基于 PKI 的在线招投标系统的设计与实现

徐 财
(上海大学 计算机工程与科学学院,上海 200444)

摘 要: 以某印刷集团的在线招投标系统的开发为背景,讨论了 PKI 技术在该网上招投标系统的设计与实现。采用新的 B/S 结构通过 PKI 技术来建设一个非常安全的在线招标、在线投标、在线开标、在线评标、在线决标的系统。

关键词: PKI; 招标; 投标
中图分类号:TP311.5 **文献标识码**:A

Design and implementation of online bid and tender system based on PKI

XU Cai
(School of Computer Engineering and Science, Shanghai University, Shanghai 200444, China)

Abstract: This article is based on the internet bid and tender system developed for printing corporation, and discusses bid and tender system's design and implementation based on PKI technical. The new internet bid and tender system includes online bid、online tender、online bid opening、online evaluation of tender and online tender decision by PKI technical.

Key words: PKI; bid ; tender

随着我国大力推行信息化建设,在线招投标系统已是各类招标机构提高市场竞争力和服务水平的必然趋势。基于 PKI 的在线招投标系统为招投标过程中的各个角色(包括招标方、投标方、评标专家、监督人员等)发放数字证书,结合 PKI 技术实现用户身份认证、访问控制,以及保证投标信息的保密性、完整性和不可否认性,将传统的招投标过程变成一个简单、方便、快捷和安全的过程。

本文以某印刷集团的在线招投标系统的开发为背景,讨论了 PKI 技术在网上招投标系统中的设计与实现。在开发该系统之前已经存在一套 B/S 结构的老招投标系统,但老系统已不能满足业务发展的需要,经常出现陪标、转包并且招投标过程的监控力度控制不够等现象,而采用新的 B/S 结构的招投标系统的目标就是通过 PKI 技术来建设一个非常安全的在线招标、在线投标、在线开标、在线评标、在线决标的系统。本文将详细讨论基于 PKI 的网上招投标系统的设计与实现。它具有如下特点:

(1)安全。采用 CA 认证机制、数字签名、数字信封、非对称密钥、对称密钥技术,保证了招投标系统用户的身份认证,投标文件传输和存储的保密性、完整性,以及招投标双方的不可否认性;

(2)公平性。投标方提交的投标文件在开标之前一直加密存储在数据库中,任何人包括系统管理员都无法查看。只有在开标时,监督人员出示正确的数字证书才能解密投标文件,体现了公开、公平、公正的招投标理念;

(3)高效。投标方不需要携带大量投标文件到达评标现场,大大降低了企业的投标成本,节省了人力、财力,提高了办事效率;

(4)科学性。评标时主要采用层次分析法,它为评标提供了一种新的、简洁而实用的建模方法,它可按建立递阶层次结构模型、构造出各层次中的所有判断矩阵、层次单排序及一致性检验、层次总排序及一致性检验 4 个步骤进行,最后选出 3 个候选中标者并按分数由高到低排序。

1 系统设计

基于 PKI 的在线招投标系统采用 B/S 架构,划分为 Web 层(应用.net2008 中的 WPF 技术)、业务逻辑层和工作流层(应用.net2008 中的 WF 技术)、数据访问层(应用.net2008 中的 Linq to sql)、数据层 4 层。其中 Web 层引用服务层,服务层引用业务逻辑层和工作流层,业务逻辑层和工作流层引用数据访问层,最后数据访问层调用数据库层,这样降低了各个层次的耦合度,遇到问题或用户需求变更时只需修改各个层次即可,简单方便,

提高了开发效率。

在项目的设计过程中，依然运用 Rational 公司的 Rose 工具，通过画 UML 活动图、状态图及类图(ER 图)来清晰化流程和方便数据库设计，同时写出相应的文档，也增加了该招投标决策支持平台的可维护性。

基于 PKI 的在线招投标系统完全遵守 PKI 规范，提供严格的身份认证、加密存储、加密传输、数字签名等功能，全面保证了保密性、安全性、权威性以及不可抵赖性。系统部署结构如图 1 所示。

