本文引用格式：柯家海,黄劲荣,杜岭,等.高校统一身份认证平台的单点登录技术探究[J].自动化与信息工程,2023,44(6):60-63.
KE Jiahai, HUANG Jingrong, DU Ling, et al. Exploration of single sign on technology for unified identity authentication platform in universities[J]. Automation & Information Engineering, 2023,44(6):60-63.

高校统一身份认证平台的单点登录技术探究*

柯家海　黄劲荣　杜岭　程湛
（广州医科大学，广东 广州 511436）

摘要：针对高校的学生和教职工需要访问数量众多的信息系统，每个系统都需要单独的用户名和密码的问题，提出高校统一身份认证平台。首先，介绍高校统一身份认证平台的具体功能；然后，分析单点登录的 3 种常见技术：中央身份服务、全断言标记语言、开放授权；最后，结合学校情况，对高校统一身份认证平台的单点登录进行应用测试。测试结果表明，用户在通过单点登录后，所有系统都能同步登入，功能和性能满足需求。

关键词：高校统一身份认证平台；单点登录技术；中央身份服务；全断言标记语言；开放授权

中图分类号：TP391.4　　**文献标志码：**A　　**文章编号：**1674-2605(2023)06-0010-04

DOI：10.3969/j.issn.1674-2605.2023.06.010

Exploration of Single Sign on Technology for Unified Identity Authentication Platform in Universities

KE Jiahai　HUANG Jinrong　DU Ling　CHENG Zhan
(Guangzhou Medical University, Guangzhou 511436, China)

Abstract: In response to the issue that students and faculty in universities need to access a large number of information systems, each system requires a separate username and password, a unified identity authentication platform for universities is proposed. Firstly, introduce the specific functions of the unified identity authentication platform for universities; Then, analyze the three common techniques of single sign on: central authentication service, security assertion markup language, open authorization; Finally, based on the situation of the school, conduct application testing on the single sign on of the unified identity authentication platform for universities. The test results show that after single sign on, users can log in to all systems synchronously, and the functionality and performance meet the requirements.

Keywords: unified identity authentication platform in universities; single sign on technology; CAS; SAML; OAuth

0　引言

随着信息技术的不断发展和普及，高校的各种教学和管理活动越来越依赖各种信息系统。在智慧校园的建设过程中，高校信息系统扮演着非常关键的角色，从办公 OA、教育教学、人事管理、教务管理、在线学习平台、科研管理、学生事务到后勤管理，高校的各种业务活动都离不开信息系统的支持。但在实际的高校环境中，这些信息系统一般由不同的供应商提供，有各自独立的账号和密码，学生和教职工需要在不同的系统之间频繁地切换，给用户带来了很大的不便。因此，实现统一身份认证，即用户只需要登录一次，就可以访问所有的系统，已成为高校信息化建设的重要课题。为解决这一问题，高校的统一身份认证平台应运而生，它可以实现用户在各个系统中的统一登录和访问控制。

1　统一身份认证平台的具体功能

统一身份认证平台是一个集中管理和提供身份认证和授权服务的平台，用于实现用户在多个系统中的单点登录和统一身份管理。为了提供集中和统一的方式来管理和验证用户的身份，统一身份认证平台通

