第 2 章　电子商务支付系统

2.1　传统的支付方式

按使用技术的不同，支付方式可以分为传统支付方式和电子支付方式两种。本节重点介绍传统的支付方式。传统支付指的是通过现金流转、票据转让以及银行转账等物理实体的流转来实现款项支付的方式。传统的支付方式主要有两种，即现金和票据。

2.1.1　现金

现金有两种形式，即纸币和硬币，是由国家中央银行发行的，其有效性和价值是由国家保证的。纸币本身价值不高，它只是一种由国家发行并强制流通的货币符号，但却可以作为货币加以流通，其价值是由国家加以保证的；硬币本身含有一定的金属成分，故而具有一定的价值。

在现金交易中，买卖双方处于同一位置，而且交易是匿名的，买卖双方不需要了解对方身份。显然，现金是一种开放的支付方式。任何人只要持有现金，就可以进行款项支付，而无须经中央银行收回重新分配。现金具有使用方便、灵活的特点，多数小额交易是由现金完成的。其交易流程一般是：一手交钱，一手交货。现金交易存在其不足，主要表现在：受时间和空间限制，这给不在同一时间同一地点的交易带来不便；受不同发行主体的限制，这给跨国交易带来不便；对于大宗交易，既不方便，也不安全。

现金的特征包括：

（1）现金支付只需在付款人和收款人之间进行，不必集中在某地某时间集中处理，具有完全分散的特性。

（2）在现金支付中，若付款人持有现金，收款人对现金本身的真实性无异议的话，支付过程可以完全脱离银行，进行离线处理。

（3）现金具有匿名性，只要持有现金就可以用于支付，不必追究持有人的合法地位等。因此现金支付过程简单，在长时期的贸易发展过程中被广泛使用。

但由于现金携带不方便，运钞成本大，无法核实现金持有人的真实合法身份，所以风险大。现金支付主要被用于个人之间，以及个人和企业间金额较小的支付关系中。

2.1.2　票据

票据是为了弥补现金交易的不足而出现的，是出票人允诺或者委托他人见票时或在约定的日期支付确定的金额给持票人的有价证券。票据分为广义票据和狭义票据。广义上的票据包括各种具有法律效力、代表一定权利的书面凭证，如股票、债券、货单、车船票、汇票等，人们将它们统称为票据；狭义上的票据指的是《票据法》所规定的汇票、本票和支票，是一种载有一定的付款日期、付款地点、付款人信息的无条件支付的流通凭证，也是一种可以由持票人自由转让给他人的债券凭证。本书所指的票据都是狭义票据。

通过使用票据，异地的大宗交易不必使用大量现金，减少了携带大量现金的不便和风险。而且，使用票据也有利于将交易中的物流和货币流分开。但票据也有其弊端，比如易伪造、

易丢失，商业承兑汇票甚至存在拒绝付款和到期无力支付的风险，因此，使用票据具有一定的风险。

票据可分为贷记支付工具（Credit Payment Instruments）和直接借记（Direct Debits）支付工具。贷记支付由付款人发出支付命令，要求银行将指定金额转移到收款人账户中，贷记支付工具常用于支付房租、水电费、电话费，纳税、发放工资等；直接借记是由收款人发出支付命令，要求付款人将指定金额从付款人银行账户中转移到收款人银行账户中，但付款人须预先授权银行，执行合法收款人发出的支付命令，常用于定期的、固定支付的各类租金、水电费等。

票据不具备现金的分散、离线、匿名等特性，但是由于不需要大量的现金，比较安全，便于携带，且转让时需要背书，贴现时需要验证身份，必要时可以通过追索挽回损失。一般用于企业之间金额较大的支付，其操作过程比较复杂，涉及收付双方和中间金融机构等多家单位。

传统支付中，支付指令的传递完全依靠面对面的手工处理和经过邮政、电信部门的委托传递。因而结算成本高，凭证传递时间长，在途资金积压大，资金周转慢。

2.2 电子支付的概念

电子支付（E-payment），也称数字化支付（Digital Payment），指的是电子交易的当事人，包括消费者、商家和金融机构，使用安全电子支付手段通过网络进行的货币支付或资金流转。与传统的支付方式相比，电子支付具有以下特征：

第一，电子支付是采用先进的技术通过数字流转来完成信息传输的，其各种支付方式都是通过数字化的方式进行款项支付；而传统的支付方式则是通过现金的流转、票据的转让以及银行的汇兑等物理实体来完成款项支付的。

第二，电子支付的工作环境是基于一个开放的系统平台（即互联网）；而传统支付则是在较为封闭的系统中运作。

第三，电子支付使用的是最先进的通信手段，如 Internet、Extranet，而传统支付使用的则是传统的通信媒介；电子支付对软、硬件设施的要求很高，一般要求有联网的微型计算机、相关的软件及其他一些配套设施，而传统支付则没有这么高的要求。

第四，电子支付具有方便、快捷、高效、经济的优势。用户只要拥有一台上网的计算机，便可足不出户，在很短的时间内完成整个支付过程。支付费用仅相当于传统支付的几十分之一，甚至几分之一。

目前已经推出的电子支付方式是以金融电子化网络为基础，以商用电子化设备和各类交易卡或数字文件为媒介，货币以电子数据（二进制数据）形式存储在交易卡中，以及银行或消费者的计算机系统中，并通过计算机网络系统以电子信息传递形式实现流通和支付功能。电子支付流程图如图 2-1 所示。

2.3 支付网关

2.3.1 什么是支付网关

支付网关是代表商户在网上的金融机构，它是设置在网上商家与传统银行信用卡处理系统之间的中间接口机构。其作用是对 Internet 上的 SET 协议与金融机构专用协议（如 ISO 8583 协议）进行转换，即为从商家返回的信息和发往银行卡处理系统的信息提供了通信和协议转换

的功能。它还提供了用户可以编程的出口，用于将 SET 信息转换为现有的卡处理系统所需要的客户化格式以进行本地处理。商户利用从消费者处获取的支付信息，通过支付网关寻求金融机构的认证。支付网关还执行所有的 SET 密码算法功能。

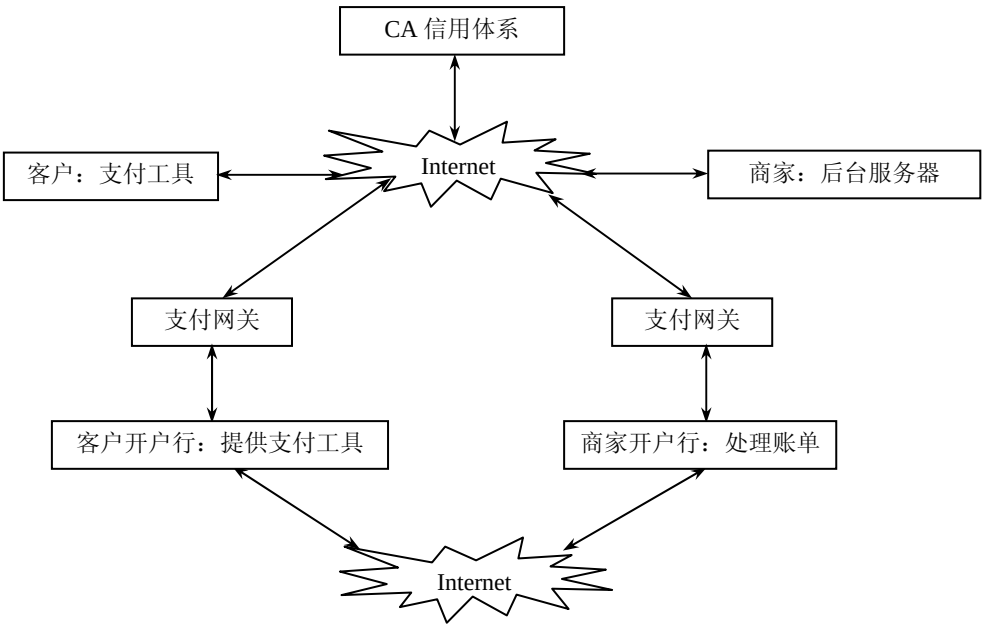

图 2-1　电子支付流程图

支付网关（Payment Gateway）是银行金融网络系统和 Internet 网络之间的接口，是由银行操作的将 Internet 上传输的数据转换为金融机构内部数据的一组服务器设备，或由指派的第三方处理商家支付信息和顾客的支付指令。支付网关可确保交易在 Internet 用户和交易处理商之间安全、无缝地传递，并且无需对原有主机系统进行修改。它可以处理所有 Internet 支付协议、Internet 安全协议、交易交换、信息及协议的转换以及本地授权和结算处理。另外，它还可以通过设置来满足特定交易处理系统的要求。离开了支付网关，网络银行的电子支付功能也就无法实现。

支付网关提供的交易类型如下：

（1）授权交易：网关将商家以 SET 方式的授权请求换成 ISO 8583 授权请求信息，通过专用网络从银行处得到应答，并将应答转为 SET 格式回送商家。

（2）授权交易取消：对于银行成功授权并已通过网关将交易应答成功返回商家的授权交易，网关将把商家获得授权取消请求的 SET 格式，转换成 ISO 8583 授权取消请求消息，通过金融专用网络从银行得到应答，并将应答转为 SET 格式回送用户。

（3）扣款交易：该交易用于扣款交易信息格式的转换和处理扣款交易的授权请求。

（4）扣款交易取消：对于银行成功扣款，并已通过网关将交易应答成功返回商家的结算交易。网关将从商家获得的授权取消请求转换成 ISO 8583 扣款取消请求消息，通过金融专用网络从银行得到应答，转换成 SET 格式回送商户。

（5）支付网关可根据客户的需要，提供 SET 标准规定的其他交易类型。

支付网关的典型应用为电子商务交易中心、在线电子支付系统、网上银行系统、移动银行系统、证券系统、网上购物系统等。

2.3.2 支付网关的主要功能

网上支付是电子商务运作过程的一个关键环节，电子商务安全支付网关为消费者、商家和金融机构提供用于交换商品或服务的安全电子交易手段，即将新型支付手段（电子现金、信用卡、借记卡、智能卡等）的支付信息通过网络安全传送到银行或相应的处理机构，利用消费者客户端的电子钱包、移动电话、呼叫中心等软件，通过商家的虚拟收银台、销售点终端（Point of Sale，POS）机等软件和银行端的支付网关软件等，完成联机订单的受理、转账申请、交易确认等支付功能，实现电子支付。电子商务安全支付系统将于电子商务安全认证系统一起搭建整个电子商务体系的核心。

将 Internet 传来的数据包解密，并按照银行系统内部的通信协议将数据重新打包；接收银行系统内部传回来的响应消息，将数据转换为 Internet 传送的数据格式，并对其进行加密。即支付网关主要完成通信、协议转换和数据的加密/解密功能，以保护银行内部网络。

1. 支付网关要完成的任务

（1）确认请求支付信息。对商家转发到支付网关的支付请求信息 PI 要进行确认，主要确认交易 ID。

（2）对支付请求指令进行解密。支付请求指令对支付信息 PI 是加密的，商家不能解读 PI 信息，智能解读 PI 订单信息，支付网关接收到 PI 加密信息，用其私钥进行解密。

（3）验证客户的电子证书是否与在使用的账号相匹配。支付网关对用户证书中所指明的账号信息，与其在发卡行使用的账号应一致，即向发卡行进行授权处理。

（4）验证支付指令的完整性。支付指令应包括支付银行卡卡号、日期与个人标识号（Personal Identification Number，PIN），还应对订单信息、交易金额、交易内容等的完整性进行验证。

（5）对响应进行数字签名。支付网关对交易请求的响应要进行数字签名，以防抵赖。

2. 支付网关的主要功能

（1）配置和安装 Internet 支付能力。

（2）避免对现有主机系统的修改。

（3）采用直观的用户图形接口进行系统管理。

（4）适应诸如扣账卡、电子支票、电子现金以及微电子支付等电子支付手段。

（5）提供完整的商户支付处理功能，包括授权、数据捕获和结算及对账等。

（6）通过对 Internet 上交易的报告和跟踪，对网上活动进行监视。

（7）通过采用 RSA 公共密钥加密和 SET 协议，可以确保网络交易的安全性。

（8）使 Internet 的支付处理过程与当前支付处理商的业务模式相符，确保商户信息管理上的一致性，并为支付处理商进入 Internet 交易处理提供机会。

3. 支付网关的详细功能

（1）完成正常的网上支付，包括格式转换和联机交易信息转换功能；交易的合法性检查功能；交易路由控制功能；商户对账、交易结算及日终批处理功能；能够支付网上银行、移动银行、证券交易、网上购物等领域的应用。

（2）采用数字签名和数字证书就是保证数据的隐私性、一致性、不可抵赖性和合法身份。支持多级证书体系，即验证双方不必持有同一认证机构发出的证书，只要双方所持有证书的认证机构中有共同信任的认证机构，即可验证。

（3）异常处理功能。除提供网上正常交易外，应能提供异常交易处理功能，如超时、线

路中断等，同时具备存储转发能力。

（4）商户和支付网关证书管理功能。

（5）网络管理和系统监控功能，以及系统参数配置管理功能。

（6）交易日志记录、查询及管理功能。

（7）网上商户管理功能。

2.3.3　支付网关的构成

1. 逻辑结构

支付网关的逻辑结构共分四大部分：最基层是 Internet；上面是连接转换的各种协议，如 HTTP、TCP/IP、ISO 8583 转换及 SET、SSL 协议等；在各种通信协议之上是应用接口 API；最上面是由应用控制模块，如格式解析、身份验证、证书存储、日常管理、审计、交易/请款、异常处理及查询模块。

（1）Crypto API：支付网关安全的基础，主要提供加密/解码、签名/验证等安全操作。

（2）查询：包括交易结果的查询、操作日志的查询、商家的查询等。

（3）格式解析：将客户或商家传来的交易信息转换为 ISO 8583 的格式。

（4）证书存储：保存用来验证商家和客户的证书信任链。

（5）审计：对日常操作的记录。当出现纠纷时作为仲裁依据。

（6）异常处理：提供支付过程中由于网络故障、超时等原因造成的无法正常完成支付时采用的处理方法。

（7）身份验证：验证商家和客户的身份是否合法。

（8）日常管理：对商家的管理、支付网关自身密钥的管理等。

（9）交易/请款：将支付指令提交给发卡中心，请求银行划款，并将交易结果返回。

2. 支付网关的物理结构

在 SET 交易环境中，支付网关位于商家与银行收单行之间。商家与支付网关的连接是通过 Internet 或专用网，支付网关与银行收单行的连接是通过金融专网。支付网关与商家、支付网关与收单行之间运行 SET 协议、流通授权与扣款信息。在持卡人与商家之间为 Internet 连通，运行 SET 协议、流通购物信息与支付信息。

