计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(7):78−83 [doi: 10.15888/j.cnki.csa.006435]

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

EAST 远程等离子体控制门户系统的安全管理①

李　刍[1], 肖炳甲[1,2], 袁旗平[2], 张睿瑞[2]

[1](中国科学技术大学, 合肥 230022)
[2](中国科学院 合肥物质科学研究院, 合肥 230031)
通讯作者: 袁旗平, E-mail: qpyuan@ipp.ac.cn

摘　要: EAST 装置是世界上第一个非圆截面全超导托卡马克核聚变实验装置, 已经发展成为国际上重要的合作实验平台. 为扩大和方便合作单位参与实验, 提出开发 EAST 远程等离子体控制系统, 系统采用 Web 开发模式, 其功能是为远程客户提供获取实验数据、即时控制服务和放电方案设置服务. 其门户系统设计主要负责身份验证与授权、请求格式检查和技术数据检查等安全性功能. 身份验证与授权阶段采用三阶段验证, 主要采用 VPN, 数字证书和随机验证码等网络安全技术. 请求格式检查和技术数据检查采用模块化技术, 针对不同放电方案单独编写模块, 保证系统的可扩展性.

关键词: EAST; 远程系统; 数字证书系统; 短信平台; 安全模块

引用格式: 李刍,肖炳甲,袁旗平,张睿瑞.EAST 远程等离子体控制门户系统的安全管理.计算机系统应用,2018,27(7):78−83. http://www.c-s-a.org.cn/1003-3254/6435.html

Security Management of EAST Remote Plasma Control Portal System

LI Chu[1], XIAO Bing-Jia[1,2], YUAN Qi-Ping[2], ZHANG Rui-Rui[2]

[1](University of Science and Technology of China, Hefei 230022, China)
[2](Hefei Institutes of Physical Science, Chinese Academy of Sciences, Hefei 230031, China)

Abstract: EAST device is the world's first non-circular cross-section superconducting Tokamak nuclear fusion experimental device, and has developed into an important international cooperation experimental platform. In order to expand and facilitate the cooperation unit to participate in the experiment, the development of EAST remote plasma control system is proposed, the system uses Web development model, functioning to provide remote customers with access to experimental data, real-time control services, and discharge program settings services. The portal system design is mainly responsible for authentication and authorization, request format inspection and technical data check, and other security features. Authentication and authorization phase use three-stage verification, the main technology includes VPN, digital certificates, random verification code, and other network security technology. Request format check and technical data check use modular technology, for different discharge program, a separate module is written to ensure system scalability.

Key words: EAST; remote system; digital certificate system; SMS platform; security module

随着磁约束核聚变科学研究的蓬勃发展, 聚变装置托卡马克在规模、复杂性以及运行费用上不断增长. 为了提高合作的便捷性, 利用先进计算机技术、网络技术构建远程合作研究平台, 可以避免传统合作方式带来的地理位置的局限性和人员精力财力的浪费, 从而推进聚变研究的发展. 随着 32 s 的 H 模和 400 s 长脉冲等离子体运行的实现和一系列物理成果的获得, EAST 已经发展成为国际上重要的合作实验平台, 因此

① 基金项目: 国家重点基础研究发展计划项目 (973 计划)(2014GB103000)
Foundation item: National Program on Key Basic Research Project of China (973 Program)(2014GB103000)
收稿时间: 2017-11-06; 修改时间: 2017-11-27; 采用时间: 2017-12-15; csa 在线出版时间: 2018-06-27

发展 EAST 上的支持远程参与的先进等离子体控制系统, 针对 EAST 等离子体远程控制的需要, 开发基于 Web 的远程等离子控制系统有着重要的意义. 基于 Web 的远程等离子体控制系统基本功能框图如图 1 所示, 主要由操作请求门户系统、即时控制服务系统、放电策略管理系统和等离子体控制 (Plasma Control System, PCS) 构成, 门户系统设计主要负责身份验证与授权、请求格式检查和技术数据检查. 当远程实验人员通过 Web 界面提交操作请求后, 将经过门户系统进行严格的安全和有效性检查, 有效的操作请求通过接口与 PCS 服务进程或者放电方案管理服务通讯, 实现等离子体放电参数的远程设置. 同时 PCS 运行的状态和本地设置参数可实时回馈给远程实验人员并在界面上显示.

