基于 PKI 的增值税发票网上认证系统的构建

Implementing an Internet Authentication System of Value-added Tax Special Invoice Based on PKI

方 俊 （越秀外国语学院 管理分院　浙江绍兴 312000）

摘要：本文给出了基于 PKI 体系构建的增值税发票网上认证系统的解决方案。实现了对增值税发票数据签名和加密方式下进行安全的传输，保证了增值税发票信息的安全，满足网上认证的安全需求，有效地防止各种网上认证的安全隐患。

关键词：PKI　公钥加密　数字签名　增值税发票

1　引言

增值税是对商品生产和流通中各环节的新增价值或商品附加值进行征税，是国家财政收入的一项重要税种。增值税防伪税控系统是运用数字密码和电子存储技术，强化增值税专用发票防伪功能，实现对增值税一般纳税人税源监控的计算机管理系统。随着增值税一般纳税人认定标准调低，更多的一般纳税人开具、取得发票，税务机关工作量加大与企业认证难的矛盾更加突出，构建增值税专用发票网上认证子系统是解决此问题的一条有效途径。网上认证系统符合现有发票认证业务流程，具体来讲，就是使用互联网代替企业到税务大厅进行认证的过程。税务机关设立一台认证服务器与互联网连接，增值税一般纳税人用扫描仪或键盘，将增值税专用发票上的“发票代码”、“发票号码”、“开票时间”、“购货方纳税人识别号”、“销货方纳税人识别号”、“金额”、“税额”、“84 位密文”采集下来加密，通过互联网传送到税务机关服务器，由服务器将信息解密和 84 位密文进行比对认证，辨别发票真伪。解密认证的结果，即网上增值税发票认证结果存放在税务机关数据库服务器上，供企业下载和税务机关内部各系统使用。

2　PKI 概述

2.1　PKI 体系原理

PKI(public key infrastructure)是指公钥基础设施。它是一个利用现代密码学中的公钥密码技术在开放的 Internet(Intranet)网络环境中提供数据加密和数字签名服务的统一的技术框架[1]。PKI 的主要目的是管理在开放网络环境中使用的公开密钥和数字证书，从而为一个机构或集团建立一个相对安全和值得信赖的网络环境。PKI 包括两个主要的安全技术：公钥加密技术、数字签名与验证技术。为此，PKI 必须建立一个权威的认证机构 CA，在公钥加密技术基础之上完成证书的生成、管理、存储分发和撤销工作。

到目前为止，完善并正确实施的 PKI 系统是全面解决所有网络交易和通信安全问题的最佳途径。根据美国国家标准技术局的描述，在网络通信和网络交易中，特别是在电子政务和电子商务业务中，最需要的安全保证包括 4 个方面：身份标识和认证、保密或隐私、数据完整性和不可否认性[2]。它从技术上解决了网络安全通信的障碍，从而有效地解决了电子商务中信息安全这一核心问题。从总体架构看，典型的 PKI 由下面几个部分组成。证书中心(CA)；注册中心(RA)；证书持有者；用户；证书库等。在 PKI 的具体部署中，这几部分可根据实际的应用进行分解，分化出其他模块，以便于实施。以数字证书为核心的 PKI 技术可以对网络上传输的信息进行加密和解密、数字签名和签名验证。

2.2　PKI 的核心服务

PKI 可提供多种网上安全服务，包括认证、数据保密、数据完整和不可否认。PKI 的核心执行机构是 CA，其中的核心元素是由 CA 签发的数字证书。利用

证书的公钥和与之对应的私钥进行加/解密，并产生对数字电文的签名及签名验证。数字签名是指使用公钥密码技术和其它密码算法(HASH 算法、MD5 算法等)对待发的数据(报文、票证等)生成一系列符号及代码组成电子密码进行签名，来代替手写签名和印章。这种电子式的签名与手写签名和印章具有同等的法律效应。

3 系统实施方案

3.1 PKI 设计

CA 证书是确保用户网络传输数据的安全性的有力工具，一般由国税局指定的服务商向用户提供。图 1 为增值税发票网上认证系统的网络拓扑图。证书的申请签发过程包括 4 个环节。

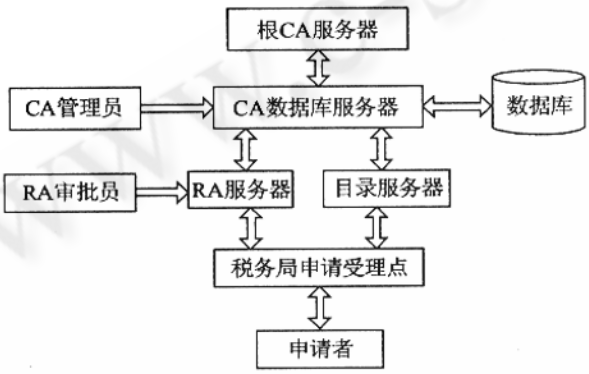

图 1　系统 PKI 设计网络拓扑图

(1) 用户申请。要求进行网上认证的纳税人需填写“网上认证申请审批表”，并报送证明纳税人身份的需要查验的资料，经主管的税务部门申请受理点审阅纳税人填报的表格是否符合要求。符合条件的，转税务审核部门。

