Computer Science and Application 计算机科学与应用, 2020, 10(4), 601-609
Published Online April 2020 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2020.104062

Hans汉斯

Application of Mobile Two-Factor Authentication and Electronic Seal in Delivery of Goods on Site

Kai Niu[1], Fanghua Hong[1], Changhong Ge[1], Zhenhui Lv[2], Feng Xiao[3], Huanwei Wang[3]

[1]State Grid Shanghai Electric Power Company Material Company, Shanghai
[2]State Grid Shanghai Electric Power Company, Shanghai
[3]Shanghai JIULONG Enterprise Management Consulting Co. Ltd., Shanghai
Email: xiaopheng@163.com

Received: Mar. 10th, 2020; accepted: Mar. 25th, 2020; published: Apr. 1st, 2020

Abstract

Electronic seal is an effective way to solve the on-site goods handover of mobile logistics equipment. Aiming at the current situation of low efficiency of goods handover and high cost of communication between the supplier and the demander, this paper integrated PKI technology and CA certificate authentication platform to design and implement the overall framework of mobile dual factor identity authentication and electronic seal system. In the process of implementation, the international RSA encryption algorithm is used to complete the design and development of software and hardware of mobile dual factor identity authentication and electronic seal equipment, and realize the function of electronic seal. The mobile logistics equipment is applied to the on-site handover of power materials, and good results are achieved.

Keywords

Two-Factor Authentication, Electronic Seal, PKI, Delivery of Goods on Site

移动双因素身份认证及电子签章在现场货物交接中的应用

牛　凯[1]，洪芳华[1]，葛长宏[1]，吕振辉[2]，肖　锋[3]，王焕卫[3]

[1]国网上海市电力公司物资公司，上海
[2]国网上海市电力公司，上海
[3]上海久隆企业管理咨询有限公司，上海
Email: xiaopheng@163.com

文章引用: 牛凯, 洪芳华, 葛长宏, 吕振辉, 肖锋, 王焕卫. 移动双因素身份认证及电子签章在现场货物交接中的应用[J]. 计算机科学与应用, 2020, 10(4): 601-609. DOI: 10.12677/csa.2020.104062

收稿日期：2020年3月10日；录用日期：2020年3月25日；发布日期：2020年4月1日

摘　要

电子签章是解决移动物流终端现场货物交接的有效方式。针对电力物资业务现场货物交接效率低下，供需双方沟通交流成本高的现状，本文结合PKI技术、CA证书认证平台，综合设计并实现了移动双因素身份认证及电子签章系统的整体架构。在实现过程中，采用国际通用RSA加密算法，完成移动双因素身份认证及电子签章设备软硬件设计开发，实现电子签章功能。将该移动物流终端应用于电力物资现场交接，取得了良好的效果。

关键词

双因素身份认证，电子签章，PKI，现场货物交接

1. 引言

建设智慧供应链体系是国网公司建设具有卓越全球竞争力世界一流能源互联网企业的内在要求，是国网公司顺应“大云物移智边链”新技术发展的必然选择。随着新一代信息技术蓬勃发展，企业发展已进入由业务驱动向数据驱动转变的时代，新技术、新思维、新方法将引领业务运作模式、管理方法、决策思路的变革，物力集约化管理必须顺应时代发展趋势，运用新技术驱动公司供应链管理向卓越、智慧模式转变。

电力物资配送及现场交接是智慧供应链的重要环节，发挥着促进企业内部融合贯通和带动外部产业协同合作的重要作用。目前，在电力行业物流领域内具有电子签章功能的移动物流终端应用还较少。本文通过调研分析电力物资业务现场单据交接的需求，设计移动双因素身份认证及电子签章设备软硬件方案，开发出具有电子签章功能的移动物流终端。通过移动双因素身份认证，在确保移动信息安全的基础上应用该移动物流终端，实现电力物资现场交接信息化、流程化和无纸化；实现合同、单据电子签名签章应用；实现移动 APP 现场货物交接，提升物资交接验收精细化管理水平。

2. 电力物资现场交接存在的问题

由于电力物资设备类型的多样性与复杂性，为保证物资现场交接的效率和信息安全，减少供需双方沟通交流成本，在物资现场交接环节建立一套移动双因素身份认证及电子签章交接体系有一定的必要性。目前电力物资现场交接面对的挑战主要体现在：