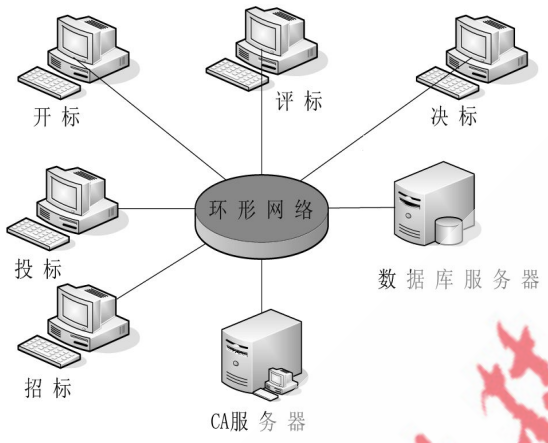

图 1 在线招投标系统部署结构

(1)项目认证及信息发布管理。

系统在收到招标方的招标申请后，对招标方的数字证书及其申请进行全面认证。对认证通过的系统将自动生成招标信息，并将信息在网上公布；

(2)投标方资质认证管理。投标方根据集团采购平台提供的招标公告信息，使用 CA 颁发的合法证书登录到系统，将投标文件通过加密的方式上传到数据库服务器；

(3)开标。投标文件在开标时统一解密，之前均为加密存储，防止有人从中舞弊；开标时，要对文件完整性进行验证，并在浏览器端通过公正人员出示的私钥证书中读取私钥，解密加密的会话密钥，将解密后的会话密钥传回服务器；在服务器端，用会话密钥解密文件，得到投标文件的明文，并提供下载；

(4)评标。评标当天，开标前从专家库中随机抽取的具有评标资格的专家使用自己的证书登录系统，运用层次分析算法进行网上评标，提交评标结果；

(5)决标。评标结果出来后，招标方决策出最终中标者并可在线公布最终中标信息，向中标方和投标方发出确定信息，待得到确认后，系统即可将拟定的合同模板发送给招投标双方。

2 系统实现

投标方负责将投标文件上传至数据库服务器，为了保证投标身份的真实性，系统要对投标方的数字证书进行合法性验证，只有通过身份验证的投标方才能进行投标。投标文件处理流程如图 2 所示。

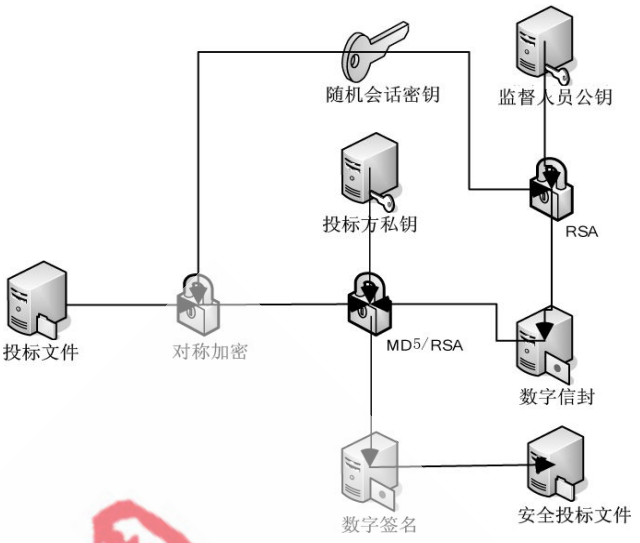

图 2 投标文件处理流程图

投标文件处理过程如下：

(1)用随机会话密钥，对投标文件进行对称加密，生成加密文件；

(2)用指定监督人员的公钥对会话密钥进行多重加密，生成数字信封；

(3)用 MD5 算法对加密文件、数字信封求取散列值，再用投标方的私钥加密散列值得到数字签名；

(4)将加密文件、数字信封和数字签名合成安全投标文件。

2.1 投标文件处理模块

招投标系统会定期查看是否有新的投标文件。如果有新的投标文件，则对投标文件进行分解，分解出签名数据和投标文件两部分；然后根据从投标文件中获得的投标方证书序列号，从证书服务器中检索出其对应公钥证书，用公钥对投标文件签名数据进行非对称解密得到投标文件的散列值。按投标文件控制信息指定的散列算法求取投标文件的散列值，将两个散列值进行比较。若相同，则签名验证通过；否则认为投标文件已被篡改。数字签名验证保证了数据在传输过程中的完整性以及投标方的合法性。

签名验证通过后，从数据库服务器中提取投标文件。为保证加密投标文件(包括投标文件密文和数字信封)的完整性，计算加密投标文件的散列值，将加密投标文件连同其散列值一起存储于数据库中，以便在开标时，解密投标文件之前能够进行完整性验证。在开标之前，投标文件在服务器端加密存储，投标文件内容不被泄漏、不被篡改，从而保证了招投标过程的公平性和公正性。

