第5章 网上交易

案例导读

支付宝——第三方平台的领头羊

支付宝(中国)网络技术有限公司是国内领先的独立第三方支付平台,是由阿里巴巴集团CEO马云先生在2004年12月创立的第三方支付平台,是阿里巴巴集团的关联公司。支付宝致力于为中国电子商务提供“简单、安全、快速”的在线支付解决方案。支付宝由买家将货款打到支付宝账户,由支付宝向卖家通知发货,买家收到商品确认后指令支付宝将货款放给卖家,至此完成一笔网络交易。支付宝公司于2010年12月宣布其用户数突破5.5亿。

从2004年建立开始,支付宝始终以“信任”作为产品和服务的核心,不仅从产品上确保用户在线支付的安全,同时让用户通过支付宝在网络间建立起相互的信任,为建立纯净的Internet环境迈出了非常有意义的一步。

在经营中,支付宝以稳健的作风、先进的技术、敏锐的市场预见能力及极大的社会责任感,赢得了银行等合作伙伴的认同。国内的中国工商银行、中国农业银行、中国建设银行、中国招商银行、中国银行、中国交通银行等各大商业银行以及中国邮政、VISA国际组织等各大机构均与支付宝建立了深入的战略合作关系,不断根据客户需求推出创新产品,成为金融机构在电子支付领域最为信任的合作伙伴。支付宝方面表示,截至2012年,支付宝快捷支付的合作银行已经超过一百六十家,覆盖了国内所有的主流银行。

支付宝交易是Internet发展过程中的一个创举,也是电子商务发展的一个里程碑。支付宝品牌以安全、诚信赢得了用户和业界的一致好评。据支付宝公布的最新数据显示,四十六万家国内独立电子商务企业使用支付宝作为网络支付工具,由此实现了日交易笔数峰值四百万笔,日均交易峰值达七亿元的交易规模。而支付宝合作商户也进一步涵盖了服装、电子、机械、家居、文化等在内的几乎所有已应用电子商务的产业领域。

在2012年的“双十一”购物狂欢节中,支付宝快捷支付支撑了当天45.8%的交易笔数,为保证支付系统顺利度过“双十一”大考立下头功。目前支付宝快捷支付的用户数已经突破一亿,快捷支付已经成为国内网上支付体系的重要补充。“双十一”购物狂欢节当天,支付宝快捷支付交易笔数占到所有交易笔数的约45.8%,鼓励用户提前充值带来的余额支付占到31%,而传统的网银支付,所有银行渠道相加也只占到23.2%。

(注:以上资料来源于http://baike.baidu.com/view/26281.htm,http://blog.alipay.com/,内容有删改。)

支付宝是电子支付的重要手段之一，它的广泛应用推动了我国电子商务的飞跃式发展。本章我们将介绍电子交易中电子商务采购、网上银行、电子支付、网络安全等相关技术。

5.1 网上商务采购

5.1.1 网上商务采购的含义

网上商务采购最先兴起于美国，它的最初形式是一对一的电子数据交换系统，即 EDI。该电子商务系统大幅度地提高了采购效率，但早期的解决方式价格昂贵、耗费庞大，且由于其封闭性仅能为一个买家服务，特别使中小供应商和买家却步。为此，联合国制定了商业 EDI 标准，但在具体实施过程中，关于标准问题在行业内及行业间的协调工作举步维艰，因此，真正商业伙伴间的 EDI 并未广泛开展。20 世纪 90 年代中期，开始兴起网上商务采购目录，这是供应商通过将其产品发布到网上，来提高供应商的信息透明度、市场涵盖面。近年来，出现了全方位综合网上商务采购平台，且通过广泛连接买卖双方来使用网上商务采购服务。

所谓网上商务采购，就是用计算机系统代替传统的文书系统，通过网络支持完成采购工作的一种业务处理方式，也称做网上采购。网上商务采购是由采购方发起的一种采购行为，是一种不用见面的网上交易，如网上招标、网上竞标、网上谈判等。人们把企业之间在网络上进行的这种招标、竞价、谈判等活动定义为 B2B 电子商务，事实上，这也只是网上商务采购的一个组成部分。网上商务采购比一般的电子商务和一般性的采购在本质上有了更多的概念延伸。它不仅仅完成采购行为，而且利用信息和网络技术对采购全程的各个环节进行管理，有效地整合了企业的资源，帮助供求双方降低了成本，提高了企业的核心竞争力。可以说，企业采购电子化是企业运营信息化不可或缺的重要组成部分。网上商务采购使企业不再采用人工办法购买和销售它们的产品。

5.1.2 网上商务采购的优势

在我们现今社会的采购中，应用电子采购技术的企业毕竟是少数，绝大多数企业依然是应用着传统模式进行采购。但是，随着时代的发展和科技的进步，电子采购替代传统采购的趋势越来越明显。在这一全新的商业模式下，随着买主和卖主通过电子网络而联系在一起，商业交易开始变得具有无缝性，其自身的优势是十分显著的。

(1) 提高采购效率，缩短了采购周期。采购方企业通过网上商务采购交易平台进行竞价采购，可以根据采购方企业的要求自由设定交易时间和交易方式，大大地缩短了采购周期。自采购方企业竞价采购项目正式开始至竞价结束，一般只需要 1～2 周，较传统招标采购节省 30%～60%的采购时间。

(2) 节约大量的采购成本。据美国全国采购管理协会(http://www.napm.org)称，使用网上商务采购系统可以为采购企业节省大量成本。采用传统方式生成一份订单所需要的平均费用为 150 美元，使用基于 Web 的网上商务采购解决方案则可以将这一费用减少到 30 美元。企业通过竞价采购商品的价格平均降幅为 10%左右，最高时可达到 40%以上。

通用电气公司估计通过网上商务采购每年将节约100亿美元。

(3) 优化采购流程。采购流程的电子化不是用计算机和网络技术简单替换原有的方式方法,而是要依据更科学的方法重新设计采购流程。在这个过程中,摒弃了传统采购模式中不适应社会生产发展的落后因素。

(4) 减少过量的安全库存。世界著名的家电行业跨国企业海尔集团在实施网上商务采购后,采购成本大幅降低,仓储面积减少了一半,降低库存资金约7亿元,库存资金周转日期从30天降低到了12天以内。

(5) 网上商务采购的另外一个优势是信息共享。不同企业,包括各个供应商都可以共享信息,不但可以了解当时采购、竞标的详细信息,还可以查询以往交易活动的记录,这些记录包括中标、交货、履约等情况,帮助买方全面了解供应商,帮助卖方更清楚地把握市场需求及企业本身在交易活动中的成败得失,为双方积累经验。这使供求双方之间的信息更加透明。

(6) 网上商务采购能帮助采购方改善客户服务和客户满意度,促进供应链绩效,以及改善与供应商关系。

(7) 网上商务采购不仅使采购企业大大获益,而且也能让供应商获益。对于供应商,通过网上商务采购可以更及时地掌握市场需求,降低销售成本,增进与采购商之间的关系,获得更多的贸易机会。

国内外无数企业实施网上商务采购的成功经验证明,网上商务采购在降低成本、提高商业效率方面,比在线零售、企业资源计划(ERP)更具潜力。网上商务采购的投资收益远远高于过去十年内已经在企业中占主导地位的任何商业革命,包括企业流程再造、策略性采购等。

5.1.3 网上商务采购的流程

电子商务采购的一般流程包括以下8个步骤。

第1步,要进行采购分析与策划,对现有采购流程进行优化,制定出适宜网上交易的标准采购流程。

第2步,建立网站。这是进行电子商务采购的基础平台,要按照采购标准流程来组织页面。可以通过虚拟主机、主机托管、自建主机等方式来建立网站,特别是加入一些有实力的采购网站,通过它们的专业服务,可以享受到非常丰富的供求信息,起到事半功倍的作用。

第3步,采购单位通过Internet发布招标采购信息(即发布招标书或招标公告),详细说明对物料的要求,包括质量、数量、时间、地点等,对供应商的资质要求等。也可以通过搜索引擎寻找供应商,主动向他们发送电子邮件,对所购物料进行询价,广泛收集报价信息。

第4步,供应商登录采购单位网站,进行网上资料填写和报价。

第5步,对供应商进行初步筛选,收集投标书或进行贸易洽谈。

第6步,网上评标,由程序按设定的标准进行自动选择或由评标小组进行分析评比选择。

第7步,在网上公布中标单位和价格,如有必要,可对供应商进行实地考察后签订采购合同。

第8步,采购实施。中标单位按采购订单通过运输交付货物,采购单位支付货款,处理有关善后事宜。按照供应链管理思想,供需双方需要进行战略合作,实现信息的共享。采购

单位可以通过网络了解供应单位的物料质量及供应情况，供应单位可以随时掌握所供物料在采购单位中的库存情况及采购单位的生产变化需求，以便及时补货，实现准时化生产和采购。

电子商务采购是一种非常有前途的采购模式，它主要依赖于电子商务技术的发展和物流技术的提高，依赖于人们思想观念和管理理念的改变。我国目前已经有不少企业以及政府采用了网上采购的方式，对降低采购成本、提高采购效率、杜绝采购腐败起到了十分积极的作用，因此应该大力提倡这一新的采购方式。

5.2 电子支付

5.2.1 电子支付的基本概念

随着 Internet 技术和电子商务的迅速发展，电子支付系统已经成为现代金融领域不可缺少的有机组成部分。从发达国家支付系统的发展进程来看，其经济活动中大约 85%～90%的交易额是通过电子方式处理的。电子商务的广阔发展前景，吸引了更多资源的投入，促使电子支付技术日益成熟和完善，而成熟、安全的电子支付技术又促进了电子商务的飞速发展。

