学校编码：10384　　分类号_____ 密级 _____

学号：X2010230424　　UDC _____

厦门大学

工 程 硕 士 学 位 论 文

政府电子印章系统的设计与实现

Design and Implementation of Government Electronic Seal System

刘 笛

指导教师姓名：姚俊峰　　教授

专 业 名 称：软 件 工 程

论文提交日期：2013 年 4 月

论文答辩日期：2013 年 5 月

学位授予日期：2013 年　　月

指 导 教 师：_____

答辩委员会主席：_____

2013 年 **3** 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

目前，国内很多地方的各级政府部门正在相继开展电子政务建设，通过网络平台，逐步开展如电子化行政审批、公文交换等一系列应用。在这一过程中，对电子文件的安全性要求越来越高。因此建立电子印章平台来解决电子文件、电子签名、身份认证的安全、合法性问题成为进一步发展推动上述应用的基础。

电子印章是物理印章授信体系电子化、网络化的展现，是网络中的身份确认与授权的手段，它将现代科学技术和人们的传统习惯结合在一起，是传统印章发展到信息社会后的一个新的阶段。电子印章也是电子签名技术的一项应用，它把难以理解的电子签名技术变成了人们习以为常的签名盖章方式，更加符合人们的传统使用习惯与公信、诚信体系，因而极大地消除了电子签名的应用障碍，对电子签名的应用推广具有巨大的价值。

本文介绍了基于 PKI 等技术的电子印章系统的设计与实现，电子印章系统主要由三部分组成：服务器端平台、客户端、电子政务信息系统的结合。服务器端平台作为系统的重要组成部分，进行了详细介绍，并对系统中的关键技术进行了分析，综合利用 PKI 技术、数字水印技术、USB-KEY 技术等实现物理印章的网络化及电子化；客户端的软件开发，主要实现了在多种数据格式中的签章应用；最后以某电子政务信息系统为例，设计电子印章系统的二次功能开发，使之符合政务信息系统的业务应用需求。

关键词：电子政务；电子印章；PKI

Abstract

At present, all domestic government departments are developing E-Government Construction One after another in china. Based on network platform, Many government affair application system such as electrical Administrative examination and approval system、Document exchange system were used. The Requirement about the safety of Electronic document is more serious in the process. So, if we want to promote above application system further more, firstly, we need to build electronic seal system to solve the problem such as the question of safety and Legitimacy.

Electronic signature or Electronic seal is the Electronic and network display of Physical seal Credit system, also the Methods of Identity confirmation and grant authorization on network, it combinate modern science technology and traditional customs, and also is a new phase for physical seal in information society. Electronic signature or Electronic seal is an application for Electronic signature technology, it has been changed from the Obscure Electronic signature technology to the mode which people are accustomed to. Certainly, it Conform to our Use custom and Credit system more than before, and eliminate the Application obstacle obviously. So it has great value for Electronic signature application Extension.

The paper introduces Design and Implementation of Electronic seal system based on PKI technology. Electronic seal system can be divided into 3 parts: Server 、Client、Combination with E-Government application system. Server is the main part of the whole system which is been introduced in detail. then try to Analysis Key technology of Electronic seal system, change physical seal into network by using PKI 、Digital watermarking、usb-key technology ; Client Software development is due to realize to sign in many data formats; finally, take one e-government application for an example , design the Two times the development of Electronic seal system function, then conform to the requirement of E-Government business system.

Key words: E-Government; Electronic Seal; PKI

目 录

Contents

第一章 绪论

1.1 研究背景及意义

随着国民经济和社会信息化的日益推进，网络与信息系统的基础性、全局性地位进一步增强，国民经济和社会发展规律对网络和信息系统的依赖性越来越紧密。这些信息系统的安全运行直接关系到国家安全和人民利益，更关系到社会的稳定。而进入 21 世纪，电子政务的建设已经成为今后一个时期我国信息化工作的重点。目前电子政务建设已被列入到国家“十二五”信息化发展规划当中，中央及各地政府部门也都高度重视。国务院关于“十二五”国家政务信息化工程建设规划的批复（国函[2012]36 号）的文件中指出：到“十二五”期末，初步建成共享开放的国家基础信息资源体系，支撑面向国计民生的决策管理和公共服务，显著提高政务信息的公开程度；基本建成国家网络与信息安全基础设施，网络与信息安全保障作用明显增强；基本建成覆盖经济社会发展主要领域的重要政务信息系统，治国理政能力和依法行政水平得到进一步提升。”