1、合同单据电子签名签章应用

业务现状：

目前国网与供应商物资采购合同、单据为纸质文件，纸质单据签署传递较慢，供应商需要投入大量差旅与时间成本，且纸质文件容易破损、丢失，不易保存。同时，纸质单据不利于流程信息化和电子签章应用。

解决方案：

实现合同单据电子化和电子签章功能，合同签订双方通过使用国家认证的第三方电子签章设备，实现合同、单据在线审签，流转方便快捷，提高效率节省成本。

2、移动 APP 现场货物交接

业务现状：

现行管理模式下，直送项目现场的物资交接工作仍主要依赖于人工作业，由供应商、项目单位、物资部门、监理单位、施工单位等五方参与现场到货验收工作。目前物资验收环节多为人工操作，线下沟通，且涉及参与单位较多，导致业务流转效率较低。

解决方案：

依托实物 ID，开发面向供应商、物资部门、项目单位使用的移动 APP，建立科学、完善的线上收货流程，实现到货物资一键扫码收货并自动校验业务信息的一致性，及时预警可能存在的异常情况，并将到货记录的电子化信息应用于物资到货情况的分析、工程现场到货情况追溯管理、供应商履约预警管理等管理工作中。

3、物资交接验收精细化管理

业务现状：

电力物资交接验收依赖手工整理和记录，数据的及时性、准确性、规范性难以保证，且单据制作较多，业务无纸化、数字化才能满足未来发展的需要。厂验中发现的需要整改的问题无法集中保存管理和查阅，历史结果无法开展统计分析；物资交接验收数据记录存在遗漏，线下存档不利于查询和分析。

解决方案：

明确物资厂验和交接验收管理范围，建立厂验结果数据库和交接验收数据库，设计各类物资专用厂验记录卡和物资交接验收记录卡，建立物资出厂验收管理平台 APP 和物资交接验收管理平台 APP，记录厂验结果和交接验收数据，实现数据的统一管理和分析，实现物资出厂验收和交接验收精细化管理。

3. 电力物资现场货物交接解决方案

(一) 应用技术

1、PKI 技术

PKI (Public Key Infrastructure)即公开密钥体系，PKI 技术是用公钥技术提供安全服务的具有普适性的安全基础设施。它由公开密钥密码技术、数字证书、证书发放机构(CA)和关于公开密钥的安全策略等基本成分共同组成。它能给网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，提供互联网环境的身份鉴别、信息加解密、数据完整性和不可否认性服务[1]。

2、数字证书

数字证书是由权威公证的第三方认证机构(即 CA，Certificate Authority)负责签发和管理的、个人或企业的网络数字身份证明。CA 是 PKI 的核心，是 PKI 应用中权威的、可信任的、公正的第三方机构，承担着公钥体系中公钥的合法性检验的责任。CA 为每个使用公开密钥的用户发放一个数字证书，数字证书的作用是证明证书中列出的用户合法拥有证书中列出的公开密钥。CA 的数字签名使得攻击者不能伪造和篡改证书，CA 还负责吊销证书并发布证书吊销列表(CRL)，并负责产生、分配和管理所有网上实体所需的数字证书。因此，CA 是安全电子政务的核心环节。

3、电子签章

电子签章包含签字和盖章两种不同的表现形式，无论是签字还是盖章，电子签章有效性鉴定只需通过鉴定数字证书完整性即可，相较于线下签字或盖章形式真伪鉴定不便等问题，电子签章模式能够实现

快速验签，提升安全防范能力。数字证书是电子签章的基础，电子签章是数字证书的一种应用结果。电子签章是电子签名的一种表现形式，利用图像处理技术将电子签名操作转化为与纸质文件盖章操作相同的可视效果，同时利用电子签名技术保障电子信息的真实性和完整性以及签名人的不可否认性[2]。

电子签章实际上本身并非是一项“签章”，而是以使用非对称性公开密钥保密系统来完成，实质上其运作方式就是一种数学运算。相比于数字水印算法的电子签章技术，基于数字签名算法的电子签章技术应用更广泛、安全性更高[3]。

4、无线通信技术

4G 通信技术也被称为第四代移动通信技术，第四代通信技术集 3G 与 WLAN 为一体，可以在一定程度上实现数据、音频、视频的快速传输。除了 4G 通信技术外，还需要集成本地无线连接技术，它们分别是无线局域网(WiFi)、蓝牙(Bluetooth)和近距离无线传输(NFC)。