受到电子商务发展的有力拉动，我国网上支付市场规模发展迅速。2001 年，我国网上支付的市场规模为 9 亿元，2005 年规模增长到 161 亿元，2007 年该规模增长到近一千亿元。随着电子商务的普及，电子支付必然成为支付方式的主要形式。快捷、方便和安全的电子支付也必将给人类的商务活动带来新的改变和发展，成为人们生活质量稳步提高的一个标尺。

电子支付是通过信息流的传输来代替现金的交换，其各种支付方式都是通过数字化方式自动完成交易款项的支付。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的支付。

电子支付的研究及应用在美国开展较早。1989 年，美国法律学会的《美国统一商法典》给出了电子支付的一个规范性定义：电子支付是支付命令发送方把存放于商业银行的资金，通过通信线路划入收益方开户银行，以支付给收益方的一系列转移过程。

立足我国社会经济发展的国情和用语措辞习惯，一个通用性的电子支付定义可以这样描述：电子支付是指电子交易的当事人通过网络以电子数据形式进行的货币支付或资金流动。电子交易的当事人一般指消费者、商家和银行等。该定义首先明确了电子支付涉及的实体，即消费者、商家和银行，三方缺一不可；其次提出了电子支付的形式和途径，它有别于传统支付方式，是以金融电子化网络为基础，以商用电子化工具和各类交易卡为媒介，以计算机技术和通信技术为手段，以电子数据（二进制数据）形式存储在银行的计算机系统中，并利用安全、认证技术通过计算机网络以电子信息传递形式实现的方便、快捷、安全的资金流通和支付。

电子支付的产品和工具种类繁多，形式多样，但一般具有下列共同特性。

（1）技术先进性。以现代计算机和网络技术为基础，电子货币的应用离不开计算机技术，其流通、储蓄、支付等功能的体现都是通过计算机和网络实现的。

(2) 多功能性。集储蓄、信贷和非现金结算等多功能于一身。

(3) 普遍适应性。可广泛应用于生产、交换、分配和消费领域。

(4) 安全易用性。使用简便、安全、迅速、可靠。电子货币使用了很多加密手段,即便丢失,只要密码不被泄露,就不会被人冒领。

(5) 可信赖性。电子支付通常要经过银行专用网络,金融企业的专业品质保证了支付工具的可靠性。

(6) 以银行卡或其他金融卡为载体。无论是磁卡形式的电子货币还是 IC 卡形式的电子货币卡本身都没有价值,只是货币载体。作为电子货币,其价值不像纸币或其他票据那样。

5.2.2 电子支付的分类

电子支付产品分为三大类:一类是电子货币类,如电子现金、电子钱包等;另一类是银行卡类,包括智能卡、借记卡、购物卡、信用卡等;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。

随着网络技术的不断发展,电子商务也加快了其发展进程,渐渐成为人们生活中不可或缺的一部分。显然,传统的支付方式采用面对面的交易模式,已经无法满足电子交易在线操作的要求,于是各种电子支付方式应运而生。它克服了传统支付方式过程复杂、耗时、携带现金不方便等局限性,因具有便利性、高效性、安全性等特点,在电子商务中显示出重要作用。目前已经广泛使用的电子支付方式分为以下几类:电子信用卡、电子现金、电子钱包、电子支票、微支付和移动支付。

1. 电子信用卡

在在线交易中,有相当一部分的支付是通过信用卡和借记卡来进行结算的。这些卡是由金融机构发行的、授权持卡人可以在商家进行记账消费的支付工具。对于信用卡而言,一般是根据用户的信用限制事先设定一个消费限度,用户可以花光卡上的余额并透支一定的额度。而对于借记卡而言,则不能透支,只能用卡上存有的金额进行支付。

由于在电子商务的支付处理中,对于真正的信用卡和对于国内一些名为信用卡实际为借记卡的处理并没有太大的差别,所以我们在这里将它们统称为信用卡。

1) 使用信用卡涉及的角色

使用信用卡一般要涉及下列角色:

- 持卡人
- 商家
- 发卡银行
- 商家开户银行
- 信用卡公司

2) 网上信用卡支付的类型

在网上进行信用卡支付操作,一般有如下三种类型。

(1) 使用不加密信用卡信息的方式进行支付。信用卡支付的最简单方法是在公共网络上交换未经加密的信用卡信息。但由于 Internet 本身的安全性很低,所以这种方法存在着很多问题,因为信用卡号有可能会被黑客窃取。此外身份的认证也是一个问题,因为卖方必

须验证信用卡的使用者就是持卡人本身。

(2) 使用加密信用卡信息的方式进行支付。使用这种方式,是在利用 Internet 传送信用卡信息前首先对信息进行加密。但这样做需要考虑其他因素,如信用卡交易本身的成本,所以对于小额支付而言,这种方式不太适用。

(3) 使用第三方验证的方式进行支付。使用这种方法,就是引入第三方来进行收款和证实,从而解决了安全和认证问题。

3) 信用卡支付的处理

信用卡的工作过程主要包括以下步骤。

(1) 使用信用卡进行网上购物。消费者将要购买的商品装入购物车后,在结账时要选择使用信用卡进行支付。商家通过自己的开户银行对信用卡进行认证,银行完成认证后通知商家交易是否继续进行,商家将订购的商品发送给消费者。注意:消费者只有在支持信用卡的网站上购物,才能使用自己的信用卡进行网上支付。

(2) 商家与银行进行资金结算。商家将加密后的信用卡号与密码发送给收单银行,同时商家也会收到经过加密的购物账单。这时,收单银行将信用卡号发送给发卡银行请求确认,发卡银行在确认与授权后将它返回给收单银行。如果消费者收到了商家发送过来的商品,商家的收单银行就与发卡银行进行资金清算。

(3) 发卡银行向客户发送账单。发卡银行向商家支付客户购物时所需要支付的货款,定期将客户的购物清单与账单发送给客户,客户要在规定的时间内将款项划拨到发卡银行的账户。

2. 电子现金

1) 电子现金概述

电子现金又叫数字现金,是一种以数据形式流通的货币。电子现金把现金数值转换成为一系列的加密序列数,通过这些序列数来表示现实中的现金数值。用户在开展电子现金业务的银行开设账户并在账户内存钱后,就可以在接受电子现金的商店购物了。电子现金不仅具有数字化带来的便利,而且具有纸质现金所不具有的安全性和隐私性,正在成为电子商务中实现网上支付的主要工具。

电子现金作为纸币现金的电子化形式,具有下述基本特性。

(1) 货币价值性。电子现金必须得到现金(货币)、银行认可的信用卡或银行承认的现金支票的支持。如果某家银行的电子现金能被其他银行接受的话,那么银行间就能毫无障碍地进行对账;但如果得不到其他银行的支持,则电子现金的流通就存在了问题。

(2) 可交换性。电子现金作为一种支付结算方式,必须能够与其他的电子现金、纸币现金、商品或服务、银行账户的存款、债券等进行交换。某种电子现金可能是依附于某家银行的,但由于电子商务交易的全球化特性,不可能让所有的顾客都通过同一家银行进行结算,所以电子现金必须具有可交换性。

(3) 可存储性。电子现金必须可储存,如存储在计算机的外存、智能卡或其他易于转换的标准或专用的设备上,在需要时进行电子现金的检索和交换。

(4) 不可重复性。电子现金和实际通货一样,只能支付一次。但由于电子现金不像纸币那样是一个实物,甲支付给乙以后,甲就不再拥有已经支付出去的现金了。电子现金只是

一些数字，本身具有无形性，所以要设法防止同一笔电子现金的复制和双重使用。

(5) 匿名性。电子现金与实际通货一样，也具有匿名性，这样买卖双方在使用电子现金时都能避免暴露自己的身份，匿名性也防止了销售商未经客户同意就收集有关个人或组织的消费习惯等信息。

(6) 可分解性。这是电子现金与纸币现金的一个重要区别。与纸币现金受所发行的纸币单位不同，电子现金可以根据交易双方达成的协议来决定支付单位的大小，电子现金的不同单位和其真实价值都能独立于现实现金进行定义，不受现实现金体系的限制。

2) 电子现金的使用

电子现金采用的是基于公开密钥进行数字签名的加密方法。该方法采用了一对密钥：一个用于上锁(加密)，另一个用于开锁(解密)。用其中一个密钥加密的信息只能用另一个密钥解密。加密密钥必须秘密保存，而解密密钥则可以公开。

银行可以向所有客户提供其公开密钥，使客户能解开用银行私有密钥加密的任何信息，如果客户的解密操作生成了可识别的消息，就可确信加密人是银行。这样的加密方法，经实际使用证明非常有效。

用户在支付了电子现金后，商家把它传送给发行该电子现金的银行，因为上面有银行的数字签名，所以银行可以确认该电子现金的真实性。但银行并不知道谁是消费者，只知道这笔电子现金是真实的，这就做到了真正的匿名现金。

3) 电子现金的优缺点

电子现金具备很多优点，主要体现在以下几个方面。

(1) 更方便、更有效。无论对消费者还是商家，电子现金都要比传统的现金、支票、信用卡结算方式更为有效、更为方便，最终能降低消费者的购物费用。

(2) 成本更低廉。在 Internet 上进行电子现金转账的成本要比处理信用卡的成本低。传统的货币交换系统要求银行、分行、银行职员、自动取款机及相应的电子交易系统来管理转账业务并保存现金，其处理成本非常高。而电子现金的转账只需利用现有的技术设施、Internet 和计算机系统就能完成，所以处理电子现金在硬件方面需要追加投入的固定成本趋近于零。

