电子商务综合辅导：搭建e银行 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/250/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_250423.htm 伴随着技术创新、金融创新及电子商务的日益盛行，人们对网上金融产品提出了越来越多的要求，于是网上银行应运而生。据调查，渴望上网购物的网民比率高达80%，由此可以预见，为适应网络经济的发展需要，网上银行的兴起和快速发展将势不可挡，网上银行必将成为各商业银行竞争的新焦点。 网上银行（Internet Banking）又称网络银行或在线银行，是指银行利用Internet网络为银行客户提供开户、销户、支付、转帐、查询、汇款、网上证券、投资理财等传统服务项目，使客户足不出户就能够安全快捷地办理银行业务。网上银行业务的出现，改变了商业银行传统的经营模式，使之在管理方式和营销观念上发生了重大变化。 目前网上银行有两种发展模式，一种是传统银行依托原有优势，在互联网上设立站点，客户通过互联网处理传统银行交易业务。这种模式为绝大部分银行所采用。另一种是基于互联网发展起来的全新网上银行，如美国安全第一网络银行（SFNB），它没有任何分支机构，只通过互联网提供全球范围的金融服务。 网上银行包括：个人银行、企业银行、网上支付和金融信息等4大块。细分起来又有：个人信用卡、个人信贷、个人自助银行、个人网上银行、对公信用卡、贷款业务、国际业务、离岸业务、对公网上银行和对公自助银行等业务。另外，客户还可以通过银行站点了解该行的基本情况及与其有业务往来的公司信息。 建立网上银行的好处：* 提升银行形象，增强客户对银行的信

心 一方面显示了银行在科技方面的领先地位，另一方面充分说明了银行雄厚的经济实力。 * 大幅度降低经营成本 银行可以将交易从成本较高的渠道（如分支机构）转向成本较低的渠道（如网上银行）。同时将宝贵的人力资源转向其它服务部门。 * 使银行专注于新产品和服务的开发 使用Internet技术，能够使银行在升级应用或安装新产品时，只需简单地更新或升级服务器应用程序，而不需对客户端作任何变动。这样银行就可以将精力集中于新产品和服务的开发，满足客户的要求，吸引更多的客户。 网上银行体系结构 HP网上银行系统体系结构 图一中外部Web信息服务器的作用是提供银行的主页服务。其中包括网上银行系统的主页内容，供客户了解的各种公共信息，提供网上银行用户在网上填写的用户申请表。 区域性网银中心的主要组成部分包括：过滤路由器、ISS安全监控工作站、VirtualVault（虚拟保险箱）交易服务器、数据库服务器、客户服务代表工作站、内部管理和维护工作站、加密和通讯网关服务器、业务主机。 过滤路由器除了具有在Internet和银行网络之间进行路由选择的功能外，还会对流入银行的数据流进行过滤。数据流分为两大类，一类是送交VirtualVault交易服务器处理的对安全要求特别高的交易数据流，如https数据流；另一类是对安全要求不是特别高的非交易数据流，如访问外部Web信息服务器和电子邮件的数据流。除了这两类数据，所有的数据都将由过滤路由器挡回去。这样做的好处是：降低了交易服务器的处理负荷，同时减少了黑客攻击系统的机会，增强了安全性。 VirtualVault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VVOS（VirtualVaultOS，简称为VVOS）之上的Web服

务器，它直接面向Internet用户。接收到用户请求后，VirtualVault会进行一系列安全检查，只有在完全确认一切正常后，才会将用户的交易请求通过特定的CGI代理程序转送至加密和通信网关服务器进行后续处理。VirtualVault交易服务器接收到用户的请求后，会及时转发至城综网，再由城综网业务处理程序去查询、更新业务主机（分行端的业务主机即现有的城综网业务主机）上的业务数据。 图一 HP网上银行系统体系结构图 在网银中心和分行端各有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可根据用户的要求定制。 ISS安全监控工作站用于对进出本区域性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、记录和回放 ”等功能，并可提供相应的报告。它对本区域性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。 客户服务代表负责接收、解答总行指定部门转发过来的网上银行用户通过Internet网络传送过来的反馈意见、咨询和投诉等。客户服务代表不直接与网上银行系统用户互通电子邮件，都通过总行指定部门转发。客户服务代表使用两台PC机，一台访问网银中心数据库，另一台通过企业网电子邮件系统收发电子邮件。 网上银行的交易流程 网上银行的交易流程包括用户与网上银行系统进行交易的流程和银行内部交易的处理流程。 用户与网上银行系统进行交易的流程为：用户连接到网银中心通过安全审核后，访问网银中心主页面，点击相应功能按钮，填写交易请示表格，查看交易处理结果。 银行内部处理的交易首先流向网银中心，然后转达到

