联合证券网上交易方案书

第一章　　金证天亿系统简介

天亿 Internet 金融资讯交易系统是深圳市金证高科技有限公司的产品之一，其主要任务是完成证券金融信息的收集、整理、发布以及交易等工作。 涉及的信息源主要包括国内各证券市场、权证市场的行情数据以及和金融市场有关的新闻、资料、评论等。系统的信息采集可选用卫星小站的可靠接收方式或者图文电视接收方式，也可以充分利用邮电系统 DDN 的网络优势从各证券营业部获得数据，汇集到中心机房。在中心机房对采集来的信息进行整理加工，然后通过网络通讯手段向用户提供信息服务。采用 CLIENT/SERVER 模式，提供动态在线服务模式和静态离线服务模式两种主要服务类型，以满足不同层次用户的需要。动态在线服务模式的用户在注册上网后实时获得最新信息，直到用户自己退出为止。静态离线服务模式的用户注册上网后按照用户的请求提供相应的历史数据及资料，然后自动退出网络。无论在何种服务方式下，用户都可以委托交易，交易指令直接进入证券营业部，与大户享有同样的速度和安全性。所有的服务着重强调实时性、可靠性及准确性。在用户端， 提供实时报价的能力、技术分析的能力、基本面分析的能力、新闻浏览的能力，还通过 WWW、FTP 提供基本面分析、浏览静态行情、下载历史数据以及向用户提供技术支持等。这样，用户只需购买一台 28.8Kbps 以上的 Modem,通过家中的电话线，就可以实现“足不出户，做大户”的梦想。

系统全天运行，不中断，不关机。

在邮电系统的中心机房和用户之间信息数据包通过 TCP/IP 来传递，其中的数据格式自定义、不可读。用户与交易管理模块的交易数据传递采用加密方法， 密码时时更改。为防止“网络黑客”与病毒的侵入，在各证券营业部的转换计算机中安插两块网卡，其中一块绑定 IPX/SPX 协议，与券商的交易局域网相连，并且通过 NOVELL 网的安全功能，使其指定只此网卡可以以某一用户名登录；另一块网卡绑定 TCP/IP 协议，与中心机房的 HUB 相连。这样网卡不同、通讯协议不同，可以有效地防止非法侵入。另一方面，中心机房在局域网和用户之间也可以采取防火墙措施，使用户只能联结到资源管理、动态数据管理、静态数据管理和交易管理模块，而用户只知道资源管理机的 IP 地址。

Internet 金融实时资讯交易系统的主要特点可以归纳为以下几点：

以邮电数据局的 169 机房为中心，多证券营业部接入，多份行情数据实时备份；多个营业部上网交易；多种财经新闻综合；用户实现统一管理，统一收费。由于以数据局中心为主机房，充分地利用了邮电部门的通讯带宽。

可扩展性强。整个系统模块化设计， 各司其职，相互监控。在原有系统的基础上， 增加一个交易点，只需增加相应的交易转换模块和行情新闻采集模块。其他模块将会自动识别所增加的站点。

可伸缩性强。采用 SQL Server 数据库，加强了数据的管理。为今后利用 CGI、ActiveX、JavaAPI 等开发浏览行情数据、财经新闻等信息的通用 Web 网页提供了一个统一的数据接口。同时在最初数据设计方案中，充分考虑了今后的金融发展，为以后的期货、外盘交易和外汇交易资讯系统留有接入点。

服务端系统在Windows NT操作平台上运行，SQL Server为数据库，充分利用Windows NT真正的对称性多进程处理机制、安全子系统模型，从网络层和应用层两个层次、Intranet防火墙和数据安全保密两个方面设计整个系统的安全策略。

传输数据组织紧凑，利用push技术将所有正在交易的品种数据推送到客户端，并且直接落盘。盘后分析可以离线实现，无须上网。

服务端各运行模块都有日志文件记录和审计，监控整个系统的连接状况、客户登录、操作失败等信息。

客户端软件操作方法简便明了，符合广大股民的习惯；分析指标多样化，网上操作与在营业部大厅中操作基本相似。

第二章 系统构成

联合证券下属 40 多个营业部遍布全国各地，并且联合证券部内部已经实现了全国连网，营业部与总部，营业部与营业部之间的通讯联系无须再进行建设。根据联合证券的现状特设计以下网上交易解决方案。