(3) 交易成本与交易距离无关。传统通货所跨越的距离和其处理成本是成正比的，通货跨越的距离越远，移动它所需要的成本也就越高。但由于 Internet 的全球性，所以距离对电子现金的移动而言根本就不是问题，将电子现金从北京转到纽约和从北京转到天津所需的成本是一样的。

(4) 人人都可使用。企业间的交易可以用电子现金来结算，消费者之间也可以用电子现金结算。

(5) 不需要特殊认证。与使用信用卡必须进行特殊认证不同，使用电子现金不需要进行特殊认证，电子现金可用于各种类型的交易。

电子现金也有其缺点，其中比较突出的是下面几点。

(1) 征税困难。如何对 Internet 上发生的业务进行征税一直是电子商务中的一个大问题，由于电子现金很难跟踪，更为征税带来了困难。

(2) 可能被用来洗钱。由于用电子现金付款就像用现金付款一样难以进行追踪，因而有些人就有可能利用非法获得的电子现金匿名采购商品，再把这些商品公开销售以换得真

正的现金。

(3) 可能被伪造。像传统的现金一样,电子现金也可能被伪造,尽管伪造的困难越来越大,但其可能性还是存在的。

3. 电子钱包

1) 电子钱包的概念

电子钱包是电子商务活动中消费者购物常用的一种电子支付工具。它的功能如同实际钱包一样,可以存放信用卡信息、电子现金、所有者的身份证书、所有者地址以及在电子商务网站的收款台上所需的其他信息。电子钱包大大提高了在线购物的效率。消费者选好商品后,只需点击自己的电子钱包,从中选择一张信用卡或其他支付工具就能自动完成付款过程。电子钱包能够帮助消费者将所需信息自动输入到收款表格里,从而大大加速了购物的过程。英国 National Westminister 银行开发的电子钱包 Mondex 是世界上最早的电子钱包系统,于 1995 年 7 月首先在有"英国的硅谷"之称的斯温顿(Swindon)市试用。

电子钱包软件的功能大致包括以下三个方面:

- 电子证书管理:包括电子证书的申请、储存及删除等。
- 交易的进行:进行 SET 交易时辨认商家身份并发送交易信息。
- 交易记录的保存:保存每一笔交易记录,以供日后查询。

2) 电子钱包的使用

使用电子钱包进行网上购物的一般方法如下所示。

(1) 如果是第一次使用电子钱包,用户首先要在相关银行开设账户,取得信用卡,并申请开通电子钱包服务功能。

(2) 从网上下载并安装相应的电子钱包软件到用户计算机中,或者直接连接到电子商务服务器上并登录到电子钱包服务系统中。

(3) 在电子钱包中注册用户,并将可用于网上支付的各种电子货币或电子金融卡添加到电子钱包中,以便将来支付使用。

(4) 登录支持电子钱包支付的在线商家网站选购商品并确定订单。

(5) 用电子钱包进行在线结算。将电子钱包装入系统,通过输入用户名和密码打开电子钱包,从中选择一张电子信用卡来付款。

(6) 在线商家收到经过加密的用户订单和信用卡信息(商家无法看到经过加密的信用卡信息),将用户编码加入电子订单后,和加密的信用卡信息一起送到提供电子钱包服务的电子商务服务器上去。电子商务服务器在确认这是一位合法用户后,即将用户信用卡信息同时送到发卡银行和商家开户银行。发卡银行对用户信用卡的有效性进行验证,验证通过后由银行负责将货款从用户账户转移到商家账户。若验证无效,则说明用户信用卡上的金额不足以支付或信用卡过期,用户可以再从电子钱包中选择另一张信用卡重复上述操作,直至完成支付。

(7) 支付完成后,由商家开户银行向电子商务服务器发出支付确认信息,再由电子商务服务器向商家发出支付确认信息,商家即可向用户发出交易确认信息,并出示一份电子收据发送给用户。

(8) 商家根据用户订单提供的送货地址,利用物流配送系统进行送货。

对于老用户，可以省略第 1 步至第 3 步。电子钱包的购物过程虽然经过发卡行、收单行等多次身份确认，银行授权和银行之间的数据交换以及用户、商家和电子商务服务器之间的身价认证和数据交换，但这些都是利用计算机在很短的时间内完成的。

3）电子钱包的特点

（1）钱包软件充分保障持卡人的个人财务机密资料，即使是商家也看不到卡号及有效期等信息。

（2）利用 SET 协议为持卡者及商家提供身份确认等必要的安全保护。

（3）钱包软件支持多用户、多类型，即多个持卡人可共用同一钱包。只需安装一次钱包软件，各持卡人均可设定自己的密码，保护个人持卡资料及消费记录；也可将钱包安装在多台计算机上，供不同场合使用。

（4）钱包软件为用户提供密码保护功能，因此，钱包的每个用户必须牢记密码，没有密码，用户不可能访问钱包中已有的信息。

（5）钱包软件支持一用户多信用卡贷记卡功能，即一个钱包可容纳多张不同类型的银行卡。

（6）通知商家接收及认可订单，并可查询历史交易记录。

4. 电子支票

1）电子支票的概念

电子支票（Electronic Check）是一种借鉴纸张支票转移支付的优点，利用数字传递将钱从一个账户转移到另一个账户的电子付款形式。比起前面几种电子支付方式，电子支票的出现和开发相对较晚。电子支票以纸质支票为模型，用电子方式生成，使得买方不必使用写在纸上的支票，而是使用显示在屏幕上的支票进行支付活动。电子支票和纸质支票一样，包含支付人姓名、支付人金融机构名称、支付人账户名、被支付人姓名、支票金额等内容。买方填好电子支票后，可以通过计算机网络将其发到卖方的电子信箱中，同时把电子付款通知单发到买方开户银行，买方开户银行随即把款项转入卖方的银行账户，这一支付过程在几秒钟内即可完成。为了确保支付的安全性，电子支票和纸质支票一样，需要数字签名、被支付人数字签名背书，并采用数字证书确认支付者及被支付者身份、支付银行以及账户，电子支票在网络上的传递也采用加密方式，以确保交易的安全。电子支票既适合个人付款，也适合企业之间的大额资金转账，因而可能是最有效率的电于支付手段之一。

2）电子支票的交易流程

在交易活动中采用电子支票作为支付手段的前提是用户必须首先在提供电子支票服务的银行开设账户，申请电子支票。具体使用电子支票的付款过程可以分为以下几个步骤。

（1）买卖双方达成购销协议，选择用电子支票支付货款。

（2）买方在计算机上填写电子支票，一般包含支付人姓名、支付人账户名、接收人姓名、支票金额等内容，然后由买方用自己的私钥在电子支票上进行数字签名，用卖方的公钥加密电子支票后形成电子支票文档。

（3）买方通过网络向卖方发出电子支票，同时向买方开户银行发出经过数字签名的付款通知单。

（4）卖方收到电于支票后用私钥解密电子支票，并用买方的公钥确认买方的数字签名，

然后卖方用数字签名的方式背书电子支票，填写进账单，并对进账单也进行数字签名。

（5）买方将经过背书的电子支票和签过名的进账单通过网络发给卖方开户银行。

（6）开户银行验证电子支票上买方的签名和卖方的背书，确认无误后进行数字签名并通过金融结算网络将电子支票发给买方开户银行。

（7）买方开户银行验证电子支票上卖方开户银行和买方的数字签名，确认无误后，通过金融结算网络从买方账户划出相应款项到卖方开户银行，卖方开户银行在卖方账户上存入相应款项。

5. 微支付

在现金、支票和银行卡等传统的支付工具中，现金最适合于低价值的交易。尽管现金具有通用性，但也具有局限性，如交易不能低于最小面值硬币（比如 1 分）的价值，这对于诸如获取股票市场上某个股票的当前报价、对数据库服务的单笔询问等一大类微价值商品和服务而言是一个问题。在传统商务中，解决该问题的方法就是采用支付的“预定模式”，即购买者提前支付并在某固定期间内使用产品或服务。尽管这种做法保证了内容提供商可以为所提供的服务获得报酬，但是在很多情况下，这实际拒绝了很大的用户群，因为有部分用户只希望十分偶然地使用该服务，同时这也限制了有些用户对该项服务进行尝试的可能性。

因为预定模式并不能很好地解决上述问题，因此需要另外一种支付系统，它可以在单笔交易中有效地转移很小的金额（可能低于 1 分钱）。这意味着通信量本身的花费也必须保持在绝对低的程度。如果传送成本比支付本身还要高，这样的支付系统就是不成功的。在以往讨论的很多支付系统中，商户与代表支付系统提供者的网络服务器进行实时对话，以验证每笔支付的有效性，或者检查资金的可用性，以完成支付，这说明每笔交易具有很高的系统开销，而在微支付系统的设计中必须减少这种开销。

交易的低价值也意味着在每笔交易中获取的利润很少，在这种条件下，为了使得服务器能够运行下去，它必须能够高速地处理交易。这意味着另外一个要求，即微支付系统必须便宜地完成支付的验证工作。如果服务器花费相当多的时间去完成公开密钥加密或解密的话，那么其交易数吞吐量就不会太大。因此，成功的微支付系统一般不能使用须在计算上投入资金的加密技术。

