）； 提供不低于 1000 个 SSL VPN 接入授权 SSL 最大加密流量≥360Mbps; SSL 理论并发用户数≥5000 个; SSL 理论新建用户数≥260 个/秒; IPSec 最大加密流量≥540Mbps; IPSec 理论并发隧道数≥6000; 防火墙理论吞吐量≥1.5Gbps; 防火墙代理理论并发会话数目≥1600000; 单电源;尺寸:2U;

	接口：≥6 个千兆电口、≥2 个千兆光口（含模块）、≥2 个万兆光口（含模块）。
部署方式	支持网关模式、单臂模式、双机模式、集群模式的部署。
加密算法	产品需符合国密算法相关要求。
基本特性	专业 VPN 设备，采用标准 SSL、TLS 协议，同时支持 IPSec VPN、SSLVPN 两种 VPN，非插卡或防火墙带 VPN 模块设备。同时支持软件化交付。
	支持 WEB VPN 功能，实现免插件登录并访问校内资源（提供操作界面截图并加盖厂商公章）；
	支持对基于 HTTP、HTTPS、FileShare、DNS、H.323、SMTP、POP3、Telnet、SSH 等的所有 B/S、C/S 应用系统，支持基于 TCP、UDP、ICMP 等 IP 层以上的协议的应用，例如即时通讯、视频、语音、Ping 等服务；
	支持 PC 终端使用包括 Windows10、Windows8、Windows7、Windows Vista、Windows xp、Mac OS、Linux 等主流操作系统来登录 SSLVPN 系统，并完整支持该操作系统下的各种 IP 层以上的 B/S 和 C/S 应用； 支持 Windows、IOS、Android、塞班、黑莓等操作系统的智能手机、PDA、平板电脑（PAD）等移动终端的 SSL VPN 接入，或通过 PPTP、L2TP VPN 方式接入；
	支持终端使用包括 IE6、7、8、10、11 或其他 IE 内核的浏览器，以及最新版本的非 IE 内核浏览器，如 Windows EDGE，Google Chrome，Firefox，Safari，Opera 最新版登录 SSLVPN 系统，登录后可完整支持各种 IP 层以上的 B/S 和 C/S 应用。

	支持 Mac 系统主流浏览器，如 Chrome、Firefox 等最新版，免安装浏览器插件登陆 SSL VPN。
	支持 Linux 系统主流浏览器，如 Firefox、Chrome 等最新版，免安装浏览器插件登陆 SSL VPN。
	WebVPN 支持跨平台免插件访问，支持 EasyLink 泛域名发布 Web 资源，简化资源发布和访问。
	产品应支持的密码算法包括：AES、DES、3DES、DH、RSA、RC4、MD5、SHA1；
	在 Windows 系统上，能同时安装并运行多个 VPN 客户端，满足有多套 VPN 的客户同时登录 VPN。
易用性	可支持虚拟门户功能，在一台设备上配置不同的访问域名、IP 地址，以及不同的使用界面，实现一台设备为多个不同用户群体服务的的使用效果；
	支持文档 WEB 化管理，用户可通过任意浏览器，对存储服务器的文件进行管理操作（包括：上传、下载、删除、重命名、剪切、复制、粘贴、新建文件目录），而不需要额外安装 FTP、文档共享软件等应用程序客户端。
	支持用户登录界面、服务界面的完全自定义，上传单独的 Web 页面作为用户登录界面、服务界面
	支持单点登录功能（SSO）,支持移动用户登录 VPN 后再登录内部 B/S、C/S 应用系统时不需要二次重复认证。支持针对 B/S 单点登录用户名密码加密传输，保证安全；支持针对不同的访问资源设定不同的 SSO 用户名和密码，支持用户

