文章编号:1674-2869(2013)01-0075-05

公钥基础设施的高校电子政务安全研究

黄兰英[1],叶从欢[2]
(1.湖北工程学院计算机与信息科学学院,湖北 孝感 432000;
2.华中科技大学计算机科学学院,湖北 武汉 430077)

摘 要:为了解决高校电子政务中的身份认证、访问控制、信息安全等安全问题,提出了一种基于公钥基础设施(PKI)核心技术的高校电子政务模型.该模型采用桥认证(CA)结构建立PKI信任机制,在各部门内部使用分级的CA认证,各部门之间通过中心CA进行桥接CA交叉认证;采用轻量目录访问协议(LDAP)建立PKI证书库,以目录复制(Replica)实现CA对主从LDAP的数据一致性,提高使用者的身份有效认证.该模型还采用角色及权限访问控制(RBAC)进行用户合法安全访问控制,在用户和访问权限之间引入角色,用户通过角色分配的权限来访问系统资源.此模型在实践中得以验证,符合安全要求.

关键词:认证中心;高校电子政务;信息安全;公钥基础设施
中图分类号:TP393.08 **文献标识码**:A **doi**:10.3969/j.issn.1674-2869.2013.01.016

0 引 言

随着信息化的发展,电子政务正在逐步取代传统办公模式,教育部办公厅在2004年先后下发了《关于加快推进教育系统政务信息化建设的通知》、《关于教育电子政务建设的指导意见》等一系列文件,确定了我国高校教育电子政务建设的整体框架,高校的电子政务就是把各学院管理系统和平台(如人事信息管理系统、教务信息管理系统、科研信息管理系统、学生信息管理系统、设备管理信息系统、财务信息管理系统)整合到一起,以避免高校各部门之间各自为政、信息孤岛的状况出现[1].但高校的电子政务安全问题随即而来[2],如:学校内部保密的信息被泄漏、信息被他人非法篡改;广大师生的身份被窃取、信息被恶意攻击和破坏;电子公文格式不规范和密码保护措施不严密;在访问信息时每个访问者角色的权限、责任以及角色的如何识别和如何鉴定等,这些隐患逐渐成为阻碍高校电子政务继续发展的主要问题.如何确保信息的安全传输,如何防止来自内部的信息泄露,身份验证,公文流转时的数据加密和数据完整性、可靠性以及不可否认性等信息安全问题已成为广泛关注的焦点.

笔者在分析公钥基础设施(Public Key Infrastructure,以下简称:PKI)的核心技术的基础上,探讨采用桥认证构建认证中心(Certificate Authentication,以下简称:CA)、使用轻量目录访问协议(Lightweight Directory Access Protocol,以下简称:LDAP)构建高校PKI的证书库、使用角色及权限的访问控制(Role Based Access Control,以下简称:RBAC)策略访问信息等方面来解决高校电子政务中对于身份认证、访问控制、信息安全的需求问题,提高高校电子政务系统的安全性和稳定性.

1 公钥基础设施技术

PKI是利用公钥理论和技术(密码技术、数字信封、数字签名技术等)建立的提供信息安全服务的基础设施,是国际标准的安全管理平台,即信息安全基础中的核心[2-5].PKI的理论基础是研究信息安全保密的密码学,它分为密码编码学和密码分析学,PKI是解决加密和信任问题的基本解决方案[5].

一个典型的PKI组成系统(如图1),主要包括以下部分[2,6]:

a. 数字证书认证中心(CA):数字证书认证中心CA是PKI的核心,CA主要负责对本系统内证书生命周期的管理:如证书的申请、更新、撤销、发布、备份、恢复和归档等[2,4].

b. 密钥管理中心(KMC):密钥管理中心(Key

收稿日期:2012-10-11
基金项目:湖北工程学院科研项目(Z2011006)
作者简介:黄兰英(1973-),女,湖北孝感人,副教授,硕士.研究方向:媒体信息检索和信息处理、电子商务.