目前已经存在 Milicent、PayWord、MicmMint 等几种微支付系统。

6. 移动支付

从电话银行到网上银行，再到手机银行，银行业务已经从柜台迅速延伸到了电子领域。作为新兴的电子支付方式，移动支付拥有随时随地，方便、快捷、安全等诸多特点。消费者只要拥有一部手机，就可以完成理财或交易，享受移动支付带来的便利。如今，手机支付正成为电子商务的新亮点。

移动支付，是指用户使用移动电子设备，通过移动运营商向约定银行提供的计算机网络系统发出支付指令，由银行通过计算机网络将货币支付给服务商的一种支付方式。

移动电子设备持有者在购物消费或缴费时，只要输入特定的银行卡号和金额，将支付请求通过短信发送到银行；银行在进行审批划账之后，通过短信反馈到特约商户或特约商户指定的银行；商户使用无线或有线 POS 机打印出消费收据，完成交易，用户就会获准得到

所需要的商品和服务，整个过程全部实现电子化。将移动电子设备和银行卡结合起来，用户将随身携带支付终端，可以在任何时间、任何地点用移动电子支付方式办理消费、缴费和转账等业务。

近年来，中国移动通过加强产业合作，全面加快了手机钱包业务的开发和市场推广步伐。手机钱包是中国移动与中国银联联合各大国有及股份制商业银行，共同推出的一项全新移动电子支付、金融信息服务。手机钱包通过把客户的手机号码与银行卡等支付账户进行绑定，随时随地为中国移动手机用户提供移动支付服务。用户可使用手机短信、语音、WAP、K-Java、USSD 购物和理财三类基本业务，具体包括查缴手机话费、手机充值、个人账户查询、购买彩票、手机订报、购买 IP 卡、手机捐款、远程教育、手机投保、公共事业缴费等多项业务。随着用户对移动支付业务需求的不断变化，手机钱包的功能将不断扩展和创新。从消费者的反应来看，目前人们最热衷使用的是查缴话费、个人账务查询以及水、电、气等公共事业缴费等。手机钱包业务资费包括基本服务费和通信费，但目前向绝大多数用户免收基本服务费，这种状态将持续一段时间，收费进程将根据市场情况分步骤、分地区、分人群地逐步推进。

中国联通也和中国建设银行联手推出了新一代手机银行业务。手机银行基于中国联通的 CDMA 1X 网络和 BREW 技术，以中国建设银行“e 路通”电子银行平台为依托，具有手机理财、手机支付及手机电子商务功能。目前，中国联通手机银行可提供的服务包括查询（账户余额、账户明细、消费积分等）、转账（本人名下转账、转账给他人）、汇款（提供异地汇款）、缴费（缴纳水、电、气、电话、交通等各项银行代理的缴费业务）、银行转账（银行账户与证券保证金账户之间资金互转）、外汇买卖（提供外汇实时行情、实时交易和委托交易）以及手机支付等。有了手机银行，客户不用亲自去银行柜台，不必排队等候，就可以通过手机随时随地办理各种银行业务。

5.2.3 电子货币的基本概念及分类

1. 电子货币的概念

在网上支付的前提下，传统形式的货币是很难进行操作的，这就要求有一种区别于传统形式的新型货币——电子货币——来完成交易。

电子货币是以金融电子化网络为基础，以电子计算机技术和通信技术为手段，以电子数据（二进制数据）形式存储在银行的计算机系统中，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的货币。

通过网上银行进行的金融电子信息交换的电子货币与纸币等其他货币形式相比，具有保存成本低、流通费用低、标准化成本低、使用成本低等优势；尤其适用于小金额的网上采购。电子货币技术解决了无形货币的存储、流通、使用等方面的技术问题，具有很大发展潜力。美国的 Mark Twain 银行是美国第一家提供电子货币业务的银行，早在 1996 年 4 月就拥有了 10 000 个电子货币客户。

电子货币的广泛使用也给普通消费者在购物、饮食、旅游和娱乐等方面的消费带来了更多的便利。电子货币是电子支付的有价凭证，它在数字化、网络化环境中完成实时在线的支付过程，比传统纸质的钞票、支票更便捷，是完全意义上的电子交易所追求的全新的支付

手段。

电子货币与传统的货币相比有以下特点。

(1) 流通便捷性：电子货币通过提供网上支付和转账结算，可以突破时空限制，实现3A(Anytime、Anywhere、Anyhow)式的便利支付，经济主体的任何支付结算都能够在瞬间轻松地完成。

(2) 无限分割性：电子货币分割性相当好，可以申请到足够小的面额或价值，满足任何微小的支付额。

(3) 货币价值性：现金替代型电子货币的价值依赖于现金或存款；独立支付型电子货币的价值是以发行银行或公司的信誉或资产为保证的；若是中央银行发行的，则是以国家信誉以及一国资源为保证的。

(4) 发行主体多元化，电子货币产生和发展的最初主体是非银行机构，特别是IT行业厂商和掌握信息技术的网络公司。

2. 电子货币的分类

人们所称的电子货币，所含范围极广，如信用卡、储值卡、借记卡、IC卡、消费卡、电话卡、燃气卡、电子支票、电子钱包、网络货币、智能卡等，几乎包括了所有与资金有关的电子化的支付工具和支付方式。

电子货币按支付方式可分为以下几种。

(1) “先存款，后消费”的预付型电子货币，如现阶段在我国广泛使用的借记信用卡和储值卡。

(2) 在消费的同时从银行账户转账的即付型电子货币，如通过ATM机和POS机使用的现金卡。

(3) “先消费，后付款”的后付型电子货币，如目前国际通用的Visa卡等贷记信用卡。

电子货币按形态可分为以下几种。

(1) 信用卡应用型：在传统信用卡基础上实现了在Internet上通过信用卡进行支付功能的电子货币，是目前发展最快、正步入实用化阶段的电子货币。

(2) 电子现金型：通过将按一定规律排列的数字串保存于计算机的硬盘内或IC卡内来进行支付，即以电子化的数字信息块代表一定金额的货币。

(3) 储值卡型：只能存取款。

(4) 存款电子划拨型：通过计算机网络转移，划拨存款以完成结算的电子化支付方法。

5.2.4 网上银行的概念

处于全球信息化进程中的银行，是以两种身份参与电子商务的。首先，银行要为所有参与电子商务的各方提供网上支付服务，因此银行是电子商务的有力推进者；其次，银行也是企业，也要通过Internet为其客户提供网上银行服务，从这层意义上说，银行是电子商务的积极参与者。银行要有效地参与上述两个方面的电子商务活动，首先必须进行网上银行建设。

网上银行(Internet Bank)，又叫做网络银行、在线银行(Online Bank)，简称网银，是指银行利用Internet和Intranet等技术，为客户提供的综合、统一、安全、实时的银行服务；包

括提供对公、对私的各种零售和批发的全方位银行业务；还可以为客户提供跨国支付与清算等其他的贸易、非贸易的银行业务服务。

网上银行是一种虚拟银行，是 Internet 上的虚拟银行柜台，是电子银行的高级形式。银行无须设立实体分支机构，就能通过 Internet 将银行服务铺向全国以致全世界，使客户在任何地点、任何时刻能以多种方式方便地享受银行的个性化的全方位服务。

网上银行从诞生之日起，就具有如下鲜明特征：

- 依托计算机、计算机网络与现代通信技术。
- 银行业务直接在 Internet 上推出。
- 支持企业用户和个人用户开展电子支付，进行电子商务。
- 采用多种先进技术来保证交易安全。

5.2.5 网上银行的特点

金融环境中的企业竞争的加剧，使得银行不得不重新审视自身的服务方式。已有多位专家预测，在未来五年里银行分行的开设将逐渐减少，自动取款机的增长率也将减缓，而电话语音及网上银行的使用将大幅度增加，新兴的网上银行无疑是对传统银行的挑战。它将取代国际金融界长期以来一直讨论而未具体实施的家庭银行（Home Banking）、企业银行（Firm Banking）等概念而成为银行最便利的服务手段。网上银行是一种高科技的银行业务手段，与传统的银行服务体系相比，具有以下明显的优势。

（1）提高了金融服务质量。网上银行方便、快捷、高效的服务更能满足客户的多样化需求。目前，客户的需求越来越多样化，而且对效率等提出了很高的要求。通过网上银行，上网客户可以在家里开立账户，进行收付交易，省去了跑银行、排队等候的时间，减少了银行服务的中间环节，网上银行可以大范围、全天候、实时提供各种服务，提供 3A 式服务，这种服务包含更多的针对性、个性化和人情味。银行的电子化大大缩短了资金在途时间，提高了资金利用率和整个社会的经济效益。

（2）打破了地域的局限。以往银行投入大笔资金开设分行，客户往往只限于固定的地域，而网上银行则打破了地域的局限，可以永久地留住客户。

（3）拓宽金融服务区域。目前银行所提供的服务，无论是分行、ATM 或电话语音，都难以像网上银行那样提供多元且交互的信息及服务。而网上银行不仅可以使企业或个人不出家门，通过网络查询信息或实现在线交易支付，还可以帮助企业实现在线理财、企业集团服务、对公账务实时查询、网上转账、国际收支申报等广泛的金融服务。

（4）大大降低服务成本。与其他银行服务手段相比，网上银行可以减少固定网点数量和银行工作人员数量，从而使银行的投入与经营成本大大减少。一方面，网上银行的设立成本低；另一方面，通过网上交易，可以大大减少交易费用。另外，由于采用了虚拟现实信息处理技术，网上银行可以在保证原有的业务量不降低的前提下，减少营业点的数量。

