数字化校园中统一身份认证平台的设计

郭楚杰

（广东工业大学 机电工程学院，广东 广州 510006）

摘 要：统一身份认证平台能在高度集成的校园网络应用环境中，将相互独立应用系统中的用户和权限资源进行统一、集中管理。统一身份认证平台的设计是在开源门户系统Liferay基础上，配置LDAP和CAS单点登录服务，通过定制CAS的认证流程实现统一身份认证。

关键词：统一身份认证；单点登录；LDAP；CAS

中图分类号：TP311 **文献标志码**：A **文章编号**：1673-9833(2010)03-0077-04

Design of Unified Identity Authentication Platform in Digital Campus

Guo Chujie

（College of Mechanical and Electrical Engineering, Guangdong University of Technology, Guangzhou 510006，China）

Abstract: Unified identity authentication(UIA) platform realizes centralization management of users and permissions of mutual independent application systems in a highly integrated campus network environment. The design of UIA platform, based on the open portal Liferay, comprises LDAP and CAS SSO and achieves unified identity authentication by customizing the CAS certification process.

Keywords: unified identity authentication (UIA); single sign-on; LDAP; CAS

随着计算机技术、网络技术的迅猛发展，大多数高校都已具备完善的基础网络环境。但由于高校数字化校园的建设缺乏整体规划以及各阶段信息化建设的局限性，使得统一身份认证很难得以实现。统一身份认证平台的建设将实现校园内网信息门户用户身份的统一认证和单点登录（singer sign-on，SSO），改变原有各业务系统中的分散式身份认证及授权管理，实现对用户的集中认证和授权管理，简化用户访问内部各系统的过程，使得用户只需要通过一次身份认证过程就可以访问具有相应权限的所有资源。

1 统一身份认证平台的特点及功能

统一身份认证平台有如下特点：1）可以实现用户信息的集中存储及管理，保证平台中用户信息的惟一性和权威性；2）可以提供安全可靠的身份认证方式，用户只需一次认证即可畅游平台上已集成的所有应用系统；3）可以提供统一的用户权限分配功能，管理员可以在统一身份认证平台中对所有用户进行集中的权限分配，确保不同的用户在不同的应用系统中权限分明、准确，同时还能够方便管理员进行管理；4）具有良好可扩展性，为应用系统提供标准规范的接口，保证平台能够与学校的信息化发展保持同步，对已存在的应用系统有高效的可集成性，避免对目标系统进行大规模修改，以此降低成本。

统一身份认证平台的核心功能是对用户进行身份认证并实现单点登录效果。传统的单点登录技术可以分为基于脚本（Script）的单点登录技术和基于票据（Access Ticket）的单点登录技术[1]。前者主要是在用户通过认证用户身份后自动产生脚本实现登录自动化，而后者则是通过改造目标系统使其接受访问票据

收稿日期：2009-12-23

通信作者：郭楚杰（1984-），男，湖南株洲人，广东工业大学机电工程学院硕士研究生，主要研究方向为计算机网络及安全，E-mail:jerryoof@yahoo.com.cn

来实现单点登录。

当前基于票据的单点登录技术已经成为了主流技术。例如，微软提供的Microsoft Passport是在多个可访问的站点和服务上支持单点登录功能，是微软公司为其客户提供的一种可在互联网范围内实现身份验证的服务[2]，但是Passport的认证机制是将所有的认证信息都集中在一个单独的服务端，这样也就增加了安全风险；IBM的WebSphere核心是依赖其Domin环境，为内网的共享用户提供含有用户标识的基于Http的Cookies，使处于该域中的服务器之间可以实现单点登录[3]；Oracle旗下的Sun Java System Access Manager[4]是通过使用集中验证点，基于角色的访问控制以及单点登录，它简化了信息交换和交易，同时能保护隐私及重要身份信息的安全。由于.Net Passport和Sun Java System Access Manager等统一身份认证技术主要适用于Internet中的各种电子商务活动和个人Web应用，而学校的应用系统不是面向大众的，不适合于加入Passport和Liberty，因此，必须设计一个数字化校园统一身份认证平台。

2 数字化校园中统一身份认证平台设计方案

2.1 设计思路

本文的统一身份认证平台是在体现J2EE开发框架的开源门户系统Liferay基础上，配置LDAP（Lightweight Directory Access Protocol）和CAS（Central Authentication Service）单点登录服务。平台结构如图1所示：