	自行修改 SSO 账号。
	支持断线重连自动技术，防止用户误操作关闭浏览器导致 VPN 隧道断开；防止用户在无线网络环境下网络正常切换时 VPN 隧道断开。 支持客户端永久在线功能，对于无人值守的设备可以设定永久在线，如果网络断开，可提供无限次重连。
	支持智能递推技术，针对多外链的门户网站进行动态嗅探页面内的链接并完成资源自动授权，防止资源漏访；支持 Web 参数修正，可针对 Flash、Java、Applet、或视频播放器对象所引用资源路径进行修正，避免无法播放的问题。
	产品应提供环境检测、自动修复工具，支持对 Windows 的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响 SSL VPN 的使用，减轻运维工作。
终端安全	产品必须支持防中间人攻击，产品可在用户登录 SSLVPN 时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象。
	支持用户终端登录前、登陆后的安全性检测，检测范围包括：用户接入 IP、接入时间、接入线路 IP、进程、文件、注册表、操作系统、使用终端，可以检测出客户端是否安装指定的防火墙或杀毒软件。
	支持客户端注销后自动清除所有缓存、Cookies、浏览器历史记录、保存的表单信息，实现零痕迹访问
	支持 VPN 专线功能，可配置用户在接入 SSL VPN 的同时，断开与 Internet 其他连接

	产品应提供 HTTPS 驱动病毒查杀工具，支持对 Windows 环境下的针对 HTTPS 拦截监听的驱动病毒进行扫描查杀，避免因为 HTTPS 驱动病毒导致无法正常接入和使用 SSL VPN。
权限、服务器安全	产品应具有用户/用户组细粒度的权限分配功能：可以针对被访问资源的 IP 地址、端口、提供的服务、URL 地址等进行权限控制；针对同一 B/S 资源，可对不同用户做到细致到 URL 级别的授权。
	产品应具有角色授权机制，支持在用户组的基础上，根据角色的不同，组合关联不同的资源权限。
	支持主从认证账号绑定，必须实现 SSL VPN 账号与应用系统账号的唯一绑定，VPN 资源中的系统只能以指定账号登陆，加强身份认证，防止登录 SSL VPN 后冒名登录应用系统。
	支持关键文件保护功能，可针对特定应用关键文件进行锁定，防止用户进行篡改进行越权
	针对服务器地址保护方面，可支持 SSLVPN 资源列表界面上的用户授权资源隐藏；针对 B/S 应用，可进行 URL 地址伪装，防止服务器真实 IP 地址泄露
身份认证	产品必须支持 Local DB 、USB KEY、短信认证、硬件特征码、动态令牌、数字证书认证、LDAP、RADIUS、等认证方式；可针对用户/用户组设置认证方式的与、或组合，可进行用户名/密码、LDAP、USB KEY、硬件特征码、短信认证或动态令牌的五因素捆绑认证
	支持有驱 USB KEY、无驱 USB KEY 认证，无驱 KEY 无需在客户端安装驱动，方

	便用户；支持配置第三方 KEY，可与其他业务系统无缝结合；支持满足中国国家标准的《智能 IC 卡及智能密码钥匙密码应用接口规范》的智能 TF/SD 卡。
	支持结合阿里钉钉、口袋助理等移动 APP，实现动态口令认证，增加认证的多样性。
	支持随机验证码短信认证，可自定义所发送短信信息格式，支持用户端短信重发功能； 支持三大运营商移动、联通、电信运营商的标准的外置短信设备或 API 接口； 支持 GSM、CDMA 制式短信猫；支持 webservice 方式短信认证，支持 webservice 嘉迅版；
	支持和企业级微信绑定，实现安全接入的统一认证。
	设备内部必须支持自建 CA 中心，便于数字证书认证平台搭建； 支持与基于 PKI 体系的第三方 CA 进行结合认证 ，可根据 CA 某字段将通过 CA 认证的用户自动映射到指定用户组，方便进行权限授权配置；支持 CRL 证书撤销列表。 单台 VPN 设备可扩展同时支持 5 套以上 CA 根证书；
高速性	必须支持至少 4 条以上的外网多线路配置；并在设备单臂部署模式下，多线路接入前置网关，仅依靠 SSLVPN 设备同样可实现 SSLVPN 接入用户的多线路自动优选功能
	支持启用多线路时，自动检测故障线路，并自动踢出故障线路；一旦线路恢复，可在一定时间内自动恢复。支持启用多线路时，自定义用户访问选路策略，包