（5）网上银行系统简单易用，便于升级维护。在网上服务中，客户处于中心地位，客户使用网上银行服务不需要特别的软件，甚至无须任何专门的培训，只要有一台计算机和调制解调器，拥有进入 Internet 的账号和密码便能在世界各地与 Internet 联网。登录网上银行后即可按照网上银行网页的提示进入自己所需的业务项目，处理个人交易。这不仅方便客户，银行本身也可因此加强与客户的亲密性。网上银行的客户端由标准浏览器软件组成，便

于维护。E-mail 通信方式也非常灵活方便，便于客户与银行之间以及银行内部之间的沟通。银行在升级应用系统或安装新产品时只需简单地更新或升级服务器应用程序即可，而无须对客户端做任何变动。

5.2.6 网上银行业务

按运行机制划分，真正的网上银行目前有两种形式。一种是完全依赖于 Internet 发展起来的全新网上银行，也叫虚拟银行，这类银行几乎所有的业务交易都依靠 Internet 进行，如美国安全第一网上银行。这种银行最大的优点就是节省费用。美国安全第一网上银行的行长估计他们的管理费用只占总资产的 1%，而一般的银行则要达到 3%～3.5%。所以它可以带给用户更多的利益，如提供优惠的利率，且收费仅为普通银行的三分之一。美国安全第一网上银行通过 Internet 提供全球性的金融服务，提供全新的服务手段，客户足不出户就可以进行存款、取款、转账、付款等业务。当然，客户进入网上银行的先决条件是要有一台连入 Internet 的计算机。在此基础上，客户即可登录到网上银行主页，这时屏幕上显示“开户”、“个人财务”、“咨询台”、“行长”等栏目，用鼠标点击所需栏目，就可以遵照各类提示进入自己所需的业务领域了。

另一种网上银行模式是在现有商业银行基础上发展起来的，是传统银行运用公共的 Internet 服务，开设新的电子服务窗口，开展传统银行业务交易处理服务，是实体与虚拟结合的银行。这种银行主要是运用计算机和网络技术开展传统银行业务，如日常交易处理、发展家庭银行、发展企业银行等。这种模式与前一种模式的不同之处在于，它是利用计算机辅助银行开展业务，而不是完全电子化。能够提供网上服务已经成为银行国际化和先进性的一项重要标志。目前我国开办的网上银行业务都属于后一种。

5.3 网上交易安全

5.3.1 网络安全面临的威胁

众所周知，Internet 是一个完全开放的网络，任何一台计算机、任何一个网络都可与之连接。借助 Internet 发布信息，获取与共享各种网站的信息资源，发送 E-mail 与开展网络办公，进行各种网上商务活动，即电子商务，这些都极大地方便了政府、企业与个人的现代事务处理，直接带动了一个网络经济时代的到来。但同时，也有很多别有用心的组织、个人或黑客(Hacker)经常在 Internet 上四处活动，寻求机会窃取别人的各种机密，如信用卡密码，甚至妨碍或毁坏别人的网络系统。依据 Warron Research 的调查，2002 年世界排名前 1000 名的公司几乎都曾被黑客闯入。据美国“金融时报”做过的统计，平均每 20 秒就有一个网络遭到入侵，虽然遭受入侵的大多是安全防护不力的网络系统或数据系统，但说明了 Internet 上这类不道德活动或非法活动的猖狂。在这种情况下，如果没有严格的安全保证，商家和客户就极有可能因担心网上的安全问题而放弃使用电子商务，从而阻碍了电子商务的发展。信息的安全、资金的安全、商务系统的安全都会直接影响到电子商务能否顺利进行。因此，保证电子商务的安全既是电子商务的核心问题，同时也是难点。从网络方面考虑电子商务

面临的威胁主要有以下几个方面。

1）系统层安全性漏洞

由于电子商务系统的运作必须以计算机系统层的软、硬件为基础，因此计算机系统层所使用的硬件设备、软件系统、数据库及网络整体结构中的安全性漏洞将直接造成电子商务中的安全性隐患。

2）数据安全性威胁

跨平台数据交换引起的数据丢失、意外情况造成的数据破坏、传输过程中的数据截获以及传输过程中的数据完整性破坏都是来自数据方面的安全性威胁。

3）计算机病毒的危害

从理论上来说，由于任何计算机系统和网络都有薄弱点，任何系统软件都不可能尽善尽美，因此可以针对这些薄弱点设计出各式各样的病毒，没有一种计算机系统能够幸免于病毒的攻击。

4）黑客攻击

电子商务起步不久，安全性措施尚不完善，因而成为网络黑客攻击的焦点。黑客往往利用电子商务系统中的种种安全性漏洞，窃取和破坏系统数据，甚至修改系统，对整个系统的正常运作造成严重危害。

5.3.2 SSL 协议和 SET 协议

如何安全地通过电子支付完成整个交易过程，是人们在选择网上交易时所必须面对的，而且是首先要考虑的问题。就目前而言，虽然电子支付的安全问题还没有形成一个公认成熟的解决办法，但人们还是不断通过各种途径进行大量探索，SSL 安全协议和 SET 安全协议就是这种探索的两项重要结果，它们在国际间的电子支付中已被广泛使用。

1. SSL 安全套接层协议

1）SSL 协议的基本概念

SSL 协议（安全套接层）是由网景（Netscape）公司推出的一种安全通信协议，它能够对信用卡和个人信息提供较强的保护。SSL 是对计算机之间整个会话进行加密的协议。在 SSL 中，采用了公开密钥和私有密钥两种加密方法，主要用于提高应用程序之间的数据的安全系数。SSL 协议的整个要领可以被总结为：一个保证任何安装了安全套接层的客户机和服务器间事务安全的协议，它涉及所有 TCP/IP 应用程序。

SSL 协议主要提供三方面的服务。

（1）认证用户和服务器，使得它们能够确信数据将被发送到正确的客户机和服务器上。

客户机和服务器都有各自的识别号，这些识别号由公开密钥进行编号，为了验证用户是否合法，安全套接层协议要求握手交换数据进行数字认证，以此来确保用户的合法性。

需要说明的是，安全套接层协议是一个保证计算机通信安全的协议，实现对通信过程的安全保护。例如，一台客户机与一台主机连接上了，首先是要初始化握手协议，然后建立一个 SSL。从对话直到结束，安全套接层协议都会对整个通信过程加密，并且检查其完整性。这样一个对话时段算一次握手。而 HTTP 协议中的每一次连接就是一次握手，因此与 HTTP 相比安全套接层协议的通信效率会高一些。

(2) 加密数据以隐藏被传送的数据。安全套接层协议所采用的加密技术既有对称密钥技术(如 DES),也有公开密钥技术(如 RSA、MD5 等)。具体是,客户机与服务器进行数据交换之前,交换 SSL 初始握手信息,在 SSL 握手信息中,采用了各种加密技术对其加密,以保证其保密性和数据的完整性,并且用数字证书进行鉴别,这样就可以防止非法用户使用一些工具(如 IP 数据包犬)进行窃听。尽管"IP 数据包犬"也能嗅到通信的内容,但无法对其进行破译。

(3) 维护数据的完整性,确保数据在传输过程中不被改变。安全套接层协议是采用 Hash 函数和公钥加密的方法来提供信息完整性的服务,来建立客户机与服务器之间的安全通道,使所有经过安全套接层协议处理的业务都能全部、完整、准确、无误地到达目的地。

2) SSL 协议的运行步骤

(1) 接通阶段。客户通过网络向服务商打招呼,服务商进行回应。

(2) 密码交换阶段。客户与服务商之间交换认可的密码。一般选用 RSA 密码算法,也可选用 Diffie-Hellman 和 Fortezza-KEA 密码算法。

(3) 会谈密码阶段。客户与服务商之间产生彼此交谈的会谈密码。

(4) 检验阶段。检验服务商取得的密码。

(5) 客户认证阶段。验证客户的可信度。

(6) 结束阶段。客户与服务商之间相互交换结束的信息。

当上述内容完成之后,两者间的资料传送就会加以密码,等到另外一端收到资料后再将编码后的资料还原,即使盗窃者在网络上取得编码后的资料,如果没有原先编制的密码算法也不能获得可读的有价值资料。

3) SSL 协议的应用

SSL 安全协议也是国际上最早应用于电子商务的一种网络安全协议,至今仍然有许多网上商店在使用。当然,在使用时,SSL 协议根据邮购的原理进行了部分改进。在传统的邮购活动中,客户首先寻找商品信息,然后汇款给商家,商家再把商品寄给客户。这里的商家是可以信赖的,所以客户需要先付款给商家。在电子商务的开始阶段,商家也是担心客户购买后不付款,或使用过期作废的信用卡,因而希望银行给予认证。SSL 安全协议正是在这种背景下应用于电子商务的。

