基于 PKI/CA 的银行与基金公司在线交易系统的构建

张书杰[1], 潘兴庆[1], 李 健[2]
(1.北京工业大学 计算机学院, 北京 100022; 2.北京银行, 北京 100031)

摘 要: 将 PKI(公钥基础设施)/CA(认证中心)体系用于网上银行同基金公司进行网上交易的系统还相当少,为了满足日益增长的银行和基金业务的需要,通过对 PKI/CA 体系和当前网上银行系统的研究,给出了一种基于 PKI/CA 体系构建网上银行和基金公司在线交易系统的解决方案,实现了对数据签名和加密方式进行安全的传输,保证了客户资料的安全,并且通过对流程的模型转换,使用户交易方便快捷,较好地满足了系统的需求.

关键词: 公钥加密; 信息技术; 数字签名; 数字安全; 网上银行; 在线系统
中图分类号: TP 393.08 **文献标识码**: A **文章编号**: 0254-0037(2006)05-0477-04

随着客户对基金交易便利性和快捷性需求的日益增加,网上交易已是大势所趋,而且发展速度非常迅猛. 基金公司采取与银行合作的形式,也就是说,基金客户把资金存放在银行借记卡账户上,在银行开立相关业务,客户直接登陆基金公司网上交易系统进行基金委托交易,银行与基金公司联合后,将资源高效整合,合理分配,实现优势互补.

PKI(public key infrastructure)指公钥基础设施. CA(certificate authority)指认证中心.

我国 863 计划连续支持的 PKI 关键技术,研究开发了 PKI 信息安全平台(智能化信任与授权服务安全平台),有效地解决了电子政务中信息安全这一核心难题,为我国电子政务建设以及密码技术的发展起到了重要的支撑和推动作用.

银行与基金公司进行网上合作将成为主流发展趋势. 基于 PKI 的网上银行系统已经发展并日趋成熟,但是,将 PKI 体系用于网上银行同基金公司进行网上交易的系统还相当少,本文给出了一种基于 PKI/CA 的网上银行与基金公司在线交易系统的构建过程.

1 公钥基础设施 PKI

1.1 PKI/CA 体系的原理[1-2]

PKI 从技术上解决了网络通信安全的障碍. CA 从运营、管理、规范、法律、人员等多个角度解决了网络信任问题. 由此,统称为"PKI/CA". 从总体构架来看,典型的 PKI 由 5 个部分构成. 证书中心(certification authority,简称 CA);注册中心(registration authority,简称 RA);证书持有者(certificate holders);用户(client);证书库(repositories);等.

在 PKI/CA 的具体部署中,这 5 个部分又可按不同的需要进行相应分解,以便管理,在实用化的 PKI/CA 中,证书中心可分化出许多其他管理模块. 以数字证书为核心的 PKI/CA 技术可以对网络上传输的信息进行加密和解密、数字签名和签名验证.

1.2 基于 PKI 的数字签名技术

基于 PKI 的电子签名被称作"数字签名",是电子签名的一种特定形式. PKI 可提供多种网上安全服务,如认证性、数据保密性、数据完整性和不可否认性,其中都需要用到数字签名技术.

收稿日期: 2005-10-14.
作者简介: 张书杰(1943-), 男, 北京人, 教授.

PKI的核心执行机构是CA,PKI签名的核心元素是由CA签发的数字证书,所提供的PKI服务就是认证性、数据完整性、数据保密性和不可否认性. 利用证书公钥和与之对应的私钥进行加/解密,并产生对数字电文的签名及验证签名. 数字签名是利用公钥密码技术和其他密码算法生成一系列符号及代码组成电子密码进行签名,来代替书写签名和印章;这种电子式的签名还可进行技术验证,其验证的准确度是手工签名和图章验证无法比拟的. 该签名方法可在很大的可信PKI域人群中进行认证,或在多个可信的PKI域中进行交叉认证,也适用于互联网和广域网上的安全认证和传输[3-4].

2 系统实施方案

2.1 PKI设计

图1是网上银行与基金公司在线交易系统的网络拓扑图. 证书申请签发过程包含5个环节.

1) 用户提出申请. 申请人首先下载CA根证书,然后,在申请证书过程中使用SSL与服务器建立安全连接,申请人填写个人信息. 客户端浏览器自动生成密钥对,并将私钥保存在客户端特定文件中,并需要用口令保护密钥文件. 客户端浏览器同时将公钥和个人信息提交,用户的申请信息存放至RA注册机构.