	括按上/下行带宽，轮询，按优先级等方式。
	支持利用网页进行动态寻址的方法，客户端无需安装插件、不依靠 IP 地址库、不依赖于第三方动态 IP 寻址、直接根据速度探测实现用户端接入线路的自动优选,用户通过访问寻址代理页面（简称 Webagent 页面），通过 Webagent 页面自动寻找 VPN 设备 IP(非 DDNS），该方法不必单独注册域名或占用 IP 地址，大大降低了系统部署难度
	仅通过 SSLVPN 设备可实现资源负载均衡功能，用户接入同一资源根据权值可动态负载到多台承载服务器上；负载均衡可基于服务器性能指标、权值轮询、轮询等不同方式。
	支持非对称式部署的传输协议优化技术（单边加速），不用在用户终端上安装任何插件和软件，即可提升用户访问应用服务的速度。
	支持 HTP 快速传输协议，大幅优化无线环境（CDMA、GPRS、WIFI、3G）、高丢包、高延等恶劣网络环境下传输速度及效率；支持根据网络境自动选择并切换至最优的传输协议
	支持针对不同的 web 页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输。
	针对 B/S 资源支持 WebCache 技术，动态缓存页面元素，提高 Web 页面响应速度。支持流缓存技术，实现网关与网关、网关与移动客户端之间进行多磁盘、双向、基于分片数据包的字节流缓存加速，削减冗余数据，降低带宽压力的同时提高访问速度；支持共享流缓存功能，实现多分支网关在总部共享流缓存数

	据，提高流缓存效果
高管理要求	支持 15 级以上的管理员分级分权限管理，从 Admin 派生树形结构下级管理员；上级管理员可分配下级管理员享有设备配置模块权限，可管理的用户、资源、角色权限，并可限制下级管理员是否允许创建下级管理员、创建资源、创建角色；上级管理员可限制下级管理员对权限内配置享有查看或配置权限
	支持设置对控制台管理员密码复杂度的要求，提升设备的安全性；
	支持 15 级以上用户组树形结构分级管理，下级组可继承上级组的角色，资源及认证方式等属性
	支持系统实时监控，图形化显示一段时间内的运行状况，可查看 CPU 占用率、各条线路网络吞吐量、各条线路的 IP 地址及发送接收流速、并发会话数、SSL 并发用户数；可查看历史最高并发用户数并显示时间记录；可实时查看 SSL 接入用户的用户名、发送流速、接收流速、发送流量、接收流量、接入时间、并发会话数、接入 IP、虚拟 IP、认证方式等信息，并可在线中断指定用户
	支持独立日志中心进行 SSLVPN 实时日志记录，可详细记录用户访问资源记录（用户、主机 IP、资源、时间）、管理员日志（管理员、主机 IP、时间、管理行为、对象）、系统日志、告警日志；可根据用户名、主机 IP 等信息进行用户行为查询；可提供用户组/用户流量排行及查询、资源流量排行及查询、资源活跃程度、用户活跃程度等记录；提供暴破登录记录；可提供用户登陆 SSLVPN 采用非绑定账号访问应用系统的记录
	支持 Syslog（系统日志）服务器，可将管理员日志，系统日志、用户日志输出

	到 syslog 服务器中。
	支持密码找回功能，当用户的密码忘记或者丢失时，可自行找回密码，减轻管理员维护压力。
	支持整体网关配置的本地及远程备份、恢复功能；支持 SSLVPN 配置的单独备份、恢复功能，并支持历史配置的回滚
稳定性、可扩展性	支持基于自组域简化部署 VPN 网络的方法，即当有多台设备处于 VPN 网络中时，通过连接任意节点的 VPN 设备，即相当于连入整个 VPN 网络,该方法解决了传统 VPN 部署是，需要部署多台；
	支持 253 台不同型号设备间进行集群（A/A），支持路由模式、单臂模式下多线路部署的集群；支持集群设备间 Session 同步，一台设备宕机后其上用户无需重新登录 SSLVPN 可继续使用；可扩展分布式集群功能，无需专门的全局负载设备即可实现异地 SSLVPN 设备间的接入用户负载分担、速度优选接入，异地设备间互为备份，分布式集群中用户可通过唯一的一个地址访问到所有加入到分布式集群的 SSLVPN 设备
	在负载均衡集群部署模式下，支持授权漂移，即当集群中一台设备宕机，该宕机设备中的并发授权自动迁移到其他正常的设备中，而无需额外购买授权。
	产品必须支持经过集成的，基于 Android IOS 平台的第三方软件开发包（SDK），并实现基于 Android IOS 平台第三方应用软件（APP）代码量不超过 20 行。支持针对移动 APP 的 VPN 安全代码的自动封装，实现 App 应用的安全加固
远程应用	产品必须在 Windows 和 MAC 操作系统下支持远程应用发布功能（提供界面截

