# 集成电子签章功能的公文流转系统的实现

李 静,韩建民,郭腾芳,罗方炜
(浙江师范大学 数理信息学院,浙江 金华 321004)

**摘 要**:为了在安全性要求较高的应用中使用公文流转系统,保证公文在流转过程中的完整性和签署者的不可否认性,论文研究了基于PKI的电子签章技术,实现了基于ActiveX技术的面向Office的电子签章控件。该控件采用USBKey技术实现身份认证,利用VBA提取Office文档内容,采用数字签名与验证技术保证文档的完整性。基于实现的电子签章控件,开发了面向Web的集成电子签章功能的公文流转系统,用户可以在公文流转过程中,加盖电子签章,保证了公文在流转过程中的完整性和签署者的不可否认性,从而提高了公文流转系统的安全性。

**关键词**:公开密钥基础设施;数字签名;电子签章;数字证书
**中图分类号**:TP309 **文献标识码**:A **文章编号**:1673-629X(2011)12-0152-03

# Implementation of a Document Circulation System With Electronic Seal

LI Jing, HAN Jian-min, GUO Teng-fang, LUO Fang-wei
(College of Mathematical Physics and Information, Zhejiang Normal University, Jinhua 321004, China)

**Abstract**: It investigates the technology of electronic seal based on PKI and implements electronic seal controls based on ActiveX technologies oriented Office documents. These ActiveX controls implement identity authentication based on USBKey, achieve content of signature document by VBA and ensure the integrity of documents by digital signatures and verification. It also develops a document circulation system with electronic seal oriented Web, in which user can add electronic seal during the document circulation to ensure the integrity of documents and non-repudiation of signature, so that the security of the document circulation system is improved.

**Key words**: PKI; digital signature; digital seal; digital certificate

## 0 引 言

电子签章[1]是一种数字签名技术,它通过一套标准化、规范化的软硬件结合,使持章者可以在电子文件上完成签字盖章,并从技术上保证签章公文的完整性和签署者的不可否认性。2005年,我国电子签名法的实施,确保了电子签章与传统的手写签名、盖章具有相同的法律效力,促进了电子签章技术的推广与应用。电子签章相关技术的研究也随之成为信息安全领域的研究热点,袁晓宇等[2]提出了基于ECDSA的电子签章方法,该方法采用椭圆曲线密码(Elliptic Curve Cryptosystems)公钥密码体制实现电子签章。祁振杰等[3]基于组件对象模型COM技术提出了一种签章控件实现方法。张飞等[4]提出基于时间戳服务的电子签章验证方法。肖攸安等[5]将数字签名方法和认证水印技术结合,提出了一种电子签章实现方法。然而,将电子签章功能应用于公文流转系统[6,7]的研究不多,文中研究了基于PKI(Public Key Infrastructure,公开密钥基础设施)[8-12]的电子签章技术,基于USBKey技术和ActiveX技术设计了一套面向Office的电子签章控件,基于该套控件,实现了一个具有电子签章功能的公文流转系统。

## 1 电子签章控件实现的关键技术

实现Office文档的电子签章可分为三个步骤,签章的流程见图1。

第一,身份认证:执行签章动作前,先要通过USBKey身份认证;

第二,盖章过程:该过程首先要通过VBA获取文档的内容,然后对文档的内容进行数字签名,再将签名信息、数字证书信息以及印章图片加载到签章控件中,最后显示印章图片;

第三,提交过程:将签章后的页面提交并保存到服

**收稿日期**:2011-04-24;**修回日期**:2011-07-26
**基金项目**:2010年浙江省大学生科技创新活动计划(新苗人才计划)资助项目(2010R404049)
**作者简介**:李 静(1986-),女,河南郑州人,硕士研究生,研究方向为信息安全;韩建民,博士,副教授,研究方向为信息安全、智能计算。

务器。

为实现图 1 的签章流程,文中采用 ActiveX 技术实现了可以嵌入到 Web 页的 OfficeSeal 控件。OfficeSeal 控件实现了身份认证、电子签章、签章验证以及文档提交等功能。OfficeSeal 控件为外部程序提供的接口主要有:

