

中国建设银行上海市分行

网上银行的实现

陈峥 周子坚 (中国建设银行上海市分行科技部)

摘要: 本文先简要介绍中国建设银行网上银行的系统架构和系统安全性, 然后主要介绍上海分行接入网银中心的实现方式和功能。

关键词: 网上银行 ES9000 新一代柜面业务系统



1 前言

在1999年初, 中国建设银行总行与合作公司在北京进行了建行网上银行业务的需求分析及软件开发。总行网上银行系统采取总行/网银中心/分行三层体系结构, 提供信息服务、客户服务、帐务查询和实时交易等功能, 其中信息服务和客户服务由总行指定部门从全行范围规划、运作和管理, 网银中心具体实现帐务查询和实时交易功

能, 分行实现业务主机系统与网银中心的实时连接。上海建行作为一个分行, 完成网银中心与分行业务主机的网络联接, 为上海建行的客户提供网上银行服务。

2 系统体系结构

系统体系结构如图1所示:

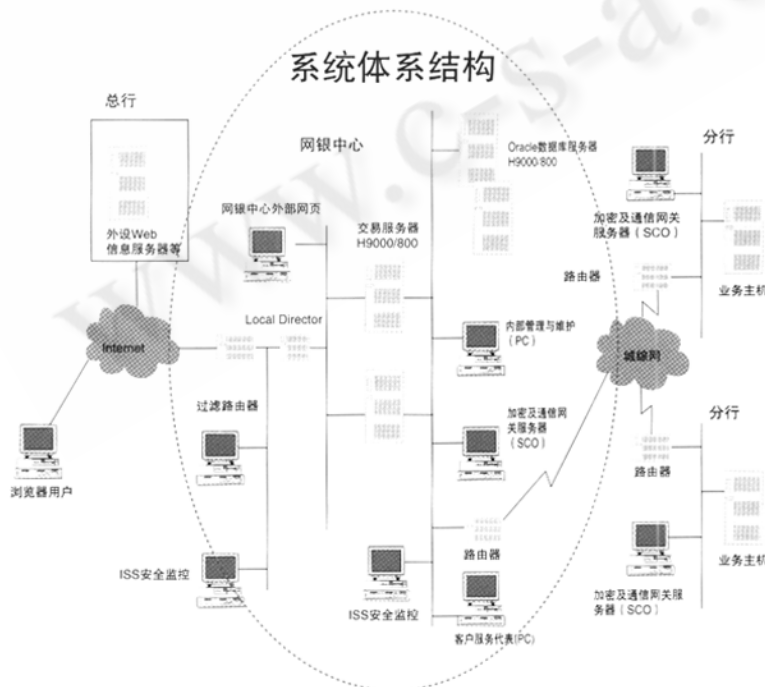


图1

3 网上银行系统的安全设计

3.1 网银中心的交易服务器是一个建立在符合美国国防部 B1 级安全标准的可信操作系统(VirtualVaultOS, 简称 VVOS)之上的安全的 Web 服务器

3.2 ISS 安全监控工作站用于对进出网银中心的各种信息进行网络监控, 可为安全管理员提供可疑信息的“报警、记录、回放”等功能, 并可提供相应的报告, 并可用于对网银中心的各种服务器进行网络层安全漏洞扫描, 为安全管理员提供漏洞报告, 并可根据提示修补漏洞。

3.3 在网银中心和分行端各加设一台加密及通信网关服务器, 负责广域网的通信和加密。所有通信均采用 TCP/IP 协议, 两台加密及通信网关服务器之间的通信及加密采用建行提供的接口程序。

3.4 上海行网银前置机与 ES9000 新一代柜面业务系统之间采用 IBM 传统的 SNA 网络传输协议。SNA 网络协议是一种 IBM 制定的封闭性协议。

3.5 采用 SSL 安全套接层协议保护客户端到 WEB SERVER 之间的数据传输安全, 防止数据在 INTERNET 传输过程中被窃听和截取。

3.6 网上 B2B 业务采用了中国金融认证中心 (CFCA) 颁发 CA 证书, 目前 CFCA 可发放 SET (安全电子交易) 和 NON-SET PKI 证书, 建行采用的是后一种证书。PKI (PUBLIC KEY INFRASTRUCTURE, 公开密钥基础设施) 是在公开密钥技术上发展起来的一种综合安全平台, 它能够透明地提供基于公开密钥的加密和数字签名等安全服务, 构建 PKI 的主要目的是为了对密钥和证书进行管理。

