**《上海建桥学院统一身份认证平台项目》项目需求**

一、概述

近年来，学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。最终建设完成学校的统一身份认证平台。

二、总体要求

本期项目建设坚持实用性和先进性原则、标准化和可扩展性原则、开放性和安全性原则、可靠性和可管理性原则。

1、实用性和先进性

充分考虑学校信息化建设的实际情况，根据现有信息系统和已有数据库情况，满足校内师生迫切需求，以用户为中心，方便易用，给师生以良好的用户体验，同时为管理服务人员提供便捷使用的操作界面。

项目的建设立足于当今世界先进且具有良好发展前景的技术，系统能够随着未来信息技术的发展而不断平滑升级。

本项目所开发的系统基于Java J2EE平台。

2、标准化和可扩展性

系统开发所使用的各类代码标准和数据标准符合国家信息标准、教育行业标准和学校信息标准。

系统建设过程中充分考虑可扩展性和灵活性，能够保证其他相关软件产品和新开发的各类信息系统的无缝接入。学校可根据需求，在现有平台上自行开发新的应用系统或功能模块。

3、开放性和安全性

系统的建设将采用开放式架构、开放标准且符合业界主流技术标准的系统开放平台。我司必须将功能性代码开放给学校，以便于学校自行进行二次开发。

系统具备完善的安全体系结构。在系统设计中，既要充分考虑信息资源的共享，更要注意保护信息资源的安全性，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。

4、可靠性和可管理性

在考虑技术先进性和开放性的同时，从系统架构、技术措施、实施过程、系统管理等方面着手，尽力减少系统缺陷，确保系统运行的可靠性和稳定性，例如不能出现单点故障；在用户访问高峰期能够通过硬件调整、软件调优、性能优化、系统设置等多个方面实现平稳可靠的服务。

1. 技术要求

1、协议：采用CAS协议4.0以上版本，支持OAuth2.0协议及其完整的管理功能；提供LDAP服务。

2、系统架构：系统基于Java J2EE平台开发。采用微服务架构，支持Docker容器标准。以服务注册与发现、服务监控、故障转移、熔断保护、虚拟化弹性计算、分布式计算、灰度发布等技术手段,实现硬件资源利用效率高、高可靠、高性能、高弹性、易运维的统一身份认证系统。系统能保证7\*24小时不间断对外服务。

3、数据库：支持Oracle/Mysql等主流数据库。系统需要支持登录日志、访问日志、审计日志等海量日志数据的存储与快速检索。支持人员账号数据库和LDAP两种存储形式，数据库和LDAP进行实时数据同步。

4、接口：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。

5、支持终端：支持PC、笔记本、PAD、智能手机等多种类型终端，支持IE、Edge、Chrome、Firefox等浏览器。

四、功能需求

统一身份认证平台是学校信息化服务平台的重要基础支撑平台，提供统一的身份认证服务，用户身份管理、个人自助服务等功能，为用户完成单点登录，向各个系统提供基础的身份认证接口。

建立全校统一的业务系统认证集成平台，通过提供的集成文档和各开发框架的示例代码，业务系统通过统一身份认证系统接口，可快速完成系统认证集成。

1. 统一认证服务

通过统一的登录界面，对用户输入的账号密码进行认证，进而为集成的应用系统提供访问控制功能。可以为PC端、手机端提供同一套登录界面。系统界面采用扁平化风格，自适应页面及分辨率。可以为不同的业务系统提供不同模板风格的登录界面。

支持单点登录、单点注销。

支持多种认证策略，如是否启动验证码，失败多次出现验证码，失败多次锁定一段时间等。

支持账号登录成功后消息提醒服务。

支持账号异动提醒，账号锁定时消息提醒等。

1. 认证方式

支持用户使用学校标准账号和自定义账号（别名/邮箱）登录，支持动态口令、APP扫码、微信扫码登录。

提供和第三方系统账号（QQ、微信）绑定登录，绑定后，第三方系统登录后，可直接登录身份认证，无需再次登录。

提供移动APP的SSO解决方案，保证第三方APP无法接触用户口令，其后台能直接使用CAS协议完成登录认证。

提供一段时间（如5天）保持登录功能。

为业务系统提供统一的自有账号登录方案。

提供业务系统基于签名模式的认证对接及开放接口。

支持应用账号的管理，针对尚未对接过任何统一认证的业务系统，提供特殊的反匹配方案，保证业务系统集成统一认证时，可以在不改变用户信息编码的情况下，直接获取和使用统一认证用户

1. 用户身份管理

从数据源头（如：人事处、学工处、研究生院、海外教育学院等）、用户状态（在校、离校、在职、离职）、用户的类型等把用户分成不同的身份群体，身份群体之间的成员可能会重复、交叉，身份数据依赖于源头提供的基础数据和公共库的同步规则形成，可以增加、减少。

