计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(4):39−46 [doi: 10.15888/j.cnki.csa.006331]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于防篡改技术的电子签约服务平台①

徐　睿[1,2], 孟祥君[3], 马　锋[1,2], 赵希超[1,2], 游　佳[1,2], 张子谦[1,2]

[1](南瑞集团 (国网电力科学研究院) 有限公司, 南京 211106)
[2](南京南瑞信息通信科技有限公司, 南京 210003)
[3](国网山东省电力公司, 济南 250001)
通讯作者: 马　锋, E-mail: mafeng1@sgepri.sgcc.com.cn

摘　要: 信息互联网的快速发展推进了电子商务的广泛应用, 用户身份被盗用、电子合同的易篡改性严重影响了网上电子交易的公平性与安全性. 对于交易主体来说, 如何确认交易对方的数据身份未被冒用, 如何确认交易的电子合同为对方发送且未被截获篡改是需要首要解决的关键问题. 通过结合用户身份认证、电子合同加密传输、公证处参与公证等方法进行电子签约服务平台的设计, 确保用户身份的唯一性、传输数据的完整性和不可篡改性、签约过程的可追溯性, 实现了平台使用的公平公正性.

关键词: 电子合同; 服务平台; 非篡改性; 公平公正; 信息安全

引用格式: 徐睿,孟祥君,马锋,赵希超,游佳,张子谦.基于防篡改技术的电子签约服务平台.计算机系统应用,2018,27(4):39–46. http://www.c-s-a.org.cn/1003-3254/6331.html

Electronic Signature Service Platform Based on Tamper Protection Technology

XU Rui[1,2], MENG Xiang-Jun[3], MA Feng[1,2], ZHAO Xi-Chao[1,2], YOU Jia[1,2], ZHANG Zi-Qian[1,2]

[1](NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 211106, China)
[2](Nanjing NARI Information Communication Technology Co. Ltd., Nanjing 210003, China)
[3](State Grid Shandong Electric Power Company, Jinan 250001, China)

Abstract: The rapid development of Internet has promoted the extensive application of e-commerce. The stolen identity of users, and the electronic contract tampering have seriously affected the fairness and security of online electronic transactions. For the main participant of the transaction, it is a primary and pivotal problem to solve how to confirm the identity of the other party is genuine and credible and how to confirm the electronic contract is sent by the other party with authenticity, credibility, and non-repudiation. In order to ensure the uniqueness of the user identity, transmission data integrity and non-tampering, the contract process traceability, this study combines the user authentication, electronic contract encryption transmission, notary office to participate in notarization and other methods to design electronic contract service platform, which achieves fairness in the use of the platform.

Key words: electronic contract; service platform; non-tampering; fairness; information security

随着信息技术和互联网的发展普及, 基于互联网的线上交易在各个领域都得到了广泛的应用, 银行、证券、P2P 金融、支付宝等企业在日常业务交易中都朝着无纸化方向迈进, 电子合同在企业资源管理的过程中已逐步替代纸质书面合同, 并发挥越来越重要的作用. 根据我国《合同法》、《电子签名法》的有关规定, 电子合同主要指: 双方或多方交易主体之间以电子数据的形式达成的有关设立、变更、终止财产性民事权利义务关系的协议. 电子合同与传统纸质合同相比, 其签署时间、签署地点、签名形式发生了变化, 给

① 基金项目: 南瑞集团公司科技项目 (WBS5246DR170009)
收稿时间: 2017-08-15; 修改时间: 2017-09-05; 采用时间: 2017-09-20; csa 在线出版时间: 2018-03-31

传统法律制度带来了冲击和挑战. 文献[1]介绍了服务方与合约主体之间的服务关系, 对于交易纠纷服务方具有居间调解的权利. 文献[2]描述了电子商务合同的订立、成立和生效及其主体身份的认定、和效力认定等新问题, 以有效保障交易各方的利益. 文献[3]对电子合同成立时间、地点、电子签名的合理有效性进行了探讨, 分析了电子合同形式的相关变化. 其他一些研究[4,5]关注电子签名技术在电子合同中的应用, 以保证电子形式的合同的法律约束力. 文献[6]设计了电子合同监管与公共服务平台, 有效实现了电子合同的监管.

以上文献已经对电子合同的法律效力和签署时间地点、及电子合同监管等问题进行了研究. 然而, 电子合同的签署双方均为数据用户身份, 并通过电子数据的形式进行传输, 用户易冒用性和合同易篡改性挑战了电子合同的真实性和合法性, 严重影响了网上交易的公平性与安全性. 因此, 在网络电子交易中, 合同的签订需要公平公正地保障到双方的利益, 如何防止任何一方的否认、抵赖和假冒行为, 防止数据被篡改的发生, 将具有非常重要的意义.

