网络身份识别系统在电子商务中的研究与应用

顾 青[1],梁佐泉[2],汪 治[2],徐 祺[2]
(1. 国家863计划信息安全基础设施研究中心,上海 201112;
2. 上海普华诚信信息技术有限公司,上海 201112)

摘 要:根据我国电子商务的现状和存在的问题,提出构建网络身份识别系统,分析了系统总体架构中的网络身份签发系统、网络身份注册管理系统、网络身份存储发布系统、网络身份状态查询系统和密码服务系统及系统的网络拓扑,给出了营业执照电子副本和第三方CA数字证书的整合技术,并对系统接口进行了详细设计。最后结合电子商务的实际情况,将网络身份识别系统应用于工商行政管理中的亮照经营,从而保障网上交易的顺利开展,为我国电子商务的健康发展提供了技术支撑。

关键词:网络身份识别系统;营业执照电子副本;数字证书
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2011)11-0247-03

Research and Application of Network Identity Authentication System in Electronic Business

GU Qing[1], LIANG Zuo-quan[2], WANG Zhi[2], XU Qi[2]
(1. National 863 Program Information Security Infrastructure Research Center, Shanghai 201112, China;
2. Shanghai Puhua Trust Information Technology Co., Ltd., Shanghai 201112, China)

Abstract: According to the current situation and existing problems of e-commerce, network identity authentication system is proposed, the general frame including network identified and issuanced system, network identified and managed system, network identified and storage issued system, network identified and state queried system and password service system and network topology of the system are analyzed, integrated technology of electronic duplicate of business license and digital certificate of the third-party CA is studied, and the detailed design of system interface is given. Finally, combining with the application of e-commerce, put network identity authentication system to use the licensed marketing in industrial and commercial administration, which gave a good passport for online transactions, and provided the technical support for the healthy development of e-commerce.

Key words: network identity authentication system; electronic duplicate of business license; digital certificate

0 引 言

随着信息技术的不断发展以及商业模式的不断创新,电子商务已经成为我国经济发展"调结构、促转型"的重要抓手。截至2010年12月,我国电子商务市场交易额已逾4.5万亿。其中B2B电子商务交易额达到3.8万亿,约占全年社会商品零售总额的3%,未来电子商务将有更大的市场应用前景[1]。但是我国电子商务处于发展阶段,对于网络市场的管理目前还未形成切实有效的监管体制。网上交易的行业和地区发展不平衡,网上交易的法律法规和技术标准等环境体制建设还不完善,交易双方的诚信等不能保证,存在不正当竞争、商业欺诈、网上虚假广告等诸多问题[2]。

收稿日期:2011-04-07;**修回日期**:2011-07-17
基金项目:国家科技支撑计划项目(2009BAH43B03);科技型中小企业技术创新项目(10C262131039083)
作者简介:顾 青(1972-),男,博士,主要从事电子政务信息安全领域的研究。

1 网络身份识别系统的设计

1.1 系统总体架构

工商行政管理电子商务网络身份识别系统总体结构如图1所示,包括网络身份签发系统、网络身份注册管理系统、网络身份存储发布系统、网络身份状态查询系统和密码服务系统等。

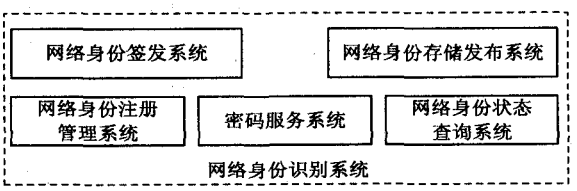

图1 网络身份识别系统体系结构

网络身份注册管理系统提供营业执照电子副本申

请、审核、下载、安全管理、安全审计、智能密码钥匙管理等功能，由注册管理、面向工商业务系统接口、数据库、信息录入、信息审核、副本制作、安全管理以及安全审计等模块构成。

网络身份签发系统提供营业执照电子副本签发、变更、吊销、吊销恢复、注销、发布、副本注销列表 EBLRL 生成与发布、副本模板管理等功能，由副本/副本注销列表 EBLRL 生成与签发、安全管理、安全审计、数据库、目录服务器以及密码设备等模块构成[3]。

网络身份存储发布系统提供营业执照电子副本和副本注销列表 EBLRL 的存储与发布功能，由从目录服务器、安全管理、安全审计等模块构成。

网络身份状态查询系统为用户以及应用提供营业执照电子副本状态查询及副本信息查询服务功能，由状态管理、接口服务、数据库、查询服务、权限管理、安全管理以及安全审计等模块构成。

密码服务系统包括服务器密码机和智能密码钥匙，均采用通过国家密码管理局鉴定的相关设备，提供数据加解密、签名及签名验证、产生随机数、数字摘要等多种密码服务，以及营业执照电子副本存储及密钥管理服务[4]。