一般支付网关由大型服务器与数据库组成，运行支付网关软件，它提供了建立和分析 ISO 8583 标准信息格式和进行格式转换的能力，它主要被客户用于网关出刊使用，用于与传统银行卡目标系统连接时的支付网关信息格式化。

在支付网关与 Internet 连接处，应设置防火墙。支付网关软件应被设计成为可以使用任何防火墙产品。

支付网关的工作流程：

第一步，商业客户向销售商订货，首先要发出“用户订单”，该订单应包括产品名称、数量等一系列有关产品问题。

第二步，销售商收到“用户订单”后，根据“用户订单”的要求向供货商查询产品情况，发出“订单查询”。

第三步，供货商在收到并审核完“订单查询”后，给销售商返回“订单查询”的回答。基本上是有无货物等情况。

第四步，销售商在确认供货商能够满足商业客户“用户订单”要求的情况下，向运输商发出有关货物运输情况的“运输查询”。

第五步，运输商在收到“运输查询”后，给销售商返回运输查询的回答，如有无能力完成运输及有关运输的日期、线路、方式等要求。

第六步，在确认运输无问题后，销售商即刻给商业客户的“用户订单”一个满意的回答，同时要给供货商发出“发货通知”，并通知运输商运输。

第七步，运输商接到“运输通知”后开始发货，接着商业客户向支付网关发出“付款通知”，再支付网关和银行结算票据等。

第八步，支付网关向销售商发出交易成功的“转账通知”。

2.4 电子支付工具

随着计算机技术的发展，电子支付的工具越来越多。这些支付工具可以分为三大类：一类是电子货币类，如电子现金、电子钱包等；另一类是电子信用卡类，包括智能卡、借记卡、电话卡等；还有一类是电子支票类，如电子支票、电子汇款（EFT）、电子划款等。这些方式各有自己的特点和运作模式，适用于不同的交易过程。

虽然电子支付的发展方向是兼容多种工具，但目前做到这一点很困难。因为不同电子支付工具在技术和原理方面有着很大的区别。从目前开发出来的电子支付系统来看，一般都是针对某种支付工具设计的，例如，SET 协议适用于信用卡支付，MSF 是针对电子支票设计的，Modex 是为电子现金而设计的。

2.4.1 信用卡支付

信用卡是网络银行的重要支付工具，是全世界最早使用的电子货币。信用卡 1915 年起源于美国，已经有 90 多年的历史。信用卡从根本上改变了银行的支付方式、结算方式，从根本上改变了人们的消费方式和消费观念，是一种重要的、广泛应用的电子支付工具。信用卡的国际组织有：维萨国际组织（VISA International）、万事达国际组织（Master Card International）、JCB（Japanese Credit Bureau）信用卡公司、美国运通公司（American Express）。信用卡有以下主要功能：

（1）ID 功能：能证明持卡人的身份，确认使用者是否为本人。

（2）结算功能：可用于支付购买商品、享受服务的款项，是非现金、支票、期票的结算功能。

（3）信息记录功能：将持卡人的个人信息和使用情况等各类数据予以记录。

此外，随着业务的扩大，信用卡也有了一些附加的功能：

（1）消费信用功能：代替现金使用消费信用进行消费活动。

（2）消费信贷功能：允许透支及收取部分透支利息。

（3）吸收存储功能：保证金按定期储蓄计息，备用金则按活期储蓄存款计息。

（4）转账计算功能：可在非特约商户购物，即到开办信用卡业务的分支机构办理异地或同域购物的转账结算。

（5）通存通兑：可在开办信用卡业务的分支机构，以及不同发卡系统的分支机构通存通兑现金。

（6）自动存取款：持信用卡可到 ATM（自动柜员机）上自动存取款、转账、查询余额和修改密码。

（7）代发工资。

（8）代理收费：银行代理公用事业单位收费。

（9）信誉标志：卡的级别本身标志着持卡人和持卡单位的信誉水平。

目前，信用卡有磁卡型信用卡和智能（IC）卡型。其中，磁卡型信用卡在全世界已经非常普及，发卡量达数十亿张，并且已经形成了全球性的信用卡应用支付与结算网络系统，使信用卡可以很方便地跨地区、跨国家进行使用。仅 VISA 国际组织的信用卡年交易额就在 8000 亿美元以上。

IC 卡是在法国问世的。20 世纪 70 年代中期，法国 Roland Moreno 公司采取在一张信用卡大小的塑料卡片上安装嵌入式存储器芯片的方法，率先开发成功 IC 存储卡。经过 20 多年的发展，真正意义上的 IC 卡，即在塑料卡上安装嵌入式微型控制器芯片的 IC 卡，已由摩托罗拉和 Bull HN 公司于 1997 年研制成功。在美国，目前人们更多地使用 ATM 卡。IC 卡与 ATM 卡的区别在于两者分别是通过嵌入式芯片和磁条来存储信息。但由于 IC 卡存储信息量较大，范围较广，安全性也较好，因而逐渐引起人们的重视。

我国 1993 年起在全国范围内开展“金卡工程”，目标是从 1993 年起，用 10 年左右的时间，在 3 亿城市人口中推广普及金融交易卡，实现支付手段的革命性变化，使其跨入电子货币时代。其总体构想是建立全国统一的金卡专用网、金卡服务中心和金卡发行体系。1997 年，中国信用卡发行总量达到 6000 万张。1999 年 6 月底，全国各银行发行的信用卡超过 1.3 亿张，2000 年年底达到 2 亿张，在“国家金卡工程全国 IC 卡应用规划”（1993～2003 年，即第一个十年规划）的基础上，国家金卡工程协调领导小组办公室组织各相关部委和金卡工程试点省市共同编制了《国家金卡工程全国 IC 卡应用（2008－2013 年）发展规划》，指出了 2008～2013 年金卡工程发展目标是：到 2013 年年末，基于磁条卡、IC 卡和 RFID（射频识别）电子标签等介质的各类卡应用系统进一步普及；信息基础设施、政策体系与制度环境建设更趋完善；为金卡工程提供配套的信息与通信产业的自主创新能力与核心竞争力显著增强，拥有的自主标准、核心技术和知识产权日益增加，为金卡工程提供技术、产品、应用软件、整体解决方案和综合信息服务的能力及信息安全保障水平大幅提高;金卡工程建设带来的经济效益与社会效益更加显著，为进一步普惠大众及推进社会信息化进程奠定坚实的技术与物质基础。

IC 卡可应用为银行电子付款卡、信用卡和电子钱包等。许多银行都使用 IC 卡发行了各种形式的银行卡。智能（IC）卡采用当今最先进的半导体制造技术和信息安全技术，比磁条信用卡更为安全，不需联网，可以脱机工作，持卡人可以直接与有关公司、商户、机构进行即时结算等优良功能，也可以作为网络电子转账支付的工具。目前，全球已发行 IC 卡型电子货币超过 5 亿张，其中 60%以上在欧洲。IC 卡相对于其他种类的卡具有以下突出的特点：

（1）存储容量大。存储容量可以从几个字节到几兆字节。

（2）体积小，重量轻，抗干扰能力强，便于携带。

（3）安全性高。IC 卡从硬件和软件等几个方面实施其安全策略，可以控制卡内不同区域的存取特性，存储卡本身具有控制密码，试图非法对之解密，则卡片自毁，即不可进行读写，所以智能卡内数据具有很高的安全性。

（4）对网络要求不高。IC 卡的绝对安全可靠性使其在应用中对计算机网络的实时性、敏感性要求降低，十分符合当前我国国情，有利于在网络质量不高的环境中应用。

信用卡简单运作流程如图 2-2 所示，信用卡详细运作流程如图 2-3 所示。

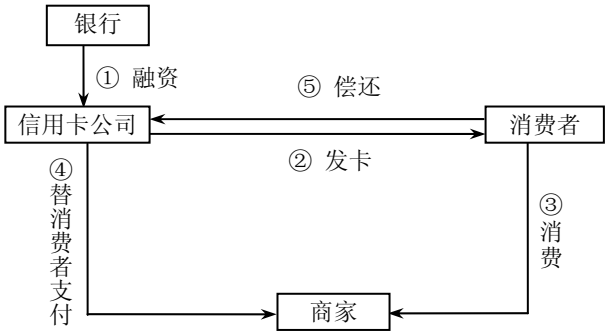

图 2-2　信用卡简单运作流程

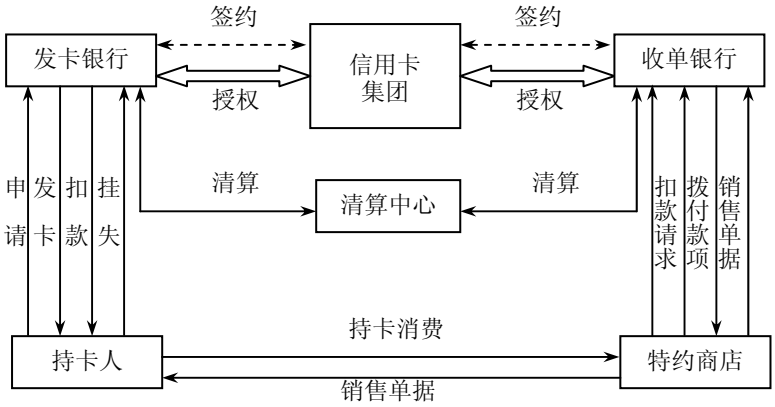

图 2-3　信用卡详细运作流程

2.4.2　电子支票

电子支票是一种借鉴纸张支票转移支付的优点，利用数字传递将钱款从一个账户转移到另一个账户的电子付款形式。这种电子支票的支付是在与商户及银行相连的网络上以密码方式传递的。多数使用公用关键字加密签名或个人身份证号码（PIN）代替手写签名，用电子支票支付，事务处理费用较低，银行也能为参与电子商务的商户提供标准化的资金信息，故而可能是最有效率的支付手段。

使用电子支票进行支付，消费者可以通过电脑网络将电子支票发向商家的电子信箱，同时把电子付款通知单发到银行，银行随即把款项转入商家的银行账户。这一支付过程在数秒内即可实现。然而，这里面也存在一个问题，那就是如何鉴定电子支票及电子支票使用者的真伪。因此，就需要有一个专门的验证机构来对此做出认证，同时，该验证机构还应像 CA 那样能够对商家的身份和资信提供认证。

电子支票交易的过程可分为以下几个步骤：

（1）消费者和商家达成购销协议并选用电子支票支付。

（2）消费者通过网络向商家发出电子支票，同时向银行发出付款通知单。

（3）商家通过验证中心对消费者提供的电子支票进行验证，验证无误后将电子支票送交银行索付。

（4）银行在商家索付时通过验证中心对消费者提供的电子支票进行验证，验证无误后即向商家兑付或转账。

电子支票的支付目前一般是通过专用网络、设备、软件及一套完整的用户识别、标准报文、数据验证等规范化协议完成数据传输，从而控制安全性。这种方式已经较为完善。电子支票现在发展的主要问题是今后将逐步过渡到公共互联网络上进行传输。目前的电子资金转账（Electronic Fund Transfer，EFT）或网上银行服务（Internet Banking）方式，是将传统的银行转账应用到公共网络上进行的资金转账。一般在专用网络上应用具有成熟的模式（如 SWIFT 系统），公共网络上的电子资金转账仍在实验之中。目前大约 80%的电子商务仍属于贸易上的转账业务。电子支票的支付流程如图 2-4 所示。

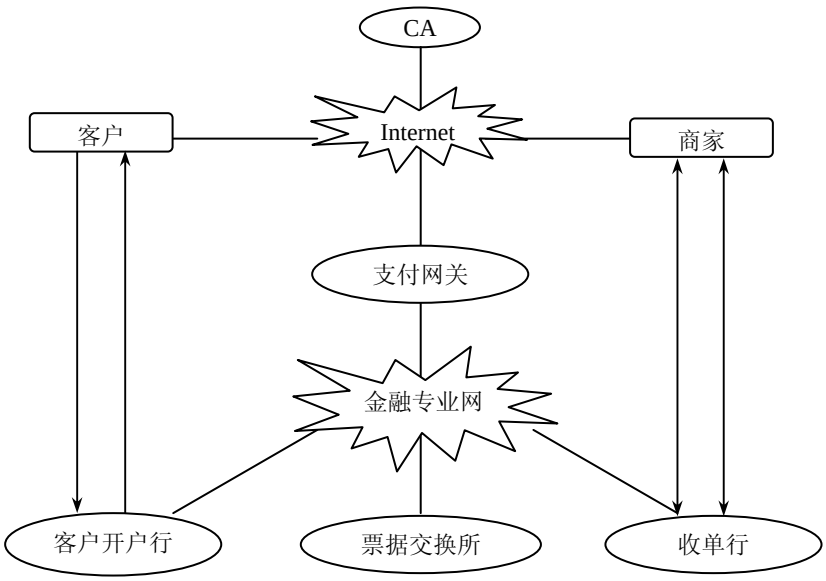

图 2-4　电子支票的支付流程

2.4.3　电子现金

电子现金，是以电子化数字形式存在的现金货币。电子现金的发行方式包括存储性质的预付卡和纯电子系统形式的用户号码数据文件等形式。它同信用卡不一样，信用卡本身并不是货币，只是一种转账手段，而电子现金本身就是一种货币，可以直接用来购物。但它与传统的货币不一样，不是一种物理实体的货币，是通过数据的交换实现现金的功能。

电子现金有两大优点：一是可经过网络瞬时把现金送到远处，即它具有极大的移动性。因为电子现金是一种数字信息，所以它与普通数据一样，可以放在计算机中并由网络传送，从消费者终端直接送到商店终端，不必向中间的清算机构支付手续费。二是可实现支付的匿名性（即不知道这笔钱原先是谁的），而电子清算服务（如信用卡）难以实现匿名性。随着各种各样社会系统的电子化，出现了自动收集有关个人秘密信息的倾向。使用电子现金将是在计算机社会中，实现自卫（保守个人秘密）的有效手段。因此，电子现金在电子商务中作为支付工具将得到重点发展。

电子现金是数字信息，它与纸币一样，本身并没有价值，所以有被伪造的危险。为此，就要使用电子签名等加密技术。从技术上说，电子签名比纸币上使用的水印更难伪造，但电子现金与其他数字信息一样容易复制，因此需要防止电子现金持有者将其复制，然后向多家店铺支付。另外，电子现金的匿名性会给来路不明的钱财提供洗钱的方便，这点也需要防范。

电子现金的支付过程可以分为 4 步：

（1）用户在 E-Cash 发布银行开立 E-Cash 账号，用现金服务器账号中预先存入的现金来购买电子现金证书，这些电子现金就有了价值，并被分成若干成包的“硬币”，可以在商业领域中进行流通。