* 基金项目：广东省大数据分析与处理重点实验室开放基金资助项目（202302）

常需实现单点登录、身份验证、用户管理、权限管理、多因素认证、审计和报告、安全性和合规性等功能。

单点登录，允许用户只需要进行一次身份验证，就可以访问多个应用和服务，不仅可以提供更好的用户体验，还可以减少密码被盗用的风险。

身份验证，通常通过用户名、密码或其他形式的凭证（如数字证书等）来验证用户的身份，确保用户是真实的。

用户管理，提供一种集中的方式来创建、更新、删除和查询用户，简化用户管理的复杂性，提高效率。

权限管理，定义和管理用户的权限，确保用户只能访问被授权的资源和服务。

多因素认证，要求用户提供多种形式的凭证来验证其身份，提高安全性。如，除密码外，还可以要求用户提供一次性的验证码或生物特征。

审计和报告，记录和报告用户的身份验证和授权活动，帮助检测和防止不正常或恶意的行为。

安全性和合规性，确保平台的安全性，并满足各种法规和标准的要求。

2 单点登录技术

单点登录（single sign on，SSO）是解决统一身份认证问题的关键技术，它允许用户通过一次登录就可以访问所有的系统。目前，常用的单点登录技术有中央身份服务（central authentication service, CAS）、安全断言标记语言（security assertion markup language, SAML）和开放授权（open authorization, OAuth）等[1-2]。

2.1 CAS 单点登录技术

CAS 是一种开源的单点登录解决方案，它提供了一个用于身份验证的中心服务器和一套客户端库。当用户首次访问任何一个系统时，CAS 会将用户重定向到中心服务器进行身份验证，并生成一个由身份认证服务授予的票据（ticket granting ticket, TGT），存储在用户浏览器的 Cookie 中。当用户访问其他系统时，CAS 会检查用户 Cookie 中的 TGT，如果存在有效的 TGT，CAS 将生成一个服务票据（service ticket, ST），并将用户重定向回该系统，该系统再次将 ST 发送给 CAS 进行验证，确认后用户便可以访问该系统[3-4]。CAS 技术原理如图 1 所示。

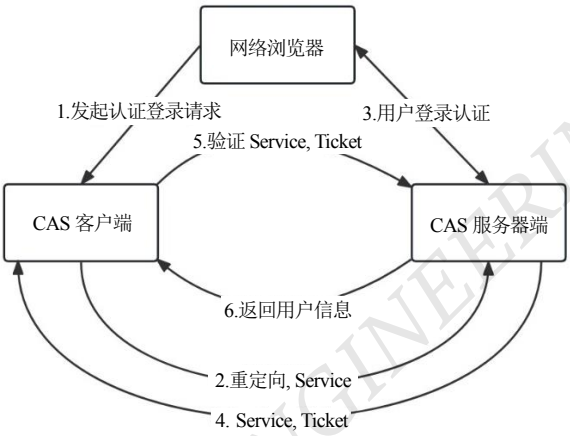

图 1 CAS 技术原理图

2.2 SAML 单点登录技术

SAML 是一种基于 XML 的开放标准，用于在安全域之间交换身份验证和授权数据，从而实现单点登录功能。SAML 定义了主体（用户）、身份提供者和服务提供者 3 种角色。在 SAML 单点登录过程中，身份提供者对用户进行身份验证，服务提供者负责提供服务。当用户首次访问服务时，如果用户还没有进行身份验证，服务提供者会将用户重定向到身份提供者进行身份验证。这个重定向请求采用 SAML 请求来进行，它包含了服务提供者的信息和请求的详细信息。身份提供者接收到 SAML 请求后，会提示用户进行身份验证，如输入用户名和密码。如果身份验证成功，身份提供者生成一个 SAML 断言，这个断言包含了用户的身份信息和其他相关属性。服务提供者接收到 SAML 响应后，验证这个响应的有效性，包括验证 SAML 断言的签名和有效期等。如果验证成功，服务提供者先提取 SAML 断言中的用户信息，再根据这些信息来进行授权，如创建用户的会话和设置用户的权限。

2.3 OAuth 单点登录技术

OAuth 是一个开放的授权协议，目前的主流应用版本为 2.0，它允许第三方应用在用户的许可下访问其存储在其他服务提供商上的资源。虽然 OAuth 主要

用于授权，但它也可以用于实现单点登录。在 OAuth 的流程中，用户首次访问应用时，应用将用户重定向到服务提供者进行身份验证。身份验证成功后，服务提供者会生成一个访问令牌，并将其发送给应用，应用使用访问令牌请求访问服务提供者的资源[5]。OAuth 技术原理如图 2 所示。