1.2 系统网络拓扑

网络身份识别系统部署于工商行政管理业务网，可以与工商行政管理业务系统结合实现营业执照电子副本的签发和发放；在工商行政管理外网部署营业执照电子副本存储发布子系统、营业执照电子副本状态查询子系统，提供营业执照电子副本发布和状态查询服务。

企业登记系统、企业管理系统、个体工商户管理系统等通过工商行政管理业务网能够与网络身份识别系统进行网络互通，为了保证系统的安全性，网络身份识别系统与其它工商行政管理业务系统之间部署防火墙；注册管理系统和签发管理系统之间部署防火墙。

1.3 系统与第三方 CA 数字认证体系相结合

网络身份识别系统签发的营业执照电子副本用于工商行政管理部门对网络市场经营主体的准入、确认、监管和服务，代表政府的公信力，是非赢利性质。

第三方数字证书认证系统签发的数字证书用于网络市场经营主体参与电子商务、电子政务活动的数字签名，保证行为不可抵赖、数据完整性和机密性等，代表社会的公正力，是赢利性质。

网络身份识别系统与第三方数字证书认证系统两者相辅相成，互为补充，是政府公信力和社会公正力的有机结合，共同支撑我国电子商务向纵深发展[5]。

图2 所示为网络身份识别系统与第三方数字证书认证体系融合方案。其中，为保证系统交互的安全性，在省级工商行政管理部门网络身份识别系统中增加与数字证书认证中心衔接服务子系统，在数字证书认证中心增加与网络身份识别系统衔接服务子系统，用于发放数字证书的同时发放营业执照电子副本。

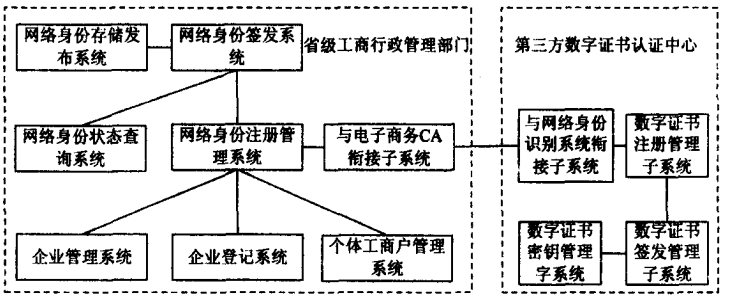

图2 系统与第三方 CA 数字认证体系的结合

1.4 系统接口设计

网络身份识别系统的接口为业务应用提供营业执照电子副本的查询验证、基于副本的密码计算、网上市场主体基础信息查询的接口服务，为企业登记系统提供副本的签发接口等功能。这里以营业执照电子副本（下称'执照副本'）查询验证接口为例，进行分析设计[6]。

1.4.1 '执照副本'注销列表获取副本注销状态

```
原型:int ECOBL_VerifyECOBLByECrl(
        void * hAppHandle,
        unsigned char * pucECOBL,
        unsigned int uiECOBLLen
        unsigned char * pucDerECrl,
        unsigned int uiDerECrlLen)
```

描述：根据副本注销列表文件验证营业执照电子副本是否被注销[7]。

参数：hAppHandle[in] 应用接口句柄
pucECOBL [in] DER 编码的副本
uiECOBLLen[in] 副本长度
pucDerECrlin[ ] DER 编码的 ECRL
uiDerECrlLen ECRL 长度

返回值：0 成功
非 0 失败，返回错误代码

1.4.2 '执照副本'状态查询系统获取副本状态

```
原型:int ECOBL_GetECOBLByOESP(
        void * hAppHandle,
        char * pcOespHostIp,
        unsigned int uiOespPort,
        unsigned char * pucUsrECOBL,
        unsigned int uiUsrECOBLLen);
```

描述：从副本状态查询系统获取用户副本的实时

状态[8]。

参数:hAppHandle[in]　应用接口句柄

pcOespHostIp[in]　副本状态查询系统服务器 IP 地址

uiOespPort[in]　副本状态查询系统服务器端口

pucUsrECOBL[in]　DER 编码副本

uiUsrECOBLLen[in]　副本长度

返回值:0 成功

非 0 失败,返回错误代码

1.4.3　目录服务查询营业执照电子副本接口

原型:int ECOBL_GetECOBLFromLdap(

void * hAppHandle,

char * pcLdapHostIp,

unsigned int uiLdapPort,

unsigned char * pucSubDN,

unsigned int uiSubDNLen,

unsigned char * pucOutECOBL,

unsigned int * puiOutECOBLLen);