如今网络的技术日益成熟, 黑客对服务器攻击逐步转移到针对应用系统, 例如 Web 站点等, 根据 Gartner Group 的调查, 信息安全攻击有 75% 都发生在 Web 应用层面上. EAST 远程等离子体控制系统连接国家大型热核聚变实验装置, 因此其门户系统是远程等离子体控制系统安全的重要因素.

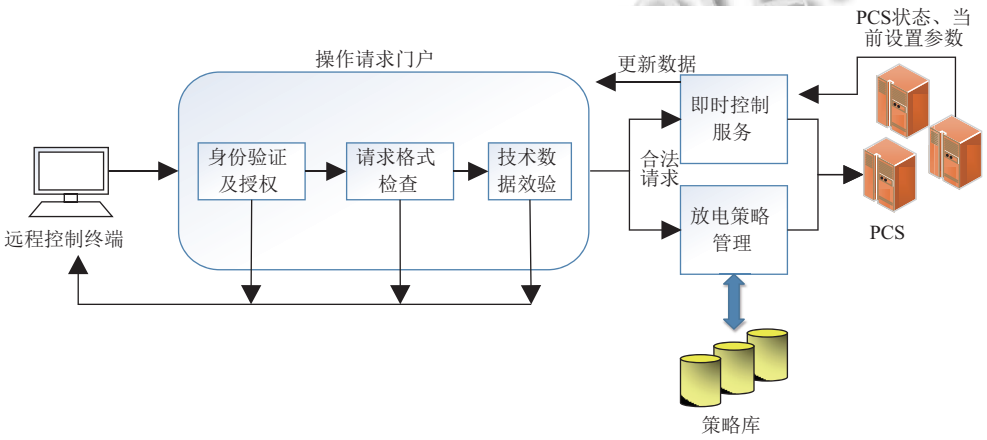

图 1 远程等离子体控制系统基本功能框图

1 门户系统总体原则和技术选择

1.1 设计总体原则

完善的纵深防御体系是 Web 站点安全的重要保证. 总体上纵深防御体系分为技术层面和管理层面两部分. 本文主要从技术层面进行对系统进行分析. EAST 远程等离子体控制系统涉及重大装置实验, 要求系统比较高的安全性能, 根据纵深防御体系原则, 设定门户系统安全性能要求[1–5]如下:

1) 用户需要登录认证;

2) 所有用户访问有记录;

3) 用户提交的数据必须有相应权限;

4) 提交数据必须符合相应的规则限制;

5) 所有提交数据有记录 (特别是有危险性的数据绕过前端和后端提交到 EAST 等离子体控制系统要及时通知管理员).

1.2 系统的技术选择

C/S(Client/Server) 结构和 B/S(Browser/Server) 结构是常用的应用系统软件结构, B/S 结构在客户端采用浏览器, 不用针对不同的操作系统开发专门的客户端软件, 具有跨平台属性, 具有开发速度快, 成本小特点. 特别是 Web2.0 时代, B/S 结构被广泛应用. B/S 结构采用 AJAX 在客户端进行局部处理, 增强了交互性, 实现实时刷新. 因此 EAST 远程等离子体控制系统其门户系统采用 B/S 结构进行设计开发.

VPN 是基于公共网络或其他网络的一种特殊通道, 其本质是一个逻辑的点到点链接, 这个链接为隧道的两个端点提供了认证、加密和访问控制, 可以提高服务器安全性. EAST 远程等离子体控制系统设定为中国科学院等离子体物理研究所的内网, 世界各地合作单位在实验期间开通 VPN 服务连接到中国科学院等离子体物理研究所所网后访问 EAST 远程等离子体控制门户系统服务器. VPN 在一定程度上加强了 EAST 远程等离子体控制门户系统的安全性, 提高了系统的服务质量.

HTTPS 双向认证在 HTTP 的基础上加入了 SSL 协议, SSL 协议依靠数字证书来验证服务器和客

户端的身份, SSL 协议为浏览器和服务器之间的通信加密. 相比于 HTTPS 单向认证, 双向认证增强了服务器对客户端的认证, 有效降低非法用户访问门户系统. EAST 用户必须安装服务器数字证书中心颁发的数字证书, 同时用户必须接受 EAST 服务器数字证书, 双方完成数字证书认证之后才进行正常通信. HTTPS 双向认证保证只有合法的客户端才可以访问 EAST 远程等离子体控制门户系统服务器. 数字证书一般放置在专门 USB 或者安装在浏览器中, 数字证书安装在浏览器中比放置专门的 U 盘中使用方便, 不需要针对不同操作系统开发不同 USB 插件, 降低了开发成本.

