

数字化校园统一身份认证平台的构建

殷娜

(兰州交通大学 信息中心, 甘肃 兰州 730070)

摘要:建设数字化校园是推动当前教育信息化的重要系统工程,而对校园原有各个信息孤岛的业务系统进行合理的整合更是十分必要的,也是当前数字化校园研究的重点。文中根据数字校园建设的需要,介绍了基于门户系统的LDAP与CAS结合的统一身份认证平台的解决方案,系统用户信息的管理使用LDAP实现,单点登录使用Yale大学开发的CAS认证。通过构建的统一身份认证平台,整合了资源,降低了开销,使得资源得到了合理利用,对建设数字化校园起到了很好的效果。

关键词:数字化校园;统一身份认证;门户;轻量目录访问协议;中央认证服务

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2014)08-0139-04

doi:10.3969/j.issn.1673-629X.2014.08.032

Construction of Digital Campus Uniform Identity Authentication Platform

YIN Na

(Information Center, Lanzhou Jiaotong University, Lanzhou 730070, China)

Abstract: The construction of digital campus is the critical system engineering to promote the education informatization, and it is necessary to integrate businesses of every single original information reasonably, it is also the focus of the current research in digital campus. According to the need of the digital campus construction, describe the solution of unified identity service adopted the LDAP integrated CAS system, which based on portal. The system management uses LDAP to achieve and single sign-on uses CAS certification developed by Yale University. Through the uniform identity authentication platform, integrating resources, reducing cost, make the rational use of resources. It will play a very good effect in the construction of the digital campus.

Key words: digital campus; unified identity authentication; portal; LDAP; CAS

0 引言

随着计算机技术、信息技术、网络技术的迅猛发展,全球正在逐步形成一个互联互通的巨大信息网络。高校作为当代社会的教育核心领域,也在这场信息科技浪潮中不断完善自身的信息网络,数字化校园成为了高校信息化发展的必经之路。

目前,高校的信息化建设使得各种应用系统层出不穷,原本单一的网络管理工作趋于复杂化。特别是各个系统身份认证机制的不同与孤立,大大增加了网络信息安全的隐患,同时也给广大的师生带来了诸多的不便,很大程度上降低了数字化校园的工作效率,原有分散的“独立认证、独立授权、独立账号管理”的模式已经不能满足目前及未来发展的需求,因此,构建一

个完整统一、高效稳定、安全可靠的集中身份管理和身份认证平台已经成为数字化校园建设的重要目标。

1 统一身份认证平台体系结构

数字化校园统一身份认证平台整合了校园网络中的信息和各种应用系统,为用户提供了一个单一的访问入口。为校园网络内的异构分散的各种应用和服务系统提供了集中的管理和安全认证机制,实现了各种应用系统的无缝接入与集成。统一身份认证需要建立每位用户针对每个管理系统的角色和身份(管理人员、高级用户、普通用户、访客)、密码、权限并进行统一的集中和管理,统一身份认证平台是数字化校园信息管理的重要组成部分,其体系结构框架如图1所示。