描述:通过 LDAP 方式获取副本[9]。

参数:hAppHandle[in]　应用接口句柄

pcLdapHostIp[in]　ldap 服务器 IP 地址

uiLdapPort[in]　ldap 服务器端口

pucSubDN[in]　需要查找的副本的 DN

uiSubDNLen[in]　需要查找的副本的 DN 长度

pucOutECOBL[out]　找到 DER 编码的副本

puiOutECOBLLen[out]　找到的副本长度

返回值:0 成功

非 0 失败,返回错误代码

1.4.4　目录服务系统获取'执照副本'注销列表

原型:int ECOBL_GetECrlFromLdap (

void * hAppHandle,

char * pucLdapHostIp,

unsigned int uiLdapPort,

unsigned char * pucECrlData,

unsigned int * puiECrlDataLen);

描述:通过 LDAP 方式根据副本获取对应的 ECRL[10]。

参数:hAppHandle[in]　应用接口句柄

pucLdapHostIp[in]　ldap 服务器 IP 地址

uiLdapPort[in]　ldap 服务器端口

pucECrlData[out]　获取的 DER 编码的 ECRL 文件[11]

puiECrlDataLen[out]　ECRL 文件长度

返回值:0 成功

非 0 失败,返回错误代码

2　网络身份识别系统的应用

国家工商行政管理总局发布的《网络商品交易及有关服务行为管理暂行办法》中规定"已经在工商行政管理部门登记注册并领取营业执照的法人、其他经济组织或者个体工商户,通过网络从事商品交易及有关服务行为的,应当在其网站主页面或者从事经营活动的网页醒目位置公开营业执照登载的信息或者其营业执照的电子链接标识"[12]。营业执照电子副本作为电子商务企业在网络中的"身份证",如同在现实世界中一样,电子商务企业在其经营网站中悬挂营业执照电子副本-"亮照经营",一方面是政府部门依法监管的需要,另一方面也是企业自身诚信经营的需要。

在电子商务交易中,商家在网上商铺"亮照经营",顾客可以点击网上商铺的营业执照电子副本标识验证其市场主体身份合法性,如果顾客要更进一步看商家的信用信息,则需要商家授权。顾客确认商家市场主体身份合法性和信用信息后,即可利用电子商务第三方数字证书与商家进行合同签订、电子支付等,从而保障电子商务交易的顺利开展。

"亮照经营",需提供营业执照电子副本在线查询验证服务,供电子商务企业交易过程中对企业注册登记信息及信用信息进行查询,规范企业交易行为[13]。

网上亮照系统体系架构如图 3 所示,网络亮照系统作为省级工商行政管理局营业执照电子副本外网服务体系的重要组成部分,与营业执照电子副本存储发

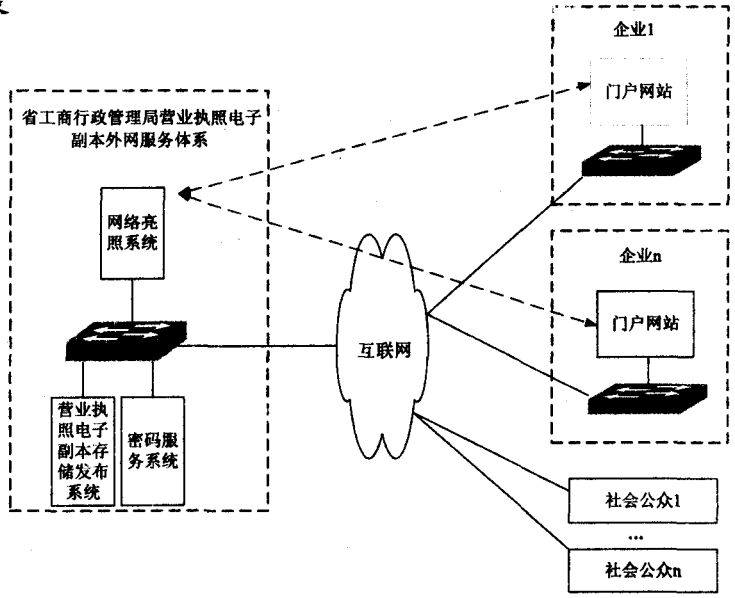

图 3　网络亮照系统体系结构

(下转封三)

状况的“和”，这样将下层的各个节点联系起来，形成对上层节点的安全状况的评测，即威胁评测的结果[9]。

(5)信息控制管理。

对上传来的报警信息进行存储和管理，并建立相关的入侵行为的知识库，主要功能是描述当前的网络安全状况、攻击者的攻击历史等，为攻击识别和威胁评测提供依据。

4 结束语

开展对网络安全预警的研究，可以更加有效地保障网络信息安全。网络安全预警对于提高网络系统的应急响应能力，缓解网络入侵攻击所带来的危害，提高系统的反击能力等具有十分重要的意义。国内目前对于网络安全预警的研究最近才开始，相关理论和技术也才刚刚兴起。

文中在深入分析国内相关研究后，建立了网络安全预警系统的结构和工作流程图，分析研究网络安全预警系统的检测域、预警代理模块、区域预警中心模块等重要组成部分。网络安全预警技术中诸如基于数据挖掘的检测技术、数据融合、可视化等方面有许多问题需要研究。

参考文献：

[1] Rathmell A, Overill R, Valeri L. Information Warfare Attack Assessment System[EB/OL]. 2003. http://www.kcl.ac.uk/orgs/icss/Old/iwaasppr.PDF.