5、双因素身份认证技术

相对于最常用的用户名/密码的身份认证方法，双因素身份认证更安全。双因素身份认证是一种采用时间同步技术的系统，采用了基于时间、事件和密钥三变量而产生的一次性密码来代替传统的静态密码。每个动态密码卡都有一个唯一的密钥，该密钥同时存放在服务器端，每次认证时动态密码卡与服务器分别根据同样的密钥，同样的随机参数(时间、事件)和同样的算法计算了认证的动态密码，从而确保密码的一致性，从而实现了用户的认证。

身份认证目前有多种技术，本项目采用移动双因素身份认证技术，即蓝牙 Key + 动态口令。其认证原理：一套动态密码认证系统由认证服务器及动态令牌两部分组成[4]。

(二) 移动双因素身份认证及电子签章设备总体架构

移动双因素身份认证及电子签章设备，即移动物流终端，其总体框架包括：感知层、网络层(本地网络层/广域网络层)、边缘层、平台层/应用层。其总体框架如图 1 所示。

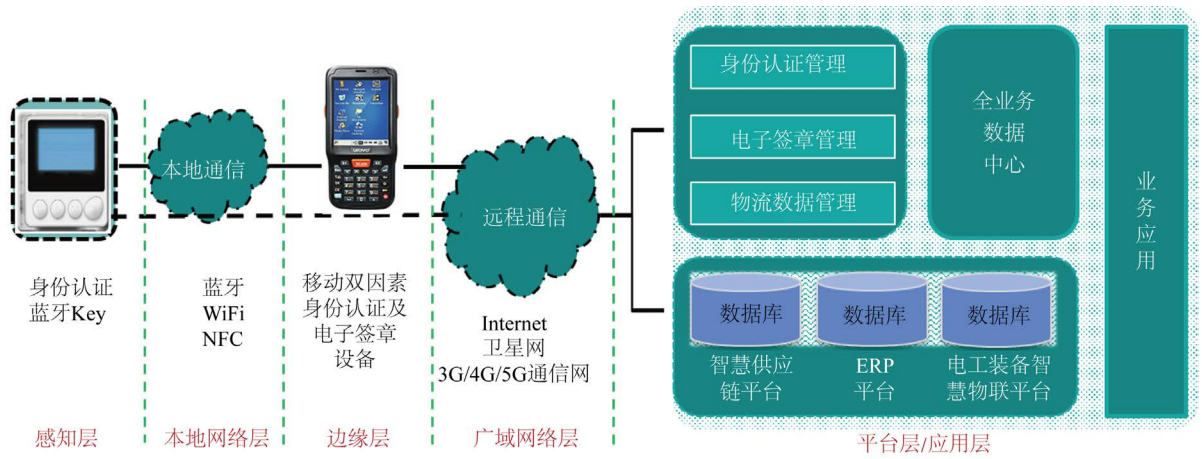

Figure 1. General framework
图 1. 总体框架

感知层：身份认证蓝牙 Key；
本地网络层：蓝牙、WiFi、NFC；
广域网络层：Internet、卫星网、专用网；
边缘层：移动双因素身份认证及电子签章设备；

应用层：身份认证管理、电子签章管理、物流数据管理；

平台层：智慧供应链平台、电工装备智慧物联平台、ERP 平台。

(三) 硬件设备解决方案

移动双因素身份认证及电子签章设备，即移动物流终端，包含四个组成部分：主控单元、无线通信单元、数据采集单元和其它单元。

主控单元：CPU 模块。CPU 模块：中央处理器是数据处理的核心模块，集成各个功能模块，进行数据运算和处理；

无线通信单元：WiFi、蓝牙模块、4G 模块、北斗、GPS；

数据采集单元：摄像头模块、RFID 模块；