验证码的功能主要是防止黑客使用程序恶意注册、暴力破解或批量发帖. 用户肉眼识别其中的验证码信息, 输入表单提交网站验证, 验证成功后才能提交数据. 随机验证码一定程度提高了系统的安全性. 邮箱验证和手机验证一般作为认证用户资料的一种方式, 同时发送验证码作为确认用户信息的验证. 邮箱和手机私密性比较高, 被窃取的可能性小. 邮箱属于虚拟物品, 手机是实物, 在安全性上手机验证码安全性高于邮箱验证码. EAST 远程等离子体控制系统属于内网, 无法利用外部短信平台发送短信, 而且存在手机号泄露风险, 建立 EAST 门户系统的专用短信平台, 不仅用户方便登录, 而且增强门户系统的安全性. EAST 用户在世界各个地方登录 EAST 远程等离子体控制系统, 国外用户可以通过邮箱验证码登录系统, 国内用户可以采用手机验证码或邮箱验证码登录系统.

2 系统实现

2.1 系统网络拓扑架构

系统网络拓扑图如图 2 所示, EAST 远程等离子体控制门户系统属于等离子所内网, 外部研究所单位和办公地点需要通过 VPN 通道进入所网访问 EAST 远程参与服务器. EAST 远程参与服务器通过内部网络访问 EAST 服务器群获取所需数据[4,6], 提供给用户. 短信平台和和邮箱系统属于门户系统的附属系统, 其功能是给用户发送邮箱验证码和手机验证码.

EAST 远程等离子体控制门户系统采用基于 MVC 设计模式的国产优秀 ThinkPHP 开源框架稳定版本. ThinkPHP 框架是一款性能卓越功能丰富的轻量级 PHP 开发框架, 支持 ORM 实现、扩展机制、分组模块、数据库特性和视图模型等众多优点. 优秀的开源框架通过专业人士不断迭代, 完善框架安全, 经过更多人的测试, 比自己单独开发更加安全, 设计更加完善. 采用 ThinkPHP 框架可以加快开发和迭代速度, 更好更快的完善系统, 降低系统开发成本.

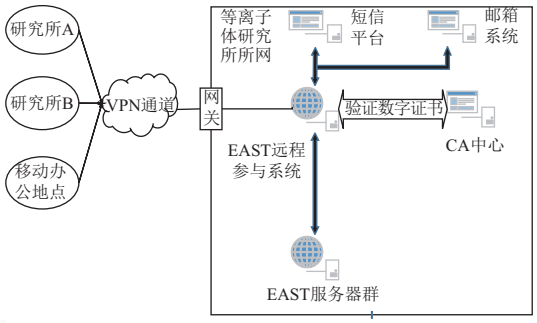

图 2 系统拓扑图

2.2 数字证书系统

EAST 远程等离子体控制门户系统数字证书系统搭建基于 OpenSSL 开源软件包. OpenSSL 软件由于其开源性使它经过众多开发和应用者的改进和完善的, 可以直接下载编译使用, 安全性可以保证, 开发容易, 是小范围系统使用自建数字证书系统的主要选择. OpenSSL 软件主要包含三大体系: 密码算法库体系、SSL 协议库体系和应用程序体系, 使用该软件包可以直接生产符合 X.509 标准的数字证书, 其中的 CA 应用程序是一个证书管理中心 (如图 2 中 CA 数字证书中心), 可以实现整数签发管理的整个流程, 修改 OpenSSL 配置, 实现 HTTPS 双向认证, 从而实现系统的身份认证功能[7–10].

2.3 门户系统短信平台

手机短信平台的构建是基于工业级 WAVE 短信猫、JAVA 和 Mysql 数据库技术. WAVE 短信猫是成熟的工业产品, 常用于公司内部短信平台的构建. 短信平台放置在 EAST 远程等离子体控制门户系统的下, 设定为只允许 EAST 远程系统访问, 拒绝其他用户随意使用, 降低短信平台被攻击的可能性. 短信平台采用单例模式开发, 数据库设定为三张表: 用户表、待发送表和发送结果表. 用户表限制发送请求人的范围, 每人都有每天数量限制, 以提高平台稳定性. 门户系统把发送短信内容和手机号写入短信发送数据库待发送表, 短信平台主机不停地扫描短信发送数据库并发送短信, 成功后写入发送结果表, 门户系统查询发送结果表.