SSL 协议运行的基点是商家对客户信息保密的承诺。如美国著名的亚马逊(Amazon)网上书店,在它的购买说明中明确表示:"当你在亚马逊公司购书时,受到'亚马逊公司安全购买保证'保护,所以你永远不用为你的信用卡安全担心。"但在 SSL 安全协议的运行步骤中,我们也注意到,SSL 协议有利于商家而不利于客户。客户的信息首先被传送到商家,商家阅读后再将其传送到银行,这样客户资料的安全性便会受到威胁。商家认证客户是必要的,但整个过程中缺少了客户对商家的认证。在电子商务的开始阶段,由于参与电子商务的公司大多是一些大公司,信誉较好,这个问题没有引起人们的重视。随着电子商务参与的厂商数量迅速增加,对厂商的认证问题越来越突出,SSL 协议的缺点被完全暴露出来。SET 协议比 SSL 协议复杂,在理论上安全性也更高。因为前者不仅加密两个端点间的单人会话,还可以加密和认定三方面的多个信息,而这是 SSL 协议所不能解决的问题。SSL 协议将逐渐被新的 SET 协议所取代,但是 SET 协议也有自己的缺陷。由于过于复杂,所以对消费者、商户和银行方面的要求都非常高,推行起来遇到的阻力也比较大,而相比之下 SSL 协

议则以其便捷和可以满足现实要求的安全性，得到了不少人的认可。目前国际上对两种网络安全协议到底哪种是未来的发展方向还没有形成共识。

2. SET 安全电子交易协议

1) SET 协议的基本概念

安全电子交易(SET)协议是世界两大信用卡巨头——万事达国际组织和 Visa 国际组织——在微软公司、网景公司、IBM 公司、GTE 公司、SAIC 公司及其他公司的支持下联合设计的、支持信用卡交易的安全协议。起初，万事达国际组织与网景公司和 IBM 公司一起开发了一种基于安全套接层协议(SSL)的交易安全系统，称为安全加密结算协议(SEPP)。而它们各自的对手 Visa 国际组织和微软公司则开发了另一种标准安全交易技术(STT)作为反击。但来自银行业的压力最终迫使双方开展合作，开发出了安全电子交易协议(SET)作为共同遵守的标准。1996 年 2 月，两大信用卡组织宣布安全电子交易(SET)协议诞生了。

SET 的目的是为通过 Internet 在网站和银行之间传输信用卡支付信息时提供安全保证。此前，虽然已经有了安全套接层(SSL)协议，可以保证在商家和消费者之间传输数据和其他敏感信息的安全，但 SSL 不能验证消费者是否就是信用卡的持有人。

虽然 Visa 国际组织和万事达国际组织声称，“提出 SET 协议的目的是为消费者和商家提供一个统一的解决方法，以便他们可用它在网络上进行结算”，但大众对于 SET 标准的接受速度还是比较慢的。

SET 协议的目标是：提供对信用卡持卡人、卖方和受让人的身份认证，保护信用卡数据的保密性、保持信用卡数据的完整性，并界定这些安全服务所需要的算法和协议。

2) SET 协议的体系结构

SET 协议中涉及的对象有：

- 持卡人，即消费者。他们通过 Web 浏览器或客户端进行购物。
- 发卡机构。它是一个金融机构，为持卡人开设账户，并且发放支付卡。
- 商家。提供在线商店或商品光盘给消费者。
- 银行。它为商家建立账户，并且处理支付卡的认证和支付事宜。
- 支付网关。由收款银行或指定的第三方操纵的设备，它处理商家的支付信息，同时也包括来自消费者的支付指令。

SET 支付系统还涉及认证机构(CA)，但是它不参与 SET 的支付流程。它给各参与方颁发证书，各参与方可以通过查看对方的证书来确定对方是准确的、而不是冒充的。要建立安全的电子商务系统，首先必须有一个健全可信的 CA。

CA 的主要功能包括接收注册请求，处理、批准/拒绝请求、颁发证书。

在实际运作中，CA 也可由大家都信任的一方担当。例如，在客户、商家、银行三角关系中，客户使用的是由某个银行发的卡，而商家又与此银行有业务关系(有账号)。在此情况下，客户和商家都信任该银行，可由该银行担当 CA 角色，接收、处理客户证书和商家证书的验证请求。又例如，对商家自己发行的购物卡，则可由商家自己担当 CA 角色。

3) SET 协议的运行步骤

电子商务的工作流程与实际的购物流程非常接近，使得电子商务与传统商务可以很容易融合，用户使用起来也没有什么障碍。从顾客通过浏览器进入在线商店开始，一直到所订

货物送货上门或所订服务完成，以及账户上的资金转移，所有这些都是通过 Internet 完成的。保证网上传输数据的安全和交易对方的身份确认是电子商务能得到推广的关键。这正是 SET 协议所要解决的最主要的问题。一个包括完整的购物处理流程的 SET 协议的工作过程如图 5.1 所示。

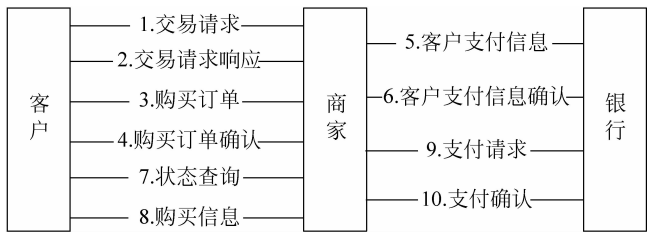

图 5.1 SET 协议流程

图 5.1 中，消息 1 和消息 2 是交易初始设置，客户与商家相互交换身份证书，建立一个交易 ID 号，在消息 3 的客户购买消息中，包含商品或服务名、客户签名、加密的客户信用卡信息，消息 4 是商家对用户购买订单的确认，消息 5 和消息 6 是商家对客户支付信息合法性的验证，在商家与银行（或其代理）间进行，消息 7 和消息 8 使用户对交易内容、状态有查询的能力，消息 9 和消息 10 是商家与银行间的兑现和平账过程。

前 3 步与 SET 协议无关，从第 4 步开始 SET 协议起作用，一直到第 9 步。SET 协议在处理过程中，通信协议、请求信息的格式、数据类型的定义等，SET 协议都有明确的规定。在操作的每一步，持卡人、商家和支付网关都通过认证机构（CA）来验证通信主体的身份，以确保通信的对方不是冒名顶替的。

4）SET 协议提供的安全服务

（1）SET 协议的主要安全目标：

- 信息在 Internet 上安全传输，保证网上传输的数据不被黑客窃取。
- 订单信息和个人账号信息的隔离，当包含持卡人账号信息的订单送到商家时，商家只能看到订货信息，而看不到持卡人的账户信息。
- 持卡人和商家相互认证，以确定通信双方的身份，一般由第三方机构负责为在线通信双方提供信用担保。
- 要求软件遵循相同协议和报文格式，使不同厂家开发的软件具有兼容和互操作功能，并且可以运行在不同的硬件和操作系统平台上。

（2）SET 协议主要提供七个方面的安全服务：

- 确保在支付系统中支付信息和订购信息的安全性。
- 确保数据在传输过程中的完整性，即确保数据在传输过程中不被破坏。
- 对持卡者身份的合法性进行检查。
- 对支付接收方的身份（即商家的身份）的合法性进行检查。
- 提供最优的安全系统，以保护在电子贸易中的合法用户。
- 确保该标准不依赖于传输安全技术，也不限定任何安全技术的使用。
- 使通过网络和相应的软件所进行的交互作业简便易行。

5）SET 协议中使用的加密技术

在 SET 协议的加密处理过程中，用到了后面将介绍的对称密钥加密和非对称密钥加密，将对称密钥加密的快速、低成本与不对称加密的方便、有效完美地结合在了一起。

为了保证发送者对所发送信息的不可抵赖性和消息的完整性，需要对信息进行验证，为此，SET 协议使用了数字签名技术和数字摘要技术。为了保证消息的保密，只让相关方看到他该看的信息，即银行应该只看到支付信息不应该看到消费者具体订购了什么，而商家应该只看到消费者的订购信息而不应该看到消费者的信用卡号等信息，SET 协议还使用了双重签名技术。

6）基于 SET 协议的认证

在整个认证体系中，除了第一层的根 CA（RCA）和第二层的品牌 CA（BCA）外，在基于 SET 协议的认证中，按照使用 SET 协议中交易的角色不同，第三层 CA 签发的证书分别为：持卡人证书（CCA）、商家证书（MCA）和支付网关证书（PCA），利用这些证书可以验证持卡人、商家和支付网关的身份。图 5.2 给出了中国金融认证中心建立的两大 CA 体系（即 SETCA 和 Non-SET CA 系统）中 SET CA 系统的结构图。

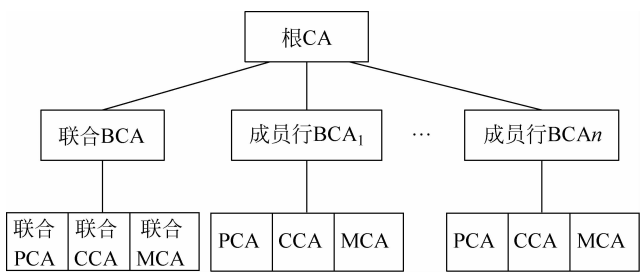

图 5.2　中国金融认证中心的 SET CA 系统

从图 5.2 可以看到，SET 证书是通过信任分组体系来验证的，其形状如一棵树根在上面的树。每一种证书都与签发它的 CA 相联系，在进行证书的验证时，沿着如图 5.2 所示的 CA 信任树往上，直到一个大家公认的可信赖 CA，就可以确认证书的有效性。位于树根的根 CA 的公开密钥对所有的 CA 来说都是已知的，因此可以校验每一个证书。

7）基于 SET 协议的信用卡支付过程

图 5.3 给出了基于 SET 协议的信用卡支付过程。在整个支付过程中要涉及持卡人、商家、支付网关、银行以及发卡机构，此外还需要由基于 SET 协议的认证中心提供对持卡人证书、商家证书和支付网关证书的验证。

