学校编码：10384　　分类号_____ 密级 _____

学号： X2010230682　　UDC _____

厦门大学

工 程 硕 士 学 位 论 文

基于 PKI 和 SSL 安全技术的地税网上报税系统的设计与实现

Design and Implementation of Local Taxation Online System Based on PKI and SSL

安志杰

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： 2012 年 10 月

论文答辩日期： 2012 年 11 月

学位授予日期： 2012 年 月

答辩委员会主席：_____

评 阅 人：_____

2012 年 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)：

2012 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）：

2012 年　月　日

摘 要

公钥基础设施（PKI）技术是目前使用最广泛的网络安全技术，是通过使用公开密钥技术和数字证书来确保系统信息安全并负责验证数字证书持有者身份的一种体系。PKI 被广泛的应用于政府部门、商业企业、企业与企业之间、区域性服务网络、电子商务网站等领域。近几年，基于 PKI 的电子政务系统得到了迅速的发展。PKI 是电子政务信息安全建设中极其关键的基础性设施，它在底层网络基础设施上构建了一个一致的信息安全服务层面，可以满足上层各种应用在安全方面的需求。Secure Sockets Layer(SSL)协议是目前 Internet 上使用最广泛的安全协议，SSL 使用加密技术、数字签名和数字证书，在客户端和服务器之间提供消息隐私、消息完整性和相互验证。

本文介绍了 PKI 的发展现状，通过对 PKI 和 SSL 的相关理论和技术的研究以及对地税网络现状的分析，提出了有效的地税网上报税安全问题的解决方案。本论文正是利用 PKI 相关技术，对整个地税的网上申报系统进行数字证书应用设计，通过电子数据的加密和第三方监控，保证电子数据传递的保密性、完整性和不可抵赖性，解决电子数据的有关法律争议，设计和实现了一个基于 PKI 技术和 SSL 协议的地税网上报税系统。利用 PKI 解决了网上报税系统中的身份认证、数据完整性、数据机密性、数据不可抵赖性的问题，进而保障了税务网上报税系统中的数据安全。实现纳税人通过互联网即可足不出户地进行纳税申报，方便纳税人，提高报税效率，提高税务机关对电子数据信息的可利用性，为日常税源管理提供必要的数据支撑。

关键词：信息安全；公钥基础设施(PKI)；安全套接字层（SSL）协议；数字证书

Abstract

Public Key Infrastructure (PKI) is the most widely used network security technology nowadays and is a system that insures the security of system information and is responsibility for validating the station of the holders who hold the digital certificate. The PKI is widely used in government departments, commercial enterprises, Business-to-Business, local area service networks and e-commerce websites and other areas. In recent years, the electronic government affairs system based on the PKI has obtained the rapid development. PKI is a crucial public facility in the security construction of Electronic Government Affairs, which builds an accordant information security service on basic network infrastructure and meets the needs from upper ranges in terms of information security. Secure Sockets Layer (SSL) is the most widely used security protocol; SSL uses encryption techniques, digital signatures and digital certificates to provide message privacy, message integrity and mutual authentication between clients and servers.

This paper introduces the development situation of PKI, It gate through to research of PKI and SSL technical theory and analyses of local taxation network, effective solutions are put forward to solve the safety problems of local taxation online. This paper is to discuss the redesign of digital certificates of local taxation online declaration system, using PKI technologies mentioned above. Through the data encryption and third-party electronic monitoring, the confidentiality, integrity and non-repudiation of electronic data transmission can be guaranteed, and legal disputes can be prevented. Designed and accomplished a Local Taxation Online System Based on PKI technology and SSL protocol. The PKI technology to provide effective information security services, and resolved the identity authentication、information integrity、information confidentiality、information non-repudiation, and protect the online tax declaration system for data security. They can file the tax returns online through this more convenient and efficient new system. Meanwhile, the availability of electronic data from the tax authorities will be enhanced in order to support the daily management of revenue sources.