其它单元：LED 显示屏、电池模块、电源控制、蜂鸣器等。

(四) 软件平台解决方案

移动双因素身份认证及电子签章软件平台 PKI 技术框架，如图 2 所示。

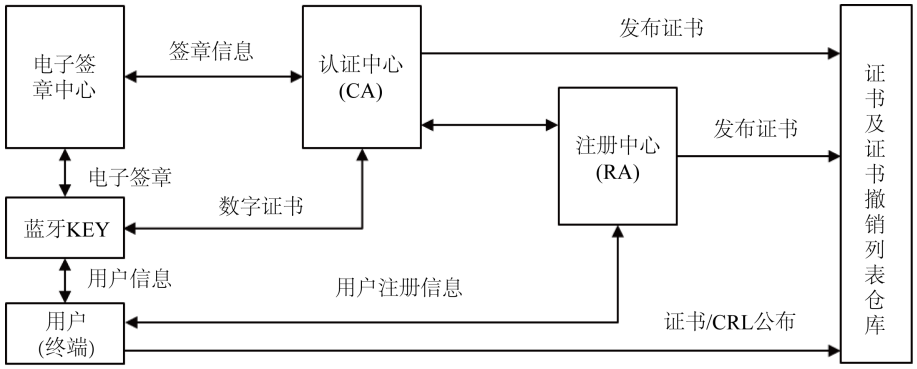

Figure 2. Platform PKI technology framework
图 2. 平台 PKI 技术框架

终端，即最终使用证书的用户，可以是普通用户，也可以是服务器。

电子签章中心，实现签章密钥管理，签章制作，签章认证服务，签章管理，包括电子签章的授权、使用、撤销、管理、维护等核心功能。

蓝牙 KEY，实现移动双因素身份认证的核心功能，包括存储用户的私钥、数字证书及密码算法。

CA (认证中心)，其核心功能是签发数字证书。通过 RA，将证书签发给最终用户。

RA (注册中心)，向最终用户提供相关证书服务的访问界面，审核用户身份，提交用户证书请求到 CA。RA 向最终用户提供的服务通常包括：证书申请、下载、查询、吊销、更新等。

证书及证书撤销列表仓库，存储证书及证书撤销列表的数据库。用户可以通过查询 CRL 来验证证书的有效性。

作为一种技术体系，PKI 可以作为支持认证、完整性、机密性和不可否认性的技术基础，从技术上解决网上身份认证、信息完整性和抗抵赖等安全问题，为网络应用提供可靠的安全保障。RSA 签名与数字水印一般的数字水印生成算法中都需要使用公钥密码学中的加密技术对原始数据进行加密，从而生成加密的水印信号，这样即使水印的提取算法被破解，窃取者也无法获得原始数据。数字签名是公钥密码学中的核心技术，将 RSA 数字签名技术与数字水印技术结合，应用于电子签章系统，是解决电子公文认证的一种更加安全有效的方案．该方案将电子公文的 RSA 数字签名用易损水印算法嵌人“图章”，将签章持有者的个人身份信息用鲁棒水印算法嵌入“图章”，实现了电子公文的信息验证与电子图章的版权

