DOI: 10.13657/j.cnki.gxkxyxb.2005.s1.043

浅析电子签名技术在电子公文流转系统中的应用

Application of Electronics Signature Technique in the Electronic Official Document System

梁 达

Liang Da

(广西数字证书认证中心有限公司,广西南宁 530022)

(Guangxi Certificate Anthority Center Ltd., Nanning, Guangxi, 530022, China)

摘要:在简述电子公文流转系统的基础上,介绍了电子签名技术在电子公文流转系统中的应用。在电子公文流转系统中使用电子签名技术,可以有效实现对用户的访问控制和实现数字签名,保证传输公文的有效性、真实性和完整性,提高公文传输的效率和公文的利用率,消除公文传输过程中的安全隐患。

关键词:电子签名 公文流转 数字签名

中图法分类号:TP399 文献标识码:A 文章编号:1002-7378(2005)S0-0129-02

Abstract Based on the system foundation of the summary electronic archives, we introduced the electronic signature technology in the system application in the electronic archives. The use of the electronic signature technology in the electronic archives can effectively realize the access control and the digital signature. This fundamentally has guaranteed the validity, authenticity and integrity, enhanced the archives transmission efficiency and the archive use factor, and eliminated security hidden danger in the archives transmission process.

Key words electronic signature, archives transmission, digital signature

传统的公文传输需要把公文打印出来,单位负责人在上面签字或者盖上单位公章后,再通过邮局或派专人寄送到接收单位。这种传统传输方式既浪费时间,又浪费财力物力。在互联网络飞速发展的今天,这样的公文流转系统已经不能适应时代的要求。在网络上传输文件不难实现,但传输政府公文,必须要有很好的可靠性,使得接收方能够确认公文可靠和真实。在传统的公文中采用签字或者盖章来确认公文的有效性和真实性。要在电子公文中实现与传统公文一样的签字或者盖章,必须使用电子签名技术,以确保公文的可靠性和真实性。

实现电子签名的技术手段有很多种,但目前比较成熟的,世界先进国家普遍使用的电子签名技术是数字签名技术。数字签名是目前电子商务、电子政务中应用最普遍、技术最成熟的、可操作性最强的一种电子签名方法。它采用了规范化的程序和科学化的方法,用于鉴定签名人的身份以及对某项电子数据内容的认可,它还能验证出文件的原文在传输过程中有无变动,确保所传输电子文件的完整性、真实性和不可抵赖性[1]。

本文在简述电子公文流转系统的基础上,介绍电子签名技术在电子公文流转系统中的实现。

1 电子公文流转系统简述

电子公文流转系统一般采用 B/S结构,利用 Web服务器对 SSL(安全套接字协议)技术的支持来实现系统的身份认证和访问控制安全需求。电子公文流转系统总共有四个部分组成,即:客户端浏览器,Web服务器,证书解析模块和访问控制列表(ACL)。在电子公文流转系统中安装有 CA认证中心颁发的服务器证书,用来表明服务器的身份,并对 Web服务器的安全性进行设置,使其具备 SSL功能。

电子公文流转系统中,不仅电子公文中需要使用电子签名技术,在登录该系统时也要用到电子签名技术。用户必须使用数字证书,确认身份,才能登

收稿日期:2005-09-20

作者简介:梁 达(1980-),男,广西南宁人,主要从事数字签名技术的应用开发工作。

录系统,使用系统发送和接收公文,电子公文流转程序如图 1所示。在电子公文流转系统中主要利用电子签名技术来实现访问控制和进行数字签名。

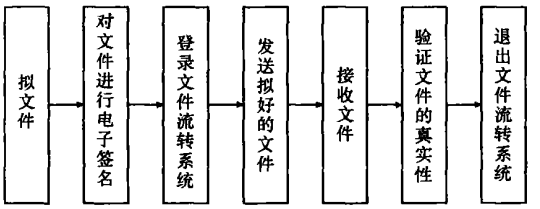

图 1 电子公文流转流程

2 电子签名技术在电子公文流转系统中的应用

2.1 访问控制的实现

用户使用浏览器访问电子公文流转系统 Web服务器时,会在客户端和服务器之间建立安全的SSL通道。SSL会话产生时,首先,服务器传送它的服务器证书,客户端自动分析服务器证书,验证服务器的身份。其次,服务器会要求用户出示客户端证书(即用户证书),服务器完成客户端证书的验证,实现用户的身份认证。对客户端证书的验证包括验证客户端证书是否由服务器信任的证书颁发机构颁发、客户端证书是否在有效期内、客户端证书是否有效(即是否被窜改等)和客户端证书是否被吊销等。验证通过后,服务器会解析客户端证书,获取用户信息,并根据用户信息查询访问控制列表来决定是否授权访问。所有的过程都会在几秒钟内自动完成,并对用户透明。

系统的服务器证书内表示了服务器的域名等证明服务器身份的信息、Web服务器端的公钥以及CA对证书相关域内容的数字签名。每个服务器证书都有一个有效期,利用服务器证书来协商、建立安全SSL安全通道。建立SSL通道过程中,把服务器的SSL功能配置成必须要求用户证书,以服务器验证用户证书来确认用户的真实身份。这样一来,当用户系统登录时要求用户插入key盘,以识别用户身份。key盘是用户证书的载体,里面标识了用户的身份信息、用户的公钥以及CA对证书相关域内容的数字签名。用户插入key盘后,证书解析模块开始解析证书中包含的信息,用于提取证书中的用户信息,根据获得的用户信息,查询访问控制列表(ACL),获取用户的访问权限,实现系统的访问控制。

2.2 数字签名的实现

电子公文流转系统中数字签名的实现表现为对发送的公文进行数字签名和数字签章,这是发送方对公文的确认,使其具有不可抵赖性,而接受方就凭签名或者签章确认公文的真实性和有效性。要对文档进行签名或者签章,首先必须安装文档签名软件,安装以后在文档的左上方(以word文档为例)出现签名的栏目,点击以后出现提示框,要求用户插入存放数字证书或者图章证书的key盘。用户插入key盘后,选择签名或者签章,点击签名,输入key盘密码正确后就可以使用该签名或者图章。这时文档上就会出现签名或者签章的图样,把它放到合适的地方,完成对文档的签名。然后保存该文档,等待下一步发送的时候使用。

公文的接收方,接受到文件后,可以查看签名或者签章的真实性,双击签名或者图章,在弹出的对话框中,点击查看签名证书或者查看图章签名证书,可以看到签名证书或者图章签名证书的有效性、真实性,检查证书是否过了有效期。若无问题,用户就可以接收文件,并把它保存到本地计算机上,完成一次使用数字签名的公文发送。用户收到公文后不能对公文进行修改,否则在签名或者图章处显示一个横线,提示已经修改文档。同时,用户也不能删除签名或者签名图章,确保文档的完整性。

3 结束语

电子公文整个传输过程通过计算机和网络实现,由于在电子公文流转系统中使用了电子签名技术,有效实现对用户的访问控制,使用数字签名或者图章签名对文档进行签名签章,如同传统的签字盖章,可以通过对数字签名或者签章证书的查看来确认签名签章的有效性,从根本上保证了传输公文的有效性,真实性和完整性,大大提高了公文传输的效率和公文的利用率,消除了公文传输过程中的安全隐患。电子公文流转系统的实施对我国推广电子政务将起到良好的促进作用。

参考文献:

[1] 关振胜.电子签名的技术实现[R].计算机世界报,2004,33,D10 D11 D12.

(责任编辑:韦廷宗)