统一身份认证平台项目

招标技术需求

2019年3月

1 项目背景

近年来，我校高度重视信息化建设，针对公共数据共享以及数据决策支持进行了长期规划。本次项目，将在原有信息化建设基础之上，完善和升级统一身份认证平台，通过本次项目的完善和升级，实现校内统一的用户管理、统一的授权管理、安全的单点登录，并支持第三方系统的认证服务。针对全局业务系统，提供统一的信息采集、安全审计以及统计分析功能。采用集中统一的用户管理模式、统一认证和授权管理平台、实现用户的一点登录、多点漫游，并建立完善的操作审计管理机制。最终建设完成我校的身份识别与访问控制平台。

1.1 项目建设原则

1）标准化、规范性和开放性

全校范围的信息化建设是一个庞大的系统工程，其体系的设计、系统的实施等必须遵循一系列的规范、标准，确保各个分系统的有效协调，整个系统能安全地互联互通、信息共享。

2）先进性、成熟性和使用性

系统设计既要采用先进技术和系统工程方法，又要注意技术的可行性和实用性，方法的正确性。实用性放在首位，先进性与成熟性并重，并符合未来的发展方向。

3）开放性与标准化原则

应用平台应是一个开放的且符合业界主流技术标准的系统平台，对网络的硬件环境，通信环境，软件环境，操作平台之间的依赖小。

4）可靠性、稳定性和容错性

在考虑技术先进性和开放性的同时，还应从系统结构，技术措施，系统管理等方面着手，确保系统运行的可靠性和稳定性，达到最大的平均无故障时间。

5）可扩展性及易升级性

为适应应用不断拓展的需要，应用平台的软硬件环境必须有良好的平滑可扩

充性。要提供简便、规范、畅通的基础数据服务。

6）安全性和保密性

在应用平台设计中，即要充分考虑信息资源的共享，更要注意信息资源的保护和隔离，应分别针对不同的应用和不同的网络通信环境，采取不同的措施，包括用户安全性、数据安全性、运行安全性等。要求对数据库提供灵活的备份和恢复机制，确保系统发生故障时，及时恢复，不会受到影响。

7）可管理性和可维护性

平台是由多个部分组成的较为复杂的系统，为了便于系统的日常运行维护和管理，要求所选产品具有良好的可管理性和可维护性。另外可管理性和可维护性还包括对平台的自身。

1.2 项目技术路线要求

标准性：采用最新的 CAS 协议，支持 OAuth2.0、OpenID、SAML 等标准协议，支持代理认证模式，提供标准的对接接口。

安全性：保证系统数据传输的安全性；用户密码采用不可逆的加密算法加密存储，支持密码强度配置，并在用户设置密码时进行检查；系统支持首次登录强制修改密码的设置；系统支持强密码策略设置功能，对用户的操作进行完整的日志记录，用户可查看用户的重要日志记录情况，提供统一的登录注销页面，并支持自定义返回页面；可开启账号恶意登陆锁定、一个账号只允许一个终端登录、多次登录失败后启用验证码、登录成功进行消息提醒等功能；

稳定可靠性：身份数据来源于学校统一建设的基础数据库，支持数据库和 LDAP 两种存储形式，数据库和 LDAP 实时进行数据同步。系统支持垂直和水平扩展，支持集群、热备和负载均衡；系统能保证 7*24 小时对外服务。

可扩展性：支持多种对接开发语言（java、.net、php、asp 等），对于不支持的语言，提供代理认证支持；支持多种对接形式（B/S、C/S、手机 app、微信公众平台等）；提供多种对接接口 API 及文档和 DEMO，并制定具体的管理制度；提供认证、身份、授权层面的接口；提供手机、邮箱、动态口令、二维码、微信、QQ、手机 APP 的对接实现；有完善的使用和二次开发培训体系。

可管控性：管理员可监控认证系统各项功能服务的运行情况状态，并对部分

参数和功能进行一定的调配，例如监控各个对接系统的认证接入情况，如果出现异常可以通过管理端进行人工干预，停止相应系统的接入服务，也可以监控具体账户的登录情况，出现异常可以人工禁用；用户可获取用户自身数据相关情况，并实施一定的控制；对于部分特殊的事项可以通过短信平台直接反馈给管理员；

可配置性：通过后端对各项功能进行配置，包括功能是否启用、功能具体参数配置等，使管理员可以通过管理端完成大部分的配置功能，而不需要通过调整配置文件甚至修改代码来完成。用户和对接人员也可以通过 web 端完成各项配置工作。

易升级性：具备系统升级的完善计划和方案，避免频繁升级、打补丁。提供产品升级的现场服务，实现功能和数据的平滑升级。提供符合行业标准的二次开发接口，保证将来能够进行升级改造。

