广西科学院学报
Journal of Guangxi Academy of Sciences

2007,23(4):347~349,359
Vol. 23,No. 4 November 2007

基于PKI技术的政府专用办公自动化系统的设计与实现

Design and Implementation of OA System for Government Units Based on PKI Technology

刘 杨,文彬宏,徐飞斯
LIU Yang,WEN Bin-hong,XU Fei-si

(广西科技信息网络中心,广西南宁 530012)
(Guangxi Science and Technology Information Network,Nanning,Guangxi,530012,China)

摘要:利用网络技术、Web技术和网络安全技术,设计实现一个政府部门专用办公自动化系统,该系统由公文处理、角色管理、流程管理、消息管理和安全管理5个模块组成,能够满足政府部门公文处理的自动化、标准化要求,有效地解决办公自动化系统的身份认证和数据安全传输问题。该系统的设计思想和方法对行政企事业单位建设办公自动化系统有一定的参考价值。

关键词:办公自动化 PKI USB安全钥

中图法分类号:TP317.1 **文献标识码**:A **文章编号**:1002-7378(2007)04-0347-03

Abstract: This paper designs and implements the special OA system for government units based on the web and PKI security technology. The system is composed of five modules including document processing, role, procedure, message and security management. The OA system can meet the need of the government units and help solve some problems such as identity authentication and transmission security. The idea and method applied to the OA system design have their value for reference during the OA construction of enterprises and administrative units.

Key words: OA, PKI, USB security keys

办公自动化系统作为信息网络的一个特殊应用领域,运行着大量需要保护的数据和信息,有其自身特殊性,如果系统的安全性被破坏,造成敏感信息暴露或丢失,或网络被攻击等安全事件,可能导致严重的后果。尤其是政府部门的办公自动化系统,每天都需要收发很多的重要公文,有的甚至是是机密文件,因此政府部门使用的办公自动化系统的安全性显得尤为重要。目前办公自动化系统安全措施最常用的就是使用用户名加口令的方式,但这也是最原始、最不安全的身份确认方式,非常容易由于外部泄漏等原因或通过口令猜测、线路窃听、重放攻击等手段导致合法用户身份被伪造。本文利用现有成熟的网络技术、Web技术和网络安全技术,设计实现一个具有高度安全性的政府部门专用办公自动化系统,为推进政府机关和企事业单位办公自动化系统的安全建设提供参考。

1 系统的设计目标

1.1 应用目标

专用办公自动化系统总体目标是:采用成熟的网络和安全技术,建成一个覆盖机关各部、处(科)室的专用办公系统,为机关办公提供安全高效的服务,实现办公现代化、信息资源化、传输网络化和决策科学化。该系统改进现有的工作环境和条件,进一步提高机关办公效率、水平和质量,实现日常办公事务、处理事务的自动化、标准化,最终实现办公过程的"无纸"化,以适应单位信息化建设的需要。

1.2 技术目标

专用办公自动化系统的应用开发技术目标是:

收稿日期:2007-09-20

作者简介:刘 杨(1963-),男,工程师,主要从事计算机网络安全研究与开发。

(1)系统覆盖面横向覆盖本单位机关各部、处(科)室,纵向机关上下各级;(2)采用JAVA网络编程技术和数据库技术[1],将公文的存放和处理的工作迁移到网上,使各级领导和单位工作人员能方便、及时地进行业务处理;(3)充分利用网络现有资源,建立高质量、高效率的管理信息网,改变目前人工传送公文的现状;(4)系统采用公钥基础措施(PKI)技术保证自动化办公的安全性,每个用户都单独拥有一个数字证书,利用该数字证书可以保证公文处理的安全性和不可否认性等。

2 系统的体系结构设计

政府专用办公自动化系统主要依据Internet/Intranet的建设原则,在基本网络平台基础上,使用"客户层/表示层/业务处理层/数据层"的四级结构,系统体系结构如图1所示。

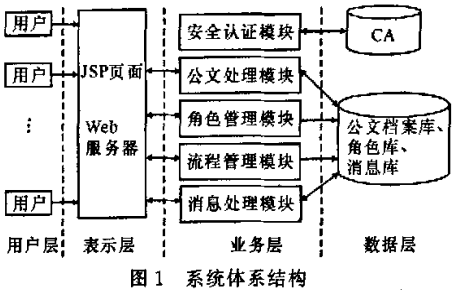

图1 系统体系结构

用户层:用户通过浏览器对系统进行访问。每个用户在身份验证成功以后才能开始在系统下进行相关的办公业务。身份的验证需要结合角色库和个人的数字证书,角色库中维持了一个角色表,该表按单位的行政级别和个人的职务来进行分类,其关系如树形结构,以便公文传送时的流程管理;个人的数字证书存放在一个USB存储卡中,数字证书与存储卡的硬件ID号相对应,以防止证书的盗用。

表示层:表示层上放置的是JSP页面,运行于Tomcat服务器(一种JSP的容器)之上。这些JSP页面主要负责接收用户的请求,将请求消息传给相应的处理模块,并接收处理结果,将结果显示到用户的浏览器。

