学校编码：10384　　分类号＿＿＿密级＿＿＿
学号：X2010230675　　UDC＿＿＿

厦门大学

工 程 硕 士 学 位 论 文

基于 PKI 的普通发票管理系统安全方案分析与设计

The Analysis and Design of System's Security Scheme for Ordinary Invoice Management Based on PKI

杨睿智

指导教师姓名：　董槐林　教授

专　业　名　称：　软　件　工　程

论文提交日期：　2012 年 10 月

论文答辩时间：　2012 年 11 月

学位授予日期：　2012 年 11 月

答辩委员会主席：＿＿＿＿＿＿

评　　阅　　人：＿＿＿＿＿＿

2012 年 10 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

随着网络和信息技术的普遍应用与快速发展，我国税务系统信息化建设水平得到显著提高，各种基于网络的应用系统应运而生，大大降低征纳双方的成本，如何提高税收各应用系统的安全性是一个不容忽视的大问题。

本文研究目标是是探讨 PKI 技术如何在普通发票管理系统中的应用，该课题研究将为做好项目建设，提供相关的技术方案。

本文基于互联网的应用系统，主要实现了在线下载发票领购信息、在线开具通用机打发票、开票信息实时上传、在线获取发票结存信息等功能。系统的成功上线后，方便了纳税人也减轻了税务人员的工作量，同时还强化了税源监控力度，解决了申报不符的问题。

本文介绍国内外税务信息安全现状，研究 PKI 的相关理论，探讨 PKI 系统的原理和机制，分析如何使用 PKI 技术提高系统的安全性。论文探索将成熟的加密算法与 PKI 技术相结合，应用于普通发票管理系统，设计实现一个具有安全性较高的应用系统。

目前，很多省市都有各自的普通发票管理系统，所用的框架或技术有所不同，但引入 PKI 技术，对于提高系统的安全性有其积极意义。

关键词：PKI；信息安全；发票

ABSTRACT

As the universal application and rapid development of network and information technology, the information level of taxation system has been improved significantly. How to improve the security of the application systems of taxation?

The dissertation objective of this dissertation is to probe into the application of PKI technology in ordinary invoice management system, and provide relevant technology scheme.

This dissertation is an application system based on the internet, which has mainly realized the functions including downloading the receiving and purchasing information of invoice on line, issuing printed general invoice on line, real-time uploading of invoice information, and obtaining invoice balance information and so on. This system has been launched on line successfully, which has provided convenience to the tax-payers and also reduced the work amount of the taxation staffs, meanwhile, the supervision of tax source control has been enhanced and the problem of unconformity of declaration has been solved.

The dissertation introduces the taxation information security status both at home and abroad, relevant theoretical concepts of PKI, Discussion of the principle and mechanism of PKI system. It analyzes how to improve the system security with application of PKI technology. The dissertation explores combined the mature cryptographic algorithm with PKI technology, apply to ordinary invoice management system for design and realization of an application system possessing comparative high security.

Currently, many provinces and cities have their own ordinary invoice management system, the applied frameworks and technology of which are differentiated, but the adoption of PKI technology to improve the security of the system has its positive significance.

Key Words: PKI; Information Security; Invoice

目 录

Contents

第 1 章 绪论

1.1 选题背景

随着电子政务和互联网技术的不断发展和普及，为税收管理现代化提供了良好的契机。目前我国很多地区已经开展通过互联网进行网上领购普通发票、网上开具普通发票的处理，给纳税人提供了新的发票管理模式，普通发票管理系统已经成为国家税收管理的重要途径。但是由于各地区税收信息化建设初期的非一体化布局， 导致信息不对称、安全性能差和使用效率不高的现状。税务系统的安全策略也仅限于简单的访问控制与授权机制，无法确保纳税人身份的真实性、行为的不可抵赖性以及报税信息的完整性和可靠性。所有这些方面的问题对税务机关未来的信息化建设提出了严峻的挑战，引入 PKI 技术，对于提高系统的安全性有其积极意义[1]。

网络涉税事项的法律地位已被确认，《电子签名法》已于 2005 年 4 月 1 日正式实施，其核心是确立了数据电文的法律地位。它的贯彻与实施将极大地改善信息化建设的法制环境， 是政府和社会各界信息化建设和信息应用与服务的重要法律准则[2]。《电子签名法》的基础是安全认证。通过第三方权威认证机构签署的安全数字证书和电子签名技术，实现人们网络交往中的身份认证、数据电文的安全加密和完整性认证、行为的法律不可抵赖性认证的过程。在税务系统中应用安全认证技术，税务信息以电子形式保障了信息传输的安全性及纳税人身份的合法性，使纳税人提供的涉税信息遵循法律规范，对各项纳税服务功能的拓展和内部数据的交互提供了安全保障。