2.4 身份验证与授权

身份验证与授权分为数字证书认证和登录认证两部分. 数字证书认证部分用户需要向管理员申请数字证书, 管理员向 EAST 远程等离子体控制门户系统的 CA 中心申请数字证书发给用户, 用户在客户端 (浏览器) 安装数字证书后[4,6], 访问的 EAST 远程等离子体控制门户系统的登录页面登录, EAST 远程等离子体控制门户系统的数字证书申请和验证流程. 在 HTTPS 双向认证的基础之上, EAST 门户系统设计为用户每次采用用户名+密码+随机验证码+邮箱验证码/手机短信验证码进行登录 (如图 3). 例如用户输入用户名密码后点击选择手机验证码后, 门户系统验证用户名密码, 然后通过用户数据和 LDAP 用户数据库进行验证, 当验证通过时, 查询用户手机号, 同时生成六位随机验证, 并向短信平台短信数据库写入发送内容和手机号, 用户填入手机验证和随机验证码后, 门户系统进行综合验证. 用户成功登录后获得相应的授权, 同时在登录界面设置本次操作的类型, 即时控制或方案设置. 用户信息及权限在用户管理数据库中记录, 登录界面从后台数据库中读取信息进行验证. 这种远程操作人员身份的双重验证, 可有效保证系统的安全. 用户可以在用户后台看到自己权限和个人资料, 可以完善手机号等信息, 可以查看自己拥有的权限并可以向管理申请提高权限. 管理员后台可以查看和修改所有人拥有的权限, 查看所有人登录记录和提交数据记录.

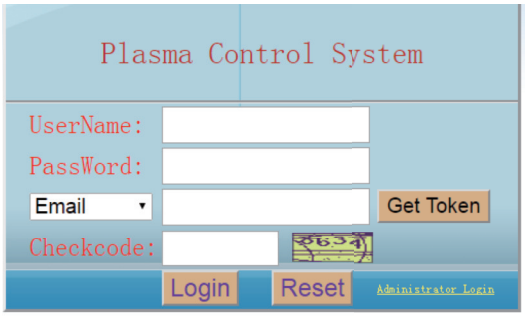

图 3 用户登录界面

2.5 请求格式检查和技术数据检查

根据远程用户操作类型的选择, 获得界面数据, 反馈到用户操作界面. 若选择了即时控制服务, 则获得当前本地控制系统所有预设信息; 而方案预设服务则可选从历史炮、已有方案中调用, 界面上的所有数据从调用文件中获得, 或者是选择默认界面. 当完成界面参数的设置并提交后, 产生一个远程请求给操作请求门户系统, 首先对请求格式按照预先的定义进行检查, 若格式不符合规范, 则可能是网络传输中造成了错误, 结果反馈给用户界面. 若格式正确则进行更为严格的技术数据检查, 如图 4 所示, 检查规则由一系列的逻辑模块构成, 如 EAST 极向场电源的最大电压限定值, 线圈电流最大值, 等离子体密度设置范围等. 采用逻辑模块的方式, 便于各系统定义检查规则并纳入门户系统中. 请求格式检查和技术数据检查是对用户提交实验数据设定的存储和数据效验规则. 为减轻 EAST 服务器的压力, EAST 远程等离子体控制门户系统设计在前端用 js 编写请求格式检查验证, 在服务器端用 php 再次编写请求格式检查和技术数据检查模块对提交数据再次验证, 防止黑客绕过前端直接提交同时对数据进行保存, 在 EAST 服务器请求格式检查和技术数据检查模块做最后验证, 最大限度过滤非法数据提交. 用户后台可以查看自己数据提交记录和自己的权限, 可以沟通管理员提高权限. 管理员后台可以修改所有用户的权限和查看用户提交所有数据记录.