	图证明）
	登录客户端兼容全平台(windows、mac、linux 主流系统)，并保持各平台易用性、用户使用习惯的一致性
	可以无需二次开发，即把 Windows 应用发布到移动智能终端中，也可以支持无需开发，将 C/S 资源 Web 化。
	手机客户端必须经过苹果公司官方检测，并发布在苹果官方应用商店 appstore，产品客户端必须通过 google 公司官方检测并发布在 google 应用商店 PlayGoogle；产品客户端必须支持非“越狱”或非“Root”权限的手机/PAD 安装。
	远程应用发布必须支持本地资源，包括：本地磁盘资源映射、本地打印机、本地串行口、本地智能卡，本地输入法；支持剪切板，并能够实现剪贴板数据流双向控制，即可以分别控制是否允许用户将“客户端复制数据到远程应用”或将“远程应用数据复制到客户端”
	产品必须有较好的易用性体验： 包括图像清晰，支持图像质量可调，包括可以调整图像显示质量，图像颜色质量，可根据当前系统分辨率自动调整图像分辨率； 支持远程播放视频、声音； 支持远程应用使用本地输入法；支持本地输入法和远程服务器输入法可切换，在小屏幕或网络带宽差的情况下，支持在本地先批量输入文字再点击发送，避免零散数据在广域网上的频繁交互； 支持一次滚屏多行；

	远程应用发布支持会话保持技术，避免网络异常中断导致会话中断； 远程应用发布支持远程应用发布支持重力感应转屏，可实现自动转屏和手动转屏； 支持 windows 快捷键组合，必须支持 Windows 常用 30 种以上快捷键组合，支持自动记录快捷键使用频度； 产品必须支持存储服务器的管理；必须针对每个用户提供独立的个人目录； 操作方式支持鼠标指针、放大镜指针、模拟键盘、滚动条、程序列表、主页切换窗口等； 远程应用发布客户端应支持 IOS 图标发布资源。 远程应用发布应该支持云存储，能够将手机、PAD、PC 电脑中的文档、照片等上传到云端，或下载到本地终端。并实现基本的复制、剪切、粘贴、新建、重命名等操作。 远程应用发布能够支持直接调用手机或 PAD 摄像头，实现拍照。或访问本地照片库，调用已拍的照片。
	产品必须支持对终端服务器的实时监测，包括服务器综合状态、CPU 使用率、内存使用率、磁盘 I/O、远程应用会话数、服务器当前会话数。
	产品必须支持会话复用功能，即当存在多台终端发布服务器且未设置集中存储时时，同一用户的同一会话必须始终发布到同一终端服务器。
	远程应用发布必须支持负载均衡策略，即当存在多台终端发布服务器时，可以根据服务器可用会话数、CPU、内存、I/O、综合性能等指标，智能的将用户分配到不同的终端服务器。

	产品应该支持企业级"云盘"（又名"网盘"、"文件共享"）功能，即可以通过手机、PC、IPAD 的客户端，将数据、文件同步到云端或和分享到终端。 也能够能够支持分享给他人。
	远程应用发布必须支持应用权限控制项，不得通过远程应用访问任何未经授权的 windows 资源，至少应该包括：未经授权的应用程序、注册表、任务管理器、资源管理器、控制面板、cmd 命令提示行、Win+R 运行命令行、管理选型、映射网络驱动器选型、断开网络驱动器选型、回收站、网上邻居等。并支持隐藏本地原有磁盘，仅提供公共磁盘。
	远程应用发布数据传输过程中使用 SSLVPN 协议加密，保证了数据传输的合法性和安全性；
	支持改写 WindowsRDP 协议，经改写的协议必须独立于 OS 运行环境，避免跨平台兼容性，针对图像数据，服务端必须支持有损压缩算法；服务端必须能够支持过滤动态内容（gif/flash/video）以减少传输流量，且根据客户需要配置。
售后服务	提供 3 年软硬件原厂质保。
服务要求	在质保期内，对于我方使用过程中遇到的问题，供应商需要提供 7×24 小时电话技术支持，1 小时内响应，2 小时内到达现场，6 小时以内解决问题。在设备整个使用期内，保证我方设备的正常使用，若短期无法修复的,6 小时内不能解决问题应提供同档次以上备机；
	质保期内，每三个月免费对系统进行一次总体检测，每半年免费对系统进行一次复调。质量保证期内的所有维护（包括人工和设备配件、备品提供等）均不