城综网处理后又回到网银中心。其中网银中心的交易流程为：接收用户连接请求→对用户进行安全审核→接收用户交易请求→审核用户交易请求→将交易请求转达到城综网。城综网的交易流程为：接收网银中心代用户转达来的交易请求→处理交易请求→将处理结果返回网银中心。然后网银中心继续：接收城综网返回的处理结果→进行必要的再处理→返回用户交易处理结果。 为了更好地满足客户不同层次的需求和适应中国金融市场，惠普公司的网上银行解决方案提供三种配置：Entry-Level配置（适用于中/小银行）、High-End 配置（适用于全国性网上银行中心/大型商业银行）和High-End HA配置（适用于较高可用性要求的环境）。 惠普成功应用：中国建设银行。 基于CBTF的IBM网上银行解决方案 CBTF（Corepoint Banking Transaction Framework-核心银行交易架构）是IBM公司为金融机构提供的多渠道金融服务综合解决方案，包括网上银行、柜员系统、手机银行和客户服务中心等。基于CBTF的网上银行解决方案构架在IBM WebSphere Application Server、Java、互联网技术和高度参数化开发环境上，支持构件重用，可以快速实施推广，并帮助银行提高生产力。 CBTF实施先进的三层应用体系结构，包括客户端用户界面、服务器端应用逻辑、数据仓库/传统系统（Data Store/Legacy System）三大独立的部分。各应用层次之间通过网络进行通信，结构灵活且不依赖于底层的硬件环境。这三个逻辑层在物理上可以根据银行的需求分别进行实施。其中，客户端用户界面包括逻辑控制展现和信息确认；服务器端应用逻辑包括业务逻辑、控制数据和消息传递的处理过程；数据仓库/传统系统包括银行后台系统的交易应用和数据存储

。IBM为上述的三层体系结构定义了一个通用构架，即基于互联网开放标准的电子商务应用构架，并针对行业特点作了进一步的完善。根据全球范围的行业经验，这种三层体系结构可以提高客户IT部门组织的灵活性，减少推出新应用的费用和时间。同时，由于在客户端采用了现代化的图形用户界面，可以提高系统用户的生产力。 解决方案成功的关键之一就是性能。WebSphere和CBTF是IBM专门为金融行业和跨行业的电子商务产品和系列解决方案设计的策略性平台。使用WebSphere和CBTF开发的应用可以广泛扩展，不断增加新的应用和新的服务渠道，为银行提供多渠道的综合解决方案。另外，CBTF采用高度参数化配置的客户化处理来匹配银行的具体需求，帮助金融机构实现资金或非资金业务的服务。通过在新的应用服务器上采用负载平衡的技术，可以轻松获得横向扩展能力，而无需重写代码。 IBM成功应用：华夏银行。 从技术角度看，网上交易至少需要四个方面功能：商户系统、电子钱包、支付网关和安全认证，其中后三者是网上支付的必要条件。为了确认交易各方的身份以及保证交易的不可否认，需要有一份数字证书进行检验，这就是电子安全证书。同时网上银行传统业务系统，即网上银行的后台业务处理环境需要更加严格的安全防护。安全性，尤其是银行客户的信息、资金和交易的安全性是网上银行存活的关键，建立网上银行首先需要考虑和解决的是 安全问题 惠普对安全问题的看法是：只要选用合适的安全产品和技术，并伴之以严格的安全管理制度，网上银行系统的安全风险是完全可以控制在能够承受的限度内的。 保护Internet与银行Web服务器互联的多数安全解决方案主要依赖防火墙及Internet信息的SSL加