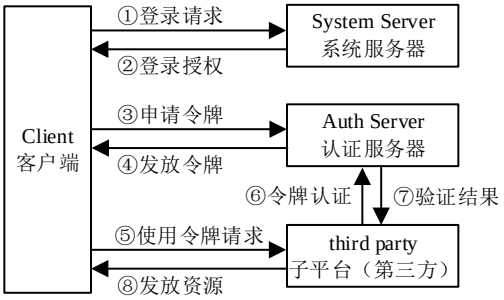

图 2　OAuth 技术原理图

3　高校统一身份认证平台实现

在实现高校统一身份认证平台时，需根据技术的成熟度、社区支持、与现有系统的兼容性等选择适合的单点登录技术。如果高校的信息系统主要基于 Java 开发，那么 CAS 是一个好的选择；如果系统之间需要频繁交换身份验证和授权数据，那么 SAML 更合适；如果需要接入第三方应用，那么选择 OAuth[6]。结合广州医科大学的实际情况，考虑到所有信息系统的历史沿革，采用以 CAS 为主要方式，搭配 OAuth 的协议；同时考虑到企业微信，采用多种单点登录技术融合，进行高校统一身份认证平台的建设。

首先，搭建 CAS 服务器，并在服务器端准备 Java 的运行环境。因为 CAS 是基于 Java 开发的，需要安装 JDK 和 Maven，同时还需要 Servlet 容器，用于管理和加载类，采用了 Apache Tomcat。

然后，下载安装 CAS 服务器端（CAS war 文件），采用 Maven 构建并配置 CAS，如 CAS 与用户目录（LDAP）进行集成、配置 SSL 证书。

接着，将 CAS war 文件部署到 Tomcat 中，将 war 文件复制到 Tomcat 的 webapps 目录下，启动 Tomcat，CAS 就会启动。

最后，通过访问 https://www.gzhmu.edu.cn/cas 来验证 CAS 是否正常工作，同时需要为每一个应用设置一个 CAS 客户端，并进行配置，启用 CAS 保护并进行对接。

本文以学校继续教育学院网络教学系统对接为例，确定系统对接地址为 http://fysso.chaoxing.com/cassso/gzhmujxjy。当浏览器访问该地址时，该地址内部需要检查访问该地址时是否携带统一认证信息。若携带，访问 CAS 认证的校验接口，校验认证信息正确性后，携带认证的账号信息跳转到学校统一身份认证平台，完成业务方自己的登录认证，流程结束。若没携带，带着自己的回调地址 https://sso.gzhmu.edu.cn/cas/login?service=http://fysso.chaoxing.com/cassso/gzhmujxjy 重定向到 CAS 认证登录页面。如果用户在没有携带统一认证信息的登录页面输入账号后，CAS 统一认证会继续访问 http://fysso.chaoxing.com/cassso/gzhmujxjy，并追加统一认证的参数，再跳转，从而实现单点登录。

考虑到企业微信的广泛应用，将企业微信的单点登录功能对接到高校统一身份认证平台。

首先，需要在企业微信的管理后台创建一个应用，并获取该应用的唯一标识（AgentId）和密钥（Secret）。

然后，当用户访问学校的应用系统时，如果用户没有登录，那么应用系统可以重定向用户到企业微信的登录页面进行登录。

其次，若登录成功，企业微信生成一个临时的登录票据并重定向用户回到应用系统，同时在重定向的 URL 中附带这个登录票据。

再次，应用系统收到重定向请求后，先从 URL 中获取登录票据，再利用这个登录票据和应用系统的密钥调用企业微信接口，获取用户的唯一标识。

最后，应用系统根据用户的唯一标识在高校统一身份认证平台中创建一个会话，再将用户认为已登录，并允许用户访问应用资源[7]。

4　高校统一身份认证平台的测试

高校统一身份认证平台实现了学校办公类、教学类、科研类、学生管理类、财务类、其他类等 40 多个

系统统一身份认证的单点登录。

为验证高校统一身份认证平台单点登录的可行性，采用 Postman 进行功能测试，Apache Jmeter 进行性能测试。测试条件包括不同的浏览器等，测试数据包括用户数据和应用数据。