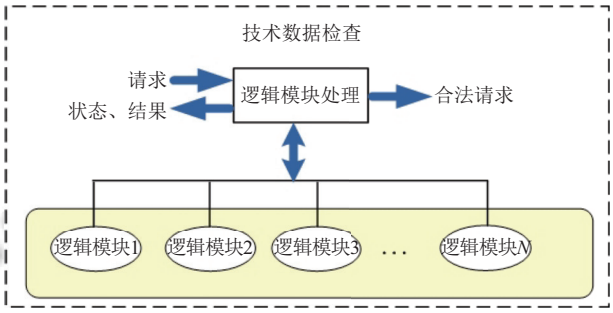

图 4 技术数据检查功能模块

3 测试应用

EAST 远程等离子体控制门户系统部署环境: centos6.7 稳定版, Apache2.2.15, mysql 14.14 稳定版. 短信平台部署环境: windowserver2008R2 版本, mysql 14.14 稳定版. EAST 远程等离子体控制门户系统的 CA 证书中心部署环境: centos6.7 稳定版. 按照企业测试流程编写测试计划、流程和测试用例, 分别进行 UI 测试、链接测试、表单测试、输入域测试、分页测试、交互性测试、功能测试和安全测试.

首先测试系统是否实现 HTTPS 双向认证: 用户必

须有经过管理员颁发数字证书才可访问 EAST 远程等离子体控制门户系统, 否则会提示服务器要求客户端提供合法数字证书. 其次进行登录功能验证测试、后台管理功能测试和用户后台测试, 经过大量测试实现预定目标. 针对手机验证和邮箱验证码功能测试, 对于邮箱验证功能测试主要在门户系统服务器端, 经过大量测试, 门户系统可以正常发送邮箱验证码. 针对短信验证功能测试包括服务器端功能测试和短信平台测试两部分, 需要编写专门的测试计划, 先测试程序无 BUG, 再进行连接 WAVE 短信猫进行发送短信测试以节约测试成本, 通过不同方案测试测试短信平台是否可以稳定运行, 经过专业测试证实短信平台可以正常工作. 测试权限验证是否有效, 用户首次登录时用户名密码来源于 LDAP 账户, 用户只有读的权限操作, 用户可以在后台完善个人信息 (手机号等)、向管理员申请提高权限. 权限测试如图 5 所示, 用户在一部分的 category 上具有写的权限, 其他部分只有读的权限, 当只有读的权限时, 用户无法提交当前 category 方案的数据. 测试技术数据检查模块是有效, 例如 PS1 放电方案约束电流值为[–350, 350], 当用户提交数据超过约束电流值范围时, 系统提示用户设定数据不符合规范, 请进行修改 (如图 6 所示). 经过大量测试, 格式检查和技术数据检查模块完全实现预期设定目标, 同时保证了系统的可扩展性.