密。HP Praesidium/VirtualVault接管了防火墙和SSL中断的地方，在Internet和银行机构之间提供关键连接的安全保护。HP VirtualVault（虚拟保险箱）是使用最广泛的安全Web服务器平台，它允许银行向客户提供对银行业务数据的访问并实现网上交易，同时保护Web服务器和后端资源不会受到来自Internet的攻击。 VirtualVault的操作系统严格符合美国国防部B1标准和欧洲E3标准，是一个安全的操作系统。该操作系统具有三个主要特征：最少特权机制、数据分区机制和命令授权。 最少特权机制主要针对应用程序设计。它将超级用户/根目录的特权划分为50多种不同的特权，对每个应用程序只给予保证运行所需的最少特权，这样就确保了即使受“特洛伊木马”侵袭的应用程序也不可能改变系统网络设置或文件系统。 数据分区机制相当于在服务器上的Intranet应用和Internet应用之间加入一道虚拟防火墙。数据分区将服务器上的所有文件和程序划分为内部分区、外部分区、系统分区和高级系统四个分区，VirtualVault限制跨分区的访问，只有获得特定的权限才可以跨区访问。内部分区和外部分区之间的所有通信由VirtualVault信任网关负责，可以保护内部分区中的应用程序不受到恶意攻击或因为中间件的错误造成内部应用损坏。 如何对管理员的责任进行划分呢？可以使用“命令授权”。它只给每个人分派某些规定的工作和权限。系统管理员只能访问他被授权的那部分系统管理功能，禁止访问其他区域。 CA认为，绝对安全与可靠的信息系统并不存在。一个所谓的安全系统实际上应该是“使入侵者花费不可接受的时间与金钱，并且承受很高的风险才能闯入的系统”。安全是一个过程而不是目的。 网上银行系统的安全分为网络安

全、服务器安全、用户安全、应用程序和服务安全、数据安全几个部分。网络安全包括什么人对什么内容具有访问权，查明任何非法访问或偶然访问的入侵者，保证只有授权许可的通信才可以在客户机和服务器之间建立连接，而且正在传输当中的数据不能被读取和改变。服务器安全包括需要控制谁能访问服务器或访问者可以干什么，防止病毒和“特洛伊木马”的侵入，检测有意或偶然闯入系统的不速之客。用户安全是管理用户账户，在用户获得访问特权时设置用户功能，或在他们的访问特权不再有效时限制用户帐户。应用程序和服务安全是指对应用程序和服务的口令和授权的管理，大多数应用程序和服务都是靠口令保护的，加强口令变化是安全方案中必不可少的手段。而授权则是用来规定用户或资源对系统的访问权限。数据安全是保持数据的保密性和完整性，不论是在储存状态还是在传递当中，保证非法或好奇者无法阅读它。数据完整性是指防止非法或偶然的数据改动。另外，风险评估被用来检查系统安全配置的缺陷，发现安全漏洞。政策审查则用来监视系统是否严格执行了规定的安全政策。身份验证用来确保用户的登录身份与其真实身份相符，并对其提供单点注册，以解决多个口令的问题。针对以上各种安全性的要求，CA均有相应的产品。CA的eTrust解决方案能保护从浏览器到主机的所有关键任务型资源，其功能包括风险评估、攻击探测、预防损失。eTrust解决方案不仅在网上支付方面拥有先进而高效的认证工具eTrust Directory和 eTrust OCSPro，还有eTrust Intrusion Detection和eTrust Access Control对网上银行后端的业务系统提供严格的网络与服务器的安全保护措施。网上银行需要高度分布式单客户安全和帐户信息

源，以便通过数字证书和智能卡支持的强有力认证，安全地提供丰富的联机银行服务。eTrust Directory就可以提供高可靠性和安全性的支持。那么目录服务如何管理呢？作为大型关键任务型目录服务应用解决方案，eTrust Directory可支持超过20,000,000个目录，并能每秒搜索1,000次。它使管理员无需停机就能更新方案，增强访问控制。 电子商务需要前所未有的更高的安全性标准，包括基于数字认证的验证和实时的认证状态确认。任何已确认的认证状态，无论有效与否，都是至关重要的信息，需要在电子商务交易进行之前加以评估。eTrust OCSPro就是在因特网上实现安全和严格授权的B2B电子商务活动的关键实施技术，它与eTrust Directory完全集成。使用目录来存储配置信息和访问状态使OCSP 响应器能充分利用与eTrust Directory 相关的各种优势，包括发布、性能复制、有效性等。 对于网上银行后端的业务系统，eTrust Intrusion Detection和 eTrust Access Control提供了严格的网络与服务器的安全保护措施。 eTrust Intrusion Detection提供限制Web访问、监控/阻塞/报警、入侵探测、攻击探测等在内的安全保护措施。它最主要的功能是入侵检测，它可以自动识别各种入侵模式，在对网络数据进行分析时与这些模式进行匹配，一旦发现某些入侵的企图，就会进行报警。 利用eTrust Access Control，安全管理员能够设定哪些人对哪些资源有什么样的访问权限。eTrust Access Control对资源的保护采用访问控制列表（ACL）的方式。它实现了在计算机系统中对用户和文件的层次化分类管理，在UNIX的访问控制中实现了某些B1级别的特征。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com