Key words: Information Security; Public Key Infrastructure(PKI); Secure Sockets Layer(SSL)；Digital Certificate

目 录

Contents

第一章 绪论

1.1 研究目的及意义

随着Internet为代表的全球性信息化浪潮迅猛发展，信息网络技术的应用日益普及和广泛,各种基于网络信息系统的应用服务蓬勃兴起，给人们的工作和生活带来了各种便利，同时也带来了新的挑战，Internet所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求。从而使网络安全也日益成为影响网络效能的重要问题，如何使网络信息系统不受黑客和工业间谍的入侵，已成为政府机构、企事业单位信息化健康发展所必需考虑和解决的重要问题。当前，网络信息安全所面临的最大的问题就是如何保障开放式网络环境中各实体建立相互之间的信任关系，以及如何保证网络上数据的机密性、完整性、可用性、可控性及不可否认性已经成为网络通信安全领域的主要问题。公钥基础设施(PKI)技术被认为是解决以上网络信息安全问题的重要技术，并在电子商务、电子政务以及安全电子邮件等众多安全领域得到了广泛的应用。以PKI技术为基础的数字签名技术能够确保数据的完整性和可靠性，又能保证信息具有不可抵赖性。随着电子签名法的实施，数字签名和手写签名效力达到了等同的地位。从法律角度，电子签名法捍卫了每个人通过数字签名保障自己的切身利益。从行业来看，电子商务、电子政务、远程教育等方面都离不开PKI技术。随着PKI技术的应用与发展，无论是在有线网络，还在无线世界，PKI必将发挥巨大作用。因此，学习和掌握PKI成为了现代网络维护人员和信息系统开发人员的迫切需求。

1.2 国内外发展现状

1.2.1 国外发展现状

美国、欧洲各国以及韩国、日本是世界上较早涉足信息安全技术及产业的国家，他们大多数对 PKI 及其相关技术、产业以法律的方式固定下来。美国是最早提出PKI概念的国家，1994年10月，美国国家标准和技术研究所（NIST）成立了 PKI 工作小组，进行 PKI 的相关研究，并于 1996 年成立了美国联邦 PKI

筹委会[1]。与 PKI 相关的绝大部分标准都由美国制定，其 PKI 技术在世界上处于领先地位。2000年 6 月 30 日，美国总统克林顿正式签署了美国的《全球及全国商业电子签名法》，这是美国历史上第一部联邦级的电子签名法[2]。这一法律的签署，给予电子签名、数字证书以法律上的保护，使电了认证问题迅速成为各国政府关注的热点。加拿大在 1993 就已经开始了政府 PKI 体系雏形的研究工作，到2000年已在PKI体系方面获得重要的进展，已建成的政府 PKI 体系为联邦政府与公众机构、商业机构等进行电子数据交换时提供信息安全的保障，推动了政府内部管理电子化的进程。加拿大与美国代表了发达国家 PKI发展的主流。

欧洲在 PKI 基础设施方面也成绩显著。为了解决各国 PKI 之间的协同工作问题，它采取了一个系统策略：如积极资助相关研究所、大学和企业研究 PKI 相关技术；资助PKI 互操作性相关技术研究，并建立 CA 网络及其顶级 CA。

在亚洲，韩国是最早开发 PKI 体系的国家。韩国的认证架构主要分三个等级：最上一层是信息通讯部，中间是由信息通讯部设立的国家 CA 中心，最下一级是由信息通讯部指定的下级授权认证机构(LCA)。韩国于 1998 年正式通过数字签名法，并且于 1999年 7 月正式实施。日本的 PKI 应用体系按公众和私人两大类领域来划分，而且在公众领域的市场还要进一步细分，主要分为商业、政府以及公众管理内务、电信、邮政三大块。由于亚洲各国的 PKI 发展步伐并不一致，为了缩小亚洲各国在技术及制度上的差异，推动 PKI 技术在亚洲的标准化和法制化建设，在 2000 年由日本、韩国、印尼等国家发起设立了“亚洲 PKI 论坛”[3]。

目前国外开发 PKI 产品的公司很多，比较有影响力的国外 PKI 公司有 Baltimore 和Entrust，它们都各自推出了可以应用的产品。Entrust 公司的 Entrust/PKI 5.0 可以提供多种功能，能够较好的满足商业企业的实际需求[4]。

1.2.2 国内发展现状

我国的 PKI 技术从 1998 年开始起步，由于政府和各有关部门近年来对 PKI 产业的发展给予了高度重视，2001 年 PKI 技术被列为“十五”863 计划信息安全主题重大项目，并于同年 10 月成立了国家 863 计划信息安全基础设施研究中心[5]。国家计委也在制定新的计划来支持 PKI 产业的发展，在国家电子政务工

