公文流转系统中PKI技术的研究及应用

沙君新

指导教师 廖明宏教授

厦门大学

学校编码：10384　　分类号_____ 密级 _____
学号：X2010230246　　UDC _____

厦门大学

硕 士 学 位 论 文

公文流转系统中 PKI 技术的研究及应用

Research and Application of PKI Technology in Documents Transmission System

沙君新

指导教师姓名：廖 明 宏 教 授

专 业 名 称：软 件 工 程

论文提交日期：2012 年 4 月

论文答辩日期：2012 年 5 月

学位授予日期：2012 年 6 月

答辩委员会主席：

评 阅 人：

2012 年 4 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（ √ ）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

公文流转系统是电子政务建设中的核心和基础系统，它的开发与应用已经成为各级政府机关政务信息化的主要内容。由于政务办公的特殊性，公文流转过程中的安全问题一直受到广泛的关注。公开密钥基础设施(Public Key Infrastructure, PKI)是迄今为止解决信息安全问题诸多方法中最全面的一种解决方案。PKI 技术采用证书管理公钥，通过第三方的可信任机构—认证中心 CA(Certificate Authority)把用户的公钥和用户的其他标识信息(如名称、E-mail,身份证号等)捆绑在一起。通过 CA 机构，较好的解决了密钥分发和管理问题，并通过数字证书，对传输的数据进行加密和鉴别，保证了信息传输的机密性、真实性、完整性和不可否认性。

本文分析对比了目前国内公文流转系统的普遍采用的体系结构和开发方式，分析了政府办公业务的实际业务流程及其特点，以公文流转过程中的安全保障为中心，提出了一个 PKI 实现模型，特别是对于其中的证书管理功能、访问控制功能、身份认证服务等方面做了认真的设计和细致的考虑。在此基础上，设计了一个集成在公文流转系统中的电子签章系统。这个系统采用基于组件的软件设计方式，实现了公文流转过程中对用户的身份认证、信息的完整性与不可否认性等方面的需求。

关键词： 公文流转；PKI；证书；电子签章

Abstract

Documents Transmission System(DTS) is core and basic system in E-Gov Systems. Its development and application has been the main subject in governments' information building. Because of the special characteristics, the security protection in the process of DTS has been focused on greatly.

Public Key Infrastructure (PKI) is the most comprehensive technology in the information secure field. PKI technology adopt certificate manage public key; through the third party organization which can be believed--CA(Certificate Authority) bundle users' public key and users' other identification information (such as name, E-mail, ID card number etc).Through CA organization, the problem of the key distribute and key management have been better solved, With the digital certificate, realizing encryption and authentication to the data transmission, guarantying the confidentiality, authentication, integrity and non-repudiation of the information transmission.

This article compares with the different normal system structures and develop ways，analyses government business process and its characteristics, discusses deeply about the security in DTS as center. In this paper, a PKI model is presented. The presentation of PKI model and the consideration of certificate manager, authentication and access control about it. Further, a Electronic Seal System integrated in DTS is implemented based on PKI. This system uses ways of module based, implements certification, information integrality and undeniable in DTS.

Key Words: Documents Transmission; Public Key Infrastructure; Certificate；Electronic Seal

目 录

Contents

第一章 引言

1.1 公文流转系统概述

电子政务办公自动化系统的建设是我国实现“信息化带动工业化”的重要表现之一，而公文流转是其核心内容，其建设是转变政府职能、推动经济、促进信息产业发展的需要，系统建设从整合政务资源的需求出发，重在提高政务效率，政务公开，充分利用计算机和现代化通讯手段面向机关服务，建立政府内部信息交流的快速通道，共享信息资源，强化部门业务管理，加强各业务部门之间的交流，实现政务信息的快速上传下达，促进协同办公，提高办公效率，为各级领导及业务人员提供辅助办公和决策服务[1]。

公文流转系统相对于传统的纸质办公具有很多的优点，如：节省纸张，加快公文流转速度等等。公文流转系统是真正意义上的现代办公自动化系统，以往对于办公自动化的应用只是独立、分离的运用类似 Office 的办公软件，而公文流转系统则是网络技术、通讯技术、数据库技术等综合的应用，使得一个公文从签收到发文均可以实现无纸化流转。

公文流转系统有其自身的特点，与金融等领域的信息系统相比有所不同。虽然公文流转系统也是以数据库为核心，但是它更需要在用户之间的协作，流程的控制这些方面提供辅助手段。一个公文流转的过程就是一个决策的过程，这个决策涉及到不同职务级别人员之间的协作[2]。针对政府机关的公文流转，各级政府办公厅还有明确的规章制度规范具体的流程。因此，公文流转系统中要完成一项工作的无纸化，必须明确这项工作的全部步骤。由于各级政府的办公流程有不同的特点，企业间的办公也千差万别，并且办公流程随着时代在改变，因此公文流转系统不是只有一个流转模式，公文流转系统在设计上与应用领域是紧密结合的。

1.2 论文的研究背景

1.2.1 问题的提出

公文流转系统在政府办公领域的广泛应用给政府办公带来极大方便的同时，也带来了安全方面的问题。公文流转系统的安全和保密问题直接关系到城市和国家的利益，信息安全问题也是电子政务建设中面临的一个不可回避的紧迫、重要的问题[3]。

公文流转系统是一种特殊的管理系统，特殊性表现在以下几个方面：

1、公文流转系统处理的是公文，涉及的往往是一些非结构化的数据，它们没有严格的长度规定，结构松散，类型多变，所以在数据处理方式上与其他系统有很大不同。在办公流程中，对不同的文档和不同的事务都有不同的处理流程，即使是相同的文档和相同的事务针对不同的办公人员可能有不同的处理流程。

2、公文流转系统中大部分事务必须要有人的参与。如：很多事务要领导批示、确认、决策。所以办公自动化只是有限意义上的自动化，不像有些系统可以完全确定执行逻辑。公文流转系统不能脱离人的干预。

3、公文流转系统是一个综合性的管理系统，一项工作往往涉及多个部门，需要多个办工人员协作才能完成。所以，协同工作在办公流转系统中表现的尤为突出。

4、公文流转系统中的可操作级别不同。公文流转中必定要流经许多的办公人员或者部门。在这个过程中，每个经手的人员或者部门的权限应该是有所不同。同一篇公文中，针对某一个内容，可能部门 A 可以浏览，而对部门 B 却是不可见的。所以在流转过程针对不同层次、级别的办公人员而言，公文的可操作程度不同，即使同一篇公文对同一层次的不同人员或者部门之间的可操作程度也可能不同。