

基于密级标志技术的电子公文安全传输支撑平台设计

骆 亮

(广西壮族自治区宏观经济研究院广西壮族自治区经济信息中心, 广西 南宁 530022)

摘 要: 为提高电子公文传输系统的安全性, 保障不同密级的电子公文在传输交换过程的安全, 本文对密级标志关键技术进行研究, 利用加密和内容混淆等技术手段将密级标识与电子公文进行绑定, 设计了基于密级标志的电子公文安全传输支撑平台。平台经过应用和测试, 实现了对电子公文进行“标志、鉴别、管控”的目标, 增强了电子公文传输系统的安全性。

关键词: 密级标志; 电子公文; 安全传输; 信息安全

中图分类号: TP317.1 **文献标识码:** A

Design of Electronic Document Security Transmission Support Platform Based on Classification Label Technology

LUO Liang

(Guangxi Economic Information Center, Guangxi Macroeconomic Research Institute, Nanning 530022, China)

Abstract: In order to improve the security of the electronic document transmission system, to ensure the security of electronic documents of different secret levels in the process of transmission, in this paper, classification label marking technology for electronic documents is studied. An electronic document security transmission system based on classification label technology, encryption and content obfuscation technology is designed in this paper. After application and testing, the platform achieves the goal of "Marking, Identification, Control" of electronic documents, and enhances the security of electronic document transmission system.

Keywords: classification label; electronic document; security transmission; information security

1 引言(Introduction)

电子政务不仅能提高工作效率和政府服务水平, 而且是建立和完善社会主义市场经济、保障社会的公正和公平、增强国家竞争力的重大战略措施之一。在电子政务的实施过程中, 电子公文系统是其重要组成成分。通过电子公文系统可以实现政府机关之间公文的共享、交换、传输和处理, 利于政府机关公文网络化传输, 以及电子化处理的促进, 使公文流转速度得到明显提升, 在提高信息资源利用率的同时有效的提升办公效率, 实现政府机关之间的信息共享, 以及跨平台的电子公文交换^[1]。

一般的电子公文交换系统, 在公文的传输和使用过程中缺少必要的安全防护措施, 无法保障电子公文在生成、使用、流转、分发、存储等过程的保密性、完整性、可用性, 为了使各个机关单位电子公文传输的信息安全问题得到有效解决, 本文基于密级标志技术设计实现了电子公文安全传输系统, 从电子公文定密、密级标志嵌入和公文加密保护方面

解决了电子公文安全管理的难题, 在保证用户操作习惯不变的前提下, 增强常规电子公文传输系统的安全性。

2 电子公文保护技术(Electronic document protection technology)

目前对电子公文进行密级标志和安全保护的相关技术主要有数字水印技术、数字版权保护(DRM)技术、文件透明加密技术三种^[2]。

2.1 数字水印技术

数字水印技术是指用信号处理的方法在数字化的多媒体数据中嵌入隐蔽的标记, 这种标记通常是不可见的, 只有通过专用的检测器或阅读器才能提取。数字水印技术利用数据隐藏原理使密级标志不可见, 可以为电子文件提供一种密级标志的隐藏方法, 从而实现基于密级标志的电子文件安全管理。

2.2 数字版权保护(DRM)技术

数字版权保护技术可以确保信息资源在未授权的情况下不被使用、复制、篡改和传播。利用DRM技术可实现电子公

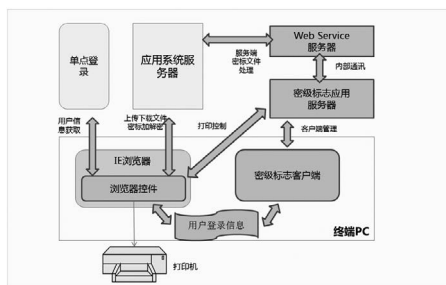


图2 集成示意图

Fig.2 Integration diagram

如图2所示,安全传输支撑平台通过浏览器控件、密级标志客户端、Webservice服务与应用系统(公文传输系统)进行集成,实现对应用系统中的电子公文进行安全保护,对公文定密、浏览、使用、流转、打印等环节进行管控。

4.2 系统应用流程设计

4.2.1 在线加密

对于在线起草和本地起草上传到公文传输系统的公文文件,可在公文传输系统中进行加密,公文传输系统调用公文安全传输支撑平台接口进行加密,加密后的公文文件依照公文传输系统流程进行流转。