系统分为网上交易服务器端，营业部交易及信息接入系统，用户客户前端系统。

网上交易服务器端一部分位于联合证券总部，一部分位于电信局中心机房。是系统中最复杂的和主要需要建设的部分。

营业部交易及信息接入。营业部通过一台专门的机器通过 DDN 专线与总部的交易接入服务器相连。处理来自于总部交易服务器转发的委托请求， 以及将营业部的信息上传到总部供查询。

用户客户前端系统。金证天亿提供二种方式的用户前端，应用程序及浏览器嵌入方式。在使用应用程序方式时，客户需要显示的将程序下载到本地，并且安装该软件，设置好连接网置即可使用。对于浏览器嵌入方式则是在用户在进入到该页面时系统直接下载， 用户只是首次使用时有一定延时。

对于网上交易服务器端的功能主要分为以下几个部分：

1. WEB 服务器。

WEB 服务器是联合证券对外提供统一的，开始的入口点。WEB 服务器上提供联合证券公司的公司主页，各营业部主页，股票资讯信息，前端软件的卸载等服务和功能。

2. 资源管理服务器。

其功能主要分成两大部分，一是它接收来自用户的注册上网请求。所有用户获得服务模块的服务必须首先建立 TCP 连接。资源管理模块接收所有用户的建立 TCP 连接请求，根据用户递交的 USERNAME 和PASSWORD，判定其是否是合法用户，资金状况如何，动态、静态以及交易权限如何等等，然后分配相应合适的服务管理模块给用户，通知用户端软件重新与其连接。并且更新相应服务模块的资源情况；另一方面它实时监控其他管理模块的运行状况以及资源情况，一旦发生故障，若系统中另有相应的备用模块存在，则热切换到使用状态。模块还设有报警功能，如果有任一服务模块非正常退出或发生故障，程序将即使给出提示信息。资源管理模块的地址对于系统的所有站点为已知，所有站点开机后向它报告信息，定时提交自己的工作状态。因为资源管理模块保存有所有用户和所有站点的重要信息，所以采用备份服务器。当站点与其连接失败或连接中断后未能恢复，即转向与备份服务器连接。

3. 动态信息管理模块。

将数据采集模块传来的数据信息包及时的发送给需要动态在线服务的用户。将用户使用情况（通讯时间和通讯量）提交计费管理模块，并根据计费管理模块的应答包决定是否继续服务。监控用户的线路联结情况，删除不合法用户的联结。及时向资源管理模块报告资源使用状况。发送的数据帧包括行情帧、时标等内容。每一个管理模块负责一定数目的用户，

现暂定为 100 个，每增加 100 个用户，增加一个管理模块。

4. 交易管理模块。

记录目前有几个证券营业部的交易转换模块正常运行，并将此情况报告资源管理模块，以便资源管理模块及时通知需要委托交易的用户，现有几个营业部可以进行远程交易。接收用户的委托指令，根据不同的交易场所进行分单，将指令发送到相应的目的地；并接收各个交易转换模块的指令应答，回送给对应的各个用户。将用户的委托情况（包括指令类型，委托成功次数等）及时报告计费管理模块，并根据计费管理模块的应答信息决定用户可否继续被服务。

5. 静态信息服务器。

响应用户的静态离线服务请求，按需服务，提供历史数据的追加、最近新闻的浏览、股票基本资料的更新等等，发送的帧包括静态行情帧、新闻帧、二进制文件（数据更新）、时标、通知等内容。将用户使用情况（通讯时间和通讯量）提交计费管理模块，并根据计费管理模块的应答包决定是否继续服务。及时向资源管理模块报告资源使用状况

6. 记费管理模块。

增加、修改、删除用户的使用权限、资金情况、信用程度、计费方式（按时、按量）、计费单位等接收来自动态数据管理模块、静态数据管理模块、交易管理模块的用户服务使用情况报表，实时计费。若用户资金已经不足，可通知相应的服务模块和资源管理模块，拒绝继续服务。用户信息都将保存在 **SQL SERVER** 数据库中，程序还设有超级管理员口令，只有合法的超级管理员才能操作用户信息库。