1 电子合同所面临的问题

电子合同与纸质合同相比, 签署环境和签署方式发生了较大的变化, 其网上电子合同交易的方式还存在以下 3 个问题.

1.1 签约用户身份冒用问题

在传统的纸质合同订立过程中, 签约用户通过在书面合同上进行当面签字或盖章来确定双方的权利义务关系. 电子合同订立过程中的要约和承诺则通过电子数据的传递来实现, 它的成立、变更和终止均不需要纸质书面形式. 若签约用户在互联网中存在唯一相对应的用户数据 (用户名+密码), 通过“用户名+密码”登录系统后进行意思的表示, 当签约用户无意泄露信息或者被黑客利用撞库攻击手段破获, 撞库攻击是一种从数据库中导出数据的攻击方式, 通过网站入侵, 非法实现对用户信息的窃取和修改[7]. 为了增强用户身份的安全识别, 目前通常采用 USB Key 与用户密码相结合的方式, 将数字证书及其对应的私钥存放在 USB Key 芯片安全区域中, 一定程度上确保了用户身份的信息安全. 但是, 文献[8]通过研究密码芯片运行时的光辐射迹及其数据依赖性, 建立了针对高级加密标准 (AES) 加密算法的密码芯片光辐射分析方法, 对 AES 密码芯片的安全性构成了严重的威胁. 安全芯片作为 USB Key 的重要组成部分, 入侵者利用半侵入式攻击、差分能量攻击、激光攻击等攻击手段[9], 将可能破获其存储的数字证书及对应私钥, 因此 USB Key 存在被破获复制的风险. 入侵者由此可以通过冒用签约用户身份进行非正常的签约操作, 从而带来签约风险和纠纷.

1.2 电子合同易篡改性问题

电子合同通常以数据电文的形式展现, 通过计算机联网的电子数据交换 (EDI), 在互联网标准协议以电子手段传送和达成交易双方的权利、义务协议. 由于电子合同的订立载体与传统合同不同. 不同于传统合同的纸质载体, 电子合同包含的信息以电子化形式存储在计算机或磁盘等载体中, 其修改、传递、储存等过程均在计算机内进行. 由于电子数据的无形性和易改动性, 为了保证电子合同传输过程的数据安全性, 常见的加密方式是采用对称加密算法, 其具有高效率、高性能和灵活易用等优点. 可以运用对称加密算法对电子合同原件信息进行加密后传输, 但是对称加密的密钥存在被破解的可能[10], 当密钥被攻击者破解后, 传输的电子合同数据内容将会被攻击者截获和篡改, 无疑存在对交易主体的合法权益造成损害的风险.

1.3 电子合同证据问题

随着企业资源管理过程中由传统的纸面形式向无纸化的数字形式的转变, 电子合同签订形式更加高效快捷、省时省力, 信息安全技术需要充分保障电子合同的完整性、真实性、不可否认性和有效性, 才能减少因双方争议引起的电子合同证据问题. 目前大多数电子合同平台只单纯的作为第三方平台, 为签约双方提供电子合同签约服务, 其利用的数字水印技术、电子签章技术等缺少监管机构的配套管理, 第三方平台很难有效保证电子合同的完整性、真实性和不可否认性. 双方主体可能因电子合同的内容产生异议而发生纠纷, 不同于传统合同的举证, 普通数据电文形式的所谓“电子合同”要成为司法证据, 需要按照司法规定, 进行公证机构陪同取证、保管、鉴定等, 通过确定电子合同签署环境的安全性、电子合同成立时间和成立地点可信性, 其过程繁琐, 成本高昂, 且举证结果无法得到法院的认可, 导致电子合同证据有效性受到影响.

综上所述, 电子合同签约用户身份冒用性、电子合同易篡改性、电子合同取证复杂性制约了电子合同的广泛应用, 对于网络交易双方来说, 如何确认对方的身份真实可信, 如何确认对方发来的电子合同真实

性、可信性和不可抵赖性, 如何实现电子合同证据便捷效力性成为当前需要解决的关键问题. 本文将结合身份认证技术、可靠的数字签名技术、第三方公证机构参与的方式, 设计与实现电子签约服务平台, 平台实现了交易者身份的确定性、发送信息的不可否认性、信息传输的保密、数据交换的完整性、完整证据链查询的快速性, 从而保证平台使用的安全性和公平性.