2.2 开标过程处理模块

开标过程处理模块负责在开标时将加密的投标文

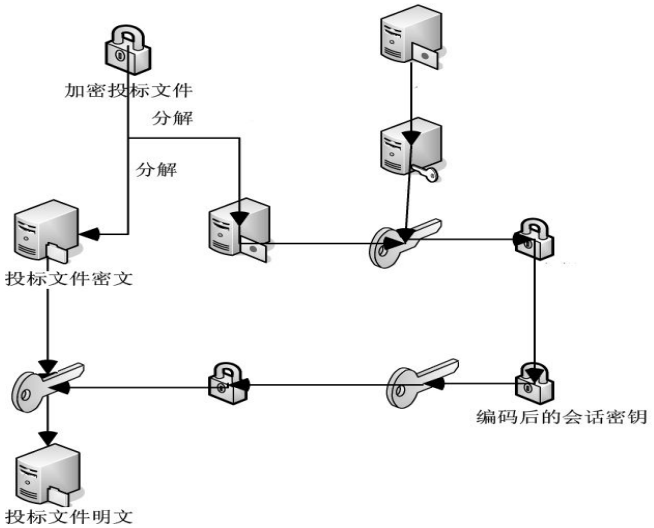

图 3 投标文件解密流程图

件解密。投标文件解密流程如图 3 所示。

投标文件的启封主要流程如下：

(1) 在监督人员私钥端，验证加密投标文件的完整性，即计算加密投标文件的散列值，并将其与数据库中存放的接收投标文件时所求取的散列值进行比较，若相等则说明加密投标文件是完整的，然后从加密投标文件中提取加密投标文件和数字信封两部分，存放到数据库系统中；

(2)在加密投标文件端，招标项目对应的几个监督人员出示私钥证书，从私钥证书中提取出私钥，按生成安全投标文件时用其公钥加密的相反顺序，多重解密数字信封，得到对称会话密钥，编码之后传回服务器，服务器端利用解码后的会话密钥解密投标文件密文获得明文形式的投标文件，存入数据库系统，供专家评标时查看。

2.3 评标决策处理模块

评标是招投标过程中最重要的、也是最关键的一环，评标的好坏直接关系着招标项目的成败。评标按照招标文件的规定进行，招标人或者招标代理负责组建评标专家组。评标专家组由招标人的代表及其聘请的技术、经济、法律等方面的专家组成，总人数一般为 5 人以上单数，其中受聘的专家不得少于三分之二。与投标人有利害关系的人员不得进入评标专家组。

评标专家组负责评标。开标后，立即进行专家评标流程。专家使用自己的专家证书登录在线招投标系统，通过身份认证后，进入评标区，独立地并且采用层次分析法对每个有效投标人的标书进行评价、打分。

评标专家组对所有投标文件进行审查，对与招标文件规定有任何不符的投标文件，应当决定其无效。评标专家组可以要求投标人对投标文件中含义不明确的地方进行必要的澄清，但澄清不得超过投标文件记载的范围或改变投标文件的实质性内容。评标专家组应当按照招标文件的规定对投标文件进行评审和比较，并向招标人推荐 3 个中标候选人。针对招投标的特点，该在线招投标系统从价格、进度、质量、成功案例和公司规模 5 个准则反复比较 3 个候选投标方。

然后系统会自动建立各层次的判断矩阵并进行层次单排序、层次总排序及其一致性检验。招标人再从最终的评标专家组推荐的中标候选人顺序表中决策出中标人。中选的投标者应当符合下列条件之一：(1)满足招标文件各项要求，并考虑各种优惠及税收等因素，在合理条件下所报投标价格最低的；(2)最大满足招标文件中规定的综合评价标准的。

最后，招标人或者招标机构应当将中标结果书面通知所有投标人。招标人与中标人应当按照招标文件的规定和中标结果签订书面合同。

本文设计并实现了一种安全的在线招投标系统，利用 PKI 的加密和数字签名技术从各个角度全方位地保证了在线招投标过程的安全性，最大限度地堵住了各方面可能存在的安全漏洞，为在线招投标过程提供了一个安全的、值得信赖的系统。该系统具有以下特点：

(1)系统采用基于 PKI 的用户管理，用户必须提供正确的数字证书才能进行相应的操作，大大增强了系统的安全性；

(2)投标文件的加密传输和存储，使得投标信息在开标之前一直处于高度机密的状态，只有在开标时，所有监督人员都到场并出示正确的数字证书的情况下，投标信息才会被解密成明文，保证了在开标之前，投标信息的机密性；

(3) 投标供应商在确认提交正确投标文件后不能修改其提交文件，保证了招投标过程的公正性；

(4)除非所有的监督人员合作，否则投标信息是保密的，具有一定强度的抗勾结性；

(5) 投标供应商的数字签名保证了他们对所投标书的不可否认性，该在线招投标系统提出的评标策略及其评估算法（层次分析法）可以在集团商务运作及其应用领域实现实用化，具有较好的发展前景。

参考文献

[1] HOUSLEY R, FORD W, POLK W, et al. Internet X.509 public key infrastructure certificate and CRL profile. Internet Request for Comments 2458, 1999.

[2] CODD E F. A relational model of data for large shared data banks. Communications for the ACM, 1970, 13(6):377-387.

[3] 张莹. 招标投标理论与实务 [M]. 北京: 中国物质出版社, 2003.

[4] 中华人民共和国政府采购法. 2002.6.

[5] 刘芳, 吴明晖. 政府采购平台的设计与实现. 计算机时代, 2002(6).

（收稿日期：2009-09-30）

作者简介

徐财，男，1980 年生，高工，研究生，研究方向：系统分析、架构设计等。