4.1 功能测试

首先，根据系统的 CAS 设置环境变量；创建一个 GET 请求到 CAS 的登录页面（https://cas.gzhmu.edu.cn/cas/login）；发送请求并在响应中查找“execution”参数，用于验证登录请求。

然后，创建一个 POST 请求到 URL（https:// www.gzhmu.edu.cn//cas/login）；POST 请求的 body 中包含 username、password 和在上一步获取的 execution 等参数；请求返回一个 ticket-granting ticket (TGT)。

接着，创建一个新的 POST 请求到 TGT 的 URL（https://www.gzhmu.edu.cn//cas/api/v1/tickets/TGTid）；POST 请求的 body 中包含要访问的服务的 URL，该请求返回一个 ST。

最后，创建一个 GET 请求到 ST 的 URL（https:// www.gzhmu.edu.cn//cas/p3/serviceValidate?ticket=ST-id&service=service-url）；该请求返回用户的身份信息，证明用户已经成功登录。

4.2 性能测试

首先，启动 Apache JMeter 应用程序并创建一个新的测试计划。在测试计划中添加一个线程组，其决定了并发用户的数量和测试的持续时间。

然后，在线程组中添加 HTTP 请求采样器，并设置请求类型为 GET，服务器名称和路径设置为 https://www.gzhmu.edu.cn/cas/login。在 GET 请求采样器下添加一个正则表达式提取器，用于从响应中获取“execution”参数。

接着，添加第二个 HTTP 请求采样器，设置请求类型为POST，在参数列表中，添加username、password 和 execution 参数。

最后，添加一个查看结果树侦听器，用于查看请求和响应的详细信息。

测试结果表明，用户通过单点登录后，所有系统均能同步登入，功能和性能满足要求。

5 结论

统一身份认证平台是高校信息化建设的重要部分，可以促进高校信息系统的集成。它提供了一个中心化的用户数据库，所有系统都可以从这个数据库中获取用户数据，使系统间更容易共享用户数据。本文通过选择合适的单点登录技术，设计和实现身份验证中心，对各个系统进行对接改造，并进行全面的测试，实现高校信息系统的统一身份认证，提高了用户体验感和系统安全性。

参考文献

[1] 龚欢欢.改进的 CAS 多 Web 应用单点登录[D].南京:南京大学,2021.

[2] 莫竣成,田秀云.基于 Java 的网上购物平台系统设计[J].机电工程技术,2021,50(1):103-105.

[3] 肖桂霞.基于 B/S 架构的 Web 单点登录协议综述[J].软件,2023,44(1):1-5.

[4] 童世华.基于 SM4 算法的移动终端接入车间信息系统的安全性设计与验证[J].机床与液压,2019,47(7):105-109.

[5] 李强.基于 CAS 和 OAuth 的统一认证授权系统设计[J].信息技术与网络安全,2021,40(6):83-88.

[6] 张黎娜,童敏.基于 SSO 的开放大学智慧化校园建设的探索与实践[J].电脑知识与技术,2022,18(4):48-50.

[7] 梁方勇,陈桂强.数字校园下基于单点登录的企业微信无感登录系统实现[J].中国新技术新产品,2023(1):49-52.

作者简介：

柯家海，男，1981 年生，高级工程师，硕士，主要研究方向：教育信息化、网络与多媒体技术、教学数据分析。E-mail: kejiahai@gzhmu.edu.cn

黄劲荣，女，1972 年生，高级工程师，硕士，主要研究方向：校园信息化、智慧医疗。

杜岭，女，1987 年生，高级工程师，硕士，主要研究方向：校园信息化、大数据分析与应用、智慧医疗。

程湛，男，1982 年生，高级工程师，硕士，主要研究方向：智慧教学、人工智能、教育资源开发。