2 电子签约服务平台的设计原理

2.1 平台基本模型

在保证用户身份强认证和电子合同公证服务的前提下, 给出了电子签约服务平台的基本模型. 该模型描述了用户使用平台的总体流程, 如图 1 所示.

作为电子合同签署的服务型平台, 其主要用户为签约用户和公证人员. 签约用户是指合同相关的各个交易方, 通过传输接口完成电子合同的上传、签署操作. 公证人员主要通过公证服务子系统存储的电子合同签署过程数据信息, 提供电子合同验真和公证服务. 其中, 签约用户在登录平台时需要进行身份认证, 验证用户账号为本人使用, 有效防止签约用户的身份冒用风险. 电子合同通过数字签名技术进行加密, 以保证电子合同传输的安全性. 公证服务子系统只记录电子合同签署的过程信息, 不涉及电子合同内容, 实现电子合同的保密性. 除此之外, 平台还包括系统管理员, 主要进行系统的日常监控运维.

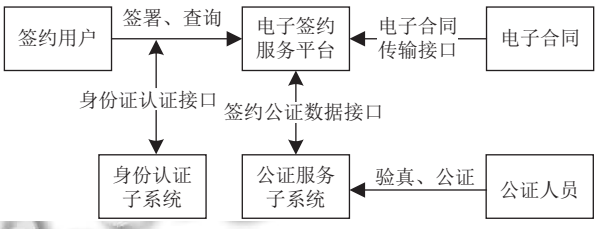

图 1 电子签约服务平台基本模型

2.2 平台设计原理

为了保证电子签约服务平台的公平性和安全性, 防止签约用户身份冒用、电子合同被篡改、合同无法被公证等问题, 本文构建了基于软硬件结合的身份认证系统、电子合同加密传输、第三方公证机构参与的签约平台, 具体设计原理如图 2.

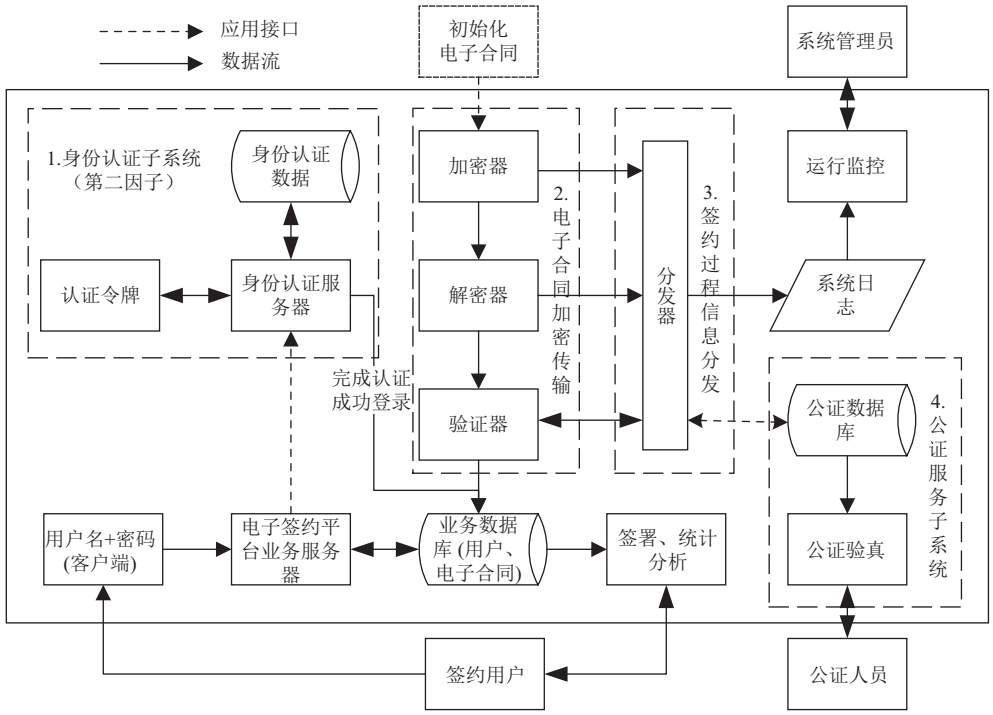

图 2 电子签约服务平台设计原理

(1) 身份认证子系统

电子合同签署方式由传统的面对面签署转变为网上签署, “用户名+密码”成为用户身份线上识别的凭证, 当受到黑客截获或用户自身无意泄露时, 由身份冒用

进行电子合同签署的行为所引起的电子合同纠纷, 无疑会影响签约平台的应用效率. 因此, 设计基于 FIDO 协议与物理不可克隆函数 (PUF) 的身份认证子系统作为用户身份认证的第二因子, 第一次“用户名+密码”认证通过后, 再进行认证令牌的第二次认证, 从而有效保证数据用户与物理用户的唯一对应性.