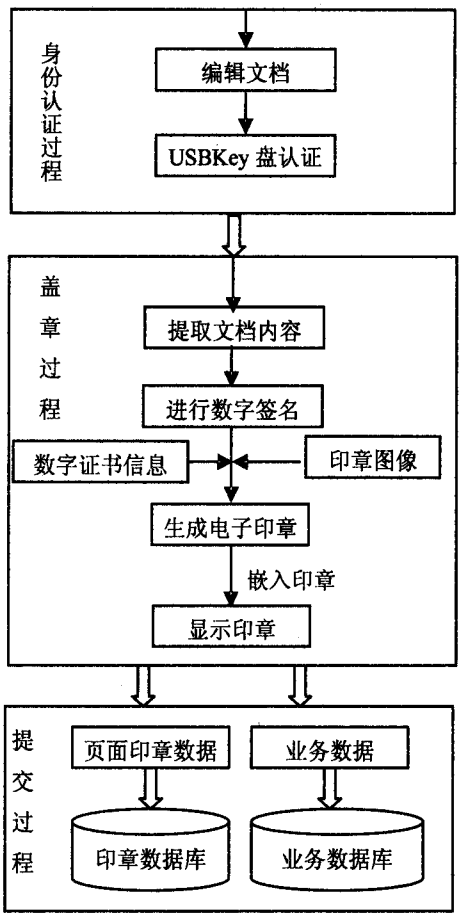


图 1　签章流程

1)用户身份认证:用户身份认证是采用 USBKey 技术来实现。USBKey 是用户数字证书、密钥、电子印章图片存储的容器以及加解密的工具。

2)加盖电子印章:用户身份认证后,利用 VBA 提取文档内容,然后提取文档的摘要,并对摘要信息进行数字签名,并把数字签名、摘要以及从 USBKey 中读取的数字证书等嵌到印章控件中,最后在 Office 文档中显示电子印章。

3)Hash 验证:用于验证文档是否被篡改。验证过程是:印章控件通过 VBA 函数获取 Office 文档内容,并提取摘要信息,再与保存在印章控件中的摘要信息进行比较,验证当前 Office 文档是否被篡改,验证流程见图 2。

4)签名验证:实现文档的完整性验证和签署者的不可抵赖性验证。验证过程是:首先利用 VBA 函数获取 Office 文档的内容,对文档的内容提取摘要信息 $D_1$,再用公钥对印章控件中的数字签名信息进行解密,得到摘要信息 $D_2$,比较两次得到的摘要信息 $D_1$ 和 $D_2$,若相等,说明文档没有被篡改,并可唯一确定签署者身份,验证流程见图 3。

5)撤销电子印章:首先检查电子印章是否处于可撤销状态,若是,再基于 USBKey 的 PIN 码进行身份认证,在满足上述 2 个条件的基础上,执行删除印章功能,将电子印章控件从文档中删除。