（2）使用计算机电子现金终端软件从 E-Cash 银行取出一定数量的电子现金存在硬盘上。

（3）用户与同意接收电子现金的厂商洽谈，签订订货合同，使用电子现金支付所购商品的费用。

（4）接收电子现金的厂商与电子现金发放银行之间进行清算，E-Cash 银行将用户购买商品的钱支付给厂商。

电子现金的支付过程如图 2-5 所示。

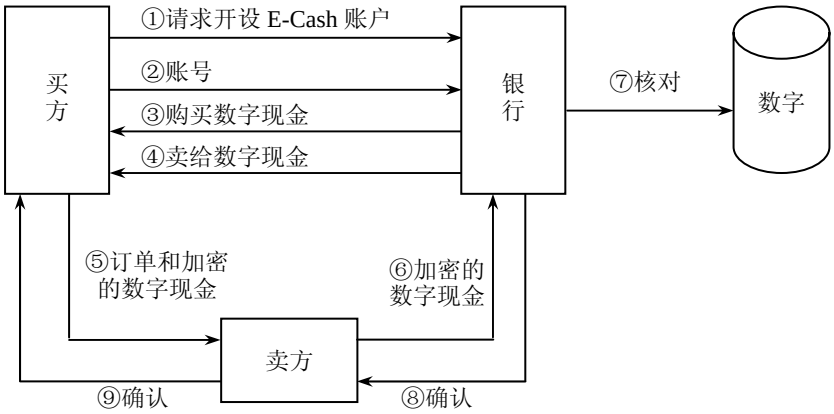

图 2-5　电子现金支付流程图

目前，电子现金支付已经使用的有两种典型的实用系统：DigiCash 系统和 NetCash 系统。DigiCash 指无条件匿名电子现金支付系统。主要特点是通过数字记录现金，集中控制和管理现金，是一种足够安全的电子交易系统。NetCash 指可记录的匿名电子现金支付系统。主要特点是设置分级货币服务器来验证和管理电子现金，其中电子交易的安全性得到保证。

2.4.4　电子钱包

电子钱包（Electronic Purse）是电子商务活动中顾客购物常用的一种支付工具，是在小额购物或购买小商品时常用的新式钱包。它是以智能卡为电子钱包的电子现金支付系统，应用于多种用途，具有信息存储、电子钱包、安全密码锁等功能，安全可靠。

Mondex 卡终端支付只是电子钱包的早期应用，从形式上看，它与智能卡十分相似。而今天电子商务中电子钱包则已完全摆脱了实物形态，成为真正的虚拟钱包。

网上购物使用电子钱包，需要在电子钱包服务系统中进行。用户可以直接使用与自己银行账号相连接的电子商务系统服务器上的电子钱包软件，也可以通过各种保密方式利用因特网上的电子钱包软件。目前世界上有 Visa Cash 和 Mondex 两大电子钱包服务系统，其他电子钱包服务系统还有 MasterCard Cash、EuroPay 的 Clip 和比利时 Proton 等。利用电子钱包在网上购物，通常包括以下步骤：

（1）客户使用浏览器在商家的 Web 主页上查看在线商品目录浏览商品，选择要购买的商品。

（2）客户填写订单，包括项目列表、价格、总价、运费、搬运费、税费。

（3）订单可通过电子化方式从商家传过来，或由客户的电子购物软件建立。有些在线商场可以让客户与商家协商物品的价格（例如出示自己是老客户的证明，或给出商家竞争对手的价格信息）。

（4）顾客确认后，选定用电子钱包来支付。将电子钱包装入系统，单击电子钱包的相应项或电子钱包图标，电子钱包立即打开；然后输入自己的保密口令，在确认是自己的电子钱包后从中取出一张电子信用卡来付款。

（5）电子商务服务器对此信用卡号码采用某种保密算法算好并加密后，发送到相应的银行去，同时销售商店也收到了经过加密的购货账单，销售商店将自己的顾客编码加入电子购货账单后，再转送到电子商务服务器上去。这里，商店对顾客电子信用卡上的号码是看不见的，不可能也不应该知道，销售商店无权也无法处理信用卡上的款项。因此，只能把信用卡送到电子商务服务器上去处理，经过电子商务服务器确认这是一位合法顾客后，将其同时送到信用卡公司和商业银行，在信用卡公司和商业银行之间要进行应收款项和账务往来的电子数据交换和结算处理。信用卡公司将处理请求再送到商业银行请求确认并授权，商业银行确认并授权后送回信用卡公司。

（6）如果经商业银行确认后拒绝并且不予授权，则说明顾客的这张电子信用卡上的钱数不够用了或者是为零，或者已经透支。遭商业银行拒绝后，顾客可以再单击电子钱包的相应项再打开电子钱包，取出另一张电子信用卡，重复上述操作。

（7）如果经商业银行证明这张信用卡有效并授权后，销售商店就可交货。与此同时，销售商店留下整个交易过程中发生往来的财务数据，并出示一份电子收据发送给顾客。

（8）上述交易成交后，销售商店就按照顾客提供的电子订货单将货物在发送地点交到顾客或其指定的人手中。

电子钱包的购物过程中间虽经过信用卡公司和商业银行等多次进行身份确认、银行授权各种财务数据交换和账务往来等，但这些都是在极短的时间内完成的，这种电子购物方式十分省事、省力、省时。而且，对于顾客来说，整个购物过程自始至终都是十分安全可靠的。由于顾客的信用卡上的信息别人是看不见的，因此保密性很好，用起来十分安全可靠。另外，有了电子商务服务器的安全保密措施，就可以保证顾客去购物的商店必定是真的，不会是假冒的，保证顾客安全可靠地购到货物。

总之，这种购物过程彻底改变了传统的面对面交易和一手交钱一手交货等购物方式，是一种很有效的而且非常安全可靠的电子购物过程，是一种与传统购物方式根本不同的现代高新技术购物方式。

2.5　电子支付的安全

现在越来越多的人通过 Internet 进行商务活动。在 Internet 环境中开展电子商务，客户、商家、银行等诸多参与者都会担心自己的利益是否能够真正得到保障。因此，各国政府、国际组织以及 IT 界都在致力于安全问题的研究，期望把网上的混沌世界逐步变得有序、可信、安全。只有保证了电子商务的安全，才能够吸引更多的社会公众投身电子商务，应用电子商务，发展电子商务，才能使电子商务健康地生存并高速地发展。

2.5.1　电子商务的安全现状

运作在 Internet 上的电子商务，每天需要进行千百万次的安全交易，而 Internet 本身又是

一个高度开发性的网络，这与电子商务所需要的保密性是矛盾的。但 Internet 又没有完整的网络安全体制，因此，基于 Internet 上的电子商务在安全上无疑会受到严重威胁，电子商务交易的安全性问题将是实现电子商务的关键。

在电子商务的发展过程中，各产业对网络的技术依赖达到空前的程度。军事、经济、社会、文化各方面都越来越依赖于网络。这种高度依赖性使社会变得十分脆弱，一旦计算机网络受到攻击不能正常运作时，整个社会就会陷入危机的泥沼。因此，电子商务的安全性日益受到各国的安全重视。

随着经济信息化进程的加快，计算机网络上黑客的破坏活动也随之猖獗起来，黑客及黑客行为已对经济秩序、经济建设、国家信息安全构成严重威胁。黑客是 Hacker 的音译，原意是指有造诣的计算机程序设计者。现在则专指那些利用自己掌握的计算机系统，偷阅、篡改或窃取他人机密数据资料，或利用网络进行犯罪的人，如利用通佰软件。通过网络非法进入他人系统，截获或篡改他人计算机数据，危害信息安全的计算机入侵者或入侵行为。

黑客的袭击在计算机网络发达的国家尤为严重。在 Internet 上，黑客组织共享服务器网址、信道，提供免费的黑客工具软件，介绍黑客手法，出版网上黑客杂志和书籍，因此普通人很容易学会网络攻击方式。目前，国际黑客对各国计算机系统中高度敏感保密信息的攻击和窃取正在日益上升，例如，对美国国防部的攻出行动每年达 25 万次以上，并且在不断增长。据相关机构估计，在全球有 80%网站都受到安全威胁，而在国内则有 90%的电子商务网络都存在着安全隐患。2004 年 2 月 7 日至 2 月 9 日，美国八大著名网站，如美国有线电视新闻网、雅虎、亚马逊等几乎同时遭到黑客接二连三的袭击，以致发生拒绝服务的时间长达 45 分钟到 5 小时不等，直接经济损失 12 亿美元。与此同时，中国的新浪网也遭到了黑客的袭击，造成其电子邮件系统瘫痪，经过工作人员 3 个多小时的抢修才恢复了正常工作。

上述情况表明，依法惩治黑客犯罪行为的难度较大，反黑客工作尚存在相当大的困难。一方面科学家很难开发出对保障网络安全普遍有效的技术，另一方面又缺乏足以保证这些手段得到实施的社会环境。随着 Internet 的普及，电子商务安全问题已成为信息时代必须尽快加以解决的重大课题。人们不难想象，黑客的攻击一旦得逞，小则使网络的某项服务瘫痪，大则导致整个商务系统的瘫痪，长时间内无法恢复，造成不可估量的损失。因此，电子商务的安全应受到我国政府与企业的高度重视。例如，著名的美国联机公司因人为操作和技术上的失误，使其 600 万用户陷入瘫痪 10 小时；另一家网络联机通信服务公司的主干网出现重大故障，40 万用户被迫中断联络 40 小时。

电子商务系统在防不胜防的破坏性活动面前，有时会显得软弱无力，谁都无法预测会受到什么样的挑战，信息安全漏洞难以堵塞。一方面，由于缺乏统一的信息安全标准、密码算法和协议，安全与效率难以两全；另一方面，由于大多数管理者对网络安全不甚了解也导致信息的不安全。此外，信息犯罪属跨国界的高技术犯罪，要用现有的法律来有效地防范十分困难，现有的科技手段也难以侦察到计算机恐怖分子的行踪，罪犯只需要一台能上网的计算机就可远距离作案。

2.5.2 电子商务安全的重要性

商务运作的一系列过程都体现着参与商务行为各方的权利、责任、义务和利益。传统意义的商务活动是人和人当面交往建立的信任，在书面契约确立的责、权、利依法保障下的经济活动，经过漫长的社会实践，在社会的意识、素质、道德、政策、法规、技术等各个层面，已经形成了逐步完善、大体适应的商务运作规范和支撑环境。而电子商务作为一种全新的商务运

作模式，其主要依托环境是当前的国际互联网（Internet）和未来的国际信息基础设施，给开放的网络带来了全球可达、全天候服务、自由浏览、高效获取和交换信息等共享信息的极大好处。从业机构的开业挂牌，广而告之，出示产品和服务，联系业务，签署交易协议，交易款项的存、取、支付，交易结果的查询追踪都要围绕网络的利用来展开。在开放的网络环境下，网络信息的安全问题日益凸显出来，电子商务必须要考虑在相隔千里，只有数字化交往和约定的情况下，如何建立相互信任，如何确定商务活动参与各方的责、权、利，如何提供有法律依据的凭证等一系列问题。这些问题用一句话来概括，就是电子商务的安全问题。

只有保证了电子商务的安全，才能保证电子商务的正常运作，才能吸引更多的社会公众投身电子商务，运用电子商务，发展电子商务，才能使电子商务健康生存和高速发展。

1. 电子商务安全涉及国家经济安全

商务活动是国家经济生活中的一个重要环节，社会生产出来的各种产品在市场经济的条件下，需要通过商务活动销售到用户手中，最终显示出其使用价值，创造出社会财富。电子商务是传统商务的革命性发展，它代表着社会的信息化进程，在这个进程中，国家的安全与经济的安全越来越不可分割，经济安全越来越依赖于信息化基础设施的安全程度。随着计算机、通信、多媒体的广泛应用，尤其是美国国家信息基础设施（NII）和全球信息基础设施（GII）投入运行，国际社会特别是发达国家对信息安全空前关注，除了重视传统意义的军事安全以外，越来越重视信息攻击的威胁性，作为国家基本经济活动的商务活动如果遭到破坏、攻击，产生混乱，社会生活就不得安宁，如果没有电子商务安全，国家的经济体制和秩序安全、金融与货币安全、产业与市场安全、战略物资与能源安全、对外贸易与投资安全就不能在数字化、网络化环境中得到有效的保障，也使诸如保障社会生产和生活的正常秩序，保持社会各阶层和睦相处，控制犯罪、贫穷、腐败等消极现象，尊重多数人权利与选择等社会和个人的安全要求在未来社会中难以实现。因此，从国家战略角度上讲，电子商务安全是国家经济安全的重要组成部分，是信息化社会可持续发展保障的重要一环。

2. 中国电子商务安全任重道远

与发达国家相比，我国的信息与网络安全状况更显脆弱，以我国金融系统计算机网络为例，目前已发生了数百起利用计算机网络进行金融犯罪的案件。专家们对我国金融系统计算机网络现状有一个形象的比喻：使用不加锁的储柜存放资金（网络缺乏安全防护）；使用“公共汽车”运送钞票（网络缺乏安全保障）；使用“邮寄托寄”方式传送资金（转账支付缺乏安全渠道）；使用“商店柜台”方式存取资金（授权缺乏安全措施）；使用“平信”邮寄机密信息（敏感信息缺乏保密措施）。另外，据国内有关部门对我国证券行业的 1564 个营业部的 23 万台微机进行抽查，基本上都存在安全漏洞。造成上述状况的原因是多方面的，许多部门只注重信息应用带来的巨大财富，对信息网络安全不予重视，忽视计算机系统的安全技术防范，给基础安全带来隐患。与此同时，信息网络安全保护工作滞后。不少单位还停滞在传统的“看家护院”的工作模式，没有从管理制度、人员和技术上建立相应的电子化业务安全防范机制，缺乏行之有效的安全保护措施。此外，发达国家限制和封锁信息安全产品的出口，也对我国信息网络安全造成了不利影响，中国电子商务安全任重道远。

总之，电子商务的安全问题是电子商务能否成功的关键所在，也是致命因素。它不仅关系到个人、企业、国家的切身利益，也是制约电子商务进一步普及的瓶颈之一，人们无法想象一个安全得不到保障的网络交易世界会是一个什么样的情形，所以对电子商务安全问题决不能等闲视之，必须将其提到重要的议事日程。

2.5.3 电子商务安全涉及的问题以及对安全的要求

电子商务安全问题涉及面很多，其主要源于交易流程中可能出现的各种风险，这些风险主要有以下几个方面。

（1）信息风险。信息风险主要来自 4 个方面：

1）冒名偷窃。假冒电子商务参与方的身份非法获取信息；对电子商务其他参与方进行攻击，破坏交易，败坏被假冒者的信誉；盗取被仿冒方的交易成果等。

2）篡改数据。入侵者未经授权进入网络交易系统，使用非法手段删除、修改、破坏某些重要信息，损害数据的真实性和完整性。

3）信息失真。信息失真包括信息的丢失和虚假信息，这可能是人为蓄意造成的，也可能是操作或网络的物理原因造成的。

4）信息泄漏。信息在网络上存储或传递时，要经过多个环节和渠道，在这个过程中，计算机病毒的侵袭、黑客非法侵入、线路窃听等因素很容易使数据在传递过程中泄漏，从而威胁企业的秘密及交易的安全。

