基于PKI的网上证券交易系统的构建

刘华春
(成都理工大学 工程技术学院,四川 乐山 614007)

摘 要:为了满足日益增长的网上证券交易安全的需要,确保数据机密性、完整性、防抵赖、身份识别是保证网上证券交易安全运行的基础。通过对PKI体系和当前网上证券交易系统的研究分析,给出了一种基于PKI体系的网上证券交易系统的解决方案,设计了PKI网络结构和安全数据交易流程,实现了对数据签名和加密方式安全的传输,保证了客户交易数据的安全,有效提高了现有网上证券交易系统的安全性。

关键词:数字证书;公钥基础设施;数字签名;信息安全;网上证券交易
中图分类号:TP309.2 **文献标识码**:A **文章编号**:1673-629X(2009)07-0173-04

Implementing a System of On-line Securities Trading Based on PKI Technology

LIU Hua-chun
(College of Engineering & Technology, Chengdu Technical University, Leshan 614007, China)

Abstract: To ensure data confidentiality, integrity, anti-denial and identification is basis of safe operation of on-line securities trading with the growing on-line securities trading. Through research and analysis of the PKI system and the current on-line securities trading system, a solution based on the PKI system on-line securities trading systems has been put forward, the method of the PKI network, the transaction data process, data signature, encrypted transmission are design and implemented in which. It ensures that customer's transaction data safe and effective to improve the existing on-line securities trading systems security.

Key words: digital certificates; public key infrastructure; digital signature; information security; on-line securities trading

0 引 言

网上证券交易以其成本低、效率高的优势快速发展,已成为各国金融市场的主要交易手段,与一般电子商务不同的是,网上证券交易实时进行,涉及金额巨大,参与人数众多,安全问题尤其突出,在线证券交易过程中,各交易实体间的信息传递面临的安全威胁主要有,信息被窃取、篡改、身份被假冒和交易行为被否认等[1~3]。

安全的网上证券交易必须保证以下4点:

①身份认证:使通信双方就是其所声明的那一方,证券公司的服务器需要认证端客户,客户也要认证服务器,要有双向认证的机制。方便而可靠地确认对方身份是交易的前提。

②数据保密性:在线证券交易是建立在一个开放的网络环境上的,要传送的交易数据需要加密传送,不能被非授权的第三方窃取,而导致信息泄漏,给证券交易方带来经济损失。

③数据完整性:确保通信数据在传输过程中没有被篡改,数据传输中信息的丢失、重复或次序差异、被篡改都可能导致证券交易信息的差异,从而影响证券交易各方信息的完整性。

④不可抵赖性:网上证券交易要求系统具备审查能力,以杜绝系统任何一方的抵赖行为。

现有的网上证券大多系统,不管是采用WEB和客户端软件形式,大多仅仅部署了SSL证书,在安全上是很不够的;其次,很多证券公司的交易系统是使用证券公司的自签证书,没有使用公认的第三方CA提供的数字证书,也没有吊销列表(CRL),这样非常不安全;第三,大多数证券公司的网上交易系统采用"用户名+密码"的认证方式,没有采用客户端证书+USB Key方式来实现强身份认证,确保客户帐户的安全。

目前的网上证券交易系统存在较大的安全隐患,为此,文中提出并设计了基于PKI的网上证券交易系统。

收稿日期:2008-11-02;**修回日期**:2009-01-20
作者简介:刘华春(1966-),男,四川泸州人,硕士,讲师,工程师,CCF会员,研究方向为计算机网络安全、智能信息处理。

1 PKI 的设计

1.1 系统结构

在实际应用中,各证券公司实际的网络环境可能各有不同,但是总体方案的实现分为以下几个系统,如图 1 所示:

1)CA 证书签发中心:是 CA 系统的核心部分,向外围系统提供证书签发、证书吊销、证书更新、证书状态查询等服务,定期发行 CRL,制定证书发行策略,管理外围系统的操作权限和操作员的远程登录,记录详细的操作日志,备份并在异常时恢复系统数据。

2)CA 分布式管理中心:是 CA 服务器的管理界面,系统管理员可以通过 CA 管理器远程登录到 CA 服务器配置系统,进行各项管理操作。操作员只能使用它创建、签发、吊销证书。CA 管理器提供友好的操作界面,方便了操作员对系统的使用和维护。

3)OCSP 服务器:OCSP 服务器响应应用系统查询证书状态的请求,将格式正确的请求数据转往 CA 服务器进行状态查询,确定证书是否是本 CA 签发的、是否已被吊销,并将结果返回给应用系统。OCSP 服务器和 CA 服务器通过网络进行连接,为保证在网络故障时 OCSP 服务器也可以提供证书状态查询服务,OCSP 服务器在本地保存了已吊销的证书数据信息。