6)证书预览:不需要身份验证,任何用户都可以查看印章所属用户的证书信息。

7)提交:把当前 Office 文档以及印章数据提交并保存到服务器端。

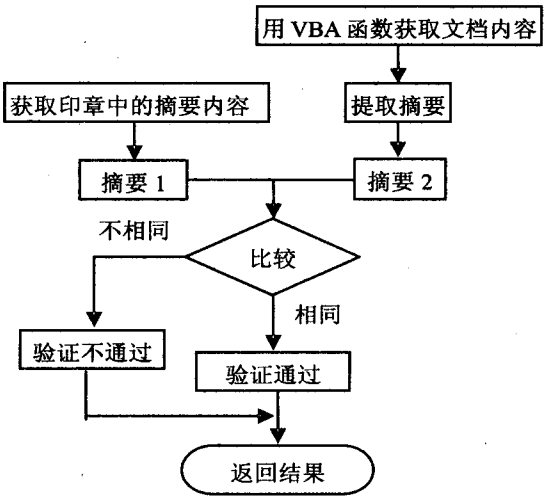


图 2　Hash 验证的流程图

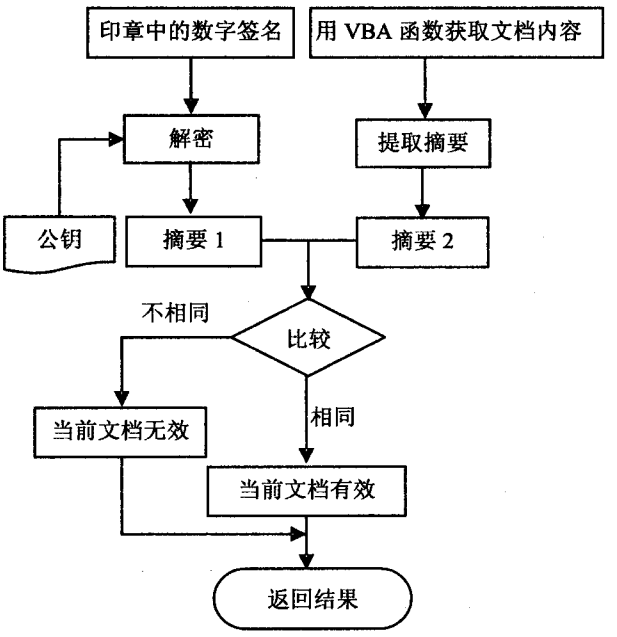


图 3　签名验证流程

## 2　集成电子签章功能的公文流转系统设计

文中在公文流转系统中嵌入了电子签章功能,系统采用的是 B/S 的模式,使用 J2EE 框架。采用 MyE-

clipse 平台和流行的 MVC(Model+View+Control)的设计模式,后台数据库使用的是 Microsoft 公司的 SQL Server 2005。集成电子签章功能的公文流转系统的总体结构图如图 4 所示。

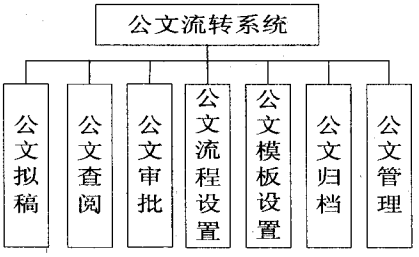


图 4 公文流转系统总体结构图

本系统的整体功能包括:

1)公文拟稿:主要包括填写公文表单、拟稿正文、上传附件、发送公文等步骤。

2)公文查阅:查阅已审批和已发送但未审批公文的流转情况。

3)公文审批:将要审批的公文按缓急情况排序,如果相同则均按时间先后排序。然后查看公文,并填写审批意见,若审批通过则可以盖章,点击开始签章按钮,就会提示输入持章人的 Key 盘密码。在审批过程的每一个步骤中,要求加入时间约束,每一步审核完成后需要审核者加盖自己的电子签章。

4)公文流程设置和公文模板设置:用于新建和修改公文流程和模板。

5)公文的归档:对已审批公文进行归档,归档后的公文可以进行公文查看的分配,归档后的公文不允许被修改。

6)公文管理:包括关键字检索、报表统计等功能。

另外还有用户权限设置和管理等功能。用户权限包括管理员用户、部门管理用户、普通用户等,分别可以进行对公文在本权限范围内进行公文的分配,查阅设置。

其中公文审批详细流程如图 5 所示。

## 3 集成电子签章功能的公文流转系统实现

电子签章在公文流转系统中主要完成文档的电子签章、文档验证、文档提交等功能。实现的主要流程如下:

1)控件加载,将电子签章控件加载到公文流转页面中。加载的方法可以用 HTML 的<Object>标签,加载代码如下:

<object id="OfficeSeal" classid="clsid:A5D95742-785E-485C-90CF-3212FCAF0F30" width=100% height=100%></object>