	收取任何费用
	承诺保质期内因设备本身缺陷造成各种故障由原厂商提供免费技术服务和维修
验收要求	提供售后服务承诺函。
	产品运输、安装、调试运行、以及与学校统一身份认证系统对接等相关费用含本项目内。

3、配套密码改造服务

3.1 登陆密码升级

项目	指标描述
基本要求	在现役升级后的 OA 系统上进行 OA 登录密码的升级； 使 OA 系统登录密码的算法符合国密要求（SM1， SM2， SM3， SM4 四种算法均可）； 算法和功能模块升级过程中不影响学校使用需求，能正常操作（读、写、改）现有数据；
技术要求	升级后系统支持 Windows 2012 Server 及以上操作系统；
	升级完成后终端使用能支持包括 IE6、7、8、10、11 浏览器； 升级完成后终端用户操作系统支持 Windows XP、Windows 7、Windows 10 等主流操作系统，且 64 位和 32 位均支持。
	升级后必须保留现有版本的操作习惯，且保存原 OA 系统数据；

3.2 电子公章密码改造

项目	指标描述
基本	电子公章设备的加密算法符合国密算法要求；

要求	
技术要求	电子公章进行升级，实现文书可在 Windows XP、Windows 7、Windows 10 等系统上操作；
	电子公章存储安全管理：必须将电子印章存放在移动存储介质上，并与存储介质绑定；
	全程加密技术：文件盖章后正文与公章立即被加密，只有持有合法解密设备的指定接收人才有权查看。
	内容验证：电子公章系统支持将电子公章和文件内容紧密绑定，支持随时对电子公章的可靠性及其绑定内容的完整性进行验证，一旦绑定内容发生变化，电子公章将失效。
	打印份数控制：可设置收文方打印红头文件的份数。

3.3 登陆验证码密码改造

项目	指标描述
基本要求	在现役 OA 系统上登陆界面新增随机数字验证码验证功能； 使得 OA 系统登录密码的算法符合国密要求（SM1， SM2， SM3， SM4 四种算法均可）
技术要求	升级后系统支持 Windows 2012 Server 及以上操作系统； 升级完成后终端使用能支持包括 IE6、7、8、10、11 浏览器； 升级完成后终端用户操作系统支持 Windows XP、Windows 7、Windows 10 等主流操作系统，且 64 位和 32 位均支持。 升级后必须保留现有版本的操作习惯，且保存原 OA 系统数据；

3.4 模块定制服务

根据学校现有需求，在现有 OA 办公自动化系统的基础，进行功能模块定制开发，实现与校园密码应用平台的封装。具体包括但不仅限于登陆验证码功能升级和公务活动管理、因私出国（境）管理、会议室管理移动端、考勤管理、值班管理等功能。

支持安卓及苹果手机与 APP 封装，启动 APP 后，后台自动启用校园密码应用服务系统（即 VPN）；

实现办公业务的手机提醒、办理、查询及跟踪。

注：新增的功能，在现有的平台上面进行新增。

3.4.1 外出公务活动模块定制

提供员工外出公务活动管理，提供外出公务申请单登记，相关信息可自动登记，并提供相关数据字典；申请单登记后，可按照定义的流程送相关领导审批；经手认可随时查询外出的审批情况；相关人员可按照部门、人员进行外出情况统计。