Management Center,以下简称:KMC)向CA服务提供相关密钥服务,它是整个信任体系的核心安全部分,主要负责密钥的管理(如密钥的生成、密钥的分发、密钥的存储、密钥的备份和更新以及密钥的撤销和恢复等[4-5,7-8])和安全.

c. 注册中心(RA):注册中心(Registration Authority,以下简称:RA)是CA认证中心的延伸,主要负责对证书申请用户信息的录入、审核及制证、发证等;RA是数字证书的审核、申请和注册中心,RA注册中心由CA认证中心授权管理[9-10].

d. 证书库与证书发布系统:CA签发证书的存储和证书吊销列表,便于用户方便地取得证书和证书吊销列表信息;还提供轻量目录访问协议(LDAP)服务和注册服务[2,6,8].

e. PKI应用:主要是在web服务器之间的通讯、电子数据交换(EDI)、电子邮件、信用卡交易和虚拟私人网络(VPN)等客户端应用软件[2].

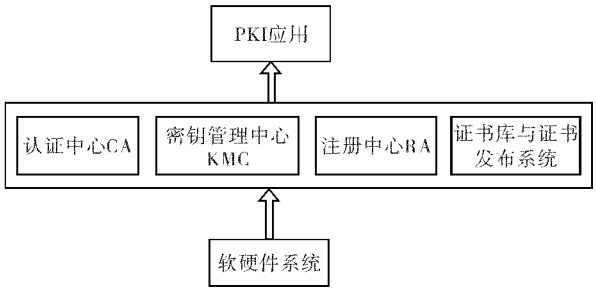

图1 PKI的组成框架

Fig. 1 PKI composition system

数字证书认证中心CA、密钥管理中心KMC、注册中心RA、证书库是PKI的关键组件;PKI通过密码加密技术、数字证书、数字签名等技术保证网络上数据的保密性、有效性、完整性、不可否认性以及身份的合法性,它为电子政务的发展提供了一套安全的基础平台、技术规范和一个安全的电子政务环境[2,4,9-10].

2 基于PKI的高校电子政务的安全构建

目前高校电子政务信息安全的解决方案主要集中在物理安全、系统安全和网络安全层面(如防火墙、入侵检测、防病毒等),还没有应用层面的信息安全平台和全网统一的安全方案;PKI技术对解决高校电子政务中存在的应用层面安全问题是一个比较好的选择(如身份验证、数据加密和数据完整性等).图2所示的高校电子政务PKI的构架模型是对文献[8]模型的修改,其中包括有端实体(即个人用户和应用系统)、目录服务、CA认证管理、RA管理器、用户管理器等,每个校园网PKI系统有一个根CA,分校区设立一个下级CA,分校校区都有一个RA与之相连,证书库位于不同的目录服务,当用户需要查询证书时,先向CA提出申请,然后由子CA从证书库中提取证书信息,CA之间是交叉认证.对于高校电子政务安全体系而言,一个高效率的CA中心、一个安全的角色访问控制和一个稳定的证书库对教育电子政务应用平台是必要的,笔者的研究是建立在高校PKI系统框架模型基础上(图2),从CA认证、证书库、访问控制等方面进行高校电子政务PKI安全体系的分析和构建.