支持集群、热备、负载均衡;系统使用 oracle 和 MySQL 主流关系数据库。

提供友好易用的界面，支持同步数据中心数据异动。

提供完善的监控功能，可对平台内的用户、应用、服务进程和服务器硬件资源进行实时监控，且可通过各类图表进行直观的结果展现。可对用户身份帐号的管理、授权以及用户的认证行为中可能存在的问题进行审计,所有操作均日志记录，能够对每个角色管理员的操作行为、用户自助管理行为和用户登录访问行为进行记录。

支持 5 万级的用户注册，单机部署时应能支持最大 500 人的并发用户数，双机负载均衡部署时支持 1000 人的并发用户数。

2 项目建设内容

2.1 统一身份认证平台

2.1.1 建设目标

随着应用建设的逐步深入，已经建成的和将要建成的各种数字校园应用系统存在不同的身份认证方式，用户必须记忆不同的密码和身份。因此，要建设以目

录服务和认证服务为基础的统一用户管理、授权管理和身份认证体系，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。即用户经统一应用门户登录后，从一个功能进入到另一个功能时，系统平台依据用户的角色与权限，完成对用户的一次性身份认证，提供该用户相应的活动“场所”、信息资源和基于其权限的功能模块和工具。

在数字校园建设中，要求采用以目录服务和认证服务为基础的统一用户管理、授权管理和身份认证体系，将组织机构信息、用户身份信息统一管理，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。

2.1.2 总体技术要求

1）平台基于 J2EE 体系结构，所有功能模块定义服务提供者接口（Service Provider Interface），可以支持第三方的服务提供者；

2）在身份认证系统设计中，为了适应当前以及今后系统的建设发展需要，采用的技术实现手段主要包括 LDAP、PKI、SSO、SSL 等等；

3）单点登录从实现技术上基于 session、cookie、rewrite 技术和采用 portal 等几种方法，根据用户的情况可以选用其中的任何一种。

4）平台的管理与维护采取分级模型支持多级的管理；

5）提供基于角色的权限控制体系（RBAC），支持多种权限管理方式，如单独授权、按角色授权和分级授权等，灵活的授权分配，满足学校未来应用授权需要。采取分级授权，可以根据业务的需要灵活制定安全策略控制授权；

6）采用灵活的基于角色的权限管理模型，集中的权限控制的授权管理面向全局的用户和数据资源，覆盖了各种应用；

7）灵活定义角色之间的继承、相容和互斥关系，授权简单、便捷；在访问控制策略上，用户可以定制不同粗细粒度的安全规则；

8）身份、授权、认证功能相对独立，可以灵活的与第三方产品对接。

2.1.3 建设内容及功能要求

统一身份认证平台是一个集用户身份、认证与权限的支撑平台，从建设内容

与功能来说，统一身份认证平台建设应至少包括以下主要内容：

序号	功能	描　述
1	统一用户管理	统一用户管理应包括用户管理、用户组管理、组织机构管理三部分功能。 实现对校内外用户的统一管理，包括用户新增、删除、冻结、解冻等； 实现不同组织机构展现和管理； 实现用户组管理实现相同权限的用户集合的管理，包括用户组维护、用户组授权等。
2	角色管理	实现以角色控制用户的功能权限，包含角色管理和角色组管理。
3	统一授权管理	实现用户的实际权限授予，可方便实现用户与角色的授权、用户组与角色的授权、组织机构的授权、用户组与角色的授权，支持根据用户属性自动授权与收回，支持无限级分级授权。
4	身份认证服务	为应用系统提供统一的用户身份认证服务，至少包括下列用户认证方式：用户名/口令认证、数字证书认证、SSO 认证、微信认证、认证集成接口。并提供多种认证接口与范例（.Net 接口、JAVA 接口、ASP 接口、PHP 接口等）
5	应用管理	对应用系统的功能进行管理，应支持应用系统注册、应用系统功能注册、应用属性注册等。
6	系统管理	要求至少能够实现分级管理、密码策略、安全问题管理、数据项扩展、默认配置管理、字典管理以及日志管理等功能。
7	★集成内容	实现现有系统平台上的所有业务系统与统一身份认证系统进行无缝免费对接，实现校内用户的统一认证、统一权限和单点登录。实现与现有公共数据平台的数据集成，保证人员、机构等数据免费无缝对接，并与现有身份认证系统的密码保持一致。支持数据库和 LDAP 的同步。