1.2 国外税务信息安全发展情况

20 世纪中期，信息技术的发展引发了一场新的全球性产业革命[3]。税务信息化是信息化技术发展到一定阶段的产物，它是信息化的一个重要组成部分。20 世纪五十年代末，美国国内收入局开始利用计算机系统进行税务工作的管理。随后，英国、日本等发达国家也于六十年代先后开始发展本国的税务计算机系统。自此，

税务信息化建设开始了在全世界许多国家的普及。

（一）美国的税务信息化及信息安全

美国从 1960 年开始，逐步在全国范围内建立了计算机征管网络[2]。税收预测、税务登记、纳税申报、税款征收、税务稽查、税源监控、纳税情况收集等方面的工作，都广泛使用了计算机。美国国内收入局通过 2 个全国性和 10 个地区性的数据中心，以及遍布全国的计算机网络，完成了美国联邦税收中约 82%的收入征收。1997 年联邦政府预算拨付 3.36 亿美元，用于税务局的技术更新，其中建造计算机信息系统就花费了 2.06 亿美元。现在，美国已利用互联网在税务机关与纳税人及其他个人和组织之间构建起了快捷的税收信息通道。纳税人通过国内收入局网站，既可以咨询到有关税收的各方面情况，还可以在网上处理纳税事宜，每年有几千万纳税人使用电子信息系统来报税。在信息安全管理上，美国注重健全信息安全管理体制和法规，不仅设立了直属总统的关键基础设施保护委员会和负责协调全国安全、基础设施防护及反恐怖行动的国家基础设施保障委员会，而且成立了信息安全测评认证机构。

（二）英国的税务信息化

英国国内收入局信息系统主要处理的税种为个人所得税。在 20 世纪八十年代末就建立了集中式的信息系统[3]。到九十年代中期，随着网络系统的发展，开始建立了电子申报纳税系统。也就是个人自 1996～1997 年，公司自 1999 年 7 月开始，实行自行计征，即由纳税人自己计算应纳税额后，再由税务局开始使用地方数据采集系统自行计征数据。后来又使用了“事后检查程序”，根据纳税人申报的情况，选定申报纳税异常的纳税人作为重点稽查对象，进行纳税申报检查。

1.3 我国税务信息安全现状

税务信息化是指以培养和发展以计算机技术、网络技术和管理科学等现代信息技术为代表的新生力量，以税务信息专门技术研发和专门人才培养为支撑，使税务活动由传统的手工向网络化转变，从而实现税务征收管理自动化处理。其核心业务系统主要涉及税收、稽核、检查、管理、实施等方面，是税收征管业务的主体。同时还与工商、审计、银行等单位相连。

信息安全是为了保证用户身份的安全认证、网络资料和数据的保密性、完整

性和不可否认性。税务机关作为政府的一个特殊职能部门，其网络上所运行的信息，直接关系国家安全和政府工作。近年来，随着我国税务部门逐步实现网上电子报税及纳税，公司信息和税务数据在网络上积累日益丰富，税务信息的安全风险度也在不断增加。比如，计算机病毒、计算机黑客、有害信息的入侵、网上信息的知识产权侵权行为。纳税人所提交纳税申报涉及的资金、税种和额度在网络传输过程中出现数据被截留、篡改。非授权用户登录系统，访问未授权信息，或者假冒身份申报错误信息。这些行为，都会给企业造成巨大的损失，严重影响纳税工作，甚至影响政府权威形象。为了维护纳税人和税务部门的利益，应积极采取安全技术防范措施来加强网络和信息安全，在纳税人和税务部门之间构建可靠的网络信任机制和信息安全屏障。这就要求政府要加强技术防范措施，在税务系统应用公钥匙基础设施[4]（Public Key Infrastructure ,PKI）体系，进行数据加密、保证数据完整机制及信息设计，病毒防范技术和认证中心（Certificate Authority，CA）安全身份认证等技术。保障税务部门的网络及重要信息的安全。

1.4 论文的研究内容与组织结构

本文将主要集中在国内外税务信息安全现状、PKI 的相关理论概念，研究和掌握 PKI 系统的原理和机制，分析了如何使用 PKI 技术提高系统的安全性，普通发票管理系统将当下成熟的加密算法同 PKI 技术相结合，设计实现一个具有安全性较高的应用系统，并介绍其中的关键技术。目前，很多省市都有自己普通发票管理系统，所用的框架或所用的计算机语言千差万别，但笔者认为如何提高系统的安全性至关重要，引入 PKI 技术是一种不错的选择。

本文共分五章：第一章绪论，介绍了国内外税务信息安全现状及选题背景和研究内容、组织结构。第二章 PKI 网络安全认证技术概论，本章研究 PKI 的理论、功能、和相关协议标准。第三章普通发票管理系统安全需求，本章简要介绍普通发票管理系统，对系统做提出了安全性需求分析，第四章普通发票管理系统的安全实现，本章针对第三章提出的安全需求，详细阐述了为各个安全需求所采用的技术手段，第五章总结及展望，本章对全文进行总结和对下一步研究提出了方向。