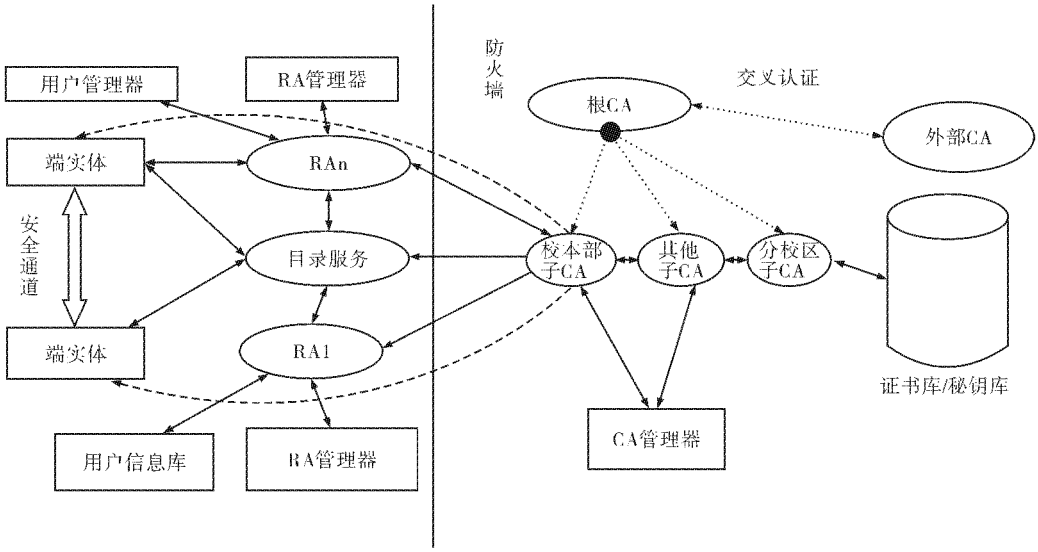

图2 高校PKI系统框架模型

Fig. 2 System framework model of colleges based on PKI

2.1　桥 CA 认证结构

CA 服务器是整个高校 PKI 电子政务证书机构的核心[2,11]，根据 CA 间的关系，PKI 的体系结构有三种情况：单个 CA，分级（层次）结构的 CA（从属关系）和网状结构的 CA（对等关系）. 三种情况各有优点且用在不同的条件下，但单个 CA 的结构不易扩展到支持大量的不同的群体的用户；分级结构的 CA 的缺点是它依赖于根 CA，若根 CA 安全性削弱，将导致整个 PKI 系统安全性削弱；分级结构的 CA 是所有的信任都集中在根 CA，而一旦该可信任点出现故障，后果是灾难性的. 高校 PKI 电子政务一般采用的是分级 CA，由于各种原因，现在很多高校都有两个甚至多个校区，校区之间的物理距离也很远，再加上各院系和部门之间功能相对独立，有必要使用多个 CA（如图 2），而且所有 CA 的公钥验证用户的证书都必须是可信的. 对于高校电子政务来说，由于高校各部门、院系之间不是从属关系，因此不能简单使用分级的 CA 结构；但在一个院系或部门内部，从属关系还是存在的，因此也不能简单地使用网状结构的 CA. 结合高校特点，在高校电子政务体系中构建桥 CA 认证体系（如图 3）：在各部门内部使用分级的 CA 认证，各部门之间通过学校的中心 CA 进行桥接 CA 认证，并且可以根据学校规模的大小设立相应的 CA 认证中心的数量，进行交叉认证，从而建立高校 PKI 的信任模型.

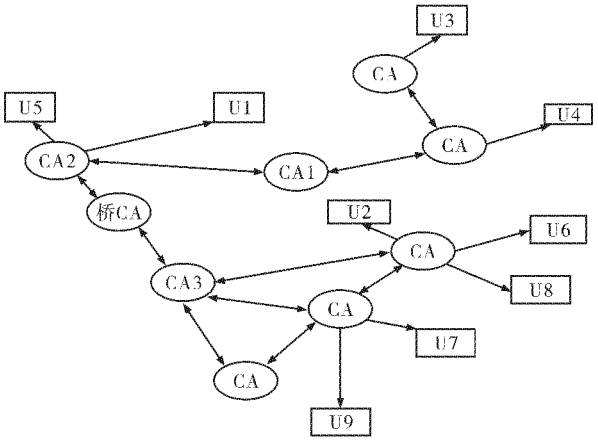

图 3　基于 PKI 的桥 CA 连接不同结构

Fig. 3　Bridge CA interface structure on PKI

在图 3 中，桥 CA 分别与 CA1、CA2、CA3 建立对等信任关系，那么 CA1、CA2、CA3 就是各自 PKI 体系中的主 CA. 用户 U1 和 U6 可以通过他们各自的可信任点 CA2 和 CA3，经桥 CA 的连接建立起信任关系，进行安全通信.

2.2　LDAP 的高校 PKI 证书库

LDAP 是轻量目录访问协议（Lightweight Directory Access Protocol），目录是一个以“树型”为数据组织结构的特殊数据库，存放信息的载体，比关系型数据库具有更高的查询速度[12]. 证书库用于发布通过认证中心 CA 认可的数字证书，是高校 PKI 电子政务系统的数据存储中心和发布中心；证书库发布的数字证书包含了证书持有者的个人详细信息、CA 的数字签名和公钥等，为了保证证书内容的可靠性，一般通过证书上 CA 的签名验证，就可以确认每个持有者的公钥的真实性和身份的合法性[12−14]. 由于高校电子政务系统中用户对证书的查询请求非常频繁，构建 LDAP 的证书库（如图 4 虚线所示）尤为重要[2]，可以大大优化证书的匹配、查询、维护等功能，避免在使用中不同数据库之间复杂的协议转换，保证对合法使用者的身份有效认证、提高查询响应频率.