4)RA 证书注册中心:系统负责对提交了证书申请的用户真实身份进行审查,只有通过了审查的申请才会向 CA 提交,由 CA 签发证书。用户证书的密钥对由 RA 客户端创建,CA 和 RA 服务器不会拥有用户证书的私钥。

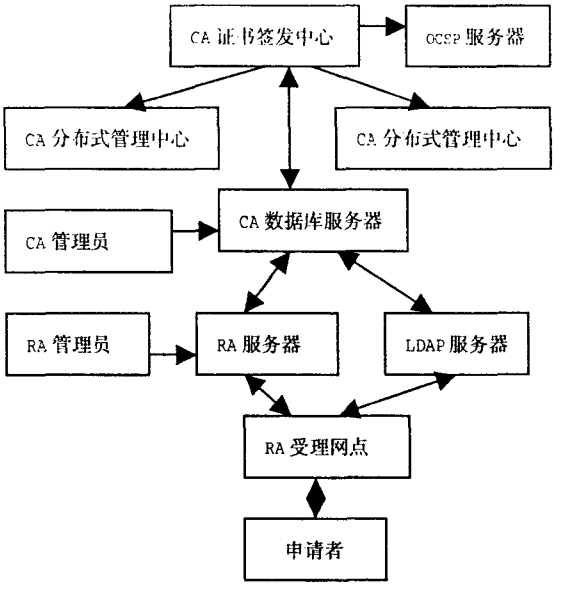

图 1 PKI 系统设计网络结构图

1.2 证书申请与发放

用户可以通过 RA Client 直接在网上进行证书的申请并获取证书[4~6],流程如下:

①用户申请:申请人填写个人信息,在申请证书过程中使用 SSL 与服务器建立安全连接,用户的申请信息存放至 RA 注册机构。

②RA 审核:注册机构操作员核实用户的真实身份。注册机构操作员与 RA 服务器之间采用 SSL 安全通信,操作员将审阅 R A 系统中的申请表,核对用户信息并批准申请。

③CA 颁发证书:RA 向 CA 传递用户申请,CA 操作员审阅申请信息,并验证操作员的数字签名,如果批准申请则颁发证书,CA 系统会自动产生证书。证书中包含关于用户及签署 CA 的各种信息,如用户唯一标识信息、证书持有者的公钥、证书有效起止日期等。

④获得证书:证书生成完毕后,CA 将证书输出到目录服务器(LDAP)以提供目录浏览服务。注册机构操作员通知申请人,并提供给用户对应的证书序列号、授权码。申请人到指定的网址下载自己的数字证书。

⑤下载证书:用户到指定的网址,键入自己的证书序列号、授权码,这个数字证书将可存储在物理介质如 USB Key 中。

1.3 证书吊销和更新

用户到营业部填写申请表,由录入操作员录入数据,审核操作员根据用户的资料进行审查,将通过审查的资料向 CA 提交。用户通过 Web 页面填写资料,发送给 RA 服务器,由审核管理员人工审核,或由 RA 服务器自动审核,RA 服务器将处理结果用 E-mail 的方式通知用户。用户通过 RA Client,填写资料,发送给 RA 服务器,由审核管理员人工审核,或由 RA 服务器自动审核,RA Client 每隔一定的时间间隔,连接到 RA 服务器,查询处理结果。

2 基于 PKI 的证券交易系统设计

2.1 委托交易系统设计

证券网上交易系统数据通信采用 SSL 安全通信协议与 PKI 体系中数字证书相结合的加密方式来防范交易通信过程中窃听、假冒、篡改、重发和交易抵赖[7~8]。

SSL 安全套接层协议是基于 Web 应用的安全协议,它包括服务器认证、客户认证、SSL 链路上的数据完整性和保密性。网上交易系统应用 SSL 协议,可以保证交易数据的真实性、完整性和保密性。但由于 SSL 不对交易数据进行数字签名,因此不能提供交易的不可否认性,这部分的工作必须由数字证书完成[9]。所以,文中采用 SSL 协议与 PKI 加密体系相结合的方式来弥补 SSL 协议的不足之处,证券交易安全系统如