湖北交通职业技术学院
外出公务活动审批单

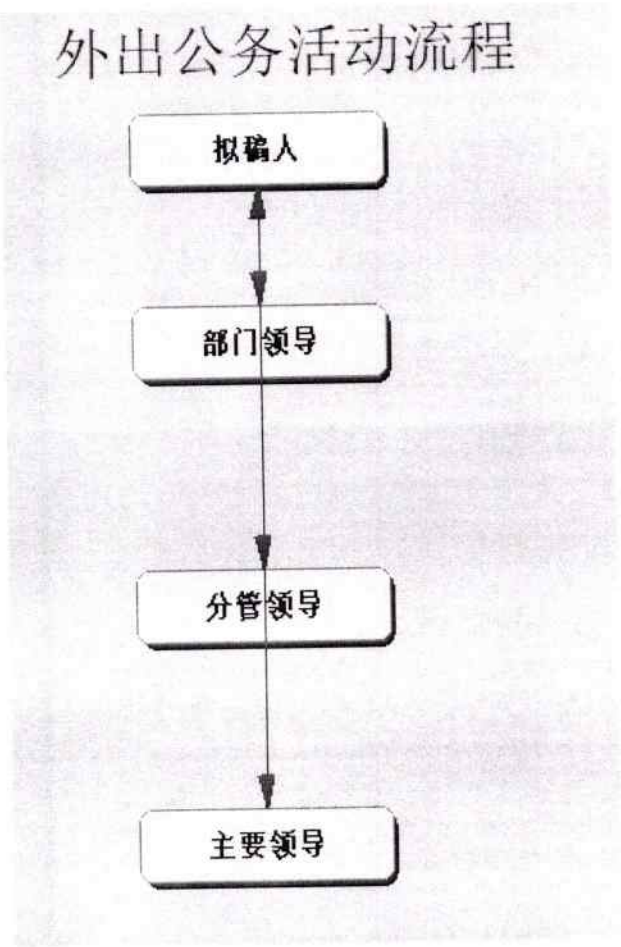
<table>
<tr><td>部门</td><td colspan="3"></td><td>填单时间</td><td></td></tr>
<tr><td>姓名</td><td></td><td>职务</td><td></td><td>活动地点</td><td></td></tr>
<tr><td>外出时间</td><td colspan="5"></td></tr>
<tr><td>外出事由</td><td colspan="5"></td></tr>
<tr><td>乘坐超标准交通工具</td><td colspan="5">轮船（二等舱□）
火车（软卧□） 高铁/动车（一等座□）
飞机经济舱□</td></tr>
<tr><td>乘坐理由</td><td colspan="5"></td></tr>
<tr><td rowspan="3">主要随行人员</td><td>姓名</td><td colspan="2">部门</td><td colspan="2">职务</td></tr>
<tr><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td rowspan="2">委托在家主持工作负责人</td><td>姓名</td><td>职务</td><td colspan="2">电话</td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td>部门负责人</td><td colspan="5"></td></tr>
<tr><td>分管领导审批意见</td><td colspan="5"></td></tr>
<tr><td>主要领导审批意见</td><td colspan="5"></td></tr>
</table>

注：1.其他校领导外出公务活动由学校主要领导审批。

2.各部门主要负责人外出公务活动逐级报分管校领导、学校主要领导审批。

3.正式通知或活动文字方案附后。

流程图：



3.4.2 出国（境）管理

提供职工因私出国（境）申请管理，提供出国（境）申请单登记，相关信息可自动登记，并提供相关数据字典；申请单登记后，可按照定义的流程送相关领导审批；经手认可随时查询出国（境）申请的审批情况；相关人员可按照部门、人员进行出国（境）统计。