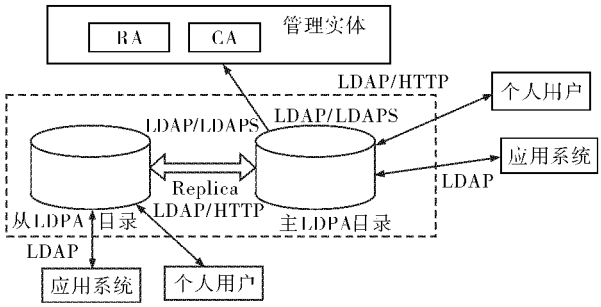

图 4　LDAP 的 PKI 证书库

Fig. 4　PKI certificate library based on LDAP

图 4 虚线部分有主库（主 LDAP 目录）和从库（从 LDAP 目录）组成，证书库的内容包括：证书和 CRL、证书库版本号、证书目录树下的修改操作日志. 管理实体负责主库中的各种数据维护（如 x. 509证书和 CRL），RA 负责向 CA 提交请求和用户证书申请，CA 负责证书的签发以及维护主 LDAP 目录（主证书库）中的证书状态；目录复制功能（Replica）是将 CA 对主库的修改操作通过主 LDP 目录（主库）实时地反映到从 LDP 目录（从库）中，LDAPS 的功能是维护、定期检测从库的数据、日志或证书库的版本号是否和主库的一致，若主库和从库有一方发生故障，Replica 能保持证书库的正常服务和数据的稳定性.

2.3　RBAC 角色的访问控制

访问控制就是用户对访问系统的请求进行控制，也就是准许或限制访问能力及范围的一种方法[15]. 通过访问控制可以防止合法用户对系统资源的非法使用和非法用户进入系统、非法访问关键资源；传统的访问控制实现通常依赖于系统安全的授权服务才能建立用户的身份[15]. 由于高校电子政务资源丰富，查询和访问的人多，且访问的

角色(如院长、主任、老师、学生)不同、权限也不同;为了确保安全、有效访问高校电子政务PKI系统中的资源,建立基于PKI的角色及权限访问控制策略RBAC(如图5)尤为重要[2].例如:一个普通教师通过证书登陆系统(他的证书的角色及权限关系已在证书扩展项中指明),系统在验证证书的过程中,自动通过检查证书的角色和权限的关系来决定这张证书的使用者可以进行考分登记或修改、查询课表和教室等操作.

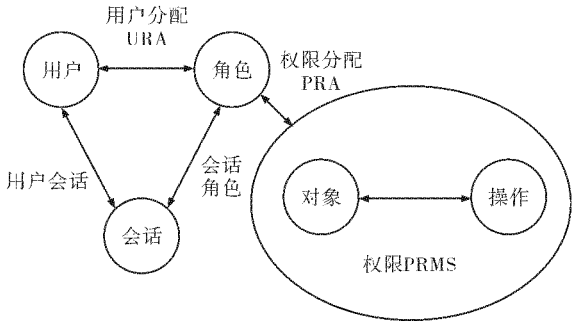

图5 RBAC访问控制

Fig. 5 Access control model based on RBAC

图5中"角色——权限"和"用户——角色"之间用双箭头相连表示角色权限分配(Permission-Role Assignment,以下简称:PRA)关系和用户角色分配(User-Role Assignment,以下简称:URA)关系都是多对多的关系.在角色权限分配PRA关系中[2]:一个角色可包含多个权限,同样一个权限可被多个角色所拥有;在用户角色分配URA关系中:一个用户可以分配多个角色(例如院长拥有老师和领导角色),一个角色可授权给多个用户.图4中基于PKI的RBAC访问控制就是在用户和访问权限之间引入角色,用户不直接与权限相关联,用户通过角色享有权限来访问系统资源.访问控制过程分成两个部分:访问权限与访问角色,RBAC访问控制中角色与权限是逻辑分离的,从而保证了高校PKI电子政务访问控制的信息安全.