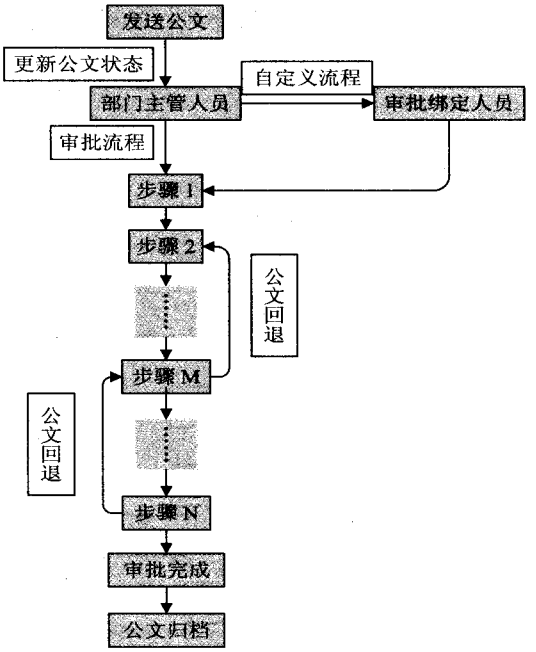


图 5 公文审批详细流程图

2)电子签章。对公文流转系统 Office 文档进行电子签章,签章时把文档的摘要信息、数字签名信息以及数字证书均嵌入在控件中,签章后的界面如图 6 所示。

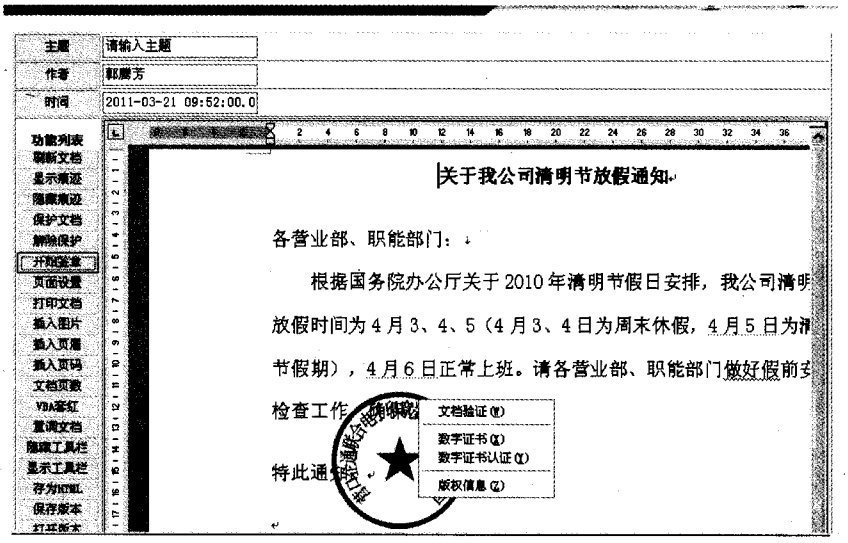


图 6 签章完成后的文件

3)文档验证。如果文档内容篡改,验证不通过,电子印章控件会在印章图片上加上两条灰色的横线,表示当前文档已失效,并提示验证失败信息。

4)文档提交。文档签章完成后,将文档和印章数据分别打包提交给服务器端,服务器端接收这些数据包,将印章数据保存到印章数据库,文档数据保存到业务数据库。

(下转第 159 页)

tems,2010,4(6): 1042-1062.

[6] Chen R, Park J, Hou Y T, et al. Toward secure distributed spectrum sensing in cognitive radio networks[J]. IEEE Communications Magazine,2008,46(4):50-55.

[7] Chen R, Park J, Reed J H. Defense against primary user emulation attacks in cognitive radio networks[J]. IEEE Journal on Selected Areas in Communications,2008,26(1):25-37.

[8] Peng Q, Cosman P C, Milstein L B. Optimal sensing disruption for a cognitive radio adversary[J]. IEEE Transactions on Vehicular Technology,2010,59(4):1801-1810.

[9] Yu F R, Tang H, Huang M, et al. Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios [C]//IEEE Military Communications Conference, MILCOM. Boston, USA: IEEE, 2009:1-7.

[10] Han Z, Li H. Blind Dogfight in spectrum: combating primary user emulation attacks in cognitive radio systems with unknown channel statistics[C]//IEEE International Conference on Communications, ICC. Cape Town, South Africa: IEEE, 2010:1-6.

[11] Chen R, Park J, Bian K. Robust distributed spectrum sensing in cognitive radio networks[C]//IEEE Communications Society Conference on Computer Communications. Phoenix, USA: IEEE, 2008:31-35.

