文章编号:1005-0523(2004)04-0099-04

“数字化校园”的基础核心—身份认证平台的设计

俞之杭,许 飞

(华东交通大学 现代教育中心,江西 南昌 330013)

摘要:“数字化校园”是随着计算机网络技术高速发展,随着高校对管理需求的深入而产生的一种新型的高校管理模式,这种管理模式涉及到高校教学、科研、后勤产业及职能部门等各个环节,它管理的对象包括与校园有关的各种人群;关于“数字化校园”发展的模式,全国目前并没有一个统一的标准,作者从目前高校的现状及将来发展趋势的角度,阐述了“数字化校园”系统设计时需要解决的最基础的问题——身份认证平台的设计思路,本文介绍了身份认证的几种模式、需解决的具体问题、所涉及到的应用技术.

关 键 词:数字校园;身份认证

中图分类号:F045.3 **文献标识码**:A

1 统一身份认证系统必须解决的问题

统一身份认证系统解决方案必须是在切实了解高等院校信息化需求的情况下,结合计算机软件、网络等技术,设计出一套能够解决高等院校软件资源和角色使用权限的管理方案.

统一身份认证是为了解决高等院校在权限管理过程中的共性问题,是集中管理高等院校资源访问权限的认证方案,降低高等院校的权限管理及维护成本,具有良好扩充性和安全性的解决方案.统一身份认证系统的核心思想是将机构、用户统一存储,对应用系统统一授权、规范应用系统的用户认证方式,从而达到提高整个系统的整体性、可管理性和安全性的效果.

从功能上来看统一身份认证平台有三大逻辑组成部分:目录服务器、用户身份管理服务和用户身份认证服务.

2 身份认证系统的组成

2.1 目录服务器

目录服务器是整个统一用户认证平台的基础,目录服务器采用标准的LDAP目录服务器产品,通过LDAP目录服务将校内的用户或组织的信息(称为属性)以层次结构,面向对象的数据库的方式加以收集和管理,对用户信息进行统一管理,保证数据一致性和完整性,为校园各类应用系统包括高校信息门户、高校URP(University Resource Planning)系统、一卡通系统、各类MIS系统提供用户信息共享和使用.

作为一个开放,独立于任何厂商的标准,LDAP为分布式系统和服务中所要求的中央化信息存贮和管理提供了一个可扩展的结构.事实上LDAP已经成为目录信息的标准方式,目前包括Sun,Netscape,Microsoft等公司都已支持该协议并推出了相应的产品,同时LDAP现在被大多数的网络操作系统,组件系统和应用所支持.目录服务存放了大量的用户信息,为此需提供方便的管理功能;通过目录服务为管理员建立了一套基于网络、应用、存储和共享数据的”注册处(Registry)”,在其中可以存储各种用户信息、组和配置信息;通过目录服务器,用户可以直接在目录中存储和查询配置信息,而不

收稿日期:2004-04-22

作者简介:俞之杭(1967-),男,浙江诸暨人,华东交通大学工程师.

是从用户的客户机内读取，做到完全的应用位置独立性，使用户可以在网络中的任何一台计算机上工作，与在自己的办公桌前无任何区别；信息部门的管理员可以无须考虑分布于目录中应用的数目，独立的管理和维护目录系统.