有时候，这些信息风险甚至可能会同时发生。

（2）信用风险。信用风险主要来自 3 个方面：

1）来自买方的信用风险。如信用卡恶意透支取货物、故意拖延付款等。

2）来自卖方的信用风险。如卖方不按时、按质完全履行合同等。

3）买卖双方存在的抵赖情况。

（3）管理方面的风险。严格管理是降低网络交易风险的重要保证，特别是在网络商品中介交易过程中，客户进入交易中心，买卖双方签订合同，交易中心不仅要监督买方按时付款，还要监督卖方按时提供符合合同要求的货物。在这些环节上存在大量的管理问题。管理方面存在的任何问题都可能会对电子商务参与者构成威胁。

（4）法律方面的风险。电子商务所采用的技术是先进的、超前的，具有强大生命力，但是在法律上，目前还很难找到现成的条文保护网络交易的交易方式，网上交易可能会承担法律滞后而造成的风险。

此外，还存在其他方面难以预料的风险。

综合上面的风险源分析，电子商务的安全问题及相应的安全要求至少涉及以下 3 个方面。

（1）技术方面。

1）有效性、真实性。它是指能对信息或实体的有效性、真实性进行鉴别。电子商务信息或实体的有效性和真实性直接关系个人、企业和国家的经济利益和声誉，因此要对网络故障、操作错误、应用程序错误、硬件故障、系统软件错误及计算机病毒的潜在威胁加以控制和预防，保证贸易数据在确定的地点、确定的时刻是有效、真实的。

2）机密性。它是指保证信息不会泄漏给非授权的人或实体。网络交易必须保证发送者和接收者之间交换信息的保密性。电子商务中信息直接代表个人、企业或国家的商业机密。传统纸面交易是通过邮寄封装的信件或通过可靠的通信渠道发送商业报文来保守机密的，而电子商务是基于开放的网络环境，因此要预防非法信息存取和信息在传输过程中被非法窃取，确保只有合法用户才能得到数据，防止泄密事件的发生。

3）完整性、一致性。它要求能保证数据的完整性与一致性，防止数据被非授权的输入、删除、修改或破坏，造成数据的丢失、失常或矛盾。

在电子商务活动中，由于数据输入时的意外差错或欺诈行为，会导致贸易各方信息的差

异；另外，数据传输过程中信息遗失、信息重复或信息传送次序差异也会导致贸易各方信息不相同，信息完整性将影响贸易各方的交易和经营策略。因此，要预防对信息的随意生成、修改和删除，同时防止数据传输过程中遗失和重复信息，并保证信息传送次序在接收方的正常恢复。

4）可靠性、不可抵赖性和可控性。可靠性即保证合法用户对信息和资源的使用不会遭到不正当拒绝；不可抵赖性即建立有效的责任机制，防止实体否认其行为；可控性即控制使用资源的人或实体的使用方式。

在电子商务中，如何确定谁与谁交易，这是保证电子商务顺利进行的关键。为了鉴别贸易伙伴，必须要在交易信息传输的过程中为参与贸易的个人、企业或国家提供可靠的标识。在互联网上每个人都是匿名的，原发方在发送数据后不能抵赖，接收方在接收数据后也不能抵赖，交易中任何一方都不能否认其在交易中的作用。为了做交易，各方必须能够鉴别另一方的身份，一旦一方鉴定交易文件后，这项交易文件就受到保护以防止被篡改或伪造。接收方可以证实收到的数据是原发方发出的，而原发方也可以证实只有指定的接收方才能接收，以防止身份假冒。根据机密性和完整性要求，应对数据审查的结果进行记录。

（2）管理方面。电子商务的安全问题不仅是一个单纯的技术问题，同时也是一个复杂的管理问题。网络交易系统的安全管理，涉及交易的安全制度、交易安全的实时监控、提供实时改变安全策略的能力、对现有的安全系统漏洞的检查以及安全教育等诸多方面的内容。

（3）法律方面。电子商务的安全问题仅靠技术上和管理上的措施来解决是不够的，因为任何安全技术和管理制度的效用都不是绝对的，它们不可能抵御所有的安全风险，电子商务安全事件总会发生，在这种情况下，为保证电子商务沿着正确的轨道健康发展，必须要有相应的事件责任人承担一定的法律责任，因此，电子商务的安全问题在某种意义上讲也是一个法律问题，电子商务安全性的真正解决需要相关法律的完善来加以保证。

2.5.4　电子商务安全的内容

电子商务的一个重要技术特征是利用 Web 技术来传输和处理商业信息。电子商务的安全从整体上可分为两大部分：计算机网络安全和商务交易安全。

1. 计算机网络安全

计算机网络安全是指计算机网络设备安全、计算机网络系统安全、数据库安全等。其特征是针对计算机网络本身可能存在的安全问题，实施网络安全增强方案，以保证计算机网络自身的安全性为目标。

2. 商务交易安全

商务交易安全则紧紧围绕传统商务在互联网上应用时产生的各种安全问题，在计算机网络安全的基础上，如何保障电子商务过程的顺利进行。即实现电子商务的保密性、完整性、可鉴别性、不可伪造性和不可抵赖性。

计算机网络安全与商务交易安全是密不可分的，两者相辅相成，缺一不可。没有计算机网络安全作为基础，商务交易安全就犹如空中楼阁，无从谈起；没有商务交易安全作保障，即使计算机网络本身再安全，仍然无法达到电子商务所特有的安全要求。

2.5.5　电子商务的安全结构层次

一个实用、安全的电子商务系统必须有机地集成现代计算机密码学、信息安全技术、网络安全技术和电子商务安全支付技术。电子商务安全技术是电子商务技术体系的重要组成部分。一个安全的电子商务体系结构如图 2-6 所示。

电子商务系统 交易支付系统
安全协议 （SET、SSL、S-HTTP 等）
安全认证 （数字摘要、数字签名、CA 体系等）
加密技术 （DES、RAS 等）
安全操作系统，安全数据库系统 安全物理设备（网络设备、安全计算机、安全通信通道等）

图 2-6　安全的电子商务体系结构

2.5.6　电子商务的安全技术

电子商务的安全技术包括加密技术、数字签名、数字证书和认证中心、防火墙技术、虚拟专用网络。

1. 加密技术

（1）数据加密技术的基本概念。

加密技术是电子商务采取的主要安全保密措施，是最常用的安全保密手段，利用技术手段把重要的数据变为乱码（加密）传送到达目的地后再用相同或不同的手段还原（解密）。加密技术能避免各种在存储介质上或通过 Internet 传送的敏感数据被侵袭者窃取。由于原文经过加密，具有机密性，所以加密技术也适用于检查信息的真实性与完整性。数据加密技术是一种主动安全防御策略，可为信息提供一定的安全保护。

一个密码体制由明文、密文、密钥与加密算法 4 个基本要素构成。如图 2-7 所示为明文加密解密过程。

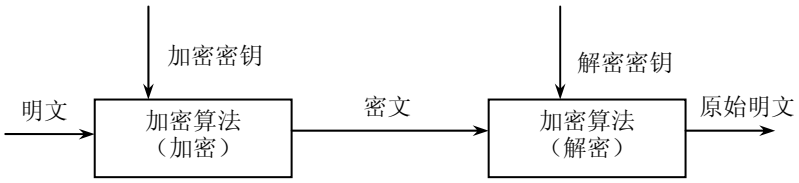

图 2-7　加密/解密过程

数据加密技术与密码编码学和密码分析学有关。密码编码学是密码体制的设计学，密码分析学是在未知密钥的情况下，从密文推出明文或密钥的技术，这两门学科合起来称为密码学。在加密和解密的过程中，原来的信息（报文）、消息称为明文，经过加密后得到的信息称密文，将明文转换为密文或将密文转换为明文的算法称为密钥，它分为加密密钥和解密密钥。解密是加密的逆过程，加密和解密过程中依靠“算法”和“密钥”两个基本元素，二者缺一不可。

根据加密技术的密码体制不同分为对称密钥体制和非对称密钥体制两种。相应地，对数据加密的技术分为两类，即对称加密（私人密钥加密）和非对称加密（公开密钥加密）。对称加密以数据加密标准（Data Encryption Standard，DES）算法为典型代表；非对称加密通常以 RSA（Rivest Shamir Adleman）算法为代表。对称加密的加密密钥和解密密钥相同，而非对称加密的加密密钥和解密密钥不同，加密密钥可以公开而解密密钥需要保密。

（2）对称加密技术。

对称加密技术从传统的简单换位代替密码发展而来，它的特点是文件加密和解密使用相同的密钥，即加密密钥也可以用作解密密钥。对称加密技术最具代表性的算法是 IBM 公司提出的 DES 算法，该算法自 1977 年被美国国家标准局（NBS）颁布为商用数据加密标准，DES 密码算法得到了广泛应用。

DES 算法的一般过程，如图 2-8 所示。

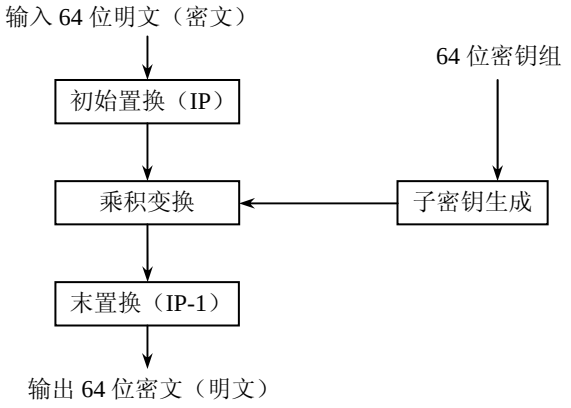

图 2-8　DES 算法的一般过程

1）初始置换（Permutation）：是按照固定的矩阵进行（换位），此部分与密钥无关。

2）子密钥生成：外部输入的 56 位密钥（64 位中去掉 8 个校验位）通过置换和移位操作生成加密和解密需要的 16 个 48 位的子密钥。

3）末置换：与初始置换类似，与密钥无关的矩阵转换。

4）乘积变换：该过程与密钥有关，且较复杂，是加密解密过程的关键。该过程包括线性变换和非线性变换。DES 采用的是分组加密。该过程通过多次重复的替代和置换方法，打乱原输入数据组，加大了非规律性，增加了系统分析的难度。

DES 解密算法与加密算法相同，解密密钥也与加密密钥相同。只是解密时逆向取用加密时用的密钥顺序。

DES 算法最主要的优点是：可靠性较高、加密解密速度快、算法容易实现、通用性强。其主要的缺点是：密钥位数少、算法具有对称性、容易被穷尽法攻击、密钥管理复杂。

自 DES 算法公布以来，出于 DES 算法本身的弱点，而出现许多 DES 的替代算法，这些算法中比较有影响力的有 AES、IDEA、TDEA（3DES）、MD5 和 RC5 等算法。

（3）非对称加密技术。

1976 年，美国学者 Dime 和 Henman 为解决信息公开传送和密钥管理问题，提出了一种新的密钥交换协议，允许在不安全的媒体上通信双方交换信息量达成一致的密钥，这就是“公开密钥系统”。相对于“对称加密算法”这种方法也叫做“非对称加密算法”。与对称加密算法不同，非对称加密算法需要两个密钥：公开密钥（Publickey，公钥）和私有密钥（Privatekey，私钥）。公开密钥与私有密钥是相辅相成的，如果用公开密钥对数据进行加密，只有对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。

非对称加密算法的基本原理是：如果发信方发送只有收信方才能解读的加密信息，发信方必须知道收信方的公钥，然后利用收信方的公钥来加密原文；收信方收到加密密文后，使用

私钥才能解密密文。显然，采用非对称加密算法，收、发信双方在通信之前，收信方必须将自己早已随机生成的公钥送给发信方，而自己保留私钥。

公开密钥密码体制的主要算法有 RSA 算法、背包算法、Elgamal 算法、Rabin 算法和 DH 算法等。

在众多的公钥体制中，RSA 倍受推崇，已被推荐为公钥数据加密标准。RSA 算法是 1978 年由三名美国 MIT 科学家 Rivest、Shamir 和 Adelman 提出的一种著名的公开密钥密码算法。它是建立在素数理论（Euler 函数和欧几里德定理）基础上的算法。

RSA 算法具有如下特点：

1）密钥管理简单（网上每个用户仅保有一个密钥，且不需密钥配送）。

2）便于数字签名。

3）可靠性较高（取决于分解大素数的难易程度）。

4）算法复杂，加密/解密速度慢，难于实现。

2. 数字签名

对文件加密只解决了传送信息的保密问题，要防止他人对传输的文件进行破坏，以及如何确定发信人的身份还需要采取其他手段，该手段就是数字签名（Digital Signature）。所谓数字签名就是附加在数据单元上的一些数据，或是对数据单元所作的密码变换，这种数据和变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性，并保护数据防止被他人（如接收者）伪造。数字签名的功能如下：

（1）接收方能够确认发送方的签名，但不能伪造。

（2）发送方发出签过名的信息后，不能再否认。

（3）接收方对接收到的签名信息也不能否认。

（4）一旦接收方出现争执，仲裁者可有充足的证据进行评判。

数字签名可解决手写签名中的签字人否认签字或其他人伪造签字等问题。因此，被广泛用于银行的信用卡系统、电子商务系统、电子邮件以及其他需要验证、核对信息真伪的系统中。

数字签名的实现过程如下：

（1）信息发送者使用单向散列函数（Hash 函数）对信息生成信息摘要。

（2）信息发送者使用自己的私钥签名信息摘要。

（3）信息发送者把信息本身和已签名的信息摘要一起发送出去。

（4）信息接收者通过使用与信息发送者使用的同一个单向散列函数（Hash 函数）对接收的信息本身生成新的信息摘要，再使用信息发送者的公钥对信息摘要进行验证，以确认信息发送者的身份和信息是否被修改过。

数字签名和数字加密的过程虽然都使用公开密钥体系，但其实现过程正好相反，使用的密钥对也不同。数字签名使用的是发送方的密钥对，发送方用自己的私有密钥进行加密，接收方用发送方的公开密钥进行解密，这是一个一对多的关系，任何拥有发送方公开密钥的人都可以验证数字签名的正确性。数字加密则使用的是接收方的密钥对，这是多对一的关系，任何知道接收方公开密钥的人都可以向接收方发送加密信息，只有唯一拥有接收方私有密钥的人才能对信息解密。另外，数字签名只采用了非对称密钥加密算法，它能保证发送信息的完整性、身份认证和不可否认性，而数字加密采用了对称密钥加密算法和非对称密钥加密算法相结合的方法，它能保证发送信息的保密性。

3. 网络认证技术

（1）网络认证的目的和基本功能。

1）网络认证的目的。验证信息发送者的真实性，此为实体认证，包括信源、信宿等的认证相识别；验证信息的完整性，此为消息的认识、验证数据在传送或存储的过程中是否被篡改、重做或延迟等。