3 项目实施要求

3.1 实施进度要求

在分阶段实施计划的基础上，进一步明确和细化每个阶段的工作范围、内容、人力投入、过程、责任、交付成果等。

3.2 成果交付要求

在本项目的开发过程中和交付使用后，各个阶段都会有各种成果和文档资料。这些成果和文档资料对所开发系统的维护和持续发展起着非常重大的作用。因此，要求将全面、规范的成果和文档资料交付给用户方，而且要提供明确的交付清单。同时，成果和文档资料必须符合软件工程的相关要求。要交付的成果和文档资料主要包括但不限于以下部分：

（1）执行代码和源代码：保证系统正常运行的所有执行代码，以及项目开发过程中为用户方定制功能的源代码（中标公司或第三方已有产品的源代码除外）。

（2）技术文档：包括项目开发中的各种技术文档，如，开发环境配置说明、需求分析说明、系统设计说明、用户手册、系统维护说明、系统培训资料以及有关系统接口的技术说明等等。

（3）以文档形式存在的项目成果：如系统建设中形成的各类标准规范、调研分析、规划设计报告等等。

（4）管理文档：包括项目开发中的一些工作文档，如，计划、报告、讨论纲要、会议记录等。

（5）提供流程实施过程中过程记录，如文档管理、版本管理、变更记录等。

交付的所有成果应包括成果的电子化版本。

3.3 服务和培训要求

投标单位需提供系统验收后 3 年的免费维护服务。规划制定系统的运行与

维护策略和具体方案，对售后服务及系统维护的技术责任、条件和支持体系作明确说明。

培训是平台建设的一个重要组成部分。在项目的不同阶段要求提供相关的培训课程，面向系统开发和管理员、各级领导、各类用户等不同群体提供系统化、定制化和有针对性的培训。

（1）培训内容应针对系统管理人员和各类用户分别进行。通过培训应使各类用户能独立进行相应应用与管理、故障处理、日常维护等工作，确保系统能正常安全运行。

（2）投标单位应在投标文件中提出培训计划，计划包括培训项目、人数、地点等详细内容。

（3）培训人员必须是投标单位的正式雇员或专业的授权培训机构雇员。如果使用第三方培训机构，投标单位应在投标文件中提供培训机构的名称，并能根据情况调整。

4. 评分标准

4.1 商务评分标准 (40 分)

序号	评审因素	评分标准说明	分值	
1	报价	满分为 20 分。投标报价的算术平均值 A 的 100%作为期望投标价（A 指在有效投标文件中各投标报价的算术平均值；投标报价等于期望投标价的得 20 分，投标报价比期望投标价每高 5%扣 1 分，每低 5%扣 1 分，依此类推，不足部分按插入法计分（保留两位小数）。	20 分	
2	企业资质与信誉	投标人拥有 ISO9001 质量体系认证证书,具备得 1 分，不具备不得分。	1 分	10 分
		投标人拥有统一身份软件著作权和产品登记证书，具备得 1 分，不具备不得分。	2 分	
		投标人拥有省级以上软件企业认证资质,具备得 1 分，	1 分	

		不具备不得分。		
		投标人拥有高新技术企业，具备得 1 分，不具备不得分。	1 分	
		投标人熟悉高校业务，具有丰富的高校行业经验，能够提供基础平台、学工、资产、后勤、教务、一卡通产品登记证书或著作权证书和相关案例，每有一项得 1 分，最多得 6 分	6 分	
3	**企业业绩**	投标人能够提供5个及以上高校统一身份认证业绩的合同案例， 每提供一个得 2 分。	10 分	10 分
合计			40 分	

4.2 技术评分标准(60 分）

序号	评审因素	评分标准说明	分值	
1	**技术指标响应情况**	专家依据技术规格偏离表响应情况评判，技术指标完全满足要求的得满分。每偏离一项的扣 3 分，满分 30 分，扣完为止。	**30 分**	
2	**实施方案**	项目实施方案（6 分） 具有详细、规范、合理的项目实施方案，并给出详细的项目进度计划安排时间表，酌情给分，得 0-6 分，没有不得分；	**6 分**	**20 分**
		项目对接实施（10 分） 与原平台数据、接口对接方案合理且满足要求的，得满分，不满足要求的得 0 分；	**10 分**	
		人员配置（4 分） 投标人需为该项目配置水平高、项目经验丰富的人员进行项目建设与实施，专家根据具体实施人员的素质、水平、经历、数量和配置情况，酌情给分，得 0-4 分，没有不得分；	**4 分**	
3	**售后服务方案**	系统培训（5 分） 投标人具有对项目中各角色人员的全面培训方案和计划，酌情给分，得 0-5 分，没有不得分。	**5 分**	**10 分**
		售后服务（5 分） 投标人具有完善的售后服务方案和计划，酌情给分，得 0-5 分，没有不得分。	**5 分**	
合计			60 分	