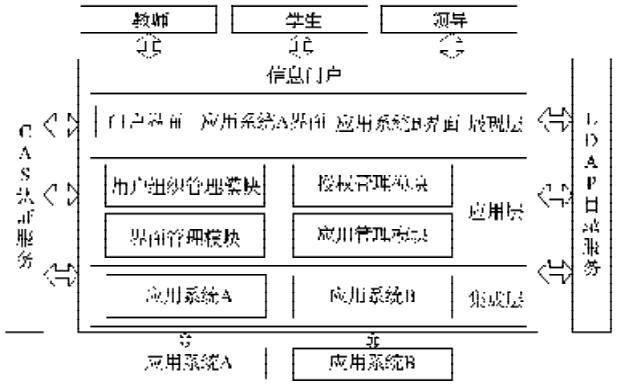

图1 统一身份认证平台结构图

Fig. 1 The structure of UIA platform

统一身份认证平台主要分为三大模块：信息门户、LDAP目录服务、CAS认证服务。信息门户为用户提供登录入口，并对各个应用系统的登录界面进行集成，实现身份认证界面的统一，同时可以整合CAS服务和LDAP服务。LDAP目录服务实现用户信息的统一管理与保存，保证用户信息的权威性和唯一性。CAS认证服务实现统一身份认证平台的核心认证功能，为用户提供基于CAS协议的统一身份认证。

2.2 Liferay信息门户

1）Liferay信息门户特点

Liferay信息门户应用SOA设计理念为企业应用提供了扩展工具和框架，采用先进的Java、EJB、JMS、SOAP、XML等技术，符合JSS-168、OpenSearch、AJAX等标准，基于XML的Portlet配置文件可以自由地动态扩展，使用Web Services来支持远程信息的获取。信息门户相当于一个容器，将校园网内的多个应用系统“放”入其中，为统一身份认证平台提供一个大集成的应用平台。

2）信息门户配置

信息门户给LDAP目录服务和CAS认证服务提供接口。当LDAP服务建立完成后，可以通过对信息门户的portal.properties文件进行配置：

```
auth.impl.ldap.enabled=true
auth.impl.ldap.required=true
auth.impl.ldap.factory.initial=com.sun.jndi.ldap.LdapCtxFactory
auth.impl.ldap.provider.url=ldap://localhost:10389/dc=gzhu,dc=edu,dc=cn
auth.impl.ldap.security.principal=uid=admin,ou=system
auth.impl.ldap.security.credentials=secret
```

将Ldap设置为true，然后将url进行设置，再将Liferay用户的信息和LDAP中属性的信息映射即可完成LDAP与信息门户的连接。

当CAS认证服务建立完成后，可以通过对信息门户的web.xml文件进行配置：

```
<filter>
<filter-name>CASRequired</filter-name>
<filter-class>edu.yale.its.tp.cas.client.filter.CASFilter</filter-class>
<init-param>
<param-name>edu.yale.its.tp.cas.client.filter.loginUrl</param-name>
<param-value>https://localhost:8443/cas/login</param-value>
</init-param>
<init-param>
<param-name>edu.yale.its.tp.cas.client.filter.validateUrl</param-name>
<param-value>https://localhost:8443/cas/serviceValidate</param-value>
</init-param>
<init-param>
```

<param-name>edu.yale.its.tp.cas.client.filter.serverName</param-name>

<param-value>localhost:8081</param-value>

</init-param>

</filter>

在 web.xml 中设置完成 CAS 过滤器后，即可实现信息门户与 CAS 服务的连接。

2.3　LDAP 目录服务

1）LDAP 的技术特点

LDAP 是一个用来发布目录信息到许多不同资源的协议。LDAP 基于 X.500 标准，但与 X.500 有所不同，LDAP 支持 TCP/IP，这是访问 Internet 的必要条件。LDAP 服务器可以用“推”或“拉”的方法复制部分或全部数据，例如：可以把数据“推”到远程办公室，以增加数据的安全性。复制技术是内置在 LDAP 服务器中的，而且容易配置。

2）LDAP 目录服务

LDAP 目录信息树中的每一个节点都应该对应一个在校园网中拥有合法身份的人，每个人的属性也就是这个节点所包含的身份信息。怎样设定每个节点的属性，以及如何组织一个结构合理的目录信息树，是统一身份认证平台设计的重要环节。