业务层:业务层负责相关的业务处理,包括公文处理模块、角色管理模块、流程管理模块和消息处理模块。这些业务处理之前都必须进行相应的安全验证,因此业务层还包括安全认证模块。业务层从表示层接收到业务消息后,调用相应的模块对消息进行处理,处理中如果需要安全认证,则调用安全认证模块,进行加密解密或者签名。

数据层:数据层负责为业务层处理业务时提供必要的数据支持。包括数据的存放、查询、修改和删除等,数据的类型有公文、角色信息、消息、证书等。数据层采用数据库服务器存放这些数据,所以数据层需维持公文档案库、角色库和信息库等,证书放置于认证中心(CA)。

3 系统的功能设计

3.1 公文处理

完成收文办理、发文办理、公文催办等功能。系统能根据不同用户的不同行文流程,自动实现收文、发文、统计查询直至办公的全过程。对整个工作流程实现实时跟踪和对修改审核信息进行记录,并能按照办公有关规定,自动地报告、提供公文在其处理中的状态,以便采取相应的措施。用户可以在浏览器上对公文进行撰写、批复、签名等,撰写或修改的公文传送到业务层之后,进行相应地业务操作。经过安全处理后的公文将存放于数据库。

根据业务操作要求,公文处理包括4个部分:公文拟制、公文传送、公文管理和立卷归档。

3.1.1 公文拟制

指公文的起草、校核、会签和领导审批签发等。机关发文一般流转程序为:首先由拟稿的机关处(科)室的办公人员负责起草,起草完毕,送本处(科)室领导进行校核,如果需要相关单位会签时,送相关单位会签;校核(含会签)完毕,转呈部门领导及单位领导审批签发。对于已经经过本单位领导人审批的文稿,在印发之前可再做校核,经校核如需作涉及内容的实质性修改,须报原审批领导人复审。如果送印,将进入发文办理程序。

3.1.2 公文传送

包括收文办理和发文办理。收文办理主要包括公文的签收、登记、拟办、分发、传阅、批示、承办和催办等程序。公文经起草、校核和领导审批签发后转入发文办理,发文办理包括公文的核发、登记、印制和分发等程序。

3.1.3 公文管理

公文大多涉及大量秘密信息,系统严格按照机关公文管理业务规范开展工作,以达到科学化、制度化、规范化。

3.1.4 立卷归档

系统中公文档案库采用根据单位、标题和发文日期来分类保存公文,用系统管理员的公钥来加密,只有管理员和他赋予权限的用户才能进行查阅,以

保证档案的安全性。系统提供公文档案库导入导出的功能,可以实现定期对数据的备份,在出现灾难式故障后,可导入最新备份以恢复公文档案库,避免出现重大损失。

3.2 角色管理

结合单位的编制,建立一个角色库,让每个角色都结合其职务级别,以便管理及公文的准确传送。根据职务级别生成的角色库是一种树形结构,公文的传送和传阅按树形目录的思想来实现。

每个单位将都有管理员对本单位的公文、角色、消息、安全证书等系统数据进行管理。上级的管理员可对下级的管理员进行管理。角色管理包括角色的注册、认证、修改、删除等。

3.3 流程管理

流程管理主要运用于公文的传送,根据公文的信息和角色库,使公文自动、准确的传送到目标位置。该模块决定了办公自动化系统的效率和可用性。采用流程管理后,可提供系统的适应性,使本系统中各种功能模块符合实际工作变动的需要。具体方法是:当用户需要传送公文时,流程管理将对角色库进行访问,根据用户身份获取其上、下级和同级单位的角色信息,将这些信息作为选项提供给用户,待其选择传送对象。

3.4 消息处理

消息处理有3个主要作用:一是在公文发送时,通知和提醒接收方及时查阅公文;二是公布一些通知通告,发布本单位的重要事件;三是用于两个用户间传送文字信息,方便用户之间的交流。

3.5 安全认证

安全认证负责解决系统对用户的身份认证和数据的安全传输问题。

4 关键技术

办公自动化系统作为信息网络的一个特殊应用领域,运行着大量需要保护的数据和信息,有其自身特殊性,如果系统的安全性被破坏,造成敏感信息暴露或丢失,或网络被攻击等安全事件,可能导致严重的后果。

目前的办公自动化系统安全措施最常用的就是使用用户名加口令的方式,但这也是最原始、最不安全的身份确认方式,非常容易由于外部泄漏等原因或通过口令猜测、线路窃听、重放攻击等手段导致合法用户身份被伪造等。专用办公自动化系统必须解决双方身份认证问题以及身份认证后数据安全传输问题。解决第一个问题时我们可以使用数字签名和电子印章技术,而解决第二个问题时可以使用加/解密技术,在这两项技术中的关键点就是签名和加密所用的私钥。