综上所述,在基于PKI的高校电子政务平台采用桥CA认证体系、LDAP的证书库、RBAC的访问控制能有效解决高校电子政务对于身份认证、访问控制、信息安全等问题.

3 结 语

PKI在高校电子政务的安全应用目前已在本院实施,取得了良好效果.如PKI中的数字签名、数字认证、角色访问控制已应用到本院信息管理系统、论文管理系统、学生实验信息管理系统等环节中.高校电子政务PKI的安全问题还必须在PKI策略的指导下进行:建立数据备份基础设施,以物理安全和人员的管理来解决高校电子政务内部人为的安全问题;制定学校的安全规定和相关的法律法规来保证高校电子政务PKI的安全;建立信息安全保护的技术机制,用技术上的安全策略来保证高校电子政务PKI的安全.随着社会信息化的不断深入,PKI作为信息安全的基础设施将逐步显示它的重要性,PKI是一项十分成熟的技术,随着PKI技术应用的不断深入发展和PKI技术本身的不断变化和完善,因特网以及高校电子政务网的应用已越来越离不开PKI技术的支持,高校电子政务PKI系统将在未来的校园信息安全领域发挥作用.

致谢

湖北工程学院对本工作提供了资金资助,华中科技大学计算机学院和湖北工程学院提供了实践基地,在此一并致以衷心的感谢!

参考文献:

[1] 李鸣.我国电子政务发展综述[J].武汉工程大学学报,2010,32(4):52-55.

[2] 张靖.公钥基础设施在高校电子政务安全中的应用[D].武汉:华中科技大学,2006.

[3] 李伟平.基于服务的公钥密码应用支持系统的设计与实现[D].长春:吉林大学,2011.

[4] 周杨,王春枝.PKI体系下的电子政务信息安全研究[J].软件导刊,2009,8(3):161-163.

[5] Adams C,Lloyd S.公开密钥基础设施——概念、标准和实施[M].冯登国,译.北京:人民邮电出版社,2001.

[6] 黄兰英.基于PKI的电子政务安全策略[J].孝感学院学报,2005.3:74-77.

[7] 范明钰,王光卫.密码学理论与技术[M].北京:清华大学出版社,2008.

[8] 聂维.PKI技术及其在校园网中的应用研究[D].上海:华东师范大学,2008.

[9] 王启建.基于PKI技术的安全电子政务系统的设计[D].曲阜:曲阜师范大学,2007.

[10] 张福宾,张春海.基于PKI的安全电子政务应用[J].计算机工程,2004,30(6):130-132.

[11] 强勇军.PKI/CA的构建与应用[D].成都:电子科技大学,2006.

[12] 高毓航,龚俭.基于LDAP目录服务的PKI证书库研究与设计[J].计算机工程,2009,12:61-67.

[13] 张靖,马丁.LDAP目录服务在PKI中的应用[J].河南科技学院学报:自然科学版,2006,1:106-109.

[14] 赵红云,赵福祥,陈砚圃.轻量级目录访问协议在证

书库中的应用[J]. 计算机应用与软件,2007,11:198-200.

[15] 侯奋飞,宋宇波. 基于 PMI 的电子政务访问控制体系[J]. 计算机工程,2004,17:114-116.

Research of security university E-government based on public key infrastructure

***HUANG Lan-ying*[1], *YE Cong-huan*[2]**

(1. School of Computer and Information Science, Hubei Engineering University, Xiaogan 432000, China;
2. Department of Computer Science, Huazhong University of Science and Technology, Wuhan 430077, China)

Abstract: A model based on the core technology in the public key infrastructure (PKI) was introduced to resolve the safety problems in the E-government affairs of colleges and universities, such as identity authentication, access control and information safety. A PKI trust mechanism was established by using the bridge certificate authentication (CA), a hierarchical CA in every internal department and the bridge CA to cross authentication between various departments through a center CA were used. A PKI certificate base was established by using the lightweight directory access protocol (LDAP), which used directory replication to realize master-slave LDAP data consistency, so the availability of identity authentication of users was enhanced. The legal safety access of users was controlled by using role based access control (RBAC), the role between the user and the access was introduced , then the user accessed system resources through the permissions granted to the roles. The model is proved in practice according to the safety requests and is useful for the development of the E-government affairs of colleges and universities.

Key words: authentication center; university E-government; information security; public key infrastructure

本文编辑:苗　变