4 上海分行接入网银中心的实现方式

上海建行网上银行接入开发分前置机接口软件开发和 ES9000 新一代柜面业务系统程序改造两部分。

4.1 前置机接口软件系统设计方案

4.1.1 开发 / 运行设备

接口开发和运行各有一套设备, 是 HP LC3 服务器, 操作系统为 SCO OPEN SERVER 5.0.4, 数据库系统采用 INFORMIX ONLINE SERVER 5.0, 内装两块网卡, 一块与总行通信, 一块与银证转帐前置机相联, 还有一块 EICON S91 通信卡, 用于与主机通信。另有一块总行要求配置的加密卡。

4.1.2 接口软件总体结构

(1) 接口软件与网银中心通过 TCP/IP 协议联接: 接

口软件作为服务方, 接收网银中心的联接请求, 交易完成后撤销该联接。

(2) 接口软件与 ES/9000 主机通过 SNA LU0 协议联接: 接口软件以 SNA LU0 协议与 ES/9000 联网。

(3) 网银中心向接口软件发起的交易格式为总行规定的报文格式。

(4) 接口软件向 ES/9000 新一代柜面系统发起交易格式为新系统规定的格式。

结构图如图 2:

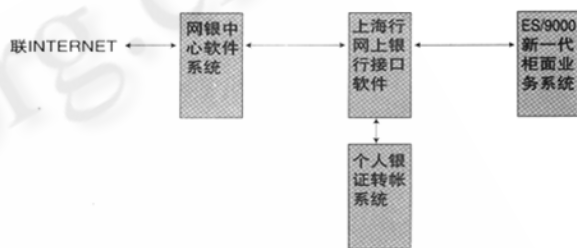


图 2

4.1.3 接口软件开发和处理流程说明

接口软件开发分为四个部分: 通信软件 联机交易处理 交易监控和业务管理。

(1) 通信软件。该通信软件主要利用 EICON 卡提供的 SNA LU0 通信函数, 实现前置机与 ES9000 主机某个 / 几个 CICS 的 SNA LU0 的通信。该通信进程个数可根据网银交易量而定, 目前上海行前置机与两个 CICS 通信, 各启了三个通信进程。(可根据交易量, 多启)

(2) 联机交易处理: 以后台守护进程形式等待网银中心的交易请求, 接收请求复制新的进程处理该交易, 另一进程继续接收下一笔交易, 处理交易的进程根据交易帐号的类别(对公和对私银行卡、活期存折、定期帐户) 分别进行不同的交易格式转换, 送 ES9000 主机处理, 并将主机返回的结果转换成网银中心要求的应答报文返回给网银中心。

(2) 交易监控: 实时监控网上银行的联机交易处理情况, 交易监控进程可以启多个。

(3) 业务管理: 包括网上支付流水查询、隔日主机帐务流水查询、报表管理等

4.2 ES9000 新一代柜面业务系统程序改造

网上银行作为传统柜台的延伸, 主要交易还是沿用柜面交易, 只是作为一个虚拟的柜员的交易。网上银行交易与传统的柜面业务有所不同, 主要体现在:

(下转第 71 页)

(上接第 55 页)

(1) 由于网上银行签约客户本身有登录密码和交易密码, 做网上交易时不需要再校验帐户本身的密码。

(2) 网上银行交易无须柜员干预, 所以柜员不需要签到, 就可做交易, 即所谓的虚拟柜员交易。

(3) 网上银行是 24 小时交易。

(4) 总行网上银行对分行的特殊要求。针对网上银行交易的特殊性 & 总行网银的要求, 对新一代柜面系统进行改造。

主机改造分为卡、活期存折、定期、公用部分、核心部分、批量部分的改造。

5 上海建行网上银行实现功能

上海建行的对私客户, 只要在网上申请网上银行功能后, 即可做申请帐户查询交易, 若要做转帐交易, 可以到上海建行任一个网点做签约。对于网上对公查询或转帐交易, 都需要到对公网点签约。

5.1 查询类

包括对公和对私的余额查询、交易明细查询、到期定期查询、帐户信息查询及消费积分查询。

5.2 转帐类

包括对私的个人活期互转、活期与定期一本通互转、约定帐户转帐、证券保证金转帐。

5.3 挂失类

包括对私的信用卡挂失、储蓄存款挂失、密码临时挂失

5.4 网上支付 (签约客户网上支付和非签约客户网上支付)

包括支付、部分/全额退款、商户交易明细查询、商户支付流水查询、商户余额查询。

5.5 网上企业客户转帐 (B2B)

包括同城建行付款、异地建行付款、主动收款、跨行付款。

6 结束语

中国建设银行上海市分行网上银行的实现, 使建行客户可以不受时间、地域等的限制, 方便而快捷地享受建行的优质服务。在信息高速发展的今天, 金融服务的方便、快捷和安全成为在市场竞争中不可缺少的要素。■