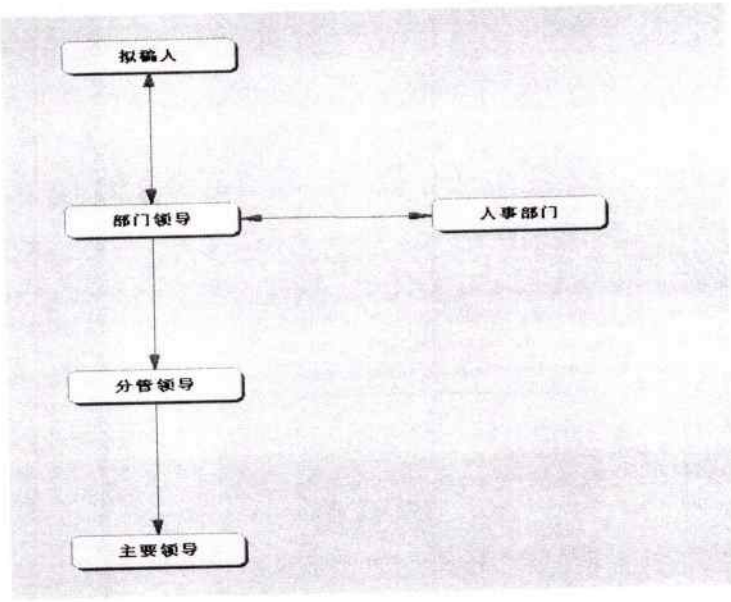
点开因私出国（境）模块，首先弹出承诺书，承诺书勾选"已同意"后才能填写以下申请单。

湖北交通职业技术学院
因私出国（境）申请审批单

<table>
<tr><td>姓　名</td><td></td><td>性　别</td><td></td><td>身份证号码</td><td></td></tr>
<tr><td>工作单位</td><td></td><td>职　务</td><td></td><td>出境目的地
及签注类型</td><td></td></tr>
<tr><td>出境日期</td><td></td><td>返回日期</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>出境事由</td><td colspan="3"></td><td>本年度申请
次数</td><td></td></tr>
<tr><td>所在处室意见</td><td colspan="2">签章
时间　　年　月　日</td><td>人事部门
意见</td><td colspan="2">签章
时间　　年　月　日</td></tr>
<tr><td>分管领导意见</td><td colspan="5">签章
时间　　年　月　日</td></tr>
<tr><td>审批意见</td><td colspan="5">签章
时间　　年　月　日</td></tr>
</table>

注：1、公务员（参公人员）护照、港澳台通行证应集中保管，因私出国（境）应按规定程序办理相关手续。2、领导干部因私出国（境）证件应在回国（返境）后 10 日内，按照规定交由人劳部门集中保管。

流程图



3.4.3 会议室管理

在现有的系统中录入会议室信息不变，在展示会议室一周使用情况一览表中把上午下午改成四个时间段展示；

上午分为：8:00--9:00　　下午分为：14:00--15:30

9:00--10:00　　15:30--16:30

10:00--11:30　　16:30--17:30

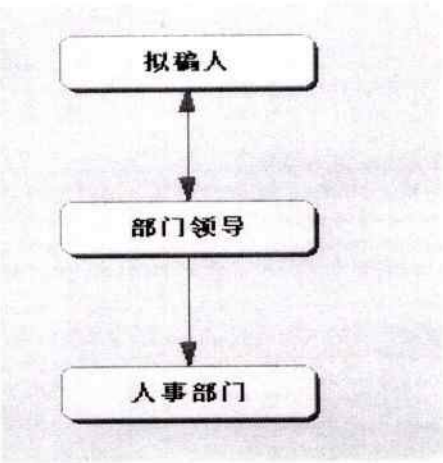
3.4.4 考勤管理

单独在系统中做一个考勤审批单，部门考勤管理员录入本月考勤情况，给部门领导审批，部门领导发给人事处归档。

考勤审批单

标题	
附件	
拟稿人	
部门领导意见	
人事部门	

流程图



3.4.5 值班管理

值班管理员在系统中导入 4 张值班表（EXCLE），给校长办公室主任审核，校长办公室主任审核通过后，进行发布。

在登录页面体现当日值班人员，在节假日体现从节假日前一天到假期最后一天的值班人员，将其他值班人员合成一张表，对当日值班人员进行平台信息提醒。

4、验收要求

1、乙方应在签订合同后 30 天内向甲方完成校园密码应用服务系统的供货、安装、调试、及配套密码改造服务。乙方必须在测试与验收前，向甲方提供按本合同的技术规格、技术规范的要求进行的测试与验收方案。

2.软件安装调试完毕，经甲方试用正常，使 OA 办公系统符合国产密码相关要求、符合学校相关部门（校长办公室）使用要求，乙方应备齐相关资料及验收文件，以书面形式向甲方提出验收申请。甲方按验收流程组织实施验收。