针对 LDAP 可读性能高，修改、删除等性能低，不易于进行大规模非查询操作的特点，初始的目录信息树结构必须完善，避免以后频繁的修补和移动。根据高校的实际情况，可以把工作关系、职能部门信息、院系信息和类似数据保存在每个用户的 LDAP 条目中。如图 2 所示。

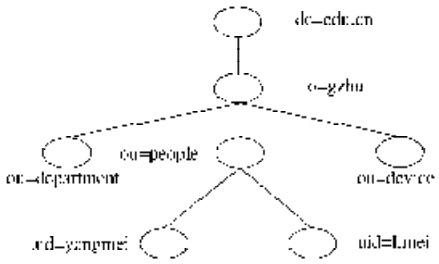

图 2　LDAP 信息目录树结构图

Fig. 2　The tree chart of LDAP information

这种目录信息树的设计在一定程度上满足各种应用系统数据需求，降低了非查询的操作次数，提高了目录服务器的查询速度，同时能够较全面地体现学校教师、学生和各部门的具体信息。

2.4　CAS 认证服务

1）CAS 的技术特点

CAS 是由美国 Yale 大学发起的开源项目，应用广泛，具有独立于平台的特性，易于理解，支持代理功能。它是一个基于 HTTP 的协议，对于组成 CAS 的每一个组件都要求访问特定的 URI（Uniform Resorce Identifier，统一资源标示符），主要的 URI 包括 Login URI，Service，ProxyValidat URI，Proxy URI。

CAS 主要分为 2 个部分：CAS server 和 CAS client。CAS Server 主要负责对用户身份的认证工作，需要进行独立部署。CAS Server 提供一种独立、灵活的接口 / 实现分离的方式来处理用户名 / 密码等凭证。具体需要什么样的认证方式可以根据具体实现细节来自主定制和扩展。CAS Client 主要部署在客户端即 Web 应用上，可以将 Web 应用原有的认证方式屏蔽，对访问 Web 应用上受保护资源的请求重新定向到 CAS Server 进行认证。目前，CAS Client 支持的客户端包括：uPortal，Ruby，ISAPI，PHP，PERL，JAVA，NET 等，几乎适用任何语言编写的客户端应用。

2）CAS 认证服务

CAS 的认证服务是集中式的认证，即统一身份认证平台上所有的认证操作均由 CAS Server 统一完成。CAS Server 认证过程是将用户输入的用户名 / 密码与 LDAP 中的用户信息匹配认证，对于通过认证的用户，CAS server 将生成一份特定的票据，这张票据只允许客户端访问指定的 Web 应用。整个认证过程都是通过 HTTPS 通道完成的，较好地保证了证书、票据的安全性。CAS 认证服务可以根据高校现在的网络安全状况进行定制，本文的统一身份认证平台采用一种较为简单的 CAS 认证服务流程，如图 3 所示。

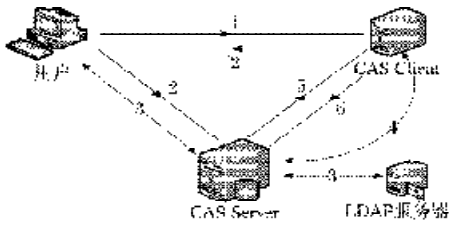

图 3　基于 CAS 的统一身份认证流程图

Fig. 3　UIA process based on CAS

步骤 1　用户通过 Web 浏览器访问已部署 CAS Client 的 Web 应用，CAS Client 的 Filter 会分析 http 中是否含有 Service Tickets，如果有则进入允许访问，如没有则进入步骤 2。

步骤 2　CAS Client 将用户的访问请求重新定向到 CAS Server。用户的 Web 浏览器将进入统一身份认证的登录界面。

步骤 3　用户通过 Web 提供用户名 / 密码，CAS Server 将在 LDAP 服务器中查询该用户提供的用户名 / 密码是否正确。

步骤 4　如果正确，CAS server 会产生一个随机的 Service Ticket，并将该 Ticket 缓存，然后重新将请求定向到用户所请求的 Web 应用，这次请求将会附带生成

Service Ticket。

步骤5 CAS Client将Ticket返回给CAS server。CAS Server将Ticket与缓冲里的Ticket列表匹配。

步骤6 如果第五步顺利完成，CAS server将该用户的Username发回给CAS Client，用户则可以顺利进入该Web应用，并获得相应的身份角色。

CAS Server与CAS Client之间的票据和用户信息的传输都是采用SSL技术，保证了通信的安全性。同时，CAS server产生的Ticket是一次性的，一旦该票据被认证过一次后即会作废，这也进一步保证了用户信息和Web应用的安全。