2）网络认证的基本功能。

①可信性：信息的来源是可信的，即信息接收者能够确认所获得的信息不是由冒充者发出的。

②完整性：要求信息在传输过程中保证其完整性，即信息接收者能够确认所获得信息在传输过程中没被修改、延迟和替换等。

③不可抵赖性：要求信息发送方不能否认自己所发出的信息，同样，信息的接收方也不能否认收到的信息。

④访问控制：拒绝非法用户访问系统资源，合法用户只能访问系统授权指定的资源。

（2）认证中心简介。CA（Certificate Authority）是数字认证中心的简称，采用则公开密钥基础架构（Public Key Infrastructure）技术，专门提供网络身份认证服务，负责签发和管理数字证书，且具有权威性和公正性的第三方信任机构，其作用类似现实生活中的颁发证件公司，如护照办理机构。

一个典型的 CA 认证系统主要由以下三个部分组成：在客户端面向证书用户的数字证书申请、查询和下载系统；在注册机构（RA）端由 RA 管理员对证书申请进行审批的证书授权系统；在 CA 控制台，签发用户证书的证书签发系统。

认证中心主要有以下几种功能：

1）证书的颁发。认证中心接收、验证用户（包括下级认证中心和最终用户）的数字证书的申请，将申请的内容进行备案，并根据申请的内容确定是否受理该数字证书的申请。如果中心接受该数字证书的申请，则进一步确定给用户颁发何种类型的证书。新证书用认证中心的私钥签名以后，发送到目录服务器供用户下载、查询。为了保证消息的完整性，返回给用户的所有应答信息都要使用认证中心的签名。

2）证书的更新。认证中心定期更新所有用户的证书，或者根据用户的请求来更新用户的证书。

3）证书的查询。证书的查询可以分为两类：其一是证书申请的查询，认证中心根据用户的查询请求返回当前用户证书申请的处理过程；其二是用户证书的查询，这类查询由目录服务器来完成，目录服务器根据用户的请求返回适当的证书。

4）证书的作废。当用户的私钥由于泄密等原因造成用户的证书需要申请作废时，用户需要向认证中心提出证书作废的请求，认证中心根据用户的请求确定是否将该证书作废。另一种证书作废的情况就是证书已经过了有效期，认证中心自动将该证书作废。认证中心通过维护证书作废列表（Certificate Revocation List，CRL）来完成上述功能。

5）证书的归档。证书具有有效期，证书过了有效期之后将作废，但是不能将作废的证书简单地丢弃，因为有时可能需要验证以前的某个交易过程中产生的数字签名，这时就需要查询作废的证书。基于此类原因，认证中心还具备管理作废证书和作废私钥的功能。

4. 数字证书

由于 Internet 上的电子商务系统技术使在网上购物的顾客能够极其方便轻松地获得商家和企业的信息，但同时也增加了对某些敏感或有价值的数据被滥用的风险。为了保证互联网上电子交易及支付的安全性、保密性等，防范交易及支付过程中的欺诈行为，必须在网上建立一种信任机制。这就要求参加电子商务的买方和卖方都必须拥有合法的身份，并且在网上能够有效

无误地进行验证。数字证书提供了一种在网上验证身份的方式。

数字证书又称为数字标识。它提供了一种在 Internet 上身份验证的方式，是用来标志和证明网络通信双方身份的数字信息文件，与司机驾照或日常生活中的身份证类似。在网上进行电子商务活动时，交易双方需要使用数字证书来表明自己的身份，并使用数字证书来进行相关的交易操作。通俗来说，数字证书就是个人或单位在 Internet 上的身份证。数字证书主要包括证书所有者的信息、证书所有者的公开密钥和证书颁发机构的签名。

数字证书是由权威公正的证书认证中心（CA）签发的，认证中心颁发的数字证书均遵循 X.509V3 标准。以数字证书为核心的加密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，确保网上传递信息的机密性、完整性、交易实体身份的真实性和签名信息的不可否认性，从而保障网络应用的安全性。

一个标准的 X.509 数字证书主要包含以下内容：

1）证书的版本信息。

2）证书的序列号，每个证书都有一个唯一的证书序列号。

3）证书所使用的签名算法。

4）证书的发行机构名称（命名规则一般采用 X.500 格式）及用私钥的签名。

5）证书的有效期。

6）证书使用者的名称及其公钥的信息。

数字证书的颁发过程一般为：用户首先产生自己的密钥对，并将公开密钥及部分个人身份信息传送到认证中心。认证中心在核实身份后，将执行一些必要的步骤，以确信请求确实由用户发送，然后，认证中心将发给用户数字证书，该证书内包括用户的个人信息和公钥信息，同时还附有认证中心的签名信息。用户就可以使用自己的数字证书进行相关的各种活动。数字证书由独立的证书发行机构发布。数字证书各不相同，每种证书可提供不同级别的可信度。

5. 防火墙

（1）防火墙的概念。如今 Internet 的安全问题成了关注的焦点，计算机和通信界一片恐慌；对安全问题的考虑，给认为 Internet 已经完全胜任商务活动的过高期望泼了一盆冷水，也延缓或阻碍了 Internet 作为国家信息基础设施或全球信息基础设施成为大众媒体的进度。一些调查研究表明，许多个人和公司之所以对加入 Internet 持观望态度，主要就是出于安全的考虑。

尽管众说纷纭，有一点大家基本同意，那就是 Internet 需要更多更好的安全机制。早在 1994 年，在 IAB（Internet 体系结构理事会）的一次研讨会上，扩充与安全就被当作关系 Internet 全局的两个最重要的问题领域。然而安全性，特别是 Internet 的安全性，是一个很含糊的术语，不同的人可能会有不同的理解。本质上，Internet 的安全性可以通过提供以下两方面的安全服务来达到：

访问控制服务：用来保护计算机和联网资源不被非授权使用。

通信安全服务：用来提供认证，数据机要性、完整性和各通信端的不可否认性服务。

这两种服务的实现，主要依赖于防火墙技术和加密技术。这里主要介绍防火墙技术。什么是防火墙呢？

古时候，人们常在寓所之间砌起一道砖墙，一旦火灾发生，它能够防止火势蔓延到别的寓所。自然，这种墙因此而得名“防火墙”，主要进行火势隔离。现在，如果一个企业的网络接到了 Internet 上面，它的用户就可以访问外部世界并与之通信。但同时，外部世界也同样可以访问该网络并与之交互。为安全起见，可以在该网络和 Internet 之间插入一个中介系统，竖起一道安全屏障。对外，这道屏障能够阻断来自外部 Internet 对内部网络的威胁和入侵，提供

把守本网络的安全和审计的唯一关卡；对内，这道屏障能够控制用户对外部的访问。这种中介系统也叫做“防火墙”或“防火墙系统”。

在使用防火墙的决定背后，潜藏着这样的推理：假如没有防火墙，一个网络就暴露在不那么安全的 Internet 诸协议和设施面前，面临来自 Internet 其他主机的探测和攻击的危险；在一个没有防火墙的环境里，网络的安全性只能体现为每一个主机的功能，在某种意义上，所有主机必须通力合作，才能达到较高程度的安全性。网络越大，这种较高程度的安全性越难管理。随着安全性问题上的失误和缺陷越来越普遍，对网络的入侵不仅来自高超的攻击手段，也有可能来自配置上的低级错误或不合适的口令选择。因此，防火墙的作用是防止不希望的、未授权的通信进出被保护的网络，迫使单位强化自己的网络安全政策。

定义：防火墙是设置在用户网络和外界之间的一道屏障，防止不可预料的、潜在的破坏侵入用户网络。防火墙在开放和封闭的界面上构造一个保护层，属于内部范围的业务，依照协议在授权许可下进行，外部对内部网络的访问受到防火墙的限制。

总之，一个防火墙在一个被认为是安全和可信的内部网络与一个被认为是不那么安全和可信的外部网络（通常是 Internet）之间提供一个封锁工具。它能增强机构内部网络的安全性。防火墙用于加强网络间的访问控制，防止外部用户非法使用内部网的资源，保护内部网络的设备不被破坏，防止内部网络的敏感数据被窃取。防火墙系统决定了外界的哪些人可以访问内部的哪些服务，以及哪些外部服务可以被内部人员访问。要使一个防火墙有效，所有来自和通向 Internet 的信息都必须经过防火墙，接受防火墙的检查。防火墙必须只允许授权的数据通过，并且防火墙本身也必须能够免于渗透。防火墙系统一旦被攻击者突破或迂回，就不能提供任何的保护了。

一般地，防火墙具有以下五大基本功能：

1）过滤进出网络的数据包。

2）管理进出网络的访问行为。

3）封堵某些禁止的访问行为。

4）记录通过防火墙的信息内容和活动。

5）对网络攻击进行检测和报警。

防火墙的设计原则包括：

1）过滤不安全服务的原则。基于这个准则，防火墙应封锁所有信息流，然后对希望提供的安全服务远程开放，对不安全的服务或可能有安全隐患的服务一律扼杀在萌芽之中。这是一种非常有效实用的方法，可以造成一种十分安全的环境，因为只有经过仔细挑选的服务才能允许用户使用。

2）屏蔽非法用户的原则。基于这个准则，防火墙应先允许所有的用户和站点对内部网络的访问，然后网络管理员按照 IP 地址对未授权的用户或不信任的站点进行逐项屏蔽。这种方法构成了一种更为灵活的应用环境，网络管理员可以针对不同的服务面向不同的用户开放，也就是能自由地设置各个用户的不同访问权限。

（2）防火墙的优缺点。利用防火墙来保护内部网主要有以下几个方面的优点：

1）允许网络管理员定义一个中心“扼制点”来防止非法用户（如黑客、网络破坏者等）进入内部网络。禁止存在安全脆弱性的服务进出网络，并抗击来自各种路线的攻击。防火墙能够简化安全管理，网络安全性是在防火墙系统上得到加固，而不是分布在内部网络的所有主机上。

2）保护网络中脆弱的服务。防火墙通过过滤存在安全缺陷的网络服务来降低内部网遭受

攻击的威胁，因为只有经过选择的网络服务才能通过防火墙，例如，防火墙可以禁止某些易受攻击的服务（如 NFS 等）进入或离开内部网，这样可以防止这些服务被外部攻击者利用，但在内部网中仍然可以使用这些局域网环境下比较商用的服务，减轻内部网络的管理负担。

3）通过防火墙，用户可以很方便地监视网络的安全性，并产生报警信息。网络管理员必须审计并记录所有通过防火墙的重要信息。如果网络管理员不能及时响应报警并审查常规记录，防火墙就形同虚设。在这种情况下，网络管理员永远不会知道防火墙是否受到了攻击。

4）集中安全性。如果一个内部网络的所有或大部分需要改动的程序以及附加的安全程序都能集中地放在防火墙系统中，而不是分散到每个主机中，这样防火墙的保护范围就相对集中，安全成本也相对便宜了。尤其对于口令系统或身份认证软件等，放在防火墙系统中更是优于放在每个外部网络能访问的主机上。

5）增强保密性、强化私有权。对一些内部网络节点而言，保密性是很重要的，因为，某些看似不甚重要的信息往往会成为攻击者攻击的开始。使用防火墙系统，网络节点可阻塞 Finger 以及 DNS 域名服务。因为攻击者经常利用 Finger 列出当前使用者的名单，以及一些用户信息。DNS 服务能提供一些主机信息。防火墙能封锁这类服务，从而使得外部网络主机无法获取这些有利于攻击的信息。

6）防火墙是审计和记录网络流量的一个最佳地方。网络管理员可以在此向管理部门提供 Internet 连接的费用情况，查出潜在的带宽瓶颈的位置，并能够根据机构的核算模式提供部门级的计费。

虽然防火墙可以提高内部网的安全性，但是，防火墙也有它的一些缺陷和不足。防火墙的主要缺陷有：

1）限制有用的网络服务：防火墙为了提高被保护网络的安全性，限制或关闭了很多有用但存在安全缺陷的网络服务（如 Telnet、FTP 等）。由于绝大多数网络服务设计之初根本没有考虑安全性，只考虑使用的方便性和资源共享，所以都存在安全问题。这样防火墙限制这些网络服务，这些服务将不能给用户提供便利。

2）不能有效防护内部网络用户的攻击。目前大部分防火墙只提供对外部网络用户攻击的防护。对来自内部网络用户的攻击只能依靠内部网络主机系统的安全性。防火墙无法禁止内部用户对网络主机的各种攻击，因此，堡垒往往从内部攻破，所以必须对雇员们进行教育，让他们了解网络攻击的各种类型，并懂得保护自己的用户口令和周期性变换口令的必要性。

3）Internet 防火墙无法防范通过防火墙以外的其他途径的攻击。例如，在一个被保护的网络上有一个没有限制的拨出存在，内部网络上的用户就可以直接通过 PPP（Point to Point Protocol）连接进入 Internet，从而绕过内部精心构造的防火墙系统提供的安全系统。这就为从后门攻击创造了极大的可能。网络上的用户们必须了解这种类型的连接对于一个有全面的安全保护系统来说是绝对不允许的。

4）防火墙也不能完全防止传送已感染病毒的软件或文件。这是因为病毒的类型太多，操作系统也有多种，编码与压缩二进制文件的方法也各不相同。所以不能期望防火墙去对每一个文件进行扫描，查出潜在的病毒。解决该问题的有效方法是每个客户机和服务器都安装专用的防病毒系统，从源头堵住，防止病毒从软盘或其他来源进入网络系统。

5）防火墙无法防范数据驱动型的攻击。数据驱动型的攻击从表面上看是无害的数据被邮寄或复制到主机上。一旦执行就开始攻击。例如，一个数据型攻击可能导致主机修改与安全相关的文件，使得入侵者很容易获得对系统的访问权。

6）不能防备新的网络安全问题，防火墙是一种被动式的防护手段，它只能对现在已知的

网络威胁起作用：随着网络攻击手段的不断更新和一些新的网络应用的出现，不可能靠一次性的防火墙设置来解决永远的网络安全问题。

（3）防火墙的类型。

1）包过滤型防火墙。顾名思义，包过滤型防火墙就是通过过滤技术实现对进出数据的控制。

2）双宿网关防火墙。双宿网关防火墙又称为双重宿主主机防火墙。双宿网关是一种拥有两个连接到不同网络上的网络接口的防火墙。双重宿主主机一般采用代理方式提供服务。采用代理服务的双重宿主主机一般也称为代理服务器。

代理服务器（Proxy Server）是接收或解释客户端连接并发送到服务器的新连接的网络节点。它是客户端服务器关系的中间人。现在，代理服务器主要用于将企业网连接到 Internet，它允许内部客户端使用常用的应用程序如 Web 浏览器和 FTP 客户端访问 Internet。而代理服务器使用单个合法 IP 地址处理所有发出的请求，因此无论客户端是否具有合法 IP 地址都允许访问 Internet。我们知道网桥和交换器是在数据链路层上将帧从一端传输到另一端，路由器在网络层上转发 IP 包。而代理服务器则是在传输层以上智能地连接客户端和服务器，并能够检查 IP 包，加以分析，最终按照相应的内容采取相应的步骤。