身份认证子系统采用软件与硬件相结合的认证方式, 其中硬件与服务器端的交互是基于 FIDO U2F 协议和国密算法 (SM2/SM3/SM4) 进行开发的, 并将物理不可克隆技术 (PUF)[11,12]集成在认证令牌中, 充分保证认证令牌的不可复制性. 主要分为用户注册协议和用户认证协议两个部分.

1) 用户注册协议

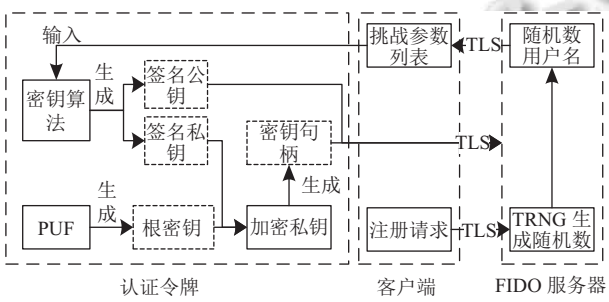

图 3 用户注册协议流程图

如图 3 所示, 用户首次登录电子签约服务平台时, 在通过“用户名+密码”第一因子认证后, 向 FIDO 服务器发送注册请求, FIDO 服务器与认证令牌通过进行数据交互生成密钥等认证信息. 具体算法步骤如算法 1.

算法1. 用户身份注册协议算法

1. 用户初次登录电子签约服务平台时, 完成“用户名+密码”第一因子认证后, 向FIDO服务器发起注册请求;

2. FIDO服务器端的随机数发生器(TRNG)生成一个随机数, 并将该随机数、用户名发送给客户端;

3. 客户端设置挑战参数列表={随机数, 用户名, TLS连接数据, 随机会话参数}, 并运用国密算法SM3对目标服务器URL进行哈希运算;

4. 客户端将挑战参数列表与URL哈希值发送给认证令牌;

5. 认证令牌首先完成URL哈希值的验证, 并通过国密算法SM2生产签名公钥、签名私钥, PUF模块生产根密钥作为对称密钥, 运用国密算法SM4对签名密钥进行加密生成对应的密钥句柄; 由于挑战参数列表唯一性, 对应产生的签名公、私钥对具有唯一性;

6. 认证令牌本身包含私钥和令牌证书, 调用自己的私钥对列表{密钥句柄、公钥、挑战参数列表}进行签名, 并将对应的签名值和令牌证书发送给FIDO服务器. 认证令牌不存储公钥、密钥句柄、PUF根密钥信息, 实现其不可复制性;

7. FIDO服务器提取令牌证书中的公钥, 对签名值进行合法性验证, 若验证正确, 则存储“用户名、签名公钥、密钥句柄”, 若验证错误, 则返回“注册信息有误”提示.

2) 用户认证协议

如图 4 所示, 用户登录电子签约服务平台, 完成第一因子认证通过后, 需要进行身份第二因子认证.

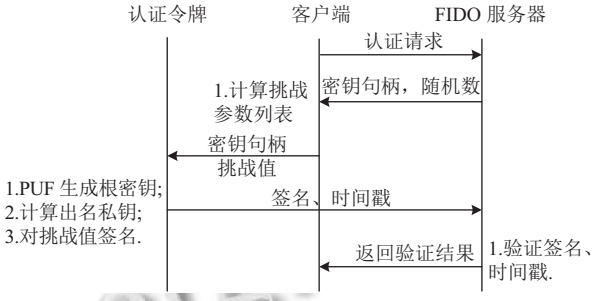

图 4 用户认证协议流程图

具体算法步骤如下:

算法2. 用户身份认证协议算法

1. FIDO服务器收到认证请求(含用户名), 根据用户名找到对应的密钥句柄, 并生成一个随机数;

2. FIDO服务器发送密钥句柄、随机数给客户端;

3. 客户端计算挑战参数列表, 生成对应的挑战值, 连同密钥句柄发送到认证令牌;

4. 认证令牌通过PUF生成根密钥, 通过国密算法SM4计算密钥句柄得到签名密钥, 并使用签名私钥执行SM2算法对挑战值和时间戳进行数字签名;

5. 认证令牌将签名、时间戳发送给FIDO服务器;

