基于身份认证的“中央债券综合业务系统”

姜 溟　王洪华（中央国债登记结算有限责任公司 100032）

摘要：与传统的系统安全策略相比，数字证书认证体系具有较大的优越性，随着各项技术的成熟，其使用越来越广泛。其核心是通过给交互双方发放数字证书实现网上信息传递的私密性、真实性、完整性和不可否认性。本文描述基于身份认证的中央债券综合业务系统实施经验。

关键词：数字证书　安全机制　负载平衡

中央国债登记结算有限责任公司成立于1996年12月2日，是为全国债券市场提供国债、金融债券、企业债券和其他固定收益证券的登记、托管、交易结算等服务的国有独资非银行金融机构，是财政部唯一授权主持建立、运营全国国债托管系统的机构，是中国人民银行指定的全国银行间债券市场债券登记、托管、结算机构和商业银行柜台记账式国债交易一级托管人。截至2003年底，债券托管总额达3.7万亿元，债券交易额在2002年突破10万亿元的基础上，2003年达到15万亿元。因此做为诸多业务承载体的“中央债券综合业务系统”的安全、稳定运行显得越发的重要。

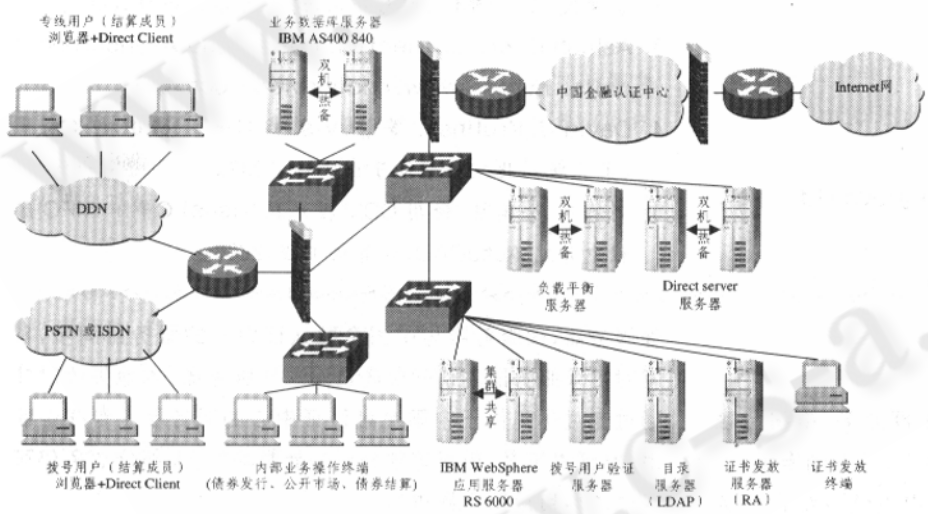

图 1　中央债券综合业务系统结构简图

1　系统概述

该系统一九九九年八月投入运行，运行期间进行了多次技术改造，既满足了业务需求又实现了系统的安全。系统简略结构图如图1。

采用数字证书机制进行系统安全建设时，可以选择自己建立证书体系或采用第三方证书体系。自己建立证书体系便于控制，灵活性强，但成本较高，不利于多机构间的合作交流，且出现与证书使用者的争议时责任界定较难。因此本系统采用中国金融认证中心的第三方证书进行系统建设。

中国金融认证中心（CFCA－China Finance Certificate Authority）作为一个权威的、可信赖的、公正的第三方信任机构，专门负责为金融业的各种认证需求提供证书服务，包括电子商务、网上银行、网上证券交易、支付系统和管理信息系统等，为参与网上交易的各方提供安全的基础，建立彼此信任的机制。并且在中国电子商务发展中，组织并参与有关网上交易规则的制定，以及确立相应的技术标准，提供网上支付，特别是跨行网上支付的相互认证等。金融认证中心为了满足金融业在电子商务方面的多种需求，采用PKI技术，建立了SET和Non－SET两套系统，提供多种证书来支持各成员行有关电子商务的应用开发以及证书的使用。