代理服务器具有以下几个主要用途：

1）节约合法的 C 类 IP 地址。FRC 1918（私用网络地址分配文档）建议在局域网中尽量使用私有 IP 地址，以节省公用合法 IP 地址，即在局域网中分配足以连接到 Internet 的合法 IP 地址就可以。这有助于企业节约申请合法 IP 地址的资源，同时提高企业局域网的安全性，因为外部网络不能直接访问内部的私有 IP 地址。

2）通过缓存能够加快浏览速度。为了节省网络带宽，减少局域网连接 Internet 的网络流量，可在代理服务器中设置缓存。具有缓存功能的代理服务器能够检查客户端请求是否已在本地代理服务器中缓存，以决定是直接从代理服务器发出响应还是建立到 Internet 上的新连接。一般流行的代理服务器均缓存 HTTP 协议，有的还可缓存 FTP 协议。

3）较好的安全性：在代理服务器中设置安全控制策略，提供认证和授权可以阻止 Internet 上非法用户访问内部局域网、以保护企业内部的资源、此时代理服务器又具有防火墙的功能。

4）可以进行过滤；可在代理服务器中设置过滤策略以过滤客户端的请求，减少不必要的 Internet 连接。过滤有不同层次，可根据用户名、源地址和目的地址以及按照内容实现过滤，有的代理服务器甚至能扫描内容中存在的病毒。

5）强大的日志功能。由于 Internet 通信都通过代理服务器，因此代理服务器能够记住处理的所有请求，并将其保存在日志文件中，以便统计、分析各个用户的使用情况，最后进行流量计费。

6）对服务器主机的依赖性高。一旦代理服务器被攻击者破坏，则内部用户都不能访问外部资源。

目前市场上代理服务器产品较多，其中比较流行的有 MS Proxy、NSProxy、WinGate、SyGate 和 WinRoute 等。

2.5.7　电子支付安全协议

伴随着因特网的普及，网络安全性问题引起了广泛的重视。特别在网上进行交易，会涉及到资金的划拨，是消费者和商家都非常关心的网络安全性问题。在网上发布信息和获取信息对安全的要求并不高，但是在因特网上进行商务活动，特别在进行交易及其支付环节上，就对

网上支付系统的安全机制提出了更高的要求。为了实现安全的电子支付，由金融部门和信息产业部门共同推出多种安全交易标准，主要包括 SSL、SET 和 3D-Secure 等。

1. SSL 协议

SSL 协议并不是专门针对电子商务开发的，它是一种广泛应用于服务器和客户端之间相互认证并建立加密的通信连接的协议。但是目前，大多数的电子商务网站和开展网上业务的银行均采用这种方式来保证交易的安全性。

（1）SSL 的产生。SSL 即安全套接层协议，最初由 Netscape 公司开发。该公司（现在已被 AOL 美国在线收购）开发的 Netscape Navigator 浏览器是 Internet 上最早普及的图形浏览器。TCP/IP 在最初设计时没有考虑安全问题，信息的传递全部采用明文方式。随着网络不断扩大，这种明文方式传递的信息在网络监听、信息的篡改及伪造等的攻击下显得非常脆弱。于是人们基于 TCP/IP 开发了各种安全协议，例如，适用于 IP 层的 IPsec，适用于应用层的 S-HTTP、S/MIME 协议等。SSL 协议位于 TCP/IP 层和应用层之间，代表高层协议使用 TCP/IP 层的服务，在 OSI 七层模型中处于会话层，如 HTTP、FTP、SMTP、Telnet 等应用层协议能透明地建立于 SSL 协议之上。SSL 协议在应用层协议通信之前就已经完成加密算法、通信密钥（会话密钥）的协商以及服务器认证工作。此后，应用层协议所传送的数据都是经加密后的密文，从而保证了通信的机密性。目前，SSL 协议已成为 Internet 上保密通信的工业标准，Web 浏览器和服务器普遍将 HTTP 和 SSL 相结合实现安全通信。

（2）SSL 提供的服务。SSL 利用公开密钥体制和 X.509 数字证书技术，提供了如下 3 种基本的安全服务。

1）机密性。SSL 客户机和服务器之间通过密码算法和密钥的协商，建立起一个安全通道。以后在安全通道中传输的所有信息都经过了加密处理，网络中的非法窃听者所获取的信息都将是无意义的密文信息。

2）完整性。SSL 利用密码算法和 Hash 函数，通过对传输信息特征值的提取来保证信息的完整性，确保要传输的信息全部到达目的地，可以避免服务器和客户机之间的信息内容受到破坏。

3）身份认证。利用证书技术和可信的第三方 CA，可以让客户机和服务器相互识别对方的身份。为了验证证书持有者是其合法用户，SSL 要求证书持有者在握手时相互交换数字证书，通过验证来保证对方身份的合法性。

（3）SSL 的不足。SSL 当初并不是为支持电子商务而设计的，所以其在电子商务系统的应用中还存在很多弊端。

1）它只是简单地在双方之间建立了一条安全通道，在涉及多方的电子交易中，只能提供交易中客户端与服务器之间的双方认证。而电子商务往往是用户、电子商务网站、银行三方协作完成，SSL 协议并不能协调各方之间的安全传输和信任关系。

2）SSL 协议不能防止心术不正的商家的欺诈，因为该商家掌握了客户的信用卡号。商家欺诈是信用卡业务发展所面临的最严重的问题之一。

3）SSL 除了传输过程以外不能提供任何安全保证，它并不能使客户确信此公司接受信用卡支付是得到授权的。

4）SSL 协议不对应用层的消息进行数字签名，因此 SSL 不能提供交易的不可否认性。

2. SET 协议

SET（Secure Electronic Transaction）即安全电子交易协议，它是由 VISA 和 MasterCard 公司于 1997 年 5 月开发的一套规范，是为了在 Internet 上进行在线交易时保证信用卡支付的安

全而设立的一个开发的规范，它得到了 IBM、HP、Microsoft、Netscape、VeriFone、GTE、Versign 等很多公司的支持，已形成了事实上的工业标准，并且获得了 IETF 标准的认可。目前，电子交易业界普遍认为 SET 将成为网上信用卡支付的一个全球标准。

SET 协议的基本设计目标是保证持卡者、商家以及收单行之间在公开的互联网上能够安全地进行支付交易。

SET 协议建立在以下 7 个商业要求的基础之上。

1）为支付信息提供机密性，保证与支付信息同时传输的订购信息的机密性。

2）保证所有传输数据的完整性。

3）为持卡人提供认证，保证一个持卡人是一个支付账户的合法用户。

4）为商家提供认证，保证商家通过一个收单行金融机构，可以接受该品牌的支付卡的交易。

5）保证使用最好的安全技术和系统设计来保护所有电子商务交易的合法参与者。

6）创建一个不依赖于传输安全机制的协议。

7）鼓励网络和软件提供商支持互操作性。

SET 规范中主要说明了 SET 证书管理、SET 支付系统、SET 协议的外部接口指导 3 个方面的内容。

（1）SET 协议的参与者。SET 协议中定义的参与者包括持卡人、商家、发卡行、收单行、支付网关和证书授权机构。下面逐一对其进行介绍。

1）持卡人（Cardholder）：在电子商务环境中，是指信用卡和数字证书的持有者，通过相应的软件，可以借助支付卡和数字证书与商家完成支付交易。

2）商家（Merchant）：是指能够为持卡人提供服务或商品的实体，SET 协议中定义的商家能够与持卡人进行安全的电子交易，并且一个商家必须与相关的收单行达成协议，保证可以接受支付卡付款。

3）发卡行（Issuer）：是指金融机构为持卡人建立一个账户并发放信用卡，保证对经过授权的交易进行付款。此外，发卡行还负责为持卡人颁发数字证书，数字证书用来鉴别持卡人的身份，证书里不包括关于标识持卡人所持有的信用卡的信息。

4）收单行（Acquirer）：是指为商家建立一个账户并处理信用卡授权和支付的金融机构。

5）支付网关（Payment Gateway）：是一个由收单行或者是指定的第三方操作的设备，是位于商家和收单行之间，连接 SET 和现有的银行支付网络，用于处理信用卡授权和支付。因此，通常商家是与发卡行的支付网关进行交互的，而不与发卡行直接进行交互。

6）证书授权机构（Certificate Authority）：是负责为持卡人、商家和支付网关签发和管理数字证书，让持卡人、商家和支付网关之间可以通过数字证书进行认证的一个机构。

（2）SET 协议的功能。

1）SET 协议位于应用层，对网络上其他各层也有涉及。它规范了整个商务活动的流程，从持卡人到商家、支付网关、认证中心以及信用卡结算中心之间的信息流走向和必须采用的加密、认证都制定了严密的标准，从而最大限度地保证了商务性、服务性、协调性和集成性。

2）SET 是一个非常复杂的协议，因为它详尽而准确地反映了参与交易的各方之间存在的各种关系，还定义了加密信息的格式和完成一笔支付交易过程中各方传输信息的规则。

3）SET 不只是一个技术方面的协议，它还说明了各方所持有的数字证书的合法含义和希望得到数字证书以及响应信息的各方应有的动作，以及与一笔交易紧密相关的责任。

4）就付款方式的实现而言，在 SET 协议中，商家在收到客户的信用卡及订单后，信用卡的信息通过支付网关自动转到传统的金融网络，在得到发卡机构的核准后银行即可进

行付款。

（3）SET 协议的工作流程。SET 协议规定的工作流程分以下 3 个阶段。

1）在购买请求阶段，持卡人选购商品，确定支付方式，向商家发送购货单和一份经过签名、加密的信托书。信托书中的信用卡号是经过加密的，商家无从得知。

2）在支付确认阶段，商家把信托书传送到收单银行，收单银行可以解密信用卡号，并通过认证验证签名。收单银行向发卡银行查问，确认持卡人的信用卡是否属实。属实则发卡银行认可并签证该笔交易，收单银行认可商家并签证此交易，最后商家向客户传送货物和收据。

3）在收款阶段，交易成功，商家向收单银行出示所有交易的细节索款，收单银行按合同将货款划给商家。发卡银行向用户定期寄去信用卡消费账单。

SET 协议在一般使用环境下的工作步骤如下。

1）持卡人利用电子商务平台选定物品，并提交订单。

2）商家接收订单，生成初始应答消息，数字签名后与商家证书持卡人联系。

3）持卡人对应答信息进行处理，选择支付方式，确认订单，签发付款指令，将订单信息和支付信息进行双重签名，它对双重签名后的信息和用支付网关公钥加密的支付信息签名后连同自己的证书发送给商家（商家看不到持卡人的账号信息）。

4）商家验证持卡人证书和双签名后，生成支付认可请求，并连同加密的支付信息转发给支付网关。

5）支付网关通过金融专网到发卡行验证持卡人的账号信息，并生成支付认可消息，数字签名后发给商家。

6）商家收到支付认可消息后，验证支付网关的数字签名，生成购买订单确认信息发送给持卡人。

7）至此交易过程结束。商家发送货物或提供服务并请求支付网关将购物款从发卡银行持卡人的账号转账到收单银行商家账号，支付网关通过金融专网完成转账后，生成取款应答消息发送给商家。

（4）SET 协议的缺陷。

1）SET 协议没有担保非拒绝服务，无法证明交易是否由签署证书的使用者发出。

2）SET 协议签名的内容无法保障持卡人和商家的权益，在协议最后收到的签名，并不是对交易的内容，而只是对一认证码签名，如果有纠纷产生，持卡人和商家都无法单独提供证据证明其与银行间的交易。

3）SET 协议没有考虑交易个体的公平性，持卡者在没有收到商家对交易信息的确认前，就送出自己的签名，如果商家和银行恶意欺骗，则持卡者会显得无助。所以，SET 仍然存在一些问题和风险。

4）SET 协议认证结构仅适应于信用卡支付，对其他支付方式有所限制。

5）SET 协议非常复杂，协议描述多达 971 页，目前国内仅有少数应用产品。SET 协议显式地允许开“后门”，商家可通过它获取客户的信用卡号码，这是一个安全隐患。

3. 3D-Secure 协议

SSL 协议因其解决了交易两端信息传输的安全问题，但无法完成电子商务支付要求的商务性、服务性、协调性和集成性而受到质疑，SET 协议也因其过程过于复杂、成本过高而始终无法在实际应用中大面积推广。2001 年 VISA 推出一种能够弥补 SSL 和 SET 不足的“VISA 验证”服务，这项服务采用全球互通付款的“3D-Secure 技术”，可有效减小信用卡在网络被盗刷的风险，对持卡人、特约商家及发卡银行都是皆大欢喜的多赢结果。

3D-Secure（3Domain-Secure，3D）是 VISA 为提高电子商务支付的有效性而提出的一种认证技术，它主要采用 SSL 加密技术和商家服务器插件（Merchant server Plug-In，MPI）技术来实现。在在线交易中，它既能够查询并鉴别持卡人的身份，又能够保护支付卡信息在网络中传递的安全性。

（1）3D 的含义。3D 的这些功能是通过一个能够在支付交易过程中明确各方责任的模型——三方域模型（Three Domain Model）来具体实现的。它包括发卡域（Issuer Domain）、收单域（Acquirer Domain）、协作域（Interoperability Domain），例如 VISA 组织。由于 3D 是由 VISA 提出的，所以在协议定义中与 VISA 服务的各个部分（如 VISA 网络、VISA 目录等）联系紧密。

1）发卡域。发卡域主要负责用户注册以及在交易中验证注册用户并为合法用户授权。发卡行系统主要通过一个充当中介的中间目录服务器与 3D 特约商家联系，它必须有能力同时处理多个用户通过浏览器访问 Internet 进行交易的操作。而持卡人不需要任何特殊的软件，他们一旦注册，就可以通过标准浏览器进行交易活动。发卡域具体包括以下几个部分。

①持卡人（Cardholder）：持卡人是在线交易的买方。在线交易结算时，直接或通过电子钱包提供卡号、卡的有效日期以完成交易。当弹出认证 Web 页时，持卡人提供认证信息（如密码或个人确认消息）即可。

②持卡人浏览器（Cardholder Browser）：持卡人的浏览器充当了商家服务器插件（位于收单域）和访问控制服务器（位于发卡域）之间的消息传递通道。

③附加的持卡人组件（Additional Cardholder Components）：其他一些可选的持卡人端的软硬件设备，如智能卡需要的专用读卡软件和读卡器。

④发卡行（Issuer）：发卡行是专门的金融机构。

⑤访问控制服务器（Access Control Server，ACS）：ACS 主要有两个功能，一是验证请求支付的某一个卡号是否在被允许参与 3D 服务的范围内（通过注册取得参与 3D 交易的权利），二是对某一笔交易的持卡人进行认证或在认证无效时提供认证的证据。