6. FIDO服务器使用公钥执行SM2算法进行签名值验证, 并向客户端返回验证结果.

其中, 硬件设备的芯片采用国密安全芯片, 充分保证硬件数据信息的不可破获性, 同时为了增强硬件设备抗复制性, 令牌支持物理不可克隆函数, 保证用户拥有设备的唯一性. 由于无法实现在物理结构和相关物理特性上都保持完全一致的两个硬件芯片, PUF 的技术原理正是通过提取硬件芯片中集成电路在制造过程中由于工艺限制而引入的“随机差异”来生成加密信息 (响应)[13], 当设备上电的时候 PUF 的响应信号就自动生成, 当设备断电时响应信号自动湮灭. 通过运用物理不可克隆函数算法, 在上电情况下提取硬件芯片唯一的数字指纹信息 (加密信息), 利用提取的加密信息 (根密钥) 对签名密钥进行加密或者对密钥句柄进行解密, 认证令牌具有芯片物理特性无法复制且上电产生根密钥的特点, 并且认证令牌不存储签名公钥、密钥句柄及根密钥信息, 能够从根本上保证令牌的不可复制性, 保障用户账号登录的唯一性和安全性.

在用户注册时, 客户端设置的挑战参数列表由用户名、随机数、TLS 数据及随机会话数构成, 充分保

证了挑战参数列表的唯一性, 对于不同的挑战参数列表, 使用 SM2 国密算法生成的签名公钥、签名私钥也不相同, 由于签名公私钥对为非对称密钥, 在进行用户认证时, 用户无法使用自己的私钥完成其他用户的挑战签名, 用户只能持有指定的认证设备才能计算出正确的应答数, 该应答数只能对应本次挑战, 不能重复使用, 因此能保证极高的安全性.

(2) 电子合同加密传输

电子合同以数据化形式在互联网中进行传输, 由于电子数据的修改、伪造不易留下痕迹, 因此需要对电子合同进行数字签名, 防止电子合同在传输过程中被截获篡改. 由于合同的内容较长, 在加密之前先使用散列技术将需要传输的文件压缩成定长的散列值. 目前最常用的散列函数是 SHA1 和 MD5, 大多是 128 位或更长. 其工作原理是: 使用散列函数将一个不定长的字符串散列成定长的散列值, 即使字符串的微小差别变化, 生成的散列值也将不同; 通过散列函数可以将要检索的项与索引 (散列值) 关联起来, 生成一种便于搜索的数据结构 (散列表), 这种散列函数是单向不可逆的运算方式, 从一个定长的散列值基本上无法还原成原先的不定长的字符串. 这使得散列技术能够有效地保证文件信息的完整性, 通过散列值的前后对比就可以有效检验和察觉电子文件是否被篡改.

本平台使用非对称加密算法 RSA 与 AES 混合加密体制[14]进行接口数据的传输, 运用 MD5 哈希算法进行电子合同的完整性验证, 有效保证电子合同不被篡改, 实现数据传输的安全性. 具体算法步骤如下:

算法3. 电子合同加密传输算法

1. 签约发送方A将电子合同信息K利用MD5算法计算, 得到一个Hash值D_1, 并用私钥运用RSA算法对Hash值D_1加密得到加密信息S;

2. 发送方A运用AES算法对电子合同信息K和数字签名S进行加密, 得到加密信息N;

3. 发送方A运用接收发的RSA公钥对AES密钥进行加密, 得到加密信息P, 以保证AES密钥的安全性;

4. 发送方A将加密信息N和P发送给接收方B;

5. 接收方B使用自己私钥解密P, 得到AES加密密钥, AES密钥对加密密钥N进行解密得到电子合同信息K和数字签名S;

6. 接收方B运行发送方A的公钥计算数字签名S, 得到电子合同的Hash值D_1, 同时运用MD5算法计算出电子合同新的Hash值D_2, 进行Hash值对比, 若不一致, 则提示电子合同被篡改, 若一致, 则进行下一步;

7. 公证服务器运用公证处数字签名对电子合同进行数字签名, 运用MD5算法生成新的Hash值D_3, 并连同签约双方基本信息, 分发至公证数据库. 公证数字签名的电子合同分发至业务数据库.

(3) 合同签约过程信息分发

电子签约服务平台以达成签约双方的电子合同签署为目的, 其整个签约过程主要包括合同上传、合同签署和合同存储. 电子合同经过加密器进行加密处理, 通过数据接口上传到平台后由解密器进行解密处理. 在签署合同时, 通过验证器对电子合同的内容进行验证, 验证合同内的数字签名是否合法, 以确定合同内容未经篡改. 合同通过签约双方签署后, 进行加密后存储到业务数据库中.