身份包括教职工（在职、离职、退休、离校）、本科生（统招生、双学位、交换生）、研究生（硕士、博士）、留学生（本科、硕士、博士）等。

支持用户、身份的互查，不同身份的组合查询。

支持用户信息在线管理、导入功能。

支持用户头像维护。

支持将用户信息同步到LDAP、AD等目录服务器中。

支持对现有的人员机构数据进行及时的梳理。

支持对用户身份分布，账号概况的统计分析。

1. 统一权限管理

支持角色自定义，可以增加、修改、删除角色。

支持对角色授权和撤销权限。

支持查询当前用户的管理权限。

支持按组织机构、用户对系统内功能模块进行授权。

支持应用的注册授权，可以根据需要停用和启用某个应用。

支持基于URL的授权访问，支持按用户、组、机构授予应用的访问权限。

1. 系统监控

提供基础环境监控，可以实施查看系统运行状态。

提供认证监控、账号概况等监控手段。

提供数据库监控，数据库连接异常时消息提醒服务。

提供弱密码监控，可疑账号监控等。

1. 审计管理

提供完备的操作日志，保证系统中所有操作可追溯。

提供统一认证日志，包括用户、时间、IP、登录结果、失败原因等。

提供对认证日志的统计分析功能。

1. 个人自助服务

支持用户通过手机号、邮箱、密保问题找回密码功能。

支持用户查询自身账号的认证记录和账号维护记录。

支持用户查询自身账号的认证概况及认证细节。

支持用户查看和维护已绑定的第三方账号（微信、QQ、钉钉等）。

支持用户对自己账号信息和密码信息的维护。

支持用户微信端、APP端的自助服务，包括用户信息的维护，密码找回等。

五、其他需求

1. 平滑升级

支持业务系统平滑升级到新的统一认证。

1. 性能

支持5万级的在线用户，单机部署时能支持最大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。

1. 安全

保证系统数据传输的安全性；用户密码采用公开不可逆的加密算法存储；提供完整的用户登录登出日志；支持恶意登录账号的锁定，多次登录失败启动验证码、一个账号只允许一个登录端、登录成功进行消息提醒等；第三方接入系统需注册后才能使用对接服务。

六、工程实施要求

1. 实施进度要求

本次项目严格按工期部署完成，并达到采购人的要求。我司需要在投标文件中给出预实施工期进度表。采购人签订合同后3个月内完成项目完成开发部署，达到验收条件，开始试运行。

1. 实施方案

该项目需求复杂，涉及部门、环节多，为了保证实施过程顺利有序，我司制定出详尽缜密的实施方案，主要内包括以下几个方面：

* **组织架构与职责**

1、描述项目成员的组成，以及成员的职责。

2、提供项目经理一人，负责全程跟踪项目的开发与实施，直至该项目验收。

* **实施阶段划分**

描述各个实施阶段的工作范围、内容、人力投入、过程、责任、交付成果等。

* **项目管理要求**

我司提出对项目的建设进行科学严格的管理方案与措施，保证项目全面顺利实施。

* **项目配置管理**

在项目的建设过程中以及交付使用后，会产生大量文档和程序，如：需求分析说明、设计说明、可执行码、用户手册、测试用例、测试结果等技术性文档以及合同、计划、会议记录、报告等管理文档，而且文档的版本在不断变迁和修改中，势必产生一个庞大、动态的信息集合。因此，必须建设相应的配置管理系统，通过一系列技术、方法和手段来维护产品的历史、鉴别和定位产品独有的版本、在产品开发和发布阶段控制变化，制定规范的配置管理工作计划和流程，沟通交流配置管理工作情况，从而使管理制度化、有效减少重复性工作、保证产品的质量和效率和系统的后续升级和维护。

* **项目管理规范和手段**

根据项目的实施方案，在实施过程中，为了保证用户方、开发方能够对项目建设实施进行监控，及时发现和解决的问题，建立相应的项目管理规范，包括项目执行监控流程、执行监控的方法、执行监控的责任等，使管理和监控工作流程化、规范化，管理和监控工作责任明确。

* **项目管理控制**

项目的管理控制包含多个方面：项目范围、风险、进度、质量、变更管理控制，贯穿项目开发建设的始终，必须做到对项目建设范围准确定义，一旦范围发生变更，要有相应的变更控制和应对措施。

* **风险管理**

项目风险管理是对项目风险从识别到分析到应对措施的一个过程，包括风险识别、风险量化、风险对策、风险对策实施控制四个方面。项目在实施过程中会出项各种各样的风险，必须做到充分、有效识别风险，应对风险和控制风险，在项目实施之初必须制定风险预测和规避风险的对策。

1. 服务与培训
* **培训要求**

1、在项目合同中将具体规定培训内容、培训时间和培训名额等。

2、我方派出的培训教员具有丰富的同类课程的教学经验和应用经验；所有的培训教员必须用中文授课；我方为所有被培训人员提供培训用文字资料和讲义等相关材料。

3、我方按合同规定安排培训时间和培训名额，在实施过程中，针对系统管理人员提供培训，保证培训的效果，让系统管理人员都能熟练掌握系统的使用方法。

* **售后服务要求**

本项目软件要求中标人提供自项目验收合格之日起为期一年的免费现场质保服务。质保期内，我司必须继续按使用单位要求修复系统存在的缺陷，保障系统的正常运行。