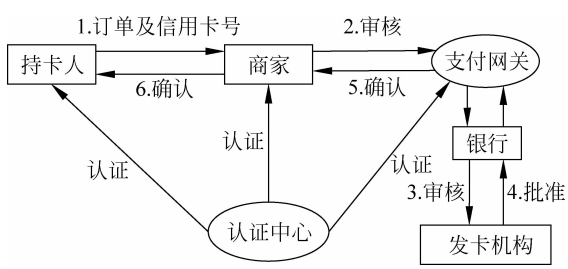

图 5.3　基于 SET 协议的信用卡支付过程

5.3.3 网络安全技术

1. 数据加密技术

1）数据加密过程

随着计算机联网的逐步实现，计算机信息本身的保密问题显得越来越重要。加密技术成为计算机信息保护的最实用和最可靠的方法。

数据加密技术是电子商务采用的最基本的安全技术，是解决诸如信息的窃取、信息的假冒、信息的篡改和信息的抵赖等问题的一种重要手段，同时也是签名技术、认证技术的基础。

数据加密技术是指将一段信息（或称明文）经过加密密钥及加密函数转换，变成无意义的密文，而接收方则将此密文经过解密函数、解密密钥还原成明文。攻击者即使窃取到经过加密的信息（密文），也无法辨识明文。这样就能够有效地对抗截收、非法访问和窃取信息等威胁。

根据密码算法所使用的加密密钥和解密密钥是否相同、能否由加密密钥推导出解密密钥，可将算法分为对称密钥加密算法和非对称密钥加密算法。

2）对称密钥加密技术

对称密钥加密是指信息发送方对要发送的信息按照一定的算法和密钥进行加密，变为密文，密文通过网络到达接收方后，接收方使用相同的算法和密钥进行解密，还原成明文。它只用一个密钥对信息进行加密和解密，如图 5.4 所示。由于加密和解密用的是同一密钥，所以发送者和接收者都必须知道密钥。

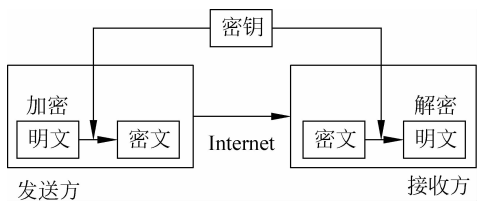

图 5.4 对称密钥加密技术

用对称密钥加密技术对信息编码和解码的速度很快，效率也很高，但也有比较大的局限性。所有各方都必须相互了解，并且完全信任，而且每一方都必须妥善保管一份密钥。如果发送者和接收者处在不同地点，就必须当面或在公共传送系统（电话系统、邮政服务）中无人偷听或偷看的情况下交换密钥。在密钥的交换过程中，任何人一旦截获了它，就可用它来读取所有加密消息。

对称密钥加密算法的典型代表是 DES 算法。1977—1998 年，DES 一直被确认为是美国国家加密标准。另一个典型代表是国际数据加密算法（International Data Encryption Algorithm，IDEA），它比 DES 的加密性更好，而且对计算机要求不高。

DES 算法是一种数据分组的加密算法，是 1972 年由美国 IBM 公司研制的对称密码体制加密算法。其密钥长度为 56 位，明文按 64 位进行分组，将分组后的明文组和 56 位的密钥按位替换或交换的方法形成密文组的加密方法。

DES 的基本工作原理是：其入口参数有 key、data 和 mode，key 为加密解密使用的密

钥，data 为加密解密的数据，mode 为其工作模式。当模式为加密模式时，明文按照 64 位进行分组，形成明文组，key 用于对数据加密；当模式为解密模式时，key 用于对数据解密。在实际运用中，密钥只用到了 64 位中的 56 位，这样就具有较高的安全性。

DES 算法具有极高的安全性，到目前为止，除了用穷举搜索法对 DES 算法进行攻击外，还没有发现更有效的办法。而 56 位长的密钥的穷举空间为 2^{56}，这意味着如果一台计算机的速度是每一秒钟检测一百万个密钥，则它搜索完全部密钥就需要将近 2285 年的时间。

3）非对称密钥加密技术

非对称密钥加密算法采用一对密钥：一个公共密钥（简称公钥）和一个私有密钥（简称私钥）。公共密钥可以发布，私有密钥要保证绝对安全。用公共密钥加密的信息只能用私有密钥解密，反之亦然。图 5.5 为非对称密钥加密过程示意图。

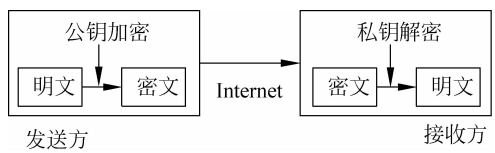

图 5.5　非对称密钥加密技术

加密过程的具体步骤如下。

（1）信息接收方先产生一对密钥，将其中一个作为私钥保存起来，将另一个作为公钥，通过非保密方式发送给信息发送方。

（2）信息发送方使用接收到的公钥和公开密钥加密算法对发送的信息进行加密，产生密文。

（3）密文通过网络被传送到信息接收方。

（4）信息接收方使用自己的私钥和公开密钥加密算法对密文进行解密，得到信息明文。

非对称密钥的优点就在于，尽管通信双方不认识，但只要提供密钥的 CA 可靠，就可以进行安全通信，这正是电子商务所要求的。非对称密钥加密算法的典型代表是 RSA 算法。

RSA 算法是美国麻省理工学院的三位教授罗纳德·里维斯特（Ronald Rivest）、埃迪·沙米尔（Adi Shamir）和伦纳德·阿德勒曼（Leonard Adleman）于 1976 年提出的，并在 1978 年正式公开发表。

在实际应用中，发送方首先获得（一般由认证机构获得）一对密钥并将其中的一个作为公开密钥向公众公开；然后得到公开密钥的接收方使用该密钥加密信息后，再发送给接收方；最后接收方再用自己保存的私有密钥对获得加密的信息进行解密。用户的公开密钥可以登记在网络上，向社会大众发布，而用户的私有密钥则必须由自己秘密保管，不能泄露。

虽然非对称密钥加密算法的保密性较高，也解决了密钥生成、分配和管理等方面的问题，但由于其采用的是大素数因子分解的算法，该算法较复杂，加密和解密时间长、速度慢，不适合对文件加密而只适用于对少量信息进行加密。在实际应用中，往往需要联合使用对称密钥和非对称密钥，即使用对称密钥对传送文件进行加密，而使用非对称密钥来加密传送加密文件的对称密钥。

2. 防病毒技术

计算机病毒对所有的计算机用户来说都不陌生，随着计算机及 Internet 的发展，有些病毒借助网络而爆发流行，如 CIH 病毒、冲击波病毒等，给广大用户带来了极大的损失。从 DOS 时代的“小球”病毒、大麻病毒、黑色星期五病毒，Windows 时代的宏病毒到网络时代通过电子邮件传播的各种病毒，计算机病毒伴随着计算机软硬件技术及网络技术的发展而繁衍成一个庞大的家族。计算机病毒已成为影响电子商务安全的重要因素之一。

1994 年，我国正式颁布实施《中华人民共和国计算机信息系统安全保护条例》，在第二十八条中明确指出“计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。此定义具有法律性和权威性。

1）计算机病毒的特点

计算机病毒是一种特殊的程序，其种类繁多，各自具有不同的特征。从计算机病毒的定义中可以看出，传染性和破坏性是其最基本的特征，其次还具有隐蔽性、可触发性等特点，具体可归纳为如下几个方面。

（1）寄生性。计算机病毒是一种特殊的程序，它寄生在正常的、合法的程序中，并以各种方式潜伏下来，伺机进行感染和破坏。在这种情况下，称原先的那个正常的、合法的程序为病毒的宿主或宿主程序。当执行这个程序时，病毒就起到破坏作用，而在未启动这个程序之前，它是不易被人发觉的。

（2）传染性。计算机病毒的传染性是衡量一种程序是否为病毒程序的首要条件。计算机病毒会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪。计算机病毒可通过各种可能的渠道，如软盘、U 盘和计算机网络去传染其他计算机。

（3）潜伏性。计算机病毒的潜伏性是指其具有依附于其他媒体而寄生的能力。一个编制精巧的计算机病毒程序，进入系统之后一般不会立刻发作，从而可以在几周或者几个月内甚至几年内隐藏在合法文件中，对其他系统进行感染，而不被发现。潜伏性越好，其在系统中的存在时间就会越长，病毒的传染范围就会越大。

（4）隐蔽性。计算机病毒在发作之前，必须能够将自身很好地隐蔽起来，不被用户发现，这样才能实现进入计算机系统，进行广泛传播的目的。计算机病毒的隐蔽性表现为传染的隐蔽性和存在的隐蔽性。传染的隐蔽性是指大多数病毒在传染时不具有外部表现，不易被人察觉；存在隐蔽性是指计算机病毒一般是具有很高编程技巧、短小精悍的程序，依附在正常程序中或硬盘中的较隐蔽的地方，也有以隐含文件形式出现的。

（5）可触发性。计算机病毒的可触发性是指因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性。病毒的触发机制就是用来控制感染和破坏动作的频率的。病毒具有预定的触发条件，这些条件可能是时间、日期、文件类型或某些特定数据等。在病毒运行时，触发机制检查预定条件是否满足，如果满足，则启动感染或破坏动作，使病毒进行感染或攻击；如果不满足，使病毒继续潜伏。