当签约用户签署电子合同时, 电子合同与签约用户对应的电子签名或电子公章进行合成, 并生成合同文件唯一的 Hash 值, 分发器主要是 (1) 将电子合同数据分发至业务数据库, (2) 将签署合同过程信息、合同 Hash 值分发至公证数据库.

如图 5 所示, 通过签约过程信息分发, 电子合同等数据存储在业务数据库中, 电子合同签约过程信息、电子合同文件的 Hash 值等数据存储在公证数据库中, 业务数据库管理权限为平台的系统管理员拥有, 公证数据库的管理权限由第三方公证机构拥有, 有效实现业务数据与公证数据的分离. 签约用户在平台进行电子合同的签署、查看下载、统计分析等日常操作, 公证人员通过公证服务子系统访问公证数据库进行电子合同的验真、公证工作.

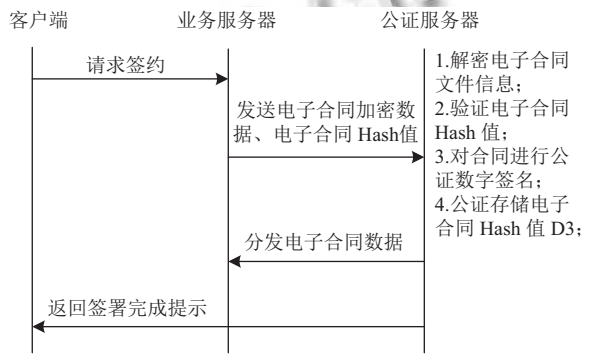

图 5 签约信息分发模型

(4) 公证服务子系统

电子合同是双方或多方交易主体之间以电子数据的形式达成的有关设立、变更、终止财产性民事权利义务关系的协议. 电子合同与纸质合同具有等同的法律效力, 若签约用户各方产生无法协商解决的合同纠纷, 可能需要进行合同的公证、诉讼. 电子合同是以电子数据的形式存在, 公证数据库存储了电子合同签约

过程信息、电子合同文件的唯一标示 Hash 值, 公证人员通过公证服务子系统, 通过对比电子合同原 Hash 值及最新生成 Hash 值来判断电子合同是否为原文件, 并提供开具电子合同对应公证文书的服务, 公证文书能够直接作为合同纠纷诉讼的法律证据. 通过合同验真公证, 交易双方能够认同该电子合同是对方签发且未被篡改, 从而保证合同的真实性和不可否认性. 公证服务子系统服务平台的所有签约用户, 通过记录电子合同签署过程的关键节点信息来保证平台的公平公正性. 公证验真模型如图 6.

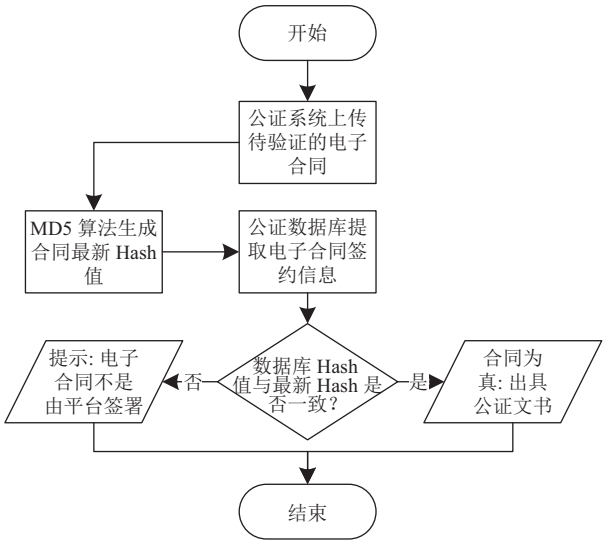

图 6 公证验真模型

3 电子签约服务平台实现方案

本平台是面向电子合同签署和公证的服务平台, 其签约用户用户分布广泛并且需求不断变化, 因此平台的设计架构应该满足两个要求. 一是用户端的易用性, 无需任何维护. 二是要能够轻松和内外部系统进行系统集成与数据交互. 平台采用“高内聚, 低耦合”的 B/S 结构 (即浏览器/服务器模式), 用户通过浏览器页面与系统交互, 用户无需安装任何专门的软件, 系统维护和升级只需要在服务端进行.