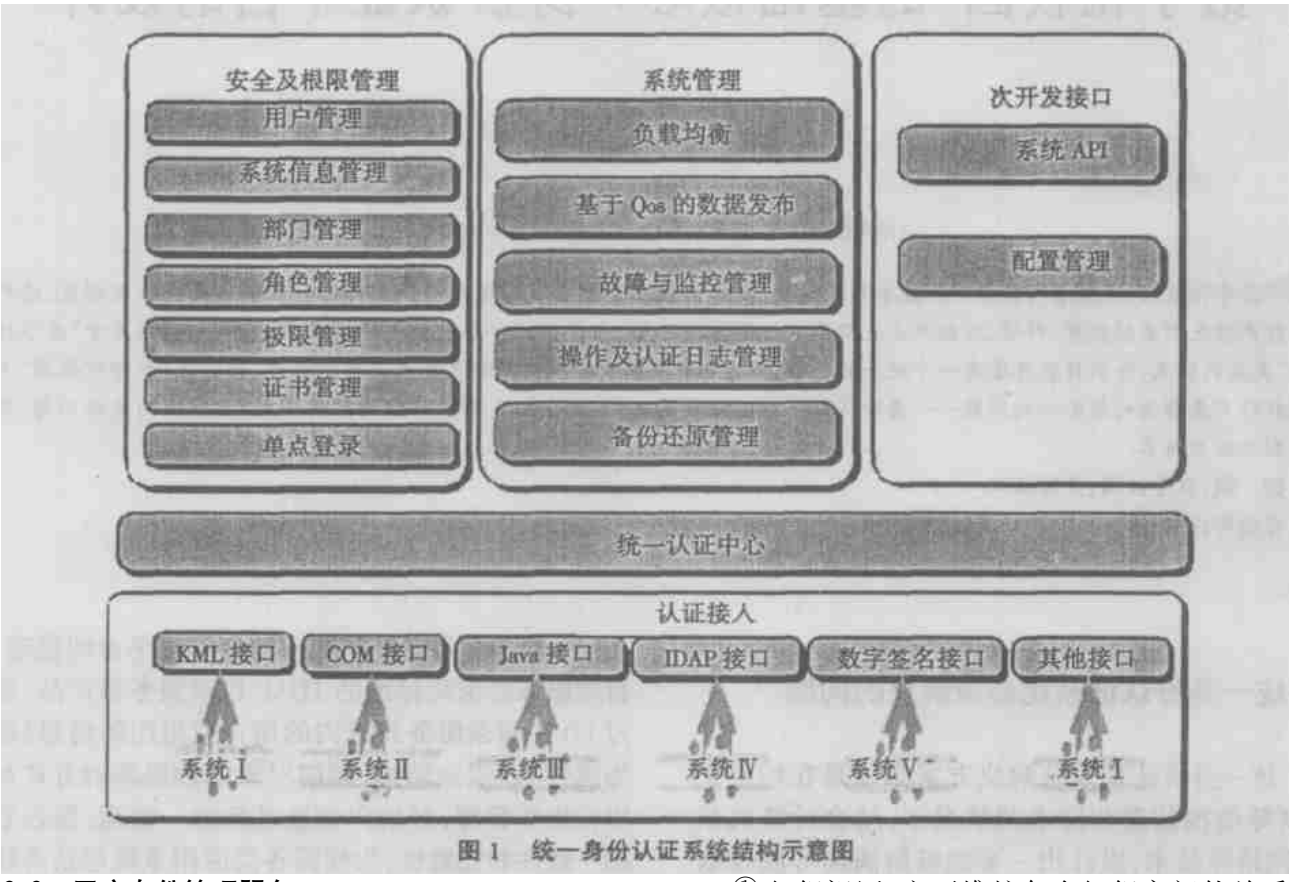

图1 统一身份认证系统结构示意图

2.2 用户身份管理服务

用户身份管理服务功能可以实现集中或分布式的工作方式，对一个中央用户资料数据库进行统一操作，用户身份管理服务可以提供集中/分布等两种用户管理方法.系统管理员权限可以分派到以组为单位，访问权限的管理可以下放在各个级别，理论上可以分无限个下放级别.通过管理权限的下放，高校可以快速实现对用户资料的更新，而无须通过一个统一的窗口单位，这样可以简化用户(组)管理带来的工作量，它能提供以下功能：

1) 提供自动和管理员确认两种模式的用户注册功能，系统支持自动根据预定义的策略完成对注册用户的授权，即自动注册功能，也支持用户注册后，由管理员进行确认并进行授权的管理模式；

2) 直观的图形化组织管理界面

3) 组织指学校内部的机关和团体.包括永久性组织(如：各学院、职能处室等)和临时性团体.组织管理模块以图形的方式支持管理员完成团体的结构以及团体内部的角色(职务)等相应信息的注册，提供组织视图和角色视图两种视图：

① 组织视图，主要维护各个组织之间的关系(包括上下级关系，协助关系等)，以及进行组织的增加、删除和修改等工作，并提供剪切、复制、粘贴以及拖拽等多种方式支持组织机构的快速重组.

② 角色视图，对于每个组织内部的角色(职务)的数据进行维护管理.包括：角色ID，角色名称，角色的工作关系，以及设置该角色(职务)的所需要的权限等.

4) 简单方便的用户管理界面

用户管理模块负责用户的数据管理，它应包括以下功能：

① 用户基本信息维护子模块，该子模块应该能完成对用户基本信息的管理和维护.用户的基本信息包括：包括个人姓名，个人在学校内的基本身份，在校时间及和身份有关的信息，包括对这些数据的录入、修改和删除等功能.

② 用户角色设置子模块，在统一认证平台中，用户享有的权限主要由其在组织机构中担任的角色(职务)来确定.一个用户可以在多个组织中担任职务；用户角色设置模块完成对用户职务的赋予，

剥夺等工作.