2）收单域。收单行负责定义一个过程，这个过程能够保证参与 3D 交易的商家所有操作符合收单行规定，收单行还要为合法交易提供具体的交易处理。收单域具体包括以下几个部分。

①商家（Merchant）：通过已安装的交易软件处理交易过程，包括获取支付卡卡号、调用 MPI 引导进入支付认证过程、认证后向收单行提交授权请求。

②商家服务器插件（MPI）：创建和处理支付认证消息，并为商家交易软件返回相应的控制消息，验证这个控制消息里的数字签名。

③验证过程（Validation Process）：确认从 ACS 返回的消息的数字签名，此过程也可以由上面的 MPI 或其他机构来完成。

④收单行（Acquirer）：金融机构成员，如银行。在 3D 服务中，它们的功能主要是与商家建立契约关系并为它们承兑支付卡，判断商家是否有资格参与 3D 服务。

3）协作域。协作域利用一般的通信协议联系发卡域和收单域，并且共享 VISA 目录和 VisaNet 网络服务，使得整个支付流程能够顺利进行。协作域具体包括以下几个部分。

①目录服务器（Directory Server）：每一次支付过程都通过这个目录服务器接收商家查询某一个支付卡卡号的请求消息，判断这个卡号是否在合法的交易卡号范围内。将持卡人账户认证信息提交到适当的 ACS，ACS 的响应可以直接返回给商家，也可以由目录服务器接收认证响应信息，并由它返回给商家。

②商业认证授权（Commercial Certificate Authority）：为使用 3D 服务的实体发放特定的证

书，包括 TLS/SSL 客户端和服务器证书。

③方案认证授权（Scheme Certificate Authority）：为使用 3D 服务的实体发放特定的证书，包括数字签名证书、支付方案所需的根证书。

④认证历史服务器（Authentication History Server）：每一次支付过程都通过它接收向 ACS 发出的支付认证请求消息和认证结果（不管认证是否成功），存储和记录这个信息。当收单行和发卡行发生争执时，可通过认证历史服务器的数据记录进行仲裁。

⑤授权系统（Authorization System）：在支付认证通过后，授权系统（如 VisaNet）开始执行它的传统功能。从收单行接收授权请求，将这些请求提交给发卡行，将发卡行的响应返回给收单行，提供发卡行和收单行之间的清理和结算服务。

（2）3D 的工作流程。根据定义，3D 在电子商务支付中整个工作流程可以分为以下 10 个步骤。

1）购物者浏览商家网站将商品放入购物车，最后请求购买结算（此时商家已经获取所有必需的数据，包括 PAN（Personal Account Number）和用户设备信息）。

2）商家通过 MPI 将 PAN 和可用的用户设备信息送到目录服务器。

3）目录服务器向匹配的 ACS 发出查询请求，验证 PAN 和设备信息是否合法（如果这时没有可用的 ACS 进行响应，那么目录服务器会为 MPI 创建一个响应消息并跳到步骤 5）。

4）ACS 向目录服务器发出响应消息。

5）目录服务器将 ACS 的响应（或它在步骤 3 中自己创建的响应）送到 MPI。如果 PAN（和可用的设备信息）是合法的，那么 3D 过程就继续进行下去；如果没有证据或相关证据来证明 PAN（和可用的设备信息）是合法的，那么 3D 处理过程就终止。

6）MPI 通过购物者的设备（如 PC 机的浏览器）将支付认证请求送到 ACS，ACS 生成认证消息 Web 页面并送到持卡人的浏览器中。

7）持卡人在认证消息框中输入认证信息，并提交给 ACS。

8）ACS 利用持卡人输入的信息鉴别购物者的身份，然后 ACS 会生成认证响应结果消息并签名。

9）ACS 通过购物者的设备将认证响应结果消息返回给 MPI，同时 ACS 将其中特定的数据送到认证历史服务器记录下来。

10）MPI 验证认证响应消息的签名，并将获得授权的交易信息提交给商家的收单行。最后，收单行和发卡行通过它们之间的授权系统（如 VisaNet）进行结算，并将结果返回给商家。

2.6 网上银行

2.6.1 网上银行的基本概念

随着时代的进步与经济的发展，整个社会的经济活动包括政府部门、企业与普通个人越来越依赖银行的参与。一个国家、一个地区、一个城市市场经济的活跃也直接体现在其金融上，特别是银行业的活跃和支持上。银行也清楚地意识到，电子商务的飞速发展给金融机构带来了前所未有的机遇和挑战。电子商务的活动空间是虚拟的，产品表现形式也是虚拟的、无形的，在电子商务环境下，电子商务的全球化使地域和范围的概念不再存在，凡是利用计算机通过互联网所进行的与 IT 资源有关的商务活动都是电子商务。因此，不管厂商和消费者距离多远，

厂商都能与消费者进行网上实时沟通，及时掌握每个消费者的需求，厂商可对消费者的需求做出快速反映，实现量体裁衣，开发出满足消费者需求的个性化产品。银行作为金融产品的提供者必须推出大量满足个性化需求的网上支付产品和金融信息增值服务的产品，并提供更加方便、快捷，适应用户网上接受的金融服务方式，这就需要传统银行在网上建立一种全新的虚拟的数字化营业模式，即网上银行模式。所谓网上银行（E-Bank 或 Online-Bank）是指商业银行通过互联网为客户提供的全方位金融产品和金融服务的新的经营方式。具体说，它是以商业银行的计算机系统及软件为服务工具，以银行内联网的国际互联网为传输媒介，以单位或个人计算机为入网操作终端的“三位一体”的新型银行业务服务模式。作为客户，无论身在何处，无论何时，只要轻点鼠标，就可通过计算机进入网上银行。网上银行是虚拟的银行，是银行互联网向客户提供金融产品和金融服务的虚拟柜台。银行通过网上银行向用户提供不受时空限制的、个性化的、全方位的服务。网上银行是金融电子化、网络化的产物，是银行发展的高级形式它主要以信息技术、通信技术、网络技术为依托，通过 Internet 向用户提供在任何时间（Anytime）、任何地点（Anywhere），以任何方式（Anyhow）都可获得金融服务。

2.6.2　网上银行发展的阶段

回顾电子技术手段应用于银行的历史，可以分为两个阶段：

（1）银行间业务电子化。银行间业务电子化主要包括银行间金融 EDI 系统的实现，实现电子资金转移（EFT）的 CHIPS 系统，还包括电汇等电子手段的最早利用形式。

（2）电子化银行。电子化银行包括电话银行、自助银行、家庭银行和企业银行等。它们虽然采用了一些计算机、通信手段，但是一般通过专用网络，如电话网络、银行和用户专用金融网络，并不是基于开放的 Internet，是服务方式的扩展。

1）电话银行只是电话自动查询系统提供的账务查询等业务。

2）家庭银行是建立在局域网基础上，使用专有的银行拨号上网服务实现和银行间联网，接受银行服务。

3）由银行或软件公司提供家庭理财软件，帮助顾客自助理财，以巩固银行的现有客户以及发展新客户。例如，微软的 Money 和美洲银行的软件服务等。

4）挂靠在一些门户网站上（如美国在线 AOL）的在线银行，顾客要享受这种服务，首先要进入 AOL 主页。

（3）网上银行。网上银行一般有两个注册地址：一个是地理位置上的注册地址；另一个就是网上的注册地址，即网址。网上银行利用 Internet 开展金融业务，它直接在 Internet 上建立站点，人们可以通过浏览等各种方式进入主页。网上银行不需要分支机构，通过 Internet 伸向全世界的每个角落，其活动的空间更广阔，时间更灵活。

网上银行与在线银行的不同点如下：网上银行顾客只需要有浏览器，或者下载银行提供的免费软件，如安全认证软件、电子钱包软件等，不需要购买任何附加软件。银行业务软件都在银行的服务器上，并以银行主页的形式呈现出来。银行业务软件可以随时更新，还可以不断地扩展和完善，它不需要客户端改变，以给客户提供便利，也不需要在计算机里存储任何数据或任何信息，所有的交易通过一个安全的互联网服务器进行。顾客可以将账户资料下载到自己选择的文件程序里。银行和客户直接建立联系，没有中间环节，不再依赖与软件公司的合作。因此网上银行属于开放系统模式，采用了标准技术和构成。网上银行根据用户提供的资料不断跟踪需求，推出个性化服务，形成独特的风格，并保持与客户的良好联系。

而经由在线服务的银行则严格地要求顾客必须在其计算机上安装特定的软件包。这就限

制了消费者只能通过特定的计算机处理银行业务，拨号连通一个单独的网络，与特定的软件公司打交道，以及在限定的营业时间内处理业务。所以软件公司往往连接银行和客户，这样可以逐步控制顾客的需求和银行服务项目，成为主动者，掌握左右市场的权利。在线银行属于封闭式系统的模式，任何改变都需要进行软件升级。

2.6.3 网上银行的功能

网上银行与传统银行的基本功能是相同的，具体功能如下：

（1）金融服务功能：这是网上银行最基本的功能，网上银行提供的服务根据对象的不同可分为两类：一类是针对企业客户提供的企业银行服务，主要包括对公业务金融信息查询、种类转账业务、贷款业务、汇兑业务、集团业务等；另一类是针对个人的网上银行服务，主要包括账户信息查询和管理、存款业务、费用代缴付业务、外汇买卖业务、国债业务等。

（2）展示功能。银行可以充分利用互联网信息发布的优势，以互联网为营销平台，通过建立自己的 Web 页面，发布广告，提供有价值的金融等方式吸引客户。如我国四大商业银行都建立了自己的网站，在网站上发布金融信息，设置网上金融服务功能模块，建立银行和金融产品介绍页面，与客户建立实时沟通渠道，提高了管理水平和服务质量。

（3）个性化服务功能。互联网为银行提供了进行实时交流的空间，银行可以通过设置 BBS、E-mail、FAQ（常见问题解答）、在线电话等方式与客户进行实时沟通，及时解决服务中出现的问题，了解客户的需求，从而建立良好的客户关系，开发出满足个性化需求的产品。如银行提供的网上理财的服务功能。

（4）认证功能。在网上支付过程中，需要对交易的各方进行身份认证，网上银行通过向参与网上支付各方，如服务器、企业、个人颁发数字证书的方式，解决了电子商务中的身份认证问题。如中国银行在提供电子钱包服务中，通过向用户、商家、支付网关颁发数字证书的方式对各个参与者进行身份认证，实现安全支付。

2.6.4 网上银行的特点

1. 以客户为中心的经营理念提供“3A”式服务

网上银行是以 Internet 为平台，利用信息技术和网络技术把自己与客户连接起来，在强有力的安全保护机制的支持下，客户可以在任何时间（Anytime）、任何地点（Anywhere），以任何方式（Anyhow）都可获得金融服务，即提供“3A”式服务。因此，它比传统银行提供的业务更多、更快、更方便，且不受时间、地点和业务的限制，客户可以随时随地在不同的计算机终端上网去申请银行业务。它的功能优势非常强大。

2. 经营服务成本低投资回报高

企业的投入与产出之比是寻找经济效益最佳的方法，在传统银行的经营中，经营的好坏与经营规模有直接的关系，体现在对固定设施的投资非常大，需要建立众多的营业网点，配备大量的经营管理人员，经营成本高。而网上银行的服务则通过计算机处理各种客户需求，从而节省了大量的人力、物力的投入，利润空间大，投资回报高。

3. 网上银行服务更加多元化、个性化

网上银行充分发挥互联网网络的互动性、敏捷性，在市场细分的基础上开发出更具有个性化的金融产品，满足消费者多元化的消费需求，甚至可以只是针对某个消费者的需求开发出其需要的金融产品，成为真正的“个性银行”。

4. 实现电子化、无纸化操作

随着作为网上银行支付工具的电子钱包、智能信用卡等网上电子货币的出现，以及电子票据支付等业务的开通，银行的支付工具从传统的纸质形式向电子化发展，银行与客户能通过计算机网络逐步实现无纸化操作。

2.6.5　网上银行模式

不同的银行根据自身的情况与业务需求，在建立网上银行的过程中采用了不同的模式或策略，就目前的网上银行的发展模式可以划分为两大类：一类是纯网上银行模式；另一类是以传统银行为基础拓展网上业务的网上银行发展模式。

1. 以传统银行为基础拓展网上业务的网上银行发展模式

传统银行经过几百年的发展已经形成了一个完整的体系，传统银行通过宽敞舒适的营业场所，密度较高的营业网点，众多的服务人员，面对面的服务，形成了相对稳定的市场，在经营中形成了品牌实力。银行在经济活动中占有举足轻重的。随着 Internet 的普及应用，商业银行认识到网上市场的重要及网上维护原有市场的优势，纷纷在原有传统银行服务形式基础上开展网上银行服务，在这种情况下，网上银行通常是作为原有银行业务的补充，依托原有银行的经营优势，同时也利用网上银行的经营优势，如市场范围大，受众对象多，信息传播速度快，经营成本低的优势，作为稳定老顾客，发展新顾客的手段，优势互补。对于一些历史悠久的规模大的银行，主要采用这种模式。例如，我国的工商银行、中国银行、建设银行等都是采用这种模式。这种模式主要是将传统银行中经营优势与网络经营优势相互补充。另外，在银行业中还有一部分经营实力略逊一筹的社区银行（城市银行），这些银行历史不是很悠久，经营实力也不能与传统大银行相比，主要是服务于城市区域内居民的，这部分银行也开展网上银行服务，主要是通过建立网上银行防止客户流失，保证市场份额。

2. 纯网上银行模式

纯网上银行是一种完全依赖于 Internet 开展起来的全新的银行形式，这类银行一般只有网络商务空间，既无分支机构，也无营业网点，几乎所有业务与服务都通过互联网进行。例如美国安全第一网络银行 SFNB（Security First Network Bank）就是纯网上银行。纯网上银行最大的优点就是节省费用与运作成本，纯网上银行主要有两种发展模式：一是提供传统银行所有的柜台业务的服务项目，这种模式的基础是认为互联网或信息网络技术能够给银行提供全面的虚拟服务平台；二是侧重于发展适合网络金融的特色业务，变种模式的基础是承认互联网或信息网络技术提供的金融服务存在缺陷，特别是不能为客户提供现金管理和个性化服务。

2.6.6　网上银行的技术要求

网上银行进行金融服务是由若干个系统共同支持的。其中技术系统是网络银行经营的基础，网上银行的技术系统是根据银行的业务需求及其现有 IT 系统，基于 CA 认证安全体系的网络银行建设。网络银行的技术架构一般由 Web 服务器、应用服务器、数据库服务器（DB 服务器）、路由器、防火墙及内部管理和业务工作平台组成。网络银行系统的具体业务功能，通常由银行端 Web 服务器和两台互为备份的应用服务器及数据库服务器完成，如图 2-9 所示。