认证[6]。

移动双因素身份认证及电子签章软件功能，如图 3 所示。

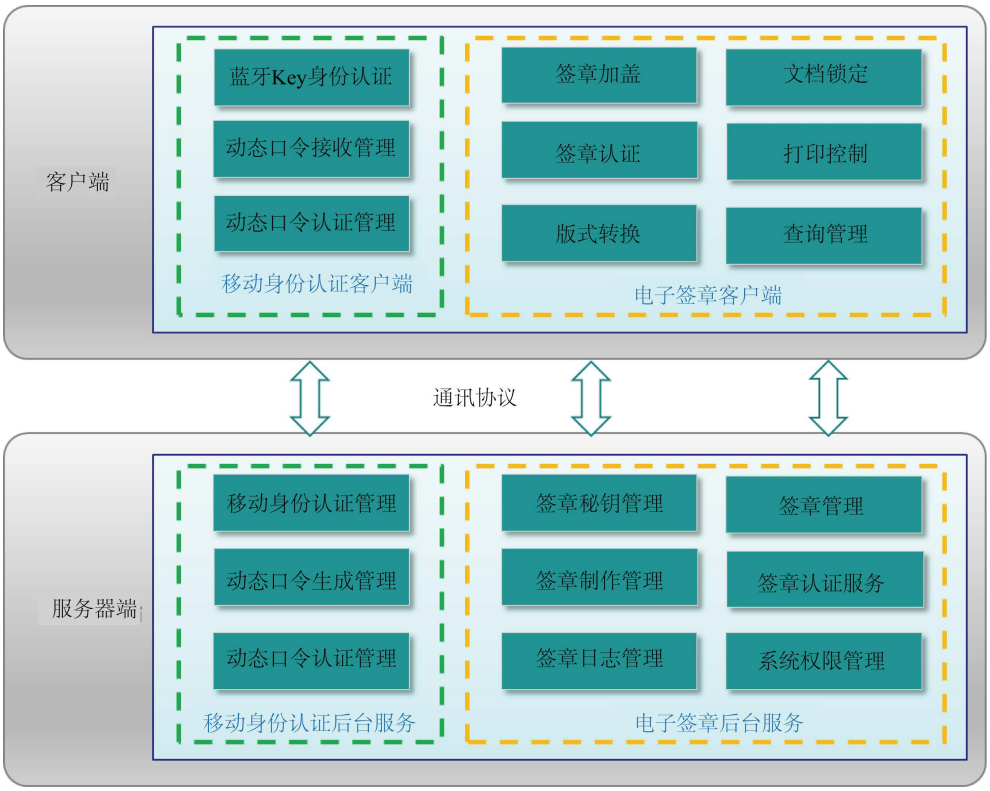

Figure 3. Software function
图 3. 软件功能

电子签章后台服务主要功能：

签章密钥管理：包括密钥制作、发放、注销、禁止、过期管理，密钥信息查看、查询、统计等功能。

签章管理：电子签章管理功能包括电子签章的授权、使用、撤销、管理、维护等一系列操作。除以上基础功能外，还支持签章权限分级管理、单次使用管理、签章使用者身份验证等功能，为企业提供便捷、安全、可靠的电子签章管理服务。

签章制作管理：包括印章制入、签字制入，制章、签字信息查看、查询、统计等功能。印章或者手写签名通过电子签章制作系统灌入到蓝牙 KEY 中，任何人都无法伪造，数字签名运算在蓝牙 KEY 内运行，确保数字签名的安全性。

签章认证服务：该模块功能包括签章验证和公文验证。签章验证是指对签章公文中的每个签章进行验证，判断公文中的签章是否由声明者签署；公文验证是指对公文进行完整性验证，同时对发送该公文的单位进行验证。

签章日志管理：包括系统日志审计、签章日志审计，日志分类、日志查询、日志统计等功能。日志信息详细记录签章的添加删除等日志信息，包括用户登录、用户 IP、操作时间等记录信息。