数字化校园统一身份认证平台主要分为三大部分:信息门户、LDAP(轻量目录服务)以及 CAS(中央认证服务)^[1-2]。

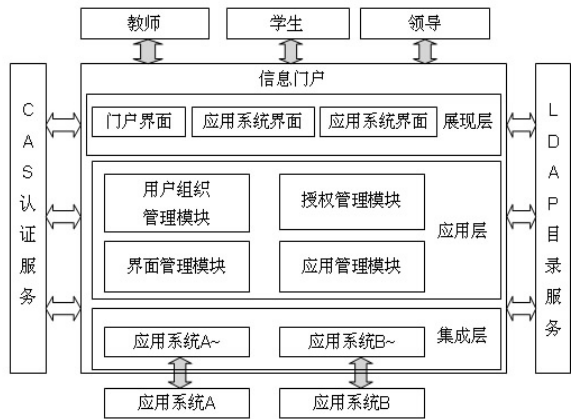


图 1 统一身份认证平台体系结构图

2 信息门户

2.1 信息门户简介

作为数字化校园的服务展示层,信息门户主要是为网络用户、手机用户等用户终端提供服务接入与信息展示。信息门户的系统功能主要涵盖以下方面:让合法用户利用互联网安全地对学校内部资源进行访问;为用户提供极具个性化的信息检索与网络资源获取的功能;把校内外的网站资源进行有效地集成、整合;通过信息门户平台,可以快速配置要求极为严格的信息门户所需的成员管理、知识管理、个性化、累积、安全和集成的服务。通过自行定制的门户通道将集成的内容、应用程序和服务进行传递,并允许合法的用户、学生和教职工从校外远程访问门户,并且不需要安装额外的客户端软件,也不需要单独进行维护。开放、灵活、个性化的信息平台使内部已开发的应用系统和第三方应用程序方便地集成在数字化校园中。

2.2 Portal 技术

Portal 是一种网络应用程序。为了消除信息孤岛,它能够快速地建立一个信息通道,将各种应用系统、数据资源和服务集成到一个信息管理平台之上。通过屏蔽应用的多样性,向合法用户提供一个信息资源访问环境,使其能够与人、内容、应用和程序进行个性的、安全的、单点式的互动交流。Portal 强调以用户为中心,提供统一的登录界面,对各种应用程序或组件进行集成,实现信息的集中访问。Portal 的基本体系结构如图 2 所示。

Portal Web Application 处理用户的请求,从用户的当前访问页中读取出门户组件(Portlets),接着调用组件容器来得到每一个组件的内容。Invoker API 是组件容器的主要调用接口,门户组件的调用主要是通过这

些组件容器提供的一些请求。Portal 通过组件容器的 Invoker API 来访问组件容器,然后回调接口为组件容器提供与 Portal 相关的信息,接口的回调主要依靠容器的使用者 Container Provider SPI(Service Provider Interface);最后组件容器依靠 PortletAPI 对所有的组件进行调用。为用户存取信息以及提供应用程序、对管理内容个性化的选择、成为提供工具及使用者的接口是 Portal 未来的发展方向。Portal 并不仅仅具有统一访问网站应用程序的功能,它还可以提供如搜索、工作流、内容管理、集成和安全性等其他有用的功能。Portal 极有成为以后桌面的可能性,因为它可以将集成的应用程序不通过网站直接给所有类型的客户端设备进行传递。

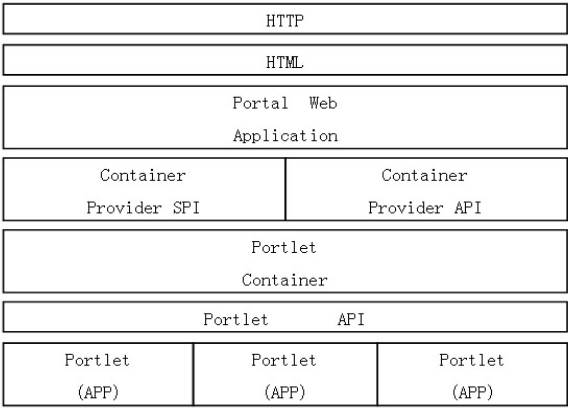


图 2 Portal 基本体系结构图

数字化校园使用开源 Portal 来建设学校的信息门户,将校园网络内的各种应用系统的身份认证界面进行集成,用户可以通过单一的认证界面进行登录,从而实现了各种应用系统身份认证的统一;同时通过开源 Portal 提供的接口将 LDAP 目录服务和 CAS 认证服务进行了整合,为统一身份认证平台提供了一个良好的基础。

3 LDAP 目录服务

3.1 LDAP 介绍

LDAP 全称是 Light weight Directory Access Protocol,是轻量目录访问协议。它是基于 X.500 标准的,但 LDAP 简化了 X.500 的许多操作,省去极少使用的特性,并且可以根据需要定制。LDAP 一开始就设计运行在 TCP/IP 协议上,是目录服务在 TCP/IP 上的实现。