3 统一身份认证平台主要实现功能

1）统一用户组织管理

统一身份认证平台通过批量导入方法，将用户的基本信息批量导入LDAP的服务器中。管理员可以按照LDAP目录树的分类和用户的实际身份进行初期的角色权限授予，同时可以通过LDAP进行统一用户管理，对组织机构内中所有应用实行统一的用户信息的存储、认证和管理。对于其它基于LDAP的应用系统，可以直接通过LDAP服务器进行集成管理。

2）统一身份认证管理

统一身份认证管理主要是对用户的单点登录进行管理。由于目前高校中的应用系统既有B/S结构，又有C/S结构，对于不同类型的应用系统，管理员可以在CAS中设置不同的身份验证方式：对于B/S结构应用系统，用户只需通过浏览器界面登录一次，即可通过SSO单点登录访问多个用户权限内的Web应用系统，无需逐一输入用户名、密码；对于C/S结构应用系统，通过IE控件来实现对C/S系统客户端的单点登录，用户输入一次用户名、密码，即可访问所有被授权的C/S系统资源。无论对于B/S和C/S结构的应用系统，实现统一身份认证的功能时，集成在信息门户的应用系统无需任何修改。同时，管理员可以通过CAS的XML中的<cas_timeout>600</cas_timeout>来设置用户在线单点登陆状态的最长时限。

3）数字证书管理

统一身份认证系统的数字证书管理主要分为数字证书的制作、数字证书的发放、数字证书的销毁等功能。管理员可以首先通过类似keytool工具完成数字证书的生成，然后将证书导入数字证书库，供需集成的应用系统下载，同时可以在线查询证书的使用情况，并可以对证书进行撤销和销毁等操作。

4）监控管理

监控管理是基于LDAP，CAS和各个系统的基本信息的展现，包括支撑服务器的运行状态监控和各个认证节点的动态拓扑监控。把常规的配置信息以只读的形式显示。能够对以CAS中心服务器为中点的各个服务器进行总体监视并对其结果进行分析，当操作系统或各个服务出现异常时，系统会自动发出告警，并通过E-mail通知相关责任人，以保证系统稳定运行。

4 结语

目前，本文设计的统一身份认证系统已在广州大学数字化校园建设中完成了基本目标，主要实现了单点登录、用户管理、统一身份认证管理、授权管理等功能。统一身份认证平台的建立将为学校管理者带来更安全更全面的网上用户管理方式，为学校用户带来更便捷、更高效的Web应用方式，达到统一认证、统一管理、单点登陆的效果。同时，为校园后续信息化应用系统建设提供必要的支撑服务。目前，我国数字化校园的建设正在逐步成熟，对统一身份认证平台提出了更多的要求，如利用集中访问控制为用户提供个性化服务，从应用权限分配向数据权限分配转变等。本文主要进行了简单的统一身份认证平台的设计，还有许多工作需要进一步研究。

参考文献：

[1] 林满山，郭荷清. 单点登录技术的现状及发展[J]. 计算机应用，2004，24(2)：247-250.
Lin Manshan, Guo Heqing. The Status and Development of Single Sign-on Technology[J]. Computer Applications，2004, 24(2)：247-250.

[2] Andrew Conry. Microsoft's Passport to Controversy[J]. Network Magazine，2002，17(3)：46-49.

[3] 杨兆赞. Lotus Domino和WebSphere平台上单点登录技术的研究与实现[J]. 计算机辅助工程，2004(1)：69-72.
Yang Zhaozan. Research of SSO between Lotus Domino and WebSphere[J]. Computer Aided Engineering，2004(1)：69-72.

[4] Sun Microsystems. SunJava System Access Manager Administration Gruide[EB/OL]. [2009-12-28]. http://java.sun.com.

[5] 王正坤，蒋涛涛. 试论数字化校园统一身份认证功能的实现[J]. 农业网络信息，2009(10)：90-92.
Wang Zhengkun，Jiang Taotao. On Implementation of Unified Identity Authentication in Digital Campus[J]. Agriculture Network Information，2009(10)：90-92.

（责任编辑：蔡燕飞）