系统权限管理：该模块对用户、角色、组不同操作权限进行权限分配，包括授权、取消等管理。

移动身份认证后台服务主要功能：

移动身份认证管理：认证保存在蓝牙 KEY 内的数字签名是否注册、是否有效。认证用于存储用户的

私钥、数字证书及密码算法是否遭到篡改[5]。

动态口令生成管理：当移动物流终端申请发送认证码时，后台服务器模块随机生成和发送 6 位数字认证码到用户绑定手机号，有效期为 60 秒。

动态口令认证管理：服务器端系统接收移动双因素身份认证及电子签章设备客户端反馈的动态口令，并与后台发送的口令进行比较，判断口令是否一致，完成动态口令认证。

4. 移动双因素身份认证及电子签章在现场货物交接中的应用

(一) 应用流程

移动双因素身份认证及电子签章设备在电力物资现场货物交接的应用流程，如图 4 所示。

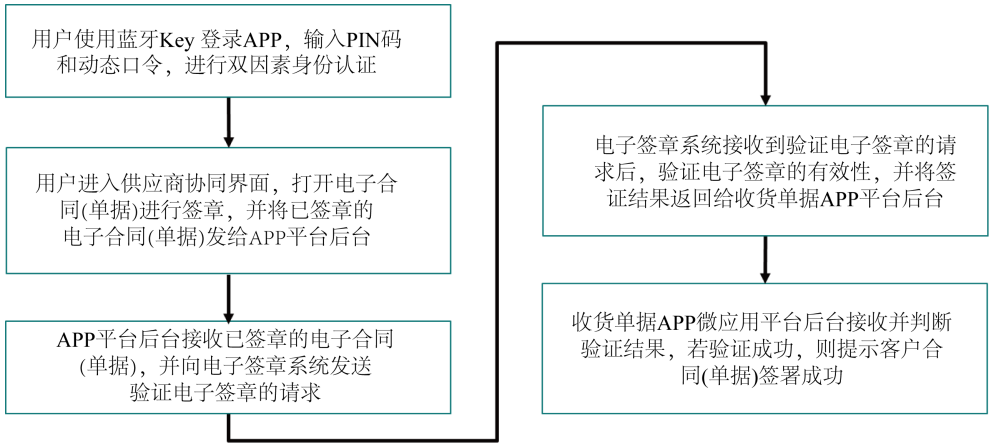

Figure 4. Application process
图 4. 应用流程

(二) 应用实例

移动双因素身份认证及电子签章设备进行现场货物验收，其操作步骤如下：

1、通过蓝牙 Key、用户密码和动态口令进行移动双因素身份认证后，登录电子签章平台网。

2、找到“待我签”的合同文件，点击“签署”。

3.添加电子签章。

若对方指定了签章位置，那么系统就会弹出提示框。这时候我们仅需点击【开始签署】，即可自动添加签章、签署日期。

系统自动添加电子签章和签署时间后，此时点击页面右上角的【下一步】，填写手机收到的验证码

即可完成签署。

确认所有盖章的信息无误后，点击页面右上角的【立即签署】，接收并填写正确的验证码即可完成签署。物资验收项目单位签章示例，如图 5 所示。

上海电力有限公司物资配送验收表

配送验收号	7342400		合同编号	XXX-00189					
卖方	XX有限公司		订单号	20190000341612					
卖方联系人/电话	张少杰/13914374016		收货联系人/电话	刘辉/13819037663					
预计发货期	2019/10/25		预计到货期	2019/10/28					
运输方式	汽车运输		承运人/电话	李明友/13857326941					
合同交货期	2019/10/30		实际交货期	2019/10/30					
序号	工程名称	物资名称	规格型号及技术参数	单位	合同数量	发货数量	退换数量	实际到货数量	交货地址
102	XXX	XXX	XXX	台	16	16	0	16	上海
验收情况	外观情况：☑合格；☐基本合格；☐不合格			货物齐全：☑是；☐否					
物流中心：签字盖章			项目单位接收人：签字盖章				供货方交付人：签字盖章		

Figure 5. Example of signature and seal of material acceptance project unit
图 5. 物资验收项目单位签章示例

5. 结束语

本文通过调研分析电力物资业务现场货物交接的需求，完成移动双因素身份认证及电子签章设备软硬件设计开发，将该移动物流终端应用于电力物资现场交接，取得了良好的效果，具有一定的应用前景。本项目实现合同、单据电子签名签章应用；实现移动 APP 现场货物交接；提升物资交接验收精细化管理水平。通过移动双因素身份认证，在确保移动信息安全的基础上实现电力物资现场交接信息化、流程化和无纸化，实现与供应商业务更广泛协同，提升智慧供应链管理水平。未来随着区块链技术的成熟应用，需要对身份认证及电子签章设备进行升级和完善。通过区块链技术确保链上数据的不可更改，依靠共识而不是中心权威节点，建立起分布式印章管理系统节点间的互信，实现异构证书域内的电子签章信息验证，达到时间无关、空间无关、认证域无关、电子签章体系无关的验证效果[7]。

参考文献

[1] 宁宇鹏. PKI 技术[M]. 北京: 机械工业出版社, 2004: 65-66.

[2] 张娴, 朱麟, 蒋建峰. 基于 PKI 技术的电子签章分析研究[J]. 科技信息, 2012(32): 285-285.

[3] 谭杰. 基于 PKI/CA 体系的电子签章系统研究与实现[D]: [硕士学位论文]. 南昌: 南昌大学, 2013.

[4] 陈卉, 徐德发. 双因素身份认证技术在上海超级计算中心的应用[J]. 高性能计算发展与应用, 2006(3): 44-45.

[5] 蒋华, 刘娟, 胡荣磊, 李浩亮. 分级管理的电子签章系统设计与实现[J]. 北京电子科技学院学报, 2013(4): 51-52.

[6] 张沈斌, 陈浩. 一种基于数字签名与数字水印认证的电子签章系统[J]. 苏州大学学报: 自然科学版, 2011(2): 27-32.

[7] 李强, 高超航, 何智, 谢京涛. 一种基于区块链的电子签章验证平台设计[J]. 信息安全研究, 2019, 5(12): 1089-1095.