5) 严格的分级用户数据访问权限控制,基于ACI(Access Control Information)机制有效保护用户的资料,并通过分级管理提高用户管理的效率和质量,包括:

① 个人用户只能访问自身基本资料的属性(例如:姓名、家庭电话、邮件地址、登录口令等基本信息),不能修改涉及系统的相关属性(例如:帐号、卡号、工号、所属角色等);

② 系统管理员可以为某一个组织或部门设置相应的二级管理员(及根据目录树的结构指定授权代理人),二级管理也可以为某一个班级或研究室设置相应的三级管理员,以此类推,原则上可以提供无限级别的分级管理功能;

6) 基于角色的授权管理模块,作为“数字化校园”的基础平台,统一身份认证平台授权范围主要是认定哪些角色可以使用哪些系统,而对于这些角色在这些系统中能够使用哪些应用,使用到什么程度是由各应用系统来确定的.但系统应为整个数字化校园的应用提供规范的权限维护和权限查询接口,基于这样一个统一的授权入口,管理员应该可以完成以下工作:

① 查询用户在整个校园应用中能够使用哪些系统,在这些系统中分别拥有什么样的权限;

② 维护用户总体权限,对于该用户能够使用的系统,该模块通过标准的接口直接调用对应子系统的授权管理,快速完成用户全部的授权管理,而不需要单个进入各应用系统本身.

7) 动态规则定义功能,统一身份认证平台的定位是解决全校所有用户的身份信息的统一管理,但由于高校人员的特殊性,会出现一些临时人员的管理问题,为解决这一问题,系统应该提供动态规则定义功能,包括:

① 命令行批处理机制,通过编辑一个简单的批处理文件,通过该文件的手工执行,批量增加或删除相应的用户,这种机制适用于周期不确定的情况,例如能快速生成有特定权限的临时用户,并能快速注销该临时用户;

② 自动规则机制,通过定义相应的动态规则以及这些规则的执行时间,由系统根据这一规则自动在所要求的时间点生成相应的用户,再在另外一个时间点自动注销这些用户.

2.3　用户身份认证服务

通过对角色的定义,用户身份认证服务允许管理员方便地对各种规模的用户授权访问或取消访问授权,必须能提供以下功能:

提供多种身份认证方式,支持下列用户认证方式

A. 数字签名认证,系统提供开放的接口,可以扩展实现和包括 CA 在内的多种数据签名的整合,实现根据用户所提供的数字证书识别用户身份,自动完成登录,或根据安全策略再得到用户密码确认后完成登录.

B. 户名/口令认证,如果该用户是第一次进入或已超时退出时,系统将自动弹出用户名和口令对话框,用户正确输入用户名和口令后,就可以根据自己的权限访问各个应用系统.

C. 卡认证,对于通过终端设备直接使用系统的用户,根据用户所提供的卡信息识别用户身份,自动完成登录,或根据安全策略再得到用户密码确认后完成登录.

3　用户资源访问控制

1) 系统根据用户的角色,允许使用某些服务或者服务中的一个子集,例如可以定义组织视图服务,满足从个人到院系再到学校这样一些分级管理流程应用的需要,也可以定义满足一卡通门禁系统的角色视图服务,满足对教师、学生进入特殊场所的不同限制要求.

2) 提供一个 API,通过它可以定义认证成功/失败后的系统动作,满足一些特殊的功能要求,例如,可以定义某 IP 持续使用不同用户和口令登录失败后,自动将该 IP 设为禁止访问等.