程中明确提出了要构建 PKI 体系。2004 年 8 月 28 日，十届全国人大常委会第十一次会议表决通过了《电子签名法》，规定电子签名与手写签名或是盖章具有同等法律效力，并从 2005 年 4 月 1 日起颁布实施。这部法律的诞生将机打的推动我国的 PKI 建设[6]。国家密码管理局也已经完成了《证书认证系统密码及其相关安全技术规范》。这些举措对国内的信息安全领域起到很大的推动作用，也促进相关研究开发人员进一步研究 PKI/CA 的构建及其应用。自从 1998 年国内第一家以实体形式运营的上海 CA 中心(SHECA)成立以来，PKI 技术在我国的商业银行、政府采购以及网上购物中得到广泛应用。但是，总体来说，我国的 PKI 体系总体发展水平不高，应用不够广泛，还没有形成集管理、法规、标准、技术、应用为一体的完善的 PKI 体系，面临许多困难[7]。

我国作为一个网络发展大国，发展自己的 PKI 技术是非常必要的。研究和开发自己的实用 PKI 技术已经刻不容缓[8,9]。目前，我国以 PKI 为基础的网络身份信任体制建设尚处于起步规划阶段。目前国内比较著名的 PKI 开发厂商有东大阿尔派，华翔腾数码，天威诚信，以及吉大正元等。它们都有相应的产品投入市场，但一般还仅仅处于示范工程阶段。因为随着许多新技术的不断的涌现，CA 之间的信任模式，使用的加/解密算法，密钥管理方法还需要不断的变换，所以 PKI 在国内市场还没有真正的推广开来。这除了技术和法规方面的原因，也有安全意识相对滞后于技术发展方面的原因。因此，一方面要大力普及信息安全知识，增强人们的信息安全观念，了解最新信息安全的发展动态；另一方面也要投入巨大的人力和物力，进行自主研究和开发完整的 PKI 系统，以支持政府、学校和企业安全地使用信息资源和国家信息基础设施已经刻不容缓，这对于我国电子商务、电子政务、电子事务的发展将是非常关键和重要的。 由于 PKI 是重大国家利益和网络经济的发展的制高点，也是推动互联网发展、保障事务处理安全、推动电子政务、电子商务的支撑点。因此，建立健全的国家 PKI 体系，将有力地促进我国电子政务以及整个国家信息化的发展。这样，政府和企业都十分重视 PKI 建设，PKI 应用有着巨大的发展前景。

1.3 论文研究内容

本次课题针对甘肃地税网上报税系统，结合 PKI 和 SSL 以及网络安全方面的

各项技术，在以甘肃地税系统网络结构和 SSL 加速器为核心的硬件进行设计与实现工作，主要研究内容为：

1．对如何实现以 PKI 为基础的数字签名技术的应用进行了研究与分析；

2．对系统硬件、网络、业务流程、安全策略等方面进行方案设计；

3．对系统的安全技术进行了软件与硬件进行详细方案设计，实现基于 PKI 和 SSL 的网上报税系统安全技术的设计与实现。

本次课题研究的目的是设计和实现基于 PKI 和 SSL 安全技术的网上报税系统。其中包括软件设计、硬件环境设计、网络环境设计、安全策略设计、业务流程设计、数字证书等一系列的设计，重点和难点主要在数字证书的设计和电子签名的实现上。设计完成后的系统，不仅满足了纳税人通过互联网作税务申报的需求，而且在纳税人和税务机关之间构建起了一道安全屏障，为解决纳税人与税务机关出现的纳税申报纠纷提供了可靠的依据。

1.4 论文组织结构

论文共分为七章，具体内容结构如下：

第一章 绪论，介绍基于 PKI 和 SSL 的网上报税系统安全设计的研究目的及意义、国内外发展现状及研究内容；

第二章 基本概念及相关技术的介绍分析，本章节主要围绕公钥基础设施 PKI 和安全套接字层协议（SSL），介绍和分析了系统开发中安全技术的基本概念及相关技术。

第三章 ，主要介绍系统的需求分析，分别分析了系统的业务流程、系统的安全需求，系统的功能性需求、非功能性需求和可行性。

第四章 系统的总体设计，主要介绍了系统的项目背景、设计思路、原则和依据，并对系统的总体框架、系统部署环境、网络环境、系统安全方面进行了总体设计。

第五章 系统的详细设计与实现，主要介绍了系统数字证书、电子签名的设计以及系统各个模块的具体设计和实现过程。

第六章 系统测试，主要通过软件测试工具和人工测试，对系统的响应速度、系统模块、数据等方面进行了测试。