LDAP 协议是标准的目录服务协议,具有跨平台性,因此就不用关心 LDAP 目录存放的服务器类型和操作系统类型,均可以直接对 LDAP 目录中的内容进行读写。同时 LDAP 协议对数据的浏览与查找进行了优化,从 LDAP 服务器中读取数据或查找数据会比关

系型数据库要快,速度要快一个数量级。LDAP 协议组织数据结构是基于树状模型,层次结构相当明晰,能有效明确地实现一个组织结构特性的相关信息。在树型结构上的每个节点称为条目(Entry),每个条目拥有全局唯一可区别的名称(DN)并且包含了基于属性的描述信息,其中 DN 是由条目所在树型结构中的父节点位置(BaseDN)和该条目的某个可用来区别身份的属性(称之为 RDN 如 uid)组合而成,所以 LDAP 也为信息的检索提供了复杂的过渡条件。

3.2 LDAP 数据库

LDAP 目录服务是用面向对象的方式以及层次化的结构将校内的用户和各种应用系统的信息进行了集中和管理,从而保证了数据的一致性和完整性,使用户信息在校园网内各种应用系统之间得以共享和使用。同时对统一身份认证系统中的用户信息、账号关联信息以及各种应用系统资源信息等进行了有效的组织和集中的管理,从而为数字化校园的信息管理提供了更为高效安全的目录访问。

设计 LDAP 目录服务的结构时,可以充分利用门户认证、应用认证等的相应用户属性数据,学校开发的各应用系统就可以共享该 LDAP 目录服务器。在 LDAP 目录服务的策略设计中,策略包信息可以包括被保护资源的 URL 等资源名称;对每个资源需要控制的操作名称,如 READ/WRITE 或者 GET/POST 等;以及对每个定义动作的访问控制,是允许还是拒绝;还可以规定具体的 IP 地址或 IP 地址段,强制使用的认证模式、起始和结束时间等^[3-7]。

在规划目录信息树(DIT)时,它的结构可以根据学校的组织结构进行确定,DIT 的根可以代表学校组织,可以将学校所有的用户信息都保存到目录数据库的 DIT 中。

4 基于 CAS 的单点登录

4.1 单点登录(SSO)关键技术

单点登录(SSO)是将一个对外认证平台作为统一身份认证的接口,合法用户只要在该接口处输入了正确的用户名和密码,就可以平滑进入其他内部的信息管理和应用系统。其认证过程是通过将用户名和密码等信息发送至核心认证系统,然后由核心认证系统对发来的认证请求进行判断,最终将认证结果以及权限等用户登录访问的信息返回给接口平台,从而实现了对于用户的认证控制。在合法用户通过单点登录认证之后,其可以访问的应用系统的权限可以通过 SSO 提供的映射授予权限来实现,用户的注销功能就可以使用映射取消权限来实现,其实现过程如图 3 所示。

单点登录与应用漫游的实现,用户通过输入用户

名和密码等信息登录统一的身份认证界面,认证信息被发送至服务器的认证模块,由认证服务器判断登录信息是否与保存在目录中的数据相符,如果是合法用户则获准进入。为了更好地集成校园网内各种应用与服务系统,统一身份认证一般会提供大量的第三方应用的身份接入接口,如用户信息与密码的修改、用户组织与角色信息的获取等。