图 2 所示。

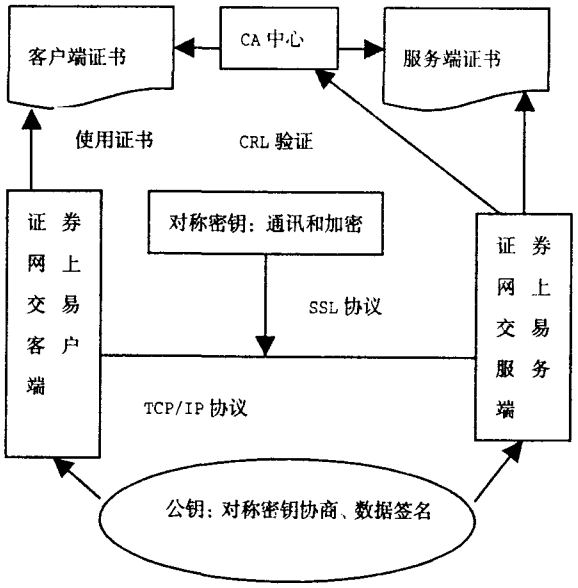

图 2　证券网上交易安全系统结构

SSL 和 PKI 加密技术在网上交易系统中的应用，使网上交易系统在通信方面的安全性大大增强，客户端和服务器端一次交易过程处理如下：

①客户端和服务器之间的证书交换和身份认证；

②客户端随机生成一个对称密钥：keyl = CenKey ( )；

③客户端用 keyl 对所有的信息加密生成 EPackl，用服务器的公钥 SerPubKey 加密 Key1 得到 Ekey1，用自己的私钥对 EPackl 签名得到 SigPack1；

EPackl = Enc(Reg Bag, keyl)

Ekey1 = Enc(keyl, SerPubkey)

SigPack1 = Sign(EPackl, CliPriKey)

④ 将 EPackl, Ekey1 和 SigPack1 通过 Internet 用 SSL 加密信道传至证券公司服务器；

⑤服务器首先验证客户端的签名，然后用自己的私钥解密 Ekey1 得到 keyl，最后用 keyl 解密 SigPackl 得到用户请求信息；

Verify(SigPack1, CliPub Key)

keyl = Dec(Ekey1, SerPriKey)

RegBag = Dec(EPackl, keyl)

⑥服务器将客户指令发给后台处理系统；

⑦后台处理系统完成处理后将处理结果传给服务器；

⑧服务器将返回信息用 keyl 加密得到 EPack2，用自己的私钥签名 EPack2 得到 SigPack2；

EPack2 = Enc(Ans Bag , keyl)

SigPack2 = Sign(EPack2 , SerPriKey)

⑨将 EPack2 和 SigPack2 通过 Internet 传给客户端；

⑩客户端用自己的私钥验证服务器的签名，然后用 keyl 解开 EPack2 得到服务器返回信息。

Verify(SigPack2, SerPubKey)

AnsBag = Dec(DPack2, key1)

因为客户端发送的请求数据和服务器返回的数据量都较小，故没有使用 Hash 函数生成摘要，而是对加密数据签名。

2.2　资金划转系统设计

证券交易系统需要实现证券买卖的资金在银行和证券公司之间划拨，目前交易资金普遍采用第三方(银行)存管，每个证券交易帐户需在银行有一个实名储蓄帐户，客户在银行存取资金，然后通过证券公司和银行之间的资金划转系统进行资金的划拨[10]。因此方案的实施需要银行系统和指定证券公司的交易系统相互协作，共同完成。

本方案中，客户在证券交易时间内进行资金的划拨，在客户端和指定证券公司的网上交易系统双向认证后，客户端采用基于 PKI 的数字签名技术将数据签名加密，传送到证券公司的服务器，证券公司将划款指令由支付网关通过银行的金融虚拟专用网(VPN)将相应款项从客户的银行帐户划转到指定证券公司的帐户。

网上证券资金化转数据的签名加密和验证过程如图 3 所示。(其中：网上银行客户端为发送方，指定证券公司的证券业务交易系统为接收方)

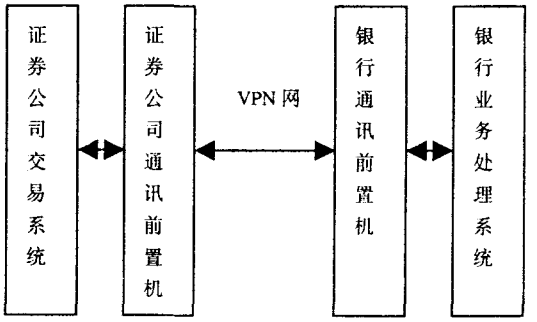

图 3　证券公司和银行的资金划转网络图

●资金划转数据的签名加密：(发送方)

①发送方生成临时对称密钥 Key，用 Key 加密交易数据(V1)形成密文；

Key1 = Cenkey( )

DPack1 = Enc(V1, key1)

②发送方用单向散列函数生成交易数据的散列值 Hash(V1)；

HV1 = Hash(V1)

③发送方使用公钥算法，用私钥生成 HV1 的数字

签名;

SigPack1 = Sign(HV1, CliPriKey)

④发送方用接收方的公钥加密对称密钥 KEY;

Ekey1 = Eec(key1, SerPubkey)

⑤发送方将交易数据密文、数字签名、加密密钥放置数字信封,发送给接收方;

Send(Dpack1, SigPack1, Ekey1)

●接收:(资金划转数据的验证)