4　统一认证流程图

提供与 portal 对接的功能,实现用户在门户上登录一次,就可以访问所有集成的应用和服务,如下图所示

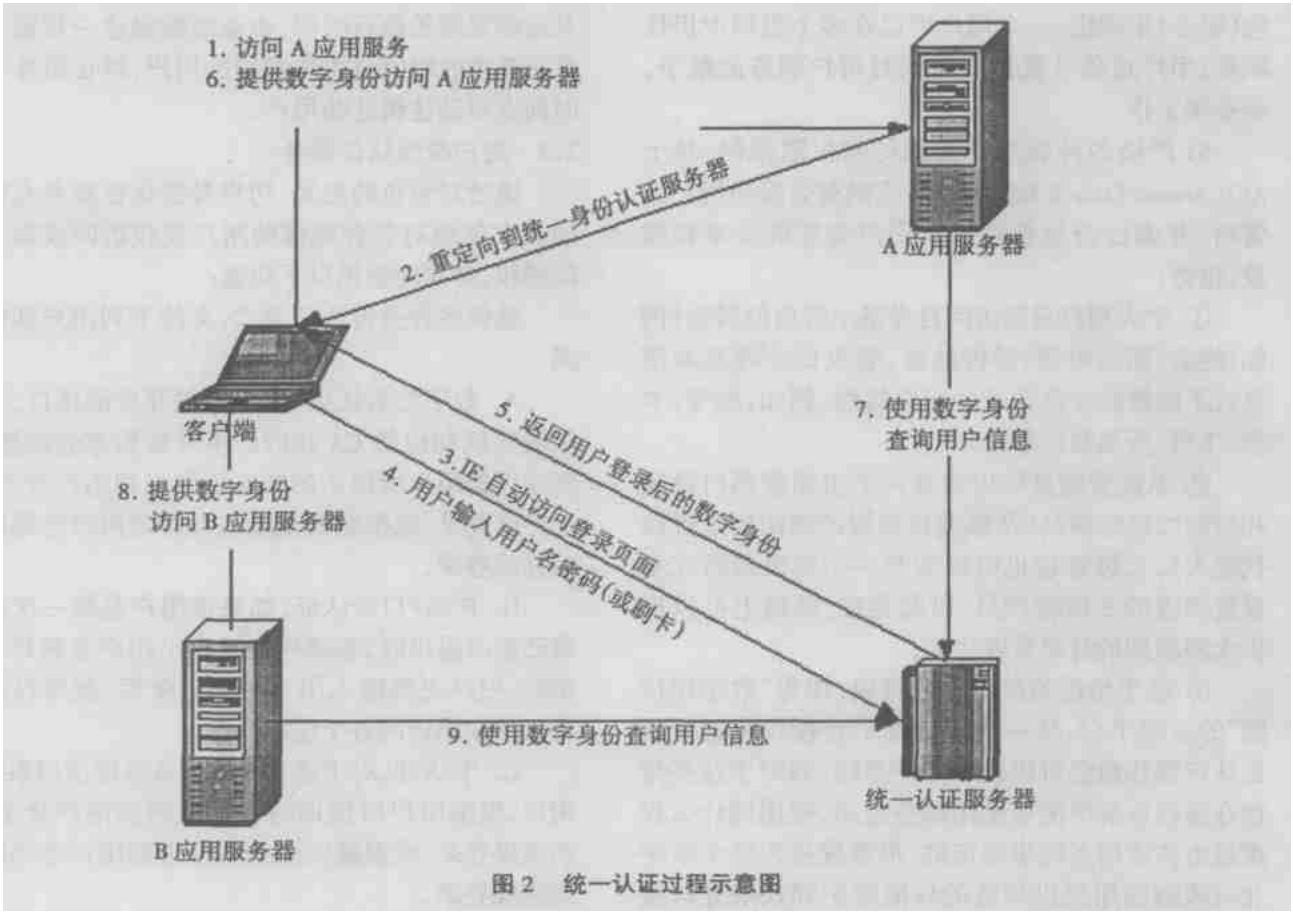

图 2 统一认证过程示意图

5 结 论

以上部分的设计思路是笔者在总结国内部分高校“数字化校园”的基础上，结合本校的管理模式而提出的；“数字化校园”是个庞大的系统工程，它不仅仅是计算机技术综合应用的体现，还涉及到复杂的行为管理模式问题，各高校目前就这一问题基本处在摸索之中，但身份认证体系作为“数字校园”的核心已确定无疑．笔者认为，身份认证系统应该是以用户信息、系统权限为核心，集成各业务系统的认证信息，为客户提供一个高度集成且统一的认证平台．其结构应该具有如下特点：

1) 健壮性：通过复制与备份机制，确保系统数据安全可靠；2) 结构灵活性：易于扩展；便于管理和挂接；3) 安全可靠性：身份认证和权限控制确保数据安全；4) 内容完整性：管理对象包括高校各类人群；5) 支持远程集中式业务处理．

The Basic Core of “Digital Campus” —— The Design of Identity Attestation

YU Zhi-hang, XU Fei

(Moden Education Technology Center, East China Jiaotong University, Nanchang 330013, China)

Abstract: “Digital Campus” is a new pattern of university management created with the fast development of computer network technology and the need of university management. The pattern involves various aspects, including teaching, scientific research, logistics and functional departments. The management subject includes all kinds of people relating to campus; There is not a formative criteria across the country for the development pattern of “Digital Campus”. The author elaborates the most basic problem which needs to be resolved when designing “Digital Campus” —— the designing thinking of identity attestation. The article introduces several patterns of identity attestation, the specific problems that need to be resolved, and the applied technology involved.

Key words: digital campus; identity attestation