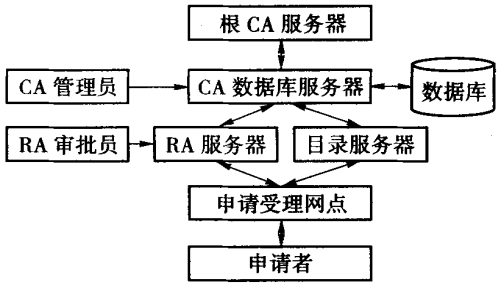

图1 系统PKI设计网络拓扑图

Fig.1 System network topology based on PKI

2) 注册机构输入和审核. 注册机构操作员与用户联系,证明用户的真实身份. 注册机构操作员与RA服务器之间采用SSL安全通信,RA系统对操作员进行严格的身份认证,包括核对操作员的数字证书和IP地址. 操作员将审阅RA系统中的申请表,核对用户信息并批准申请,随后,通过注册机构管理员授权.

3) 认证系统颁发证书. 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) 下载有效证书. 用户使用证书申请时的浏览器到指定的网址,键入自己的证书序列号、授权码,用户必须使用申请证书时的浏览器,因为浏览器需要用该证书相应的私钥去验证数字证书,只有保存了相应私钥的浏览器才能成功下载用户的数字证书,这个数字证书将被存储在物理介质USB Key中.

登录验证由安全客户端和安全代理服务器构成[5]. 安全代理服务器串联在网络入口和Web服务器之间,与安全客户端建立加密通道,保证信息传递的保密性. 安全代理服务器同时利用目录服务和权限管理基础设施,控制证书的有效性和访问范围. 在证书使用过程中,安全代理服务器要获取信息发送方的公钥证书以及CA根证书,以验证发送者证书的真实性.

2.2 技术方案

银行网点要对客户进行身份验证,帮客户办理银行卡. 然后,客户登陆基金公司网站直接开立基金账户并进行基金交易. 基金公司网上交易系统接受客户申请,传递到直销系统并上传到注册登记系统;同时基金公司将划款指令传递到银行,由银行系统将相应款项从客户银行账户上划转到基金公司开立的账户上. 也就是说,由基金公司交易网站将交易数据按照某种格式打包后发送给银行网上基金交易平台的固定端口,银行网上基金交易平台处理后将交易结果按照某种格式打包后回送给基金公司交易网站. 其流程如图2

所示.

2.3 实施方案条件

实施方案需要基金公司系统同网上银行系统相互协作,基金公司系统采用当前业界流行的、且成熟的 J2EE 架构作为交易平台,安全、便捷地实现支持银行卡的开放式基金网上交易. 基金管理公司提供应用服务器和登记过户(TA)系统、销售系统的交易接口,网上交易系统直接通过 J2EE 中的消息机制(EJB 调用、JMS 或 XML 数据)与核心的交易或销售系统进行通讯. 如图 3 所示. 系统软件模块分为基金网上查询及交易系统和实时资金结算系统.

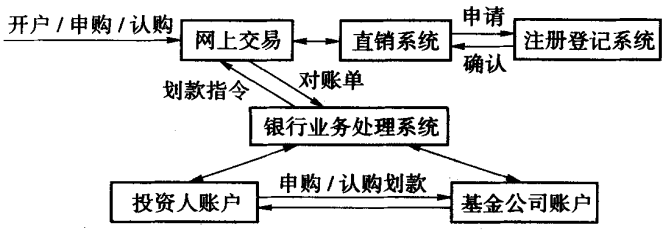

图 2　基金公司网上交易流程图

Fig.2　Flow chart for online transaction of Fund Company

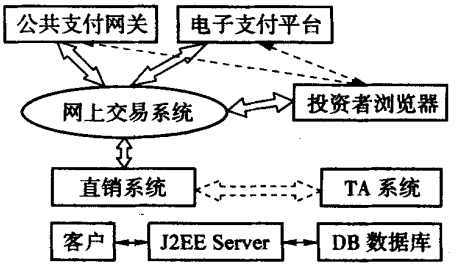

图 3　系统构架图

Fig.3　System framework chart

网上交易系统包含网上交易业务处理系统、支付网关或支付平台接口处理系统 2 部分内容. 网上交易业务处理系统包括各类交易、查询、后台对帐、清算的管理功能,WEB 部分采用组件模式结构和页面 Session 缓存技术,以保证交易的安全性、一致性. WEB 服务端组件又分为交易组件和查询组件 2 部分,采用高级配置方式,使后台业务逻辑的修改不影响前端功能,对客户来说是透明的,支付网关及支付平台接口处理系统负责处理与不同银行间的划账鉴权.