2　证书类型的选择与证书的存储介质

根据客户不同层次的安全需求，CFCA提供企业（个人）高级证书、企业（个人）普通证书、WEB站点证书、STK手机证书、VPN设备证书等。本系统中使用证书全部为企业高级证书，即加密密钥与签名密钥分离。

数字证书可以存放在计算机的硬盘、随身软盘、IC卡或CUP卡中。

用户数字证书在计算机硬盘中存放时，证书以EPF文件的方式存在，受密码保护。使用方便，但存放证书的PC

机必须受到安全保护，否则一旦被攻击，证书就有可能被盗用。

使用软盘保存证书，证书以 EPF 文件的方式存在，受密码保护。被窃取的可能性有所降低，但软盘容易损坏。一旦损坏，证书将无法使用。

IC 卡中存放证书是一种较为广泛的使用方式。证书存放在 IC 卡中，使用时通过读卡器读出密钥。成本较低，与软盘相比不易被损坏。但使用 IC 卡加密时，用户的密钥会出卡，造成安全隐患。

使用 CUP 卡存放证书时，用户的证书等安全信息被加密存放在 CUP 卡中，无法被盗用。在进行加密的过程中，密钥可以不出卡，安全级别最高，但相对来说，成本较高。

由于本系统的结算成员范围广，涉及到各类金融机构，技术水平、安全防犯意识相差较大，同时也为便于结算成员使用和中心统一管理，要求所有结算成员使用 CUP 卡存放证书。

3 有关技术与软件的应用

3.1 Direct 安全代理软件的应用

Direct 安全代理软件是中国金融认证中心(CFCA)为使用高级证书的客户提供的一种安全代理软件，是实现证书安全认证机制的一个重要组成部分。

Direct 安全代理软件由 DS(Direct Server)和 DC(Direct Client)两部分组成：DS 运行于中心端；DC 运行于结算成员客户端。Direct 安全代理软件的主要作用就是在客户的浏览器和网站的服务器之间建立一个安全通道，使得相互之间可以安全的传递信息，同时完成对证书的自动管理。

通过 Direct 软件，客户无须过多地理解证书和密钥就可以轻松实现信息的安全传递。Direct 能够自动地执行 CFCA 提供的一整套完整的安全机制，如身份识别、信息加密、数字签名以及证书自动更新等一系列工作。整个过程对客户都是透明的，为客户提供可靠、便捷的网上安全服务。

Direct 安全代理软件是处于应用层面并直接面向证书用户的，其主要功能包括：自动查询证书黑名单(CRL)；实现双向身份认证，对传输信息自动加/解密，保证信息的私密性；通过"证书恢复"功能，解除客户遗忘口令的后顾之忧；实现证书生命周期的自动管理；多种证书存放方式；支持时间戳等多项功能。

3.2 证书安全机制与业务安全机制的结合

为了将证书安全机制与业务安全机制相结合，Direct 提供了多种机制。

用户识别名－－－到达 Direct 代理服务器的每一个 http 请求将连同用户验证证书和识别名一起发给 web 服务器。这个识别名能和密钥一样用于查询访问权限。

头影射－－－每一个 http 请求都要通过 Direct 服务器的处理，那就是通过调用动态连接库或共享库把 DN 转化成 http 鉴定头信息。缺省情况是这个动态连接库从 DN 里返回一个 cn，然后放在 http 头信息的用户名和密码两字段内。这种方法能用于从一些 web 服务器访问控制列表里自动查询。