①接收方使用公钥算法,用私钥解密对称密钥 key; Key1 = Dec(Ekey1, SerPubkey)

②接收方用发送方的公钥解密数字签名,得到发送的 Hash(V1); HV1 = DEC(SigPack1, CliPubKey)

③接收方用匹配的对称密钥 key1 解密交易数据密码,获得 V1; V1 = Dec(Dpack1, key1)

④接收方用发送方相同的散列函数生成交易数据的 Hash(V1); HV2 = Hash(V1)

⑤比较两个散列值是否相等,验证交易数据的真实性。

若 HV1 = HV2,表明数据传送真实有效,根据指令进行资金的划转。

3 结束语

针对目前网上证券交易系统安全性的不足,设计了基于 PKI 的网上证券交易系统。采用了安全认证服务器证书,实现了客户端和服务器的双向认证,确保了网上客户端和服务器端的真实性和唯一性,防止了伪造攻击。同时利用对称密码技术加密交易数据,临时产生对称密钥,不重复使用,有效防范强力攻击。然后使用公钥算法将对称密码密钥加密再传送的数字签名技术,保证了交易双方的不可抵赖性。数据在客户端和证券公司服务器端传送采用 SSL 安全协议,大大加强了数据的机密性,防止了对交易数据的截取和篡改攻击。在客户端采用客户端证书加 USB Key 的强身份认证方式,确保证券帐户的安全。因此,使用基于 PKI 体系的信息安全技术保证了证券交易数据的真实性、完整性、保密性、不可抵赖性和银行资金的安全。

参考文献:

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

[2] PSTN. 电子签名基础知识[EB/OL]. [2005 - 01 - 04]. http://tech. ccidnet. com/pub/artic le/c1096_a198449_p1. html.

[3] Jacob E, Liberal F, Unailla J. PKIX-based certification infrastructure implementation adapted to non - personal end entities [J]. Future Generation Computer Systems, 2003(19):263 - 275.

[4] 张书杰,潘兴庆,李 健. 基于 PKI/CA 的银行与基金公司在线交易系统的构建[J]. 北京工业大学学报,2006,32(5):477 - 480.

[5] 时贵霞,杨家明. 基于 PKI 技术的网上交易系统[J]. 东华大学学报:自然科学版,2006,32(6):83 - 85.

[6] 刘 渊,周世民,孙亚民. 网上在线支付的数字签名的研究与设计[J]. 计算机应用研究,2003(11):110 - 112

[7] 雷 蕴. 基于 SSL 协议的网上证券交易系统的安全方案[J]. 北京电子科技学院学报,2007,15(2):17 - 20.

[8] 吕格莉,王 东,戴 骥,等. 基于 PKI 的网上交易安全中间件的研究与实现[J]. 微型电脑应用,2005,21(12):52 - 54.

[9] 将 韬,伍 萍,徐正文. 一种基于 PKI/PMI 技术的安全的网上证券交易模型的研究与实现[J]. 信息安全与通讯保密,2007(10):44 - 46.

[10] 王淑清,齐景佳. 兴安证券网上交易安全方案[J]. 哈尔滨金融高等专科学校学报,2006(1):50 - 52.

(上接第 172 页)

参考文献:

[1] 石 静,王 平. 论校园网的安全和防护[EB/OL]. 2008 - 08. http://www. 60553878. com/Article/ShowArticle. asp?ArticleID=40.

[2] 杨富华,彭 钢,潘 宏. 关于 802.1x 认证技术在校园网应用中问题的探讨[J]. 中国医学教育技术,2006(6):260 - 263.

[3] 马育峰,胡修林,张蕴玉. 网络管理热点问题研究的现状、问题与展望[J]. 计算机应用研究,2005(10):10 - 13.

[4] 董贞良,吕述望,王昭顺. 内网安全管理系统认证模块的设计基于 802.1X 的内网安全管理系统认证模块设计[J]. 计算机工程,2007(6):193 - 198.

[5] 王 倩,薛德黔. 802.1x 接入认证技术分析及展望[J]. 福建电脑,2007(8):8 - 10.

[6] 秦 刘,智英建,贺 磊,等. 802.1x 协议研究及其安全性分析[J]. 计算机工程,2007(4):153 - 157.

[7] Carey N. The evolving virus threat[C]//23th NISSC Proceedings. Baltimore, MD, USA:[s. n.],2000:141 - 153.

[8] Mishra A, Arbaugh W A. An Initial Security Analysis of the IEEE 802.1x Standard[EB/OL]. 2002 - 02. www. ieee802. org/1/files/public/docs2000/ieee_plenary. PDF.

[9] Anthon J. Using IEEE 802.1x to Enhance Network Security [EB/OL]. 2002 - 10 - 28[2005 - 12 - 20]. http://whitepapers. zdnet. co. uk/0,39025945,60043454p - 39000378q,00. htm.