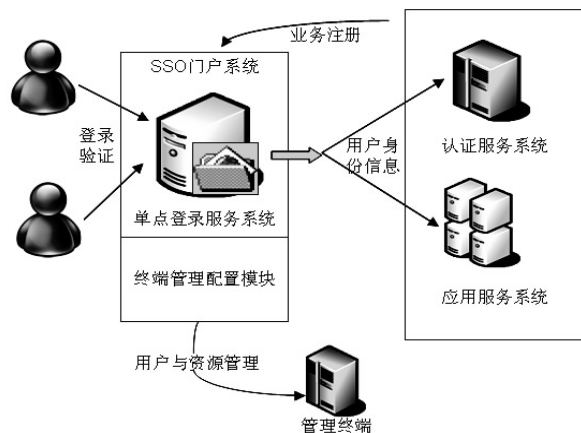


图3 单点登录的认证方式实现过程

4.2 CAS 简介及其应用

中央认证服务(Central Authentication Service, CAS),是美国耶鲁大学发起的一个实现 Web 应用单点登录的开源项目。在 CAS 的体系中,有 3 种角色:用户、CAS 认证中心以及 Web 应用系统,从角色划分就可以看出,CAS 非常适合引入到数字化校园统一身份认证平台中,但 CAS 在用户授权的功能方面存在一定的缺陷,这对于统一身份认证平台中一些安全性较高的子系统,如 OA、选课系统、网教平台等,存在一定的局限性。因此在 SSO 机制中应该根据用户的角色来进行用户的访问控制,在不同的应用系统中赋予用户不同的访问权限,要尽量避免将用户权限之外的应用系统一并倾倒给用户,从而提高系统的安全性。因此,数字校园统一身份认证平台应保证“认证时即授权”,这样才能避免暴露太多的信息给非授权的用户,也不会给用户展示大量对自己没用的信息,从而提高了用户体验,保证了对应用系统的安全访问^[8-14]。

4.3 集成身份认证

数字化校园统一身份认证平台是以 CAS 作为实现单点登录的底层技术,CAS 认证的数据源是 LDAP 目录服务。CAS 在结构上包含两个部分:CAS Server 认证中心和 CAS Client 认证服务。CAS Server 认证中心是与 LDAP 目录服务连接,负责用户信息查询并认证工作;CAS Client 是部署在服务上,负责接收客户端的请求并决定用户是否能访问所需的资源,需要登录时,重定向到 CAS Server。

根据 CAS 的原理,CAS 客户登录的过程如下:用

户通过单点登录页面进行登录,系统将用户信息提交到 CAS 的认证页面进行认证,CAS Client 接收 Http 请求并分析其请求是否包含 Service Ticket,如果 Service Ticket 的值为空,则说明该用户第一次应用,没有登录,则将该用户的请求转向 CAS Server 的登录地址进行身份认证,并且带去访问应用系统的地址,在 CAS Server 中用户信息认证成功后则进行到要访问的应用系统中。如果用户直接请求 CAS Server 认证,成功后则进入单点登录系统,并且随机产生一个唯一的 Service Ticket,并且以 Cookie 形式存放在客户端,以待将来验证,如图 4 所示。

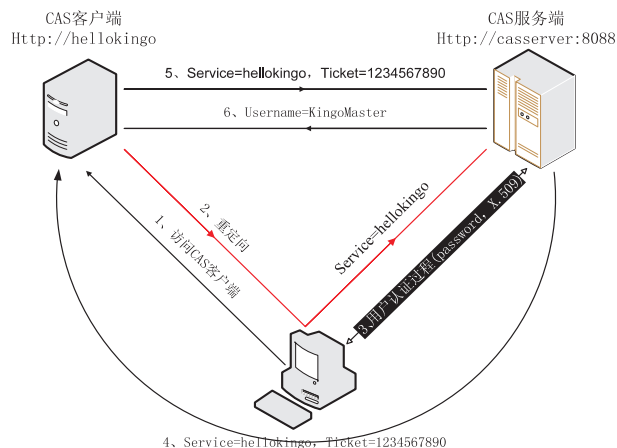


图 4 统一身份认证过程

5 结束语

数字化校园统一身份认证平台解决了校园网内各种应用和服务系统之间用户名、密码和权限的不统一,用户信息的管理和用户使用不方便等问题,是数字化校园建设的重要组成部分。文中将 LDAP 目录服务、CAS 服务相结合设计提出了一个基于信息门户的数字校园统一身份登录认证模型。利用目录服务技术实现对用户信息的快速查找,利用 CAS 实现用户的认证并登录,使得多应用系统可以方便切换。最终,为整个校园网内各应用系统间的信息共享、整合打下了坚实的