本系统主要实现的是银行端的交易处理及 PKI 体系电子签名加密传输的工作. 需要银行端建立网上银行同基金的网上交易平台.

2.4 交易安全性

采用安全认证服务器证书,以确保网站的真实性、唯一性以及网站与用户之间信息传递的保密性、完整性. 网上交易平台采用最高等级的 128 位 SSL 通道加密技术及应用服务器中的数字签名技术来保证,将客户的交易过程加密,以防不当入侵与资料外泄,实时资金结算系统中还采用第 3 方的安全认证证书来保证第 3 方 CA 中心发放和管理数字证书以及进行安全认证. 对于用作验证身份的签名私钥,由持有者保管,不能进行备份和恢复;对于用作加密数据的加密私钥和会话密钥(对称密钥),在由持有者保管的同时,为防止因加密私钥丢失而不能恢复原加密数据的现象发生,还要采取安全策略对它们进行备份,并建立异常情况下的非正常恢复机制[6].

另外,网上银行的安全通行证还可以参考银行颁发的 USB Key 客户证书,客户有关信息一经下载到 USB Key 客户证书内,即具有唯一性和不可复制性,网上所有涉及账户资金的对外转移都必须事先通过 USB Key 客户证书进行唯一认证,可以有效防范各类可能的风险.

银行和基金公司之间的数据交换采用安全的数字信封和数字签名方式,通过调用由银行提供的安全接口函数对明码报文加密和签名后产生数字密文包和数字签名,如图 4 所示.

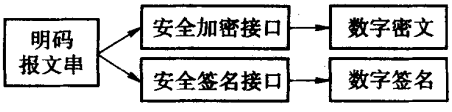

图 4　银行和基金公司之间的数据交换

Fig.4　Data exchange between Band amd Fund Company

3 结束语

本文给出的基于PKI/CA的网上银行与基金公司在线交易系统具有以下几方面的优点.

1) 充分利用基金公司和银行目前所有的软硬件资源,尽可能的节省成本,并能为以后的业务扩展提供足够的空间.

2) 借助银行基金公司转账功能,能够为投资者提供单独的实时资金划转功能.

3) 加快赎回及分红资金的到帐时间.

4) 系统的安全性包括资金划转的安全以及投资者、基金公司、银行数据一致性方面的安全.

参考文献:

[1] Antiy Labs. Introduction to Best Truest PKI/CA[OL]. [2002-01-29]. http://www.antiy.net/products/00000003.htm.

[2] ADAMS C, LLOYD S. 公开密钥基础设施——概念、标准和实施[M]. 冯登国, 译. 北京:人民邮电出版社, 2001.

[3] NASH A, DUANE W, JOSEPH C, et al. 公钥基础设施(PKI):实现和管理电子安全[M]. 张玉清, 译. 北京:清华大学出版社, 2002.

[4] PSTN. 电子签名基础知识[OL]. [2005-01-04]. http://tech.ccidnet.com/pub/article/c1096_a198449_p1.html.
PSTN. Basic Knowledge of Digital Signature[OL]. [2005-01-04]. http://tech.ccidnet.com/pub/article/c1096_a198449_p1.html.

[5] 周惠清. 银行网上工资管理系统中的PKI技术实现[J]. 计算机与现代化, 2004(1):77-81.
ZHOU Hui-qin. Implementing PKI technology in banking betwork wage management system[J]. Computer and Modernization, 2004(1):77-81. (in Chinese)

[6] JACOB E, LIBERAL F, UNZILLA J. PKIX-based certification infrastructure implementation adapted to non-personal end entities[J]. Future Generation Computer Systems, 2003(19):263-275.

Implementing a System of Online Transaction Between the Internet Banking and Fund Company Based on PKI/CA Technology

ZHANG Shu-jie[1], PAN Xing-qing[1], LI Jian[2]

(1. College of Computer Science, Beijing University of Technology, Beijing 100022, China;
2. Bank of Beijing, Beijing 100031, China)

Abstract: At present, the system of using PKI(public key infrastructure)/CA(certificate authority) technology in the online transaction between Internet Banking and Funding Company is quite few. In order to adapt the increasing business requirement of bank and fund company, after a long-time research on PKI/CA technology and Internet Banking System, this paper presents a solution to implement on-line transaction between Internet Banking and Fund Companies by using the PKI/CA technology. This solution has realized a scure data transmission by digital signature and encryption, guaranteed the information security of customers'. And it has made the transaction more convenient and faster, satisfactorily met the demands of the system by modeling the workflow.

Key words: public key cryptography; information technology; digital signature; security of data; internet banking; online systems