第三章 安全认证技术

电子商务的安全是通过使用加密的手段来达到的，非对称密钥加密技术（公开密钥加密技术）是电子商务系统中主要的加密技术，主要用于对称加密密钥的分发（数字信封）和数字签名，来保证电子商务的安全性需求，实现数据传输的安全性、身份认证、信息的完整性检验以及交易防抵赖性。CA 中心为用户的公钥签发证书，以实现公钥的分发并证明其有效性。该证书证明了该用户拥有证书中列出的公开密钥。证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。CA 机构的数字签名使得攻击者不能伪造和篡改证书。证书的格式遵循 X.509 标准。

CA 机构应包括两大部门：一是审核授权部门（简称 RA，Registry Authority），它负责对证书申请者进行资格审查，并决定是否同意给该申请者发放证书，并承担因审核错误引起的、为不满资格的证书申请者发放证书所引起的一切后果，因此它应由能够承担这些责任的机构担任；另一个是证书操作部门（简称 CP，Certificate Processor），负责为已授权的申请者制作、发放和管理证书，并承担因操作运营错误所产生的 一切后果，包括失密和为没有获得授权者发放证书等，它可以由审核授权部门自己担任，也可以委托给第三方担任。

当前在建和已经正式投入使用的国内 CA 中心有以下二家

（1）中国电信 CA 安全认证中心

中国电信采用北京创原世纪信息技术有限公司研制开发的“NETWORLD CA 安全认证系统”建设了“中国电信 CA 安全认证中心。”该系统于 1998 年 11 月投入实际运行，为社会公众提供各种安全服务，是国家批准的最大的 CA 运营系统。该系统于 1999 年 8 月通过国家密码管理委员会办公室和信息产业部联合组织的技术鉴定，并通过国家信息安全产品测评认证中心的认

证，获系统认证证书，是第一个经国家认证的最大的 CA 运营系统。
中国电信 CA 安全认证系统按照统一的体系建设。

（2）上海市 CA 中心

上海市政府采用“NETWQRLD CA 安全认证系统”建设了“上海市电子商务 CA 安全认证中心”，该中心是国内区域最大并投入实际运行的 CA 认证系统。

金证天亿网上交易系统使用的加密认证系统是来自于国家认证的第三方技术及产品（北京创原世纪信息技术有限公司研制开发的“NETWORLD CA 安全认证系统”）符合证监委及信息部有关规定。

第四章 金证天亿系统的安全性

天亿系统有关投资者资金帐户、股票帐户、身份识别等数据的处理均由证券经营机构的系统处理，与外部各子系统没有关系，较好地保存投资者的敏感资料。

天亿系统接入经营机构的业务系统时除了采用安全传输技术外，还经过代理转发、协议网关、存取控制等技术与其他业务系统。

天亿系统有着完善的防单点故障和主系统或设备备份能力。

天亿系统有着完善的系统安全手段。

1. 网络安全：

系统通过可选的防火墙、基于数字证书的安全技术、通讯代理、协议网关、权限控制等多种手段来保障网络安全，特别是 IP/IPX 协议网关是一道天然的防火墙，目前还没有成功攻击的案例。

2. 传输安全：

天亿系统采用基于数字证书的安全技术来保障传输安全，它是目前国际上一种解决电子商务的得到广泛认可的办法，它主要采取以下技术：

1）利用数字信封技术进行敏感数据的加密（防窃取）

2）利用安全的散列函数、数字签名（双重数字签名）技术来保证数据的完整性和一致性（防篡改）。

3）利用数字签名技术来保证交易的不可否认（防否认）。

3. 身份认证：

天亿系统采用基于数字证书的身份认证技术来保证参与交易各方的真实性。以上基于数字证书的加密算法和产品均通过了中国密码办的鉴定。

4. 存储安全：

系统将主要的私有的密钥均存储在硬件加密设备中，做到加密在黑盒子中进行，所有秘密密钥不出设备，极大地保证了秘密密钥的安全。

5.访问控制：

系统可采用网络权限控制、SQL 访问控制等手段进行访问安全控制；证券经营机构还可根据本公司的具体情况，采取技术和管理措施，限制每位投资者通过网上委托的单笔委托最大金额、单个交易日最大成交总金额来进行附加的安全控制。

6.监控日志：

系统包含有实时监控日志和非法访问日志，以便对系统进行实时和事后的监控。