如图 7 所示, 在硬件基础上, 本平台实现架构可以划分为三层, 即数据访问层、业务逻辑层和界面层. 数据访问层就是通过 DAO/DAL 对数据库进行的 SQL 语句等操作, 来实现对数据表的 Insert (插入)、Delete (删除)、Update (更新)、Select (查询) 等操作. 如果要加入 ORM 的元素, 那么就会包括对象和数据表之间的映射关系, 以及对象实体的持久化. 简言之, 数据访问层就是在对数据库的操作基础上, 为业务逻辑层或界面层提供数据读取和传递服务. 业务逻辑层是平台架构中的核心部分, 主要集中在业务规则的制定、业务流程的实现等与业务需求有关的系统设计. 业务逻辑层在数据访问层与表示层中间关键位置, 对数据交换起承上启下的作用. 身份认证 BLL 设计用户身份的验证逻辑, 确保数据用户与物理用户的对应性; 用户关系 BLL 设计用户角色与权限的配置逻辑, 实现权限的灵活配置; 合同签署 BLL 进行合同状态的逻辑判断并完成合同的签名合成; 统计分析 BLL 进行合同的查询、统计分析等逻辑设计; 公证验签 BLL 主要通过提取合同的 Hash 值进行对比分析, 进行合同真假的判断; 组件部分提供多种功能组件, 如加解密组件、数字签名组件、合同解析组件、日志分析组件等; 接口主要进行平台与外部信息系统、身份认证子系统、公证服务子系统等的数据传输设计. 由于层是一种弱耦合结构, 层与层之间的依赖关系由上向下的, 底层对于上层而言是“无知”的, 上层设计的改变对其调用的底层不产生任何影响. 业务逻辑层根据界面层需求的变更进行对应的调整, 系统的集成难度较低并提高了重用性. 界面层主要是为用户提供交互式操作界面, 用于显示数据和接收用户输入的数据. 不同用户其对应的操作权限也不相同, 用户可以实现用户管理、日志查询、在线合同签署、合同查询分析、合同验签等功能.

该架构平台进行模块化处理, 将各个模块的的主要功能封装成标准服务, 有利于提升平台软件代码的重用性; 通过系统接口进行模块间良好的数据交互, 实现各模块之间的有效集成.

4 系统展示

电子签约服务平台通过强化身份认证、电子合同加密传输、合同签署公证记录、公证验真服务等系统功能, 充分保证了电子合同签署的完整性、真实性、不可否认性和有效性. 具体系统展示如下.

系统用户登录平台时, 首次完成“用户名+密码”的第一因子认证, FIDO 服务器接收到用户第二因子认证请求后, 客户端显示第二因子认证交互提示界面, 如图 8 所示, 用户按照提示插入认证令牌, 按压认证令牌按钮后完成身份认证.

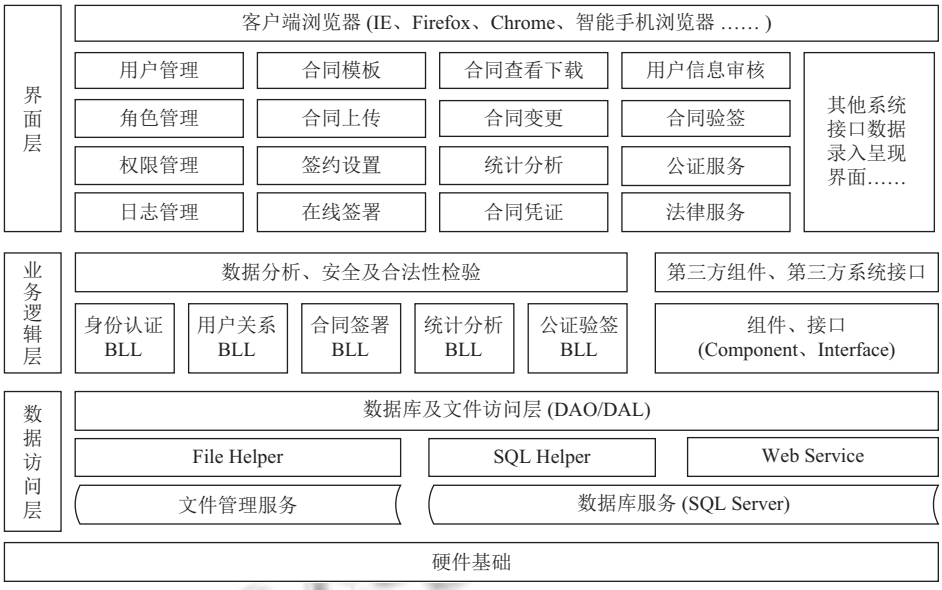

图 7 电子签约服务平台实现架构图

图 8 身份第二因子认证

签约用户成功登录电子签约服务平台后, 其具有待签合同、签署完成合同列表, 点击待签合同中的合同项, 进行内容审核并完成电子合同的公证签署, 如图 9 所示.