[12] Kun Z, Paweczak P, Cabric D. Reputation-based cooperative spectrum sensing with trusted nodes assistance [J]. IEEE Communications Letters, 2010, 14(3):226-228.

[13] Zhu F, Seo S W. Enhanced robust cooperative spectrum sensing in cognitive radio[J]. Journal of Communications and Networks, 2009, 11(2):122-133.

[14] Hu F, Wang S, Cheng Z. Secure cooperative spectrum sensing for cognitive radio networks[C]// IEEE Military Communications Conference, MILCOM. Boston, MA, United States: IEEE, 2009:1-5.

[15] Li H, Han Z. Catching attacker(s): for collaborative spectrum sensing in cognitive radio systems: an abnormality detection approach[C]//IEEE Symposium on New Frontiers in Dynamic Spectrum. Singapore: IEEE, 2010:1-12.

[16] Rawat A S, Anand P, Chen H, et al. Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks[J]. IEEE Transactions on Signal Processing, 2011, 59(2):774-786.

[17] Xu Shaoyi, Shang Yanlei, Wang Haiming. Double thresholds based cooperative spectrum sensing against untrusted secondary users in cognitive radio networks[C]//IEEE 69th Vehicular Technology Conference, VTC. [s. l.]: [s. n.], 2009:1-5.

[18] Min A W, Shin K G, Hu X. Attack-tolerant distributed sensing for dynamic spectrum access networks[C]//17th IEEE International Conference on Network Protocols, ICNP. Princeton, NJ, United states: IEEE CS, 2009:294-303.

[19] Li Z, Yu F R, Huang M. A cooperative spectrum sensing consensus scheme in cognitive radios [C]//IEEE Communications Society Conference on Computer Communications. Leblon, Brazil: IEEE, 2009:2546-2550.

(上接第 154 页)

## 4 结束语

文中将电子签章功能集成到公文流转系统中,从技术上保证签章文档的真实性、完整性和签署人的不可否认性,从法律上保证了签章行为的法律效力,提高了公文流转系统的安全性,扩展了系统的适用范围,可以实现真正意义上的无纸化办公。

**参考文献:**

[1] 刘宏伟. 基于身份的电子签章系统设计研究[J]. 计算机工程与设计, 2008, 29(7):1735-1738.

[2] 袁晓宇,张其善. 基于 ECDSA 的电子签章系统研究[J]. 计算机工程与设计, 2005, 26(5):1233-1235.

[3] 祁振杰,蒋朝惠. 电子签章控件透明化技术的研究与实现[J]. 计算机应用与软件, 2009, 26(11):124-126.

[4] 张　飞,肖　刚,程振波. 基于时间戳服务的电子签章验证方法研究[J]. 浙江工业大学学报, 2009, 37(3):300-305.

[5] 肖攸安,刘俊波. 一种新型的电子签章技术[J]. 武汉理工大学学报, 2009, 31(13):123-126.

[6] 盛津芳,王　斌,桂卫华. 基于 XPDL 的可视化流程定义工具及公文流转系统[J]. 计算机技术与发展, 2007, 17(7): 193-195.

[7] 王文玉,曲传幸,宋淑梅. 基于 Lotus Domino/Notes 平台的电子公文审批系统[J]. 计算机技术与发展, 2007, 17(2): 156-158.

[8] Denning D E. Protecting Public Keys and Digital Signatures [J]. Computer, 1993(2): 27-35.

[9] Polk W. Federal public key infrastructure (PKI) technical specifications (version 1) Part A: Requirements[EB/OL]. 1996. http:// citeseer. ist. psu. edu/394045. html.

[10] Kim S G. Designing a Domain Framework with Component Management Model[J]. Journal of Software, 2002, 13(3): 335-341.

[11] 陈雪珲,李建华. 电子签章系统在企业 OA 系统中的应用[J]. 信息技术与信息化, 2008(3):49-51.

[12] 袁珍珍,朱荆州. 基于 PKI 技术的数字签名在办公网上的实现[J]. 计算机与数字工程,2010, 28(2):104-109.