基础。

参考文献:

- [1] 段海波. 高校数字化校园的统一身份认证解决方案[J]. 中国信息化,2010(9):43-46.
- [2] 郭楚杰. 数字化校园统一身份认证平台的研究与设计[D]. 广州:广东工业大学,2010.
- [3] 孙甲泉. 基于 LDAP 的 CAS 的校园统一身份认证系统的研究[J]. 电脑知识与技术,2013,9(6):1318-1320.
- [4] 贺玉明,李晋宏,唐辉. LDAP 在数字校园统一身份认证系统中的应用[J]. 计算机技术与发展,2011,21(5):139-142.
- [5] 刘永亮,张卫红,周骏. 基于 LDAP 的校园网统一身份认证的设计[J]. 计算机与数字工程,2008,36(4):116-118.
- [6] Qadeer M A, Salim M, Sana A M. Profile management and authentication using LDAP[C]//Proceedings of 2009 international conference on computer engineering and technology. [s.l.]:[s.n.],2009:247-251.
- [7] The OpenLDAP Project. OpenLDAP 2.2 administrator's guide[EB/OL]. 2004. <http://www.openldap.org/doc/admin22>.
- [8] 张平,郑津,汪立欣. 一种基于 CAS 的校园网统一平台单点登录方法[J]. 电脑编程技巧与维护,2013(16):146-146.
- [9] 高俊,李长云,刘小飞,等. 基于 Portlet 的数字化校园信息门户的设计[J]. 计算机工程与设计,2009,30(17):4006-4008.
- [10] Nakano H, Sugitani K, Nagai T, et al. Web-based time schedule system for multiple LMSs on the SSO/portal environment[C]//Proc of education engineering. Madrid: IEEE, 2010: 153-158.
- [11] 罗辉琼,聂瑞华. 基于 Portal 的门户开发技术研究[J]. 计算机技术与发展,2012,22(8):100-102.
- [12] Radha V, Reddy D H. A survey on single sign-on techniques[J]. Procedia Technology, 2012(4):134-139.
- [13] 高静,涂庆华. 南理工数字化校园统一身份认证平台的构建与实施[J]. 现代计算机:上下旬,2013(6):43-47.
- [14] 刘峰,王峥,曹华平,等. 基于 CAS 的门户单点登录方案[J]. 计算机系统应用,2011,20(6):77-80.

(上接第 116 页)

- Proc of 2012 IEEE wireless communications and networking conference. Shanghai:IEEE,2012:125-130.
- [11] Sadek M, Tarighat A, Sayed A H. A leakage-based precoding scheme for downlink multi-user MIMO channels[J]. IEEE Transactions on Wireless Communications, 2007, 6(5):1711-1721.
 - [12] Kim Hak-Jin, Baek Jong-Seob, Oh Ji-Myung, et al. Improved leakage-based precoding with vector perturbation for MU-MI-

MO systems[J]. IEEE Communications Letters, 2012, 16(11):1868-1871.

- [13] Boyd S, Vandenberghe L. Convex optimization[M]. New York:Cambridge University Press,2004.
- [14] Fang Wei, Sun Huan, Yang Lin. Power allocation for maximizing sum capacity of multiuser MIMO downlink with transmit precoding based on SLNR[C]//Proc of 2011 IEEE 73rd vehicular technology conference. Budapest:IEEE,2011:1-5.

数字化校园统一身份认证平台的构建

作者：[殷娜](#)，[YIN Na](#)

作者单位：[兰州交通大学 信息中心, 甘肃 兰州, 730070](#)

刊名：[计算机技术与发展](#)

英文刊名：[Computer Technology and Development](#)

年，卷(期)：2014(8)

本文链接：http://d.g.wanfangdata.com.cn/Periodical_wjfz201408032.aspx