其他证书信息－－－－为对访问控制组件提供更多的信息，Direct Server Proxy 可以被配置成通过 http 头传送更多的证书信息。

本系统采用上述第二种方式，即头影射。应用服务器根据 DIRECT 提供的 CN 信息识别不同的结算成员，进行业务授权的实现。

3.3 建立负载平衡机制，减轻 DS 的压力，提高系统运行效率

运行 DS 的主机负责接收 DC 端发送的请求，要进行加/解密、签名、记录签名信息、并与应用服务器进行数据通讯，因此其运行负荷较大。为不使其成为系统瓶颈，安装了负载平衡服务器，负责将用户的请求分发给多台 DS 服务器，既保证了每台 DS 服务器的高效运行，又实现了 DS 服务器的相互备份。

本系统的负载平衡软件采用 IBM 的 Edge Components 软件，运行平台为 WINDOWS 2000，双机热备。

3.4 证书发放系统(RA)的建立

由于结算成员数量较多且结算成员的信息已经在中央债券综合业务系统的系统数据库中存在，故该系统建立了自己的证书发放系统。该证书发放系统通过应用服务器获取到结算成员的信息，经经办人员确认后形成证书申请信息发往中国金融认证中心，并将中国金融认证中心返回的参考号和授权码打印到密码新封并交给结算成员，结算成员根据参考号和授权码即可在 DC 端下载证书。

证书发放系统由证书发放服务器及操作终端组成，证书发放服务器与金融认证中心及证书发放服务器与操作终端间的通讯连接采用证书技术实现认证、保密。

除证书申请外，证书发放系统还承担着证书暂停、注销及数据统计等若干功能。

证书发放系统虽然并不存放证书本身，但其中的内容涉及证书发放过程中的诸多内容，其安全性也很重要，在本系统中采用了双机冷备、硬盘热备等措施。

证书发放服务器操作系统为 WINDOWS 2000 SERVER、操作终端为 WINDOWS 2000 PROFESSIONAL，数据库为 ORQCLE。

(下转第 47 页)

(上接第 49 页)

3.5 网络的隔离

为便于使用机构在 Internet 网上发展业务，中国金融认证中心的证书体系提供了 Internet 接口，证书的申请、下载、使用均可在 Internet 网上进行。因中央债券综合业务系统的重要地位及相应的安全要求，该系统不能与 Internet 网连接，各结算成员只能通过专用线路与中心系统相连，不允结算成员同时连接业务系统和 Internet 网。为解决此问题，建立了一条与中国金融认证中心 2 兆专线连接，直接与其内部服务器相连，中间通过若干防火墙隔离，从而既保证了身份认证、加密的各项要求，又保证了中央债券综合业务系统与 Internet 网及中国金融认证中心网络的隔离。

由于在业务进行中结算成员 DC 及中心 DS 均要频繁访问中国金融认证中心的目录服务器，通信量较大，且连接专线一旦产生故障中断，业务将无法进行，专线连接很可能成为系统瓶颈及系统的薄弱点。为此我们一方面建立与中国金融认证中心的 ISDN 备份线路连接以确保通信的畅通，另一方面在中心系统建立中国金融认证中心目录服务器的镜像服务器，该服务器与中国金融认证中心的服务器同步，日常对目录服务器的访问优先访问本地服务器，本地失效时才通过专线访问位于中国金融认证中心的服务器。专线中断时，除证书下载、更新等部分业务受影响外，大部分业务仍可通过本地目录服务器进行。

由于早期的中央债券综合业务系统未考虑与 Internet 网相连的问题，大部分计算机 IP 地址均为 Internet 地址，其与中国金融认证中心进行通信时会产生一定的问题。我们安装了一台代理服务器，该服务器负责代理全部到中国金融认证中心的通信连接，从而既解决了地址冲突问题，又保证了系统间的清晰接口，提高了系统的独立性、安全性。

参考文献

1 《CA eTrust 整体安全方案将管理手段技术化》。

2 《计算机世界》，信息安全专刊。

3 《构筑因特网防火墙》，{美} D. Brent Chapman Elizabeth D. Zwicky 著，自《电子工业出版社》。