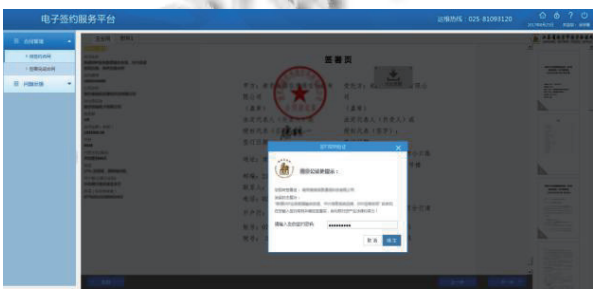

图 9 签约用户签署合同

当签约双方对签署完成的电子合同产生纠纷时, 可以向公证机构发起验真申请, 公证人员在公证服务系统上传待验真的电子合同, 进行公证验真, 如图 10 所示.

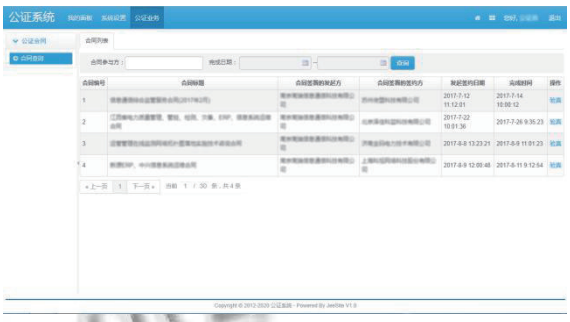

图 10 公证验真服务

5 结论

本文给出了电子签约服务平台的设计与实现方案, 通过运用身份强化认证、数据传输加密、签约过程公证记录等手段确保了平台的公平性与安全性. 统计分析功能可以使签约用户方便的掌握交易信息, 公证参与可以通过公证出证服务来有效解决交易纠纷, 平台采用“高内聚, 低耦合”的 B/S 结构降低了系统的集成难度、提高了重用性, 试运行表明平台有效提升了企业合同业务的签署效率. 在未来的优化提升中, 将进一步提供在线法律与仲裁等服务, 实现签约用户的交易一体化服务.

参考文献

1 王珉. 电子商务合同主体地位与法律关系研究——以淘宝

网 C2C 交易模式为例. 行政与法, 2012, (5): 118–121.
2 程庆水, 李青. 浅论电子商务合同的订立及其法律效力. 特区经济, 2011, (8): 245–247.
3 周洪政. 电子合同成立的相关法律问题探析. 广西大学学报 (哲学社会科学版), 2012, 34(1): 58–62.
4 Wang X, Sun J. The research of operation model for electronic contract services platform. Applied Mechanics and Materials, 2010, 40-41: 438–442. [doi: 10.4028/www.scientific.net/AMM.40-41]
5 Gu JT, Zhu XD. Designing and implementation of an online system for electronic contract negotiation based on electronic signature. Journal of Software, 2014, 9(12): 3020–3027.
6 刘树发, 柴跃廷, 刘义. 电子合同监管与公共服务平台的设计. 清华大学学报 (自然科学版), 2010, 50(5): 724–728, 734.
7 唐翠微. 网络撞库攻击信息特征潜在博弈欺骗鉴别算法. 科技通报, 2015, 31(8): 144–146.
8 王红胜, 徐子言, 张阳, 等. 基于 Hamming weight 和泄漏光子数的高级加密标准密码芯片光辐射分析攻击. 物理学报, 2016, 65(11): 118901. [doi: 10.7498/aps.65.118901]
9 张俊彦, 陈清明. 基于攻击树的安全芯片穿透性测试评估. 计算机工程, 2014, 40(6): 115–119, 124.
10 王爱文, 温涛, 张永, 等. WSN 中基于乱序多项式对偶密钥的攻击方案. 通信学报, 2015, 36(8): 2015116.
11 张紫楠, 郭渊博. 物理不可克隆函数综述. 计算机应用, 2012, 32(11): 3115–3120.
12 刘伟强, 崔益军, 王成华. 一种低成本物理不可克隆函数结构的设计实现及其 RFID 应用. 电子学报, 2016, 44(7): 1772–1776.
13 Rührmair U, Holcomb DE. PUFs at a glance. Proceedings of 2014 Design, Automation & Test in Europe Conference & Exhibition. Dresden, Germany. 2014. 1–6.
14 肖振久, 胡驰, 姜正涛, 等. AES 与 RSA 算法优化及其混合加密体制. 计算机应用研究, 2014, 31(4): 1189–1194, 1198.