当前，我国各级政府部门都在积极开展电子政务建设。一大批重要的政务信息系统诸如行政审批系统、政府电子公文交换系统、财政预算管理系统、政府采购系统等等都相继上线运行。而这些信息系统都面临着一个巨大的风险和威胁就是缺乏合法有效的电子签名体系。例如，在网络中传输的一份电子公文怎样才能保证其具有和纸质文件同样的法律效力？怎样才能保障其在应用过程中的安全保密、不可篡改和不可抵赖？如果上述要求无法达到，那么任何电子政务信息系统的应用都将无法开展。

因此，需要建立一套合法有效的电子签名系统，利用科技手段，充分保障政府电子政务信息系统的应用安全。而“电子印章”是中国化的一种电子签名形态，它是解决电子政务、甚至电子商务应用中“身份认证”、“合法签名、”“认可交易”等要求的一个必要手段。

1.2 论文研究目标

在符合《中华人民共和国电子签名法》和国家密码管理局、国家公安部、国家保密局等部门颁布的各项关于信息安全国家标准的前提下，研究设计政府电子

印章系统，使之具有造印、发印、印章管理和用印电子化等功能，并且具备为政府部门的政务信息系统提供盖章、签字、身份确认、原件检验、加密和解密等功能。政府部门通过对电子印章系统的使用，不仅在网络中拓展了物理印章的使用，完善了政务信息系统的架构，更能大大加强政务信息系统本身的身份安全、数据安全与应用安全。

1.3 论文研究内容

1．电子印章的实现

综合利用 PKI 技术、数字水印技术、USB-KEY 技术等实现物理印章的网络化及电子化。并将电子印章数据封装于 USB-KEY 设备中。

2．电子印章服务器端平台设计

服务器端平台采用多层架构设计，采用大型关系数据库，包括由数据库存储、中间应用层、Web 服务层构成。实现电子印章的制作和发放、印章数据的存储和管理、单位、用户、日志的管理。

3．电子印章客户端功能设计

客户端软件设计实现在多种数据格式中的签章应用，例如 Microsoft Word、Excel、Web 页面等。同时实现电子印章盖章后的验证及盖章后文档数据的加、解密等功能。

4．电子政务信息系统结合设计

以某电子政务信息系统为例，设计电子印章系统的二次功能开发，使之符合政务信息系统的业务应用需求。

1.4 论文组织结构

本文共分为六章。

第一章，对当前电子政务应用中存在的安全风险和问题进行分析，阐明课题的研究意义与主要研究内容。

第二章，介绍在研究政府电子印章系统中应用到的基本概念及关键技术。

第三章，详细分析政府电子印章系统的需求与总体设计。

第四章，详细描述政府电子印章系统的设计和实现过程。

第五章， 对政府电子印章系统的展示与测试.

第六章，总结和展望，对项目的主要工作和论文的主要内容进行总结，并对政府电子印章系统的进一步研究进行展望。

第二章 基本概念与相关技术介绍

2.1 电子印章概述

电子印章是物理印章体系的电子化和网络化，是网络中的身份确认与授权的手段，它将现代科学技术和人们的传统习惯结合在一起，是传统印章发展到信息社会后的一个新的阶段[1]。

电子印章通过使用硬软件技术，以电子化的方式模拟物理印章的使用，使用户在电子政务、电子商务等活动中拥有一种符合传统用章习惯的应用体验；同时电子印章又采用了先进的加密，签名，信息隐藏等安全技术，从而具有物理印章不可比拟的安全性和可追溯性。

电子印章也是数字签名技术的一项应用，它把难以理解的电子签名技术变成了人们习以为常的签名盖章方式，更符合人们的传统信用习惯与公信、诚信体系，因而极大地消除了电子签名的应用障碍，对电子签名的应用推广具有非常巨大的价值[2]。

在很多国家，电子签名已具有法律效力。《中华人民共和国电子签名法》第十三条规定同时满足下列四个条件的电子签名就视为可靠的电子签名，同时规定了可靠的电子签名与手写签名或者盖章具有同等的法律效力[3]。

（一）电子签名制作数据用于电子签名时，属于电子签名人专有；

（二）签署时电子签名制作数据仅由电子签名人控制；

（三）签署后对电子签名的任何改动能够被发现；

（四）签署后对数据电文内容和形式的任何改动能够被发现。

电子签名法所指出的“电子签名”实质“大于并包括”我们所说的电子印章，“签名”代表了双层意义：一层为名词概念，“签名”含括通常我们所指的公章、私章、签字、签名等各类代表单位、个人在政务、商务活动中权威、信用、权责的确认。二层为动词概念，其代表了单位、个人在政务、商务活动中“签字、签章”的过程、动作的不可否认、可追溯效力。同时，在国际惯例、国际贸易中，Sign 中文译为签名，即等同我们中国所说的签字、签章、签名，为顺应 WTO，并与国际接轨草案之初的“电子签章法”最后定名为“电子签名法”以综合考虑各种情况，适应用国情发展之需要。