第 2 章 PKI 网络安全认证技术概述

全球经济发展正在进入信息经济时代，知识经济初见端倪，作为 21 世纪的主要经济增长方式——电子商务，将给世界经济带来巨大的变革，产生深远的影响，通过电子商务可大幅度降低交易成本，增加贸易机会，简化贸易流程，提高贸易效率；电子商务还能提高生产力，改善物流系统，并推动企业和国民经济结构的改革，对电子商务的关注和投入可以发展新兴产业，创造就业机会，推动国家和全球经济的发展。电子商务是一个新兴市场，而且是一种替代传统商务活动的新形式。它有可能彻底改变贸易活动的本质，形成一套全新的贸易活动框架。但如何保证 Internet 网上信息传输的安全，是发展电子商务的重要环节。

为解决互联网的安全问题，世界各国对其进行了多年的研究，初步形成了一套完整的 Internet 安全解决方案，即目前被广泛采用的 PKI 技术，此项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[7]（Certificate Authority，CA）。把用户的公钥和其它标识信息(如名称、Email、身份证号等)捆绑在一起，在 Internet 网上验证用户的身份。目前，通用的办法是采用建立在 PKI 基础之上的数字证书，通过把要传输的数据信息进行加密和签名，保证信息在传输的机密性、真实性、完整性和不可否认性，从而保证信息的安全传输。

2.1 PKI 理论基础

由于 PKI 基础设施是目前比较成熟、完善的 Internet 网络安全解决方案[1]。国外的一些大的网络安全公司纷纷推出一系列的基于 PKI 的网络安全产品，这些安全产品供应商为用户提供了一系列的客户端和服务器端的安全产品，为电子商务的发展以及政府办公网等提供了安全保证。简言之，PKI 公钥基础设施就是提供公钥加密和数字签名服务的系统，目的是为了管理密钥和证书、保证网上数字信息传输的机密性、真实性、完整性和不可否认性。

2.1.1 对称加密算法

对称密钥加密也称为秘密/专用密钥加密，是指发送和接收数据的双方使用相

同的密钥对明文进行加密和解密运算。使用发件人和收件人共同拥有的同一个密钥。此密钥既用于加密，也用于解密，叫做秘密/专用密钥。对称密钥加密是加密大量数据的一种行之有效的方法。对称密钥加密体制最大的优势就是开销小，加密速度快。它的缺点是由于加解密双方要使用相同的密钥，因此在发送数据之前，必须完成密钥的分发，以使接受者能够解密数据，然而各种基本手段都不能保障安全的完成此工作，因此密钥的分发即为此类加密体系最薄弱的环节；且由于加密解密使用相同的密钥，假设有 n 方参与通信，则系统维护密钥的数量就是 n，这便大大增加了系统中密钥的管理开销；而且对称密钥加密体制功能较为单一，不能实现数字签名，常用的对称加密算法。

（一）DES 算法。

DES(Data Encrypt Standard，DES)算法是一个分组加密算法，于 1977 年被美国国家标准局（American National Standards Institute，ANSI）纳为数据加密标准[5]。标准的 DES 算法的密钥长度为 64 位(其中只有 56 位是有效位)，明文按 64 位进行分组，将分组后的明文组和 56 位有效密钥按位替代或交换的方法，形成 64 位密文组的加密方法。解密则使用了和加密相同的步骤和相同的密钥。时至今日，穷举搜索法仍是对 DES 最为有效的攻击手段。在如今的设备条件下，56 位和 64 位密钥的 DES 算法已经不再安全，只有将密钥提升至 80 位以上才能达到较为理想的安全效果，但是如果按目前的形势继续发展下去的话，这种情况将会在 30 年内发生改变。因此在实际使用时可以适当增加 DES 密钥的长度来达到更好的保密效果（80 位以上）。还需说明一下的是，在使用 64 位密钥的 DES 算法时，要注意其密钥的有效数据位只有 56 位，若将密钥中剩余的 8 位也作为有效数据使用，则不能保证 DES 算法的安全性，这个误区是各级管理员和用户在使用过程中应当绝对避免的。DES 在相当长的时间内成为事实上的国际标准，由于安全性原因，1998 年正式退役。

（二）TDES 算法。

TDES(Triple DES，TDES)算法是 DES 算法的一种替代物，它使用三个密钥，并执行三次 DES 算法[5]。加密函数遵循加密—解密—加密的次序。由于在 TDES 算法中执行了三次 DES 算法，所以说，TDES 算法消耗的时间是 DES 算法的三倍，但是作为补偿 TDES 算法也大大提高了对穷举攻击的抵抗性。