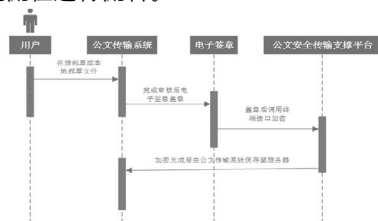


图3 在线加密流程

Fig.3 Process of online encryption

4.2.2 在线预览

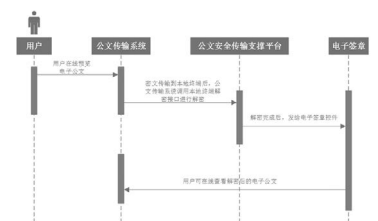


图4 在线预览流程

Fig.4 Process of online preview

4.2.3 解密下载

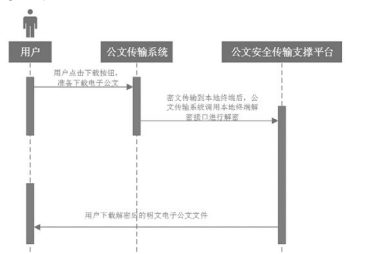


图5 解密下载流程

Fig.5 Process of decryption download

4.3 系统创新点

本系统实现电子公文的密级标志及其全流程安全管控,并在不同格式、不同应用系统间进行电子公文的安全流转和使用,在电子公文的全生命周期中提供身份鉴别、访问控

制、权限管理、安全审计等功能^[6]。主要创新点包括:

(1)采用驱动级透明加解密技术,对电子公文添加密级标志并进行加密保护,采用信息隐藏技术和自主研发的专用混淆算法对电子公文进行内容加扰,保障了文档的安全性和完整性,并能够管理多个缓存区,实现不同进程的读取被导向不同的缓存块,提高与杀毒软件等第三方应用系统的兼容性。

(2)电子公文DPI检测与流转管控。在不同安全域之间或网络出口处,基于网络协议及流量分析,能够及时发现违规的敏感公文外流并进行阻断,杜绝敏感数据非法外流。

(3)创新的文档标志管理模式和文档分级保护策略。对公文起草、标志、使用、流转、外发、归档、销毁等全生命周期的管控,基于密级标志实现分级保护策略。

5 性能测试(Performance testing)

5.1 集群部署

应用服务器、数据库服务器均可采用两台或者多台服务器向客户端提供服务,集群服务与单机系统向客户端提供的服务,从通讯协议上保持二进制兼容。既可配置为同步集群,亦可配置为异步集群。

5.2 系统安全性

系统均架设在经过安全加固的Linux操作系统上,裁剪了与系统功能不相关的软件库,关闭非必要的服务及端口,采用复杂度高的身份认证模式,整个系统的防攻击能力得到大幅增强。系统从代码上识别并过滤了网络攻击指令,能抵御SQL注入、跨站攻击、目录遍历等攻击行为,且系统上线前均经过严格的漏洞扫描和安全补丁升级。

5.3 系统可靠性

两起系统故障间隔的平均时间>100天,系统故障恢复正常的平均时间<10分钟。

6 结论(Conclusion)

本文介绍了电子公文传输的安全需求与密级标志技术,并基于密级标志技术设计实现了电子公文安全传输支撑平台,对平台的技术架构、关键技术、集成接口,以及系统性能进行了阐述与验证,通过对电子公文全生命周期各环节的安全性分析与针对性加固,达到对电子公文进行“标识、鉴别、管控”的最终目标,增强了电子公文传输系统的安全性。

参考文献(References)

- [1] 唐秀忠.基于XML加密技术的电子公文传输系统设计与实现[J].西安文理学院学报(自然科学版),2017,20(5):82-85.
- [2] 汪萌,欧京义.基于密级标志的商业秘密保护技术研究与应用[J].计算机工程与应用,2017,53(S3):50-53.
- [3] 王昕彤.电子公文传输系统设计与实现[D].西安电子科技大学,2017.
- [4] 李梅梅.电子文件密级标志相关技术浅析[J].保密科学技术,2011(5):31-34.
- [5] 吴滨.密级标识技术在分级保护中的应用[J].信息安全与技术,2010(8):76-79.
- [6] 武越,刘向东,石兆军.文件密级标识全程管控系统的设计与实现[J].计算机工程与设计,2013,34(10):3437-3442.

作者简介:

骆亮(1984-),男,硕士,高级工程师.研究领域:信息系统设计开发,数据库,大数据分析挖掘,计算机网络及系统集成。