4.1 基于PKI的认证

针对办公网络系统的身份认证、权限控制、加密传输和异地办公的安全问题,系统采用PKI体系。PKI是一种遵循既定标准的密钥管理平台,是一个利用现代密码学中的公钥密码技术在开放的Internet网络环境中提供数据加密以及数字签名服务的统一技术框架[2]。PKI最主要的安全技术包括两个方面:公钥加密技术、数字签名技术。公钥加密技术可以提供信息的保密性和访问控制的有效手段,它保证了利用公钥加密后的数据,如果没有提供相应的私钥来解密的话,窃密者即使获得密文也难以知晓其中的内容。而数字签名技术则提供了在网络通信之前相互认证的有效方法、在通信过程中保证信息完整性的可靠手段以及在通信结束之后防止双方相互抵赖的有效机制。

4.2 USB安全钥的应用

签名和加密所用的私钥使用USB安全钥的方法实现。USB安全钥内置CPU或智能卡芯片,可以实现PKI体系中使用的数据摘要、数据加解密和签名的各种算法,加解密运算在USB安全钥内进行,保证了用户密钥不会出现在计算机内存中,从而杜绝了用户密钥被黑客截取的可能性[3]。基于USB的随身携带,热插拔、传输速度快以及硬件等优势,将私钥存储于USB硬件中,结合加密算法,可以比较好地解决系统中身份认证以及数据加密传输问题。

在使用过程中,所有有关安全性的操作都在USB安全钥和服务器内部完成,极好地保护了安全数据。在这一前提下,用户可以携带USB安全钥在任意一台网络终端上进行业务处理,而不必担心会有任何重要数据留在使用过的网络终端上。而且每一个USB安全钥都具有硬件个人识别码(PIN)保护,PIN码和硬件构成了用户使用USB安全钥的两个必要因素,即所谓"双因子认证"。用户只有同时取

(下转第359页)

等日志,不定期升级相关 IPS 库、策略模版即可实现对网络内的管理。同时,Sygate 内置的邮件通知功能可以通过配置直接将上述日志报表发送到管理员的邮箱。

3 结束语

广西柳工机械股份有限公司使用这套网络准入控制管理方案后,可以实现合法用户正常连接进入到网络,非法用户无法连接进入网络,远程连入的用户也能够按照企业的网络管理规则签到而进入网络。这套方案为对于在网络内如何做好安全控制提供了新的思考方向。

参考文献:

[1] 雷震甲. 网络工程师教程[M]. 北京:清华大学出版社,2004.

[2] 王春森. 系统设计师[M]. 北京:清华大学出版社,2001.

[3] 郭军. 网络管理[M]. 北京:北京邮电大学出版社,2001.

[4] 张炯明. 电子商务安全使用技术[M]. 北京:清华大学出版社,2005.

[5] 劳帼龄. 网络安全与管理[M]. 北京:高等教育出版社,2003.

[6] 祁明. 网络安全与保密[M]. 北京:高等教育出版社,2005.

[7] 白以恩. 计算机网络基础及应用[M]. 哈尔宾:哈尔宾工业大学出版社,2004.

(责任编辑:邓大玉)

(上接第 349 页)

得了 USB 安全钥和用户 PIN 码,才可以登录系统。即使用户的 PIN 码被泄漏,只要用户持有的 USB 安全钥不被盗取,合法用户的身份就不会被仿冒;如果用户的 USB 安全钥遗失,拾到者由于不知道用户 PIN 码,也无法仿冒合法用户的身份。

USB 安全钥在系统中的认证流程如图 2 所示。

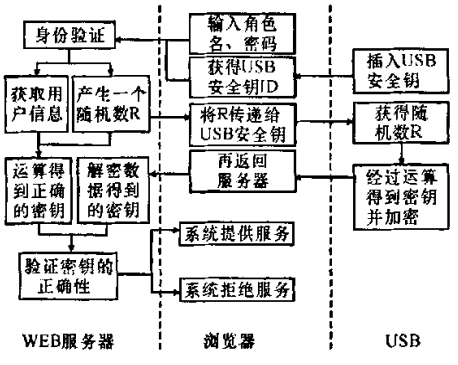

图 2 USB 安全钥在系统中的应用流程

5 结束语

本文实现的政府部门专用的办公自动化系统充分利用了 Internet/Intranet 的优势,采用成熟的网络和安全技术,保障了政务的安全传送和处理,为政府部门及时掌握和处理信息提供了一个先进、可靠、安全保密的系统。通过使用该系统,可以不断改进现有的工作环境和条件,进一步提高机关工作的效率、水平和质量,实现日常办公事务、处理事务的自动化、标准化,最终实现办公过程的"无纸"化,以适应办公信息化建设的需要。本文所介绍的系统对行政单位、企事业单位建设办公自动化系统有一定的参考价值。

参考文献:

[1] RICH HELTON, JOHENNIE HELTON. Java 安全解决方案[M]. 北京:清华大学出版社,2004.

[2] 祝晓光. 网络安全设备与技术(公钥基础设施(PKI)部分)[M]. 北京:清华大学出版社,2004.

[3] 冯世立,李鹏飞,张海峰. USB 安全钥在电子政务系统的应用[J]. 计算机安全,2006(2):31-32.

(责任编辑:韦廷宗)