[2] Sandia National Laboratories. US Infrastructure Assurance Strategic Roadmaps-Strategies for Preserving Our National Security[R]. [s.l.]: Sandia National Laboratories, 1998.

[3] The national strategy to secure cyberspace[EB/OL]. 2003. http://www.us-cert.gov/readingroom/cyberspace strategy.pdf.

[4] Kijewski P. ARAKIS-An earlywarning and attack identification system[C]//The 16th Annual First Conf. Dudapest, Hungary: [s.n.], 2004.

[5] 胡华平，何利民，肖枫涛，等. 网络安全预警模型的研究[J]. 计算机研究与发展，2006，43(z2)：353-359.

[6] 张险峰，秦志光，刘锦德. 网络安全分布式预警体系结构研究[J]. 计算机应用，2004，24(5)：42-49.

[7] 胡 亮，金 刚，于 满，等. 基于异常检测的入侵检测技术[J]. 吉林大学学报理学版，2009，47(6)：1264-1270.

[8] 刘上伟. 基于网络的分布式安全预警系统的研究与设计[D]. 成都：四川大学，2006.

[9] 陈彦德，赵陆文，王 琼，等. 网络安全态势感知系统结构研究[J]. 计算工程与应用，2008，44(1)：100-102.

[10] 彭云峰，沈明玉. 入侵防御系统在应急平台的应用研究[J]. 计算机技术与发展，2009，19(2)：162-164.

[11] 孙怿昉. 数据挖掘在入侵检测系统中的应用研究[D]. 大连：大连海事大学，2008.

[12] 李 生，邓一贵，唐学文，等. 基于移动代理的分步式入侵检测系统的研究[J]. 计算机技术与发展，2009，19(9)：132-135.

(上接第 249 页)

布系统、密码服务系统相互配合，部署在省级工商行政管理局电子政务外网中，通过互联网与电子商务网站相连，提供网络亮照服务。

3 结束语

网络身份识别系统是密码技术与工商行政管理业务相结合的产物，适用于工商行政管理行业，支撑工商行政管理部门颁发，具有权威性、防伪性和全国一致性的营业执照电子副本，有效保障工商行政管理部门对网络市场的监管和服务，有利于促进我国电子商务又好又快的发展。

参考文献：

[1] 范玉贞. 我国电子商务发展对经济增长作用的实证研究[D]. 上海：上海师范大学，2010.

[2] 王珏辉. 电子商务模式研究[D]. 长春：吉林大学，2007.

[3] 荆继武，林璟锵，冯登国. PKI 技术[M]. 北京：科学出版社，2008.

[4] 邓晓军. PKI 技术及其应用的分析[J]. 计算机技术与发展，2008，18(6)：144-147.

[5] 冯相忠. 基于 J2EE 技术的电子商务系统的开发[J]. 计算机技术与发展，2007，17(8)：33-36.

[6] Zhang Jinlong, Du Xiaofang. A Study on the Application Model of B2B E-Commerce in the Agricultural Sector[J]. Journal of Electronic Science and Technology of China, 2004(3): 134-139.

[7] Pei Songwen, Wu Baifeng, Zhu Kun, et al. Novel Software Automated Testing System Based on J2EE[J]. Tsinghua Science and Technology, 2007(s1): 51-56.

[8] He Xinwen, Wang Xuehua. Strategic Analysis and Choice for Forestry Enterprises Developing E-business[J]. Chinese Forestry Science and Technology, 2007(4): 80-88.

[9] 信息技术安全技术公钥基础设施在线证书状态协议[S]. 中华人民共和国国家标准，2005.

[10] 侯 灿，杨宗凯，刘 威. J2EE 架构下连接池技术的应用与改进[J]. 计算机技术与发展，2006，16(10)：8-10.

[11] 张登辉，高 济. 基于 Web Service 的可组合电子商务实验平台[J]. 计算机技术与发展，2006，16(2)：110-113.

[12] 网络商品交易及有关服务行为管理暂行办法[S]. 国家工商行政管理总局，2010.

[13] 张大强，殷世民，程家兴，等. 基于 Web Service 的电子商务体系结构[J]. 计算机技术与发展，2006，16(7)：23-25.