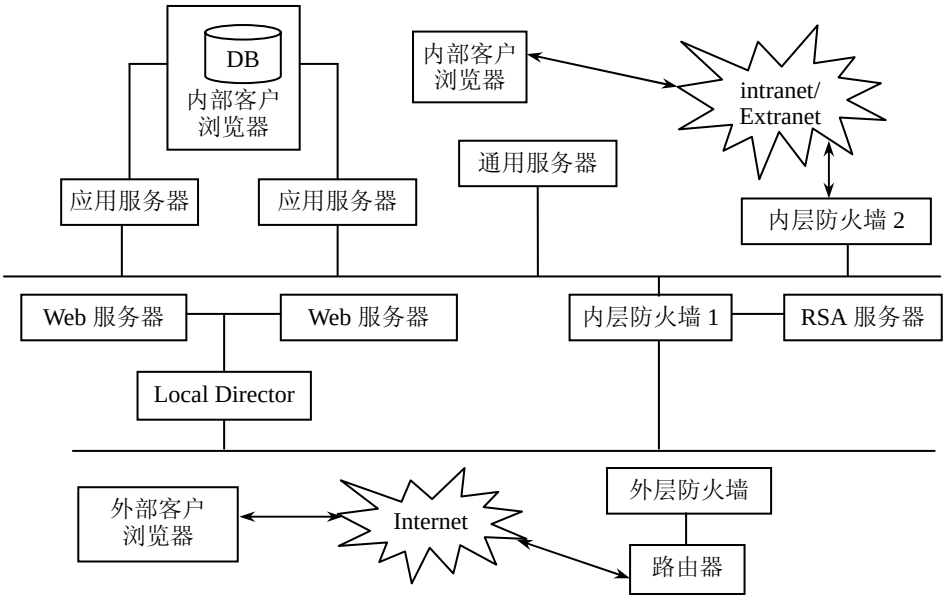

图 2-9　典型的网络银行技术结构图

网上银行的用户分为内部和外部用户，内部用户主要指银行内部管理用户及企业的使用伙伴，外部用户主要指通过 Internet 访问网络银行的用户。外部用户可以采用 DDN 接入，Modem 拨号接入，通过 PC 机的浏览器访问网上银行网站，还需要通过防火墙的认证，才能登录到网上银行系统，防火墙将 Internet 用户与系统外界隔离，以保护 Intranet 的安全。

路由器和防火墙对流入网络银行系统的数据进行过滤，并且隔离银行内部网络与非安全 Internet。系统一段采用两层防火墙，外层防火墙放在 Web 服务器与 Internet 之间，目的将 Web 服务器与外部网络隔离，阻止非法的访问者和数据进入。内层防火墙用于隔离网上银行的 Web 服务器与应用服务器，内层防火墙在软件上增加管理手段，如内部数据库可设定只对从特定接口来的请求做出反应，对其他的 IP 地址则不理会，以保证数据和文件的保密性。通过内外两层防火墙隔离 Internet 和网上银行的核心业务系统，内层和外层防火墙配合形成非军事化区，形成对 Internet 访问的双重隔离，使网络体系结构受到更好的保护。除 Web 服务器在非军事化区内，其他如应用和数据库服务器等均位于内部应用区，该区主机不允许外部用户直接访问。内层防火墙用来阻止非法用户和数据通过金融专用网 Internet、Extranet 进入系统。

Web 服务器存放和管理 Web 网页，向前台提供客户交易界面，同时对外提供基本的静态信息传递服务，并管理网上结算业务信息系统的网页文件和银行的其他网上信息发布。静态页面的安全性没有网上结算业务系统要求高，但有更大的访问量需求，因此将其设置在外层防火墙的后面。Web 服务器使用超文本传输协议（HTTP）和超文本标志语言（HTML），对客户浏览器提供标准的通信支持。

应用服务器是装载银行具体业务应用程序的地方，支持 Java Server、JSP 等业界标准的服务器端的 Java 应用，它与 Web 服务器一起构成了网上结算应用系统的运行环境，实现网上交易业务的逻辑控制和流程处理，完成 Web 服务器之间和与数据库服务器之间的信息交换。

银行数据库用于存放各种应用数据，包括各种应用系统参数、客户信息、账户信息、交易信息等。为便于发展综合业务服务，建议将数据库集中统一存放于总行。对于大的商业银行，由于数据量大，应设立独立的数据库服务器。如果是中小商业银行，可将数据库服务器与应用

服务器软件结合在一起，应用服务器及数据库服务器可通过双机互为备份方式保证数据的高可靠性。一旦其中一台意外停机，另一台立即就可以接管全部工作，从而实现系统的高可用性。

为确保内部网络和数据库存储的安全，可与内层防火墙平行，设立加密认证系统（RSA 服务器）来对内部网络的访问权作加密认证。当用户访问受保护的系统时，可以通过设置安全认证服务器，如 RSA 认证服务器，应用相关 RSA 代理软件等启动一个认证会话设置并且实施安全策略，保护对专用网络系统、文件及应用的访问。这套系统是以 Client/Server 结构为基础，使用内层防火墙和中心认证系统（RSA）相结合的内部网络加密认证办法来进行严密的安全检验。

为了网络银行系统有更好的扩展性，在网络银行总中心还可放置一台加密和通信服务器，负责与各电脑中心连接，通信协议采用 TCP/IP 协议，客户的交易请求都通过此服务器分发到各电脑中心的通信服务器上。通信服务器具有均衡负载、加密和解密的功能。

2.6.7　网上银行的营销

营销战略的核心理念是“顾客需要”。因此要分析顾客要求，引导需求，设计适当的产品和服务，以正确合理的价格，通过一定的手段、渠道来满足顾客的需求。营销战略包括 4 个部分：产品策略、价格策略、促销策略和渠道策略。

网上银行的营销管理，应注重以下几点；

（1）要使网上银行界面设计友好、方便、容易掌握，能正确回答网上银行对顾客的好处增强顾客的信心。

（2）满足顾客对于安全性能的心理需求。采用各种安全措施确保个人信息的安全。

（3）提供具有吸引力的产品、服务组合，并体现个性，给顾客以深刻的印象。

（4）在线银行的定价问题。顾客对价格非常敏感，当上网费和服务费稍高时，顾客便失去了兴趣。

（5）比便利更重要的是银行长期控制与管理个人金融事务能力的提高。

（6）采用先进技术保证服务的质量。

从目前来看，网上银行的发展中还存在很多问题，仍需解决一些关键性的技术难题，如金融专用网络和 Internet 的连接、网络安全技术，保证实时的服务质量以及后台的批处理方式作业的办公系统和前台的实时服务系统的融合等。采用多家银行联合开发的合作方式可以降低加盟银行的投资成本和风险，而且能确保对未来金融交易网络系统的支配权，更重要的是，能够参与相关网络技术标准的制定。

小结

本章主要介绍了电子支付的基本概念，电子支付系统的概念和基本构成，电子支付系统体系结构，电子支付的主要模式；电子支付技术的发展情况，电子支付工具和电子支付系统的种类；目前常用的电子支付工具，网上银行的概念，网上银行的业务模式，网上银行的特点，电子支付中存在的一些问题。电子商务的安全问题，电子商务安全体系、安全控制要求，以及电子商务安全管理的措施；电子商务的安全协议的种类，以及各自的长处和存在的不足；认证中心的作用以及认证机制。

习题

一、单选题

1．不属于电子信用卡类的电子支付工具是（　　）。

A．借记卡　　B．电话卡　　C．智能卡　　D．电子划款

2．SET 协议是一个在互联网上实现安全电子交易的协议标准，下面的叙述不正确的是（　　）。

A．SET 通过使用数字签名来确定数据是否被篡改，以保证数据的一致性和完整性，益于完成交易防止抵赖

B．规定了交易各方进行交易结算时的具体流程和安全控制策略

C．SET 通过使用公开密钥和对称密钥方式加密保证了数据的保密性

D．SET 是网络层的网络标准协议

3．用户可以采用自己的私钥对信息加以处理，由于密钥仅为本人所有，就形成了（　　）。

A．数字签名　　D．公开密钥　　C．私有密钥　　D．数字证书

4．以下关于数字签名的说法不正确的是（　　）。

A．数字签名的加密方法用目前计算机技术水平破解是不现实的

B．采用数字签名，能够保证信息自签发后至收到为止未曾作过任何修改

C．真实文件名不容易否认

D．用户可以来用自己的私钥对信息加以处理，形成数字签名

5．电子货币是相对传统货币而言的一种新型的支付手段，以下说法错误的是（　　）。

A．使用电子货币需要直接与银行连接才可以进行操作

B．电子货币具有用途广、使用灵活、匿名性、快速简便等特点

C．电子货币主要有智能卡形式的支付卡或数字方式的货币文件

D．Mondex 卡用于网下的支付，E-Cash 用于网上的支付

6．电子钱包运行在（　　）。

A．客户所在的计算机上　　B．银行的交易服务器上

C．支付网关　　D．电子商厦的服务器上

7．电子商务中的电子支付相对于传统支付的特点是（　　）。

A．通过物理实体完成款项支付　　B．基于开放的系统平台

C．对通信设施要求较低　　D．用户支付成本高

8．SET 协议运行的目标不包括（　　）。

A．保证信息在互联网上安全传输

B．保证电子商务参与者信息的相互沟通

C．保证网上交易的实时性

D．效仿 EDI 贸易的形式，规范协议和消息格式

9．有关电子钱包的说法正确的是（　　）

A．电子钱包适用于大额支付　　B．电子钱包最早出现于美国

C．Mondex 卡是一种电子钱包　　D．电子钱包可以放入非电子货币

10．目前我国智能卡的推广应用中还存在一些障碍，主要是安全问题和（　　）。

A．资金问题　　B．政策问题　　C．成本问题　　D．观念问题

11．如果一个电子邮件的内容被篡改成完全相反的意思，我们就说破坏了（　　）。

A．数据的完整性　　B．数据的可靠性

C．数据的及时性　　D．数据的延迟性

12．电子商务认证机构的职能有（　　）。

A．发放数字证书

B．对买卖双方的交易信息进行加密和解密

C．防止计算机病毒和网络黑客的入侵

D．管理用户的数字证书

13．下面有关信息加密的论述正确的有（　　）。

A．加密是指采用物理方法对信息进行再组织，使之成为乱码

B．密钥的位数越长，加密系统就越牢固

C．对称加密需要有一对密钥

D．非对称的加密与解密使用不同的密钥

14．当前所采取的主要防范黑客的措施有（　　）。

A．使用防火墙技术，建立网络安全屏障

B．使用安全扫描工具发现黑客

C．使用有效的监控手段抓住入侵者

D．时常备份系统，若被攻击可及时修复

15．数字证书包括（　　）。

A．证书拥有者的姓名和公钥

B．公钥的有效期

C．颁发数字证书的单位及其数字签名

D．数字证书的序列号

16．下面有关防火墙局限性的论述不正确的有（　　）。

A．防火墙可以抵御来自内、外部的攻击

B．不能防范外来人为因素的攻击，但可以防止内部人员的恶意攻击

C．不能防止数据驱动式的攻击

D．可以防止已感染的文件的扩散

二、多选题

1．电子支票支付方式包括（　　）。

A．E-Check　　B．NetBill　　C．NetCheque　　D．电子邮件

2．电子钱包的高级功能包括（　　）。

A．管理账户信息　　B．管理电子证书

C．处理交易记录　　D．连接商家和银行网络的支付网关

3．在 Internet 上，典型的电子支付方式包括（　　）。

A．电子货币支付方式　　B．电子支票支付方式

C．银行卡支付方式　　D．现金支付方式

4．SET 协议运行的目标主要有（　　）。

A．保证信息在互联网上安全传输

B．保证电子商务参与者信息的相互隔离

C．提供商品或服务

D．通过支付网关处理消费者和在线商店之间的交易付款问题

5．SSL 协议能确保两个应用程序之间通信内容的保密性和数据的完整性，以下对 SSL 协议的解释错误的是（　　）。

A．SSL 协议属于网络应用层的标准协议

B．SSL 记录协议基本特点：连接是专用的，连接是可靠的

C．SSL 握手协议基本特点：连接是专用的，连接是可靠的

D．SSL 可用于加密任何基于 IPX/SPX 的应用

三、填空题

1．电子商务安全的威胁包括_____、_____和_____。

2．电子商务安全从整体上可分为_____和_____两大部分。

3．电子商务采取的主要安全保密措施，是最常用的安全保密手段，利用技术手段把重要的数据变为乱码（加密）传送，到达目的地后再用相同或不同的手段还原（解密）这就是_____。

4．对称加密技术是从传统的简单换位代替密码发展而来的，它的特点是文件加密和解密使用相同的密钥，即_____。

5．对文件进行加密只解决了传送信息的保密问题，而防止他人对传输的文件进行破坏，以及如何确定发信人的身份还需要采取其他的手段，这一手段就是_____。

6．数字加密使用的是接收方的密钥对，这是多对一的关系，任何知道接收方公开密钥的人都可以向接收方发送加密信息，但只有唯一拥有_____的人才能对信息解密。

7．通俗地讲，_____就是个人或单位在 Internet 上的身份证。

四、判断题

1．电子钱包必须经持卡人在线申请电子证书并获批准后方可使用。　　（　　）

2．SSL 协议能确保两个应用程序之间通信内容的保密性和数据的完整性。　　（　　）

3．电子钱包内可装入电子零钱、电子信用卡和电子借记卡等多种电子货币。　　（　　）

4．数字证书就是网络通信中标志通信各方身份信息的一系列数据。　　（　　）

五、简答题

1．电子支付的工具和特征有哪些?

2．什么是电子支付？什么是电子支付系统?描述一下电子支付系统的基本构成。

3．目前电子支付还存在哪些方面的问题?

4．数字支票支付系统如何运作和使用?

5．试分析网上银行发展的背景。

6．网上银行具有哪些主要业务?

7．试总结网上银行区别于传统银行的特征。

8．什么是网络银行？它与传统银行有何区别?

9．与传统的商业银行相比，网络银行体现了哪些优势?

10．上网查询 2～4 个银行的个人网上银行和企业网上银行，了解其流程并比较各个网上

银行的区别。

11．通过各银行的网上银行的业务比较，写出各银行网上银行的业务异同。

12．实际申请网上银行，进行一次购买，并在线支付，了解电子商务的在线支付过程，并写出支付过程与支付时的安全问题。

13．电子商务安全的基本要求是什么？

14．电子商务安全的内容是什么？

15．电子商务安全的结构如何？

16．简述防火墙的原理。

六、网络操作题

1．登录中国工商银行网站（http://www.95588.com 或 http://www.icbc.com.cn），申请灵通卡并在网上购物。

2．在网站 http://www.bank-of-china.com 申请电子钱包，并利用电子钱包进行网上购物。