(2) 注册机构审核。税务机关审核部门对纳税人报送的资料进行审核，证明用户的真实身份，审核无误后，注册机构工作人员与 RA 服务器之间进行安全通信，RA 系统对工作员进行严格的身份认证，包括核对工作人员的数字证书和 IP 地址。工作人员将审阅 RA 系统中的申请表，核对用户信息并批准申请，随后，通过注册机构管理员授权。

(3) 认证系统颁发证书。RA 向 CA 传递用户申请，CA 操作员审阅申请信息，并验证操作员的数字签名，如果批准申请则颁发证书，CA 系统会自动产生证书(采用 X.509 V3 标准)。证书中包含关于用户及签署 CA 的各种信息，如用户唯一标识信息、证书持有者的公钥、证书有效起止日期等。

(4) 获得证书。证书生成完成后，CA 将证书输出到目录服务器以提供目录浏览服务。同时注册机构操作员通知申请人，将 CA 证书通过软盘或 U 盘考给申请人，并将有关审批资料返回纳税人，再由申请人导入到客户端软件中。

在进行网上认证时，登录验证由安全客户端和认证受理服务器构成。认证受理服务器串联在网络入口和税务内网 Web 服务器之间，与安全客户端建立加密通道，保证信息传递的保密性。认证受理服务器同时利用目录服务和权限管理基础设施，控制证书的有效性。在证书使用过程中，认证受理服务器要获取信息发送方的公钥证书以及 CA 根证书，以验证发送方证书的真实性。

3.2 技术方案

(1) 首先，纳税人利用扫描仪将增值税专用发票抵扣联上的主要信息(包括“发票代码”、“发票号码”、“开票时间”、“购货方纳税人识别号”、“销货方纳税人识别号”、“金额”、“税额”、“84 位密文”)扫描录入到企业端系统中，通过 OCR(Optical? Character? Recognition，光学字符识别)软件识别出发票数据或手工输入到客户端系统中。

(2) 纳税人检索出需要认证的发票数据，将发票数据进行签名、加密(采用数字信封技术[3])、压缩，通过互联网上传到认证受理平台。

(3) 认证受理平台接收到加密的待认证发票数据后，先进行解压缩、解密(进行 CA 解密)，通过合法性验证后，再通过安全网闸转发给税务内网的防伪税控认证子系统，由防伪税控认证子系统对发票数据进行认证。

(4) 认证子系统将 84 位密文解密还原为明文，并与票面上的明文比对，产生并记录认证结果，将认证结果回传给认证受理平台，并将数据插入到认证数据库。

(5) 纳税人向认证受理平台发出接收认证结果请求，认证受理平台从认证数据库取出认证结果数据，将认证结果签名、加密、压缩，回传给纳税人。

(6) 网上认证客户端对回传的认证结果进行解压缩、解密(进行 CA 解密及验证合法性),将认证结果存入本地数据库。这时,纳税人就能查看认证结果了。其流程如图 2 所示。

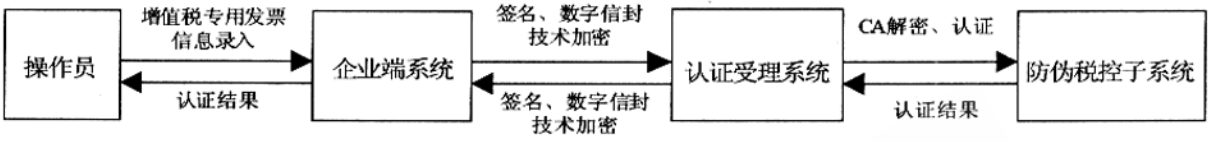

图 2　增值税专用发票网上认证流程图

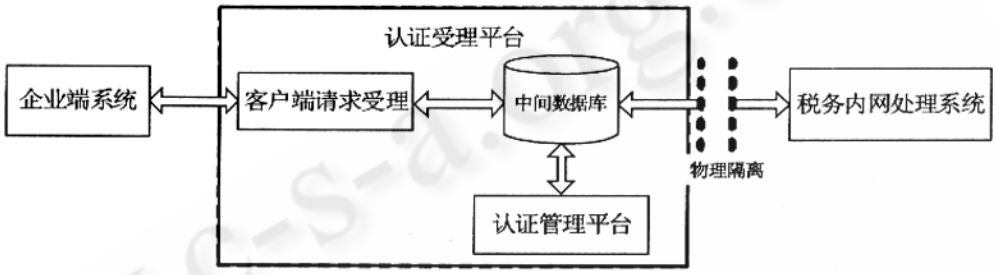

图 3　系统架构图

从上面的业务流程说明中可以看出数据在传输中经过了多层加密和签名,保证了数据的安全性。体现在:

(1) 企业端的数据在和认证受理平台进行交互时,使用了 CA 证书的双向加密和签名(企业端有认证受理平台的公钥和自己的私钥,认证受理平台有用户的公钥和自己的私钥)。

(2) 对于待认证数据及认证结果数据采用了认证密钥加密(企业端与认证受理平台都有用户的认证密钥)。

3.3　系统实施方案

系统采用 C/S 模式,C/S 模式的特点是数据处理能力强、响应速度快、开发周期短、能脱机使用、有实物。在客户端的可执行程序是经过编译的,不但运行速度快,而且用户看不到程序的源代码,代码安全性较高。从使用者的角度出发,C/S 模式的这些优点更实用。C/S 模式增加智能升级后,从一定程度上弥补了需要升级的缺陷。纳税人与税务机关之间数据传递采用接口文件方式,接口文件符合 XML 规范。接口文件内容分三部分:XML 文件头、文件描述部分和数据记录部分。增值税专用发票网上认证需要处理二种接口文件,接口文书标识用于识别此二种文件,具体如表 1 所示:

表 1　接口文书标识

接口文书标识	接口文书名称
RZ00100	增值税专用发票抵扣联信息企业采集待认证数据
RZ00101	增值税专用发票抵扣联信息企业采集认证结果数据

整个软件系统由企业端系统、认证受理平台和税务内网处理系统三部分。企业端系统主要完成发票抵扣联上的信息获取、数据加密、数据输出、结果接受和查询统计等功能。认证受理平台包括客户端请求受理和认证管理平台,主要功能是接收纳税人发送上来的数据,然后解压缩、CA 解密,将数据转发给内网,同时接收内网的认证结果,然后对认证结果进行 CA 加密、压缩,等待纳税人下载。税务内网处理系统主要功能是接收认证受理平台转发的数据完成防伪解密认证,认证完后,将认证结果返回给认证受理平台。如图 3 所示。

3.4　系统安全性

认证受理平台的系统安全性不容忽视,在进行系统设计时,将采用多种安全技术手段加以保证,对相关的主机系统、应用数据库提供严密的保护。受理平台系统服务网站的结构采取分区和层次化,使用防火墙以及入侵检测系统,所有访问均在各层应用系统和程

序的严格控制下进行，一方面可以防范公用因特网上非法用户的访问，另一方面可以防止系统的一些重要数据被不合法的用户所获取或破坏。此外，还将采用网络安全漏洞检测、网络防黑客、防病毒等系统和手段，最大限度地加强受理平台的安全性。同时系统应具备完善的数据备份、恢复和清理功能，支持自动和手动备份方式。并且在系统设计时要严格遵守行业规范和技术标准，确保业务处理符合税务行业的行业规范。

为了确保 CA 用于签名证书的非对称密钥的安全性，CA 用于签名私钥长度必须足够长，以防止被破译。密钥备份及恢复是密钥管理的主要内容，用户由于某些原因将解密数据的密钥丢失，从而使已被加密的密文无法解开。为避免这种情况的发生，PKI 提供了密钥备份与密钥恢复机制[4]。当用户证书生成时，密钥即被 CA 备份存储；当需要恢复时，用户只需向 CA 提出申请，CA 就会为用户自动进行恢复。证书信息资料的管理，要求在证书使用中确定并检查证书的有效期，保证不使用过期或已作废的证书，确保网上交易的安全。发布和维护作废证书列表(CRL)，因某种原因证书要作废，就必须将其作为“黑名单”发布在证书作废列表中，以供在线查询，防止风险。对已签发证书的使用全过程进行监视跟踪，作全程日志记录，以备发生交易争端时，提供公正依据。

4 结束语

本文给出了基于 PKI 的网上增值税发票认证系统的构建，介绍了网上认证的模式和认证过程，并较详细地对网上认证的企业端和认证受理平台进行了综合分析。增值税发票网上认证系统的运行，不但减轻了税务局的工作量，也方便了纳税人，提高了认证的效率。

参考文献

1 张春起、李新、杨义先等，PKI 技术及评估[J]，计算机系统应用，2002，(1)：76－78.

2 Christopher M King，Cutis E Dalton，Ertem Osmanoglu T. 安全体系结构的设计、部署与操作[M]. 北京：清华大学出版社，2003.

3 DamelID. PGP or PKI The future of Internet security. EdiForum：the journal of electronic commerce，Publisher：EDIGroup，USA. 1999，12(1)：59－62.

4 JACOB E，LIBERAL F，UNZILLA J. PKIX－based certification infrastructure implementation adapted to non－personal end entities [J]. Future Generation Computer Systems，2003(19)：263－ 275.

5 曹天杰、张永平、苏成，计算机系统安全[M]，北京：高等教育出版社，2003.