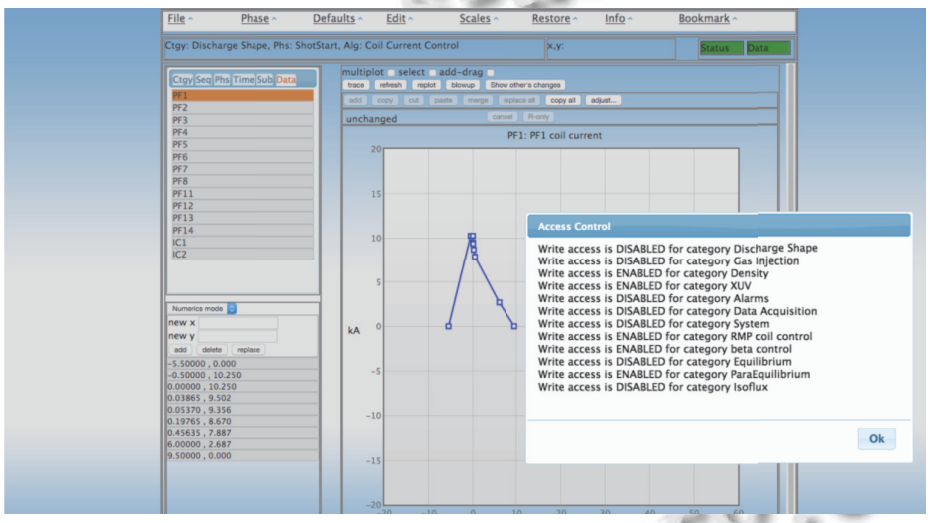

图 5 权限检查

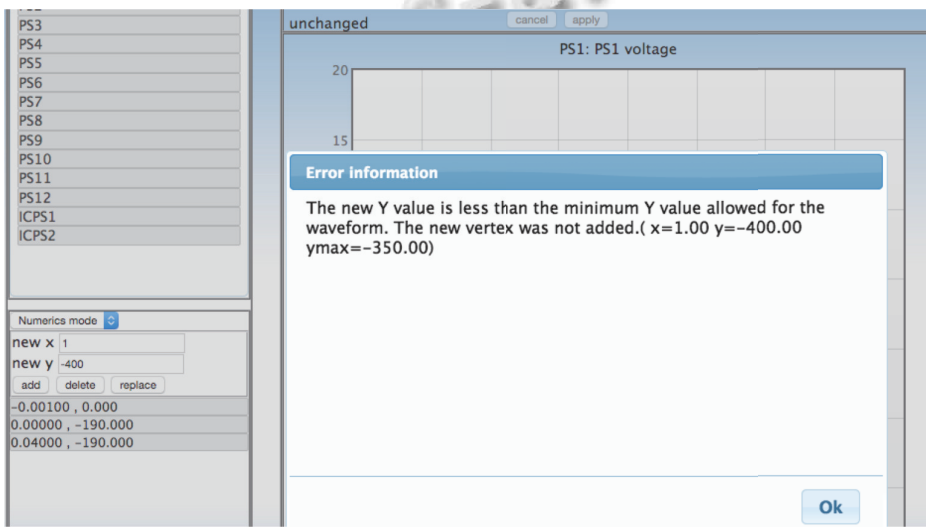

图 6 数据有效性检查

4 总结

EAST 远程等离子体控制门户系统采用 VPN、数字证书认证系统和 ThinkPHP 框架等技术构建了完善的纵深防御体系, 保证了系统的安全性, 实现了 EAST 远程等离子体控制门户系统的身份验证与授权、请求格式检查和技术数据检查功能, 系统采用成熟的 java 和 WAVE 短信猫构建了 EAST 远程等离子体控制门户系统的短信平台, 同时利用现有的邮箱系统实现邮箱验证码发送, 建立功能完善的邮箱验证码和短信验证码发送功能. 采用独立的技术数据检查模块对各个放电方案分别进行检查, 保障了系统可扩展性. EAST 远程等离子体控制门户系统设计和实现三大设定功能目标, 保证了远程等离子体控制系统的安全性、可扩展性和易维护性, 后续工作主要是根据科研工作需要进行扩展和升级门户系统功能.

参考文献

1 Stepanov D, Abla G, Ciarlette D, *et al*. Remote participation in ITER exploitation-conceptual Design. Fusion Engineering and Design, 2011, 86(6-8): 1302–1305. [doi: 10.1016/j.fusengdes.2011.01.120]

2 Lister JB, Farthing JW, Greenwald M, *et al*. The ITER CODAC conceptual design. Fusion Engineering and Design, 2007, 82(5-14): 1167–1173. [doi: 10.1016/j.fusengdes.2007.01.013]

3 TER Project Requirements. ITER D 27ZRW8 v4.6. ITER baseline documentation, 2010.

4 Schissel DP, Abla G, Fredian T, *et al*. An investigation of secure remote instrument control. Fusion Engineering and Design, 2010, 85(3-4): 608–613. [doi: 10.1016/j.fusengdes.2010.03.019]

5 Yuan QP, Xiao BJ, Zhang RR, *et al*. The design of remote participation platform for EAST plasma control. Fusion Engineering and Design, 2016, (112): 1045–1048. [doi: 10.1016/j.fusengdes.2016.04.044]

6 Schissel DP, Farthing JW, Schmidt V. Advances in remote participation for fusion experiments. Fusion Engineering and Design, 2005, 74(1-4): 803–808. [doi: 10.1016/j.fusengdes.2005.06.066]

7 关振胜. 公钥基础设施 PKI 及其应用. 北京: 电子工业出版社, 2008.

8 林东岱, 曹天杰. 应用密码学. 北京: 科学出版社, 2009.

9 Peng YH. The application of PKCS#12 digital certificate in user identity authentication system.2009 WRI World Congress on Software Engineering. Xiamen, China. 2009. 351–355.

10 Hsu CM. A group digital signature technique for authentication. IEEE 37th Annual 2003 International Carnahan Conference on Security Technology. Taipei, China. 2003.