（6）破坏性。计算机病毒的破坏性取决于计算机病毒的设计者。计算机中毒后，可能会导致正常的程序无法运行，删除计算机内的文件或使文件受到不同程度的损坏，并不是所

有的病毒都会对计算机系统产生极大的破坏。但是，由于计算机病毒是一种非法的可执行程序，其存在一个普遍的危害，即降低计算机的工作效率。

2）计算机病毒的分类

按病毒感染的途径，病毒可分为如下三类。

（1）引导型病毒。它是藏匿在磁盘片或硬盘的第一个扇区中的。每次启动计算机时，在操作系统还没被加载之前就被加载到内存中，这个特性使得病毒完全控制 DOS 的各类中断，并且拥有更大的能力进行传染与破坏，如 Michelangelo、Disk Killer 等病毒。

（2）文件型病毒。文件型病毒通常寄生在可执行文件中，当这些文件被执行时，病毒的程序就跟着被执行。根据病毒传染方式的不同，可分为非常驻型和常驻型。非常驻型病毒是将自己寄生在 *.COM、*.EXE 或是 *.SYS 的文件中。当感染病毒的程序被执行时，它将尝试去传染其他文件，如 Datacrime Ⅱ、Vienna 等病毒。常驻型病毒常驻内存。只要执行文件被执行，它就对其进行感染，如 Friday the 13^{th}、Sunday 等病毒。

（3）复合型病毒。这类病毒兼具引导型病毒以及文件型病毒的特性。它们可以传染 *.COM 和 *.EXE 文件，也可以传染磁盘的引导区。

3）计算机病毒的预防

为了避免计算机病毒的感染和传播，应该从预防和清除两个方面着手。预防就是通过采取积极稳妥的应对策略，阻止计算机病毒进入网络计算机系统，使其免于病毒感染，做到防患于未然。采取有效的计算机病毒预防措施，是实现电子商务系统病毒防治的重中之重。预防病毒的主要措施如下所示。

（1）安装防病毒软件。防病毒软件可以有效地阻止已知病毒的侵入，安装完操作系统后的第一件事情就应是安装防病毒软件和进行病毒库的升级。

（2）备份重要资料。资料是最重要的，程序损坏了可重新复制或再买一份，但是因为病毒而损坏了的资料，则难以恢复，所以经常备份重要资料是很必要的。

（3）小心使用可移动存储介质。尽量避免在无防毒软件的计算机上使用可移动储存介质。

（4）先扫描后使用。使用新软件时，先用扫毒程序检查，可减少中毒机会。

（5）使用硬盘恢复工具恢复数据。重建硬盘是有可能，救回的几率相当高。若硬盘资料已遭破坏，不必急于格式化，因病毒不可能在短时间内将全部硬盘资料破坏，故可利用杀毒软件加以分析，恢复至受损前状态。

（6）不要在 Internet 上随意下载软件。病毒的一大传播途径就是 Internet。病毒可能潜伏在网络上的各种可下载程序中，如果随意下载、随意打开，就有可能中毒。因此，当软件下载后，应执行杀毒软件彻底检查。

（7）不要轻易打开电子邮件的附件。近年来造成大规模破坏的许多病毒，都是通过电子邮件传播的。恰当的做法应是先将附件保存下来，用查毒软件彻底检查后再打开。

4）计算机病毒的清除

清除就是通过定期或不定期对网络上的计算机系统进行检查，一旦发现存在计算机病毒，就利用相应的方法将其清除掉。

在清除计算机病毒之前，应注意如下原则：

- 清除病毒之前，一定要备份所有重要数据以防万一。

- 清除病毒时，一定要用干净的系统引导计算机，保证整个清除病毒过程在无毒的环境下进行，否则病毒会重新感染已除毒的文件。
- 备份磁盘引导扇区的文件，在文件名上要反映出该盘的型号、容量和版本。因为不同磁盘的分区表不同，引导记录的 BPB（磁盘基数表）也不同，一旦恢复时不对应，被恢复的磁盘将无法被读取。
- 操作中应谨慎处理，对所读取的数据应进行多次检查核对，确认无误后再进行相关操作。

清除计算机病毒可采用如下方法：

- 恢复主引导扇区信息的方法。对于感染主引导型病毒的计算机可采用事先备份的该硬盘的主引导扇区文件进行恢复。恢复时可使用 DEBUG 或 NORTON 软件。
- 程序覆盖方法。适用于文件型病毒，一旦发现文件被感染，可将事先备份的无毒版本重新存入系统。
- 低级格式化或格式化磁盘。不要轻易格式化磁盘，它会破坏硬盘所有数据。低级格式化磁盘对硬盘有损害，不到万不得已不要使用该方法。使用该方法也必须保证系统无病毒，否则也不起作用。
- 手工清除方法。使用杀毒软件删除或隔离被感染病毒的文件。

3. 防火墙技术

防火墙是保护本地系统或网络、抵制网络攻击的最重要的网络安全防范技术，作为访问控制技术的代表，防火墙产品是目前世界上用得最多的网络安全产品之一，其功能还在不断增加，并且最近还融入了 VPN（虚拟专用网）等功能。

1）防火墙的功能特征

防火墙是设置在被保护网络和外部网络之间的一道屏障，以防止发生不可预测的、潜在破坏性的侵入。防火墙是指设置在不同网络（如可信任的企业内部网和不可信的公共网）或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口，能根据企业的安全政策控制（允许、拒绝、监测）出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。

防火墙可通过监测、限制、更改跨越防火墙的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，以此来实现对网络安全的保护。

归纳起来，防火墙具有如下一些功能。

（1）防火墙是网络安全的屏障。一个防火墙（作为阻塞点和控制点）能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击。如 IP 选项中的源路由攻击和 ICMP 重定向路径。

（2）防火墙可以强化网络安全策略。通过防火墙为中心的安全方案配置，能将所有安全软件（如密码、加密、身份认证、审计等）配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更加经济。

（3）对网络存取和访问进行监控审计。如果所有的访问都经过防火墙，那么，防火墙就

能记录下这些访问并做出日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当报警，并提供网络是否受到监测和攻击的详细信息。

(4) 防止内部信息的外泄。通过利用防火墙对内部网络的划分，可实现对内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。再者，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至因此而暴露了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些能够透露内部细节的服务，如 Finger、DNS 等。如防火墙可以阻塞有关内部网络中的 DNS 信息，这样一台主机的域名和 IP 地址就不会被外界所了解了。

(5) 防火墙的抗攻击能力。作为一种安全防护设备，防火墙在网络中自然是众多攻击者的目标，因此抗攻击能力也是防火墙的必备功能。网络攻击手段一般包括 IP 地址假冒攻击、病毒攻击、口令字探询攻击、网络安全性分析攻击等。

除了安全作用，防火墙还支持具有 Internet 服务特性的企业内部网络技术体系 VPN。通过 VPN，将企事业单位在地域上分布在全世界各地的 LAN 或专用子网有机地联成一个整体。不仅省去了专用通信线路，而且为信息共享提供了技术保障。

尽管利用防火墙可以保护安全免受外部黑客的攻击，但其目的只是能够提高网络的安全性，不可能保证网络绝对安全。事实上仍然存在着一些防火墙不能防范的安全威胁，如防火墙不能防范不经过防火墙的攻击。例如，如果允许从受保护的网络内部向外拨号，一些用户就可能形成与 Internet 建立直接连接。另外，防火墙很难防范来自网络内部的攻击以及病毒的威胁。由于边界内部支持的操作系统和应用程序的不同，采用防火墙来扫描所有进入的文件、电子邮件和报文来查找病毒是不现实的，也许是不可能的。

2) 防火墙的基本类型

防火墙技术可根据防范的方式和侧重点的不同而分为很多种类型，但总体来说可分为包过滤、应用级网关和代理服务等几大类型。

(1) 数据包过滤型防火墙。数据包过滤(Packet Filtering)技术是在网络层对数据包进行选择，选择的依据是系统内设置的过滤逻辑，被称为访问控制表(Access Control Table)。通过检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态等因素，或它们的组合来确定是否允许该数据包通过。

数据包过滤防火墙的逻辑简单、价格便宜、易于安装和使用，网络性能和透明性好，它通常被安装在路由器上。路由器是内部网络与 Internet 连接必不可少的设备，因此在原有网络上增加这样的防火墙几乎不需要任何额外的费用。

包过滤的优点是不用改动客户机和主机上的应用程序，因为它工作在网络层和传输层，与应用层无关。但其缺点也是明显的：过滤判别的只有网络层和传输层的有限信息，因而不可能充分满足各种安全要求；在许多过滤器中，过滤规则的数目是有限制的，且随着规则数目的增加，性能会受到很大的影响；由于缺少上下文关联信息，不能有效地过滤如 UDP、RPC 一类的协议；另外，大多数过滤器中缺少审计和报警机制，且管理方式和用户界面较差；对安全管理人员素质要求高，建立安全规则时，必须对协议本身及其在不同应用程序中的作用有较深入的理解。因此，过滤器通常是和应用网关配合使用，共同组成防火墙系统。

(2) 应用级网关型防火墙。应用级网关(Application Level Gateways)是在网络应用层上建立协议过滤和转发功能。它针对特定的网络应用服务协议使用指定的数据过滤逻辑，

并在过滤的同时，对数据包进行必要的分析、登记和统计，以形成报告。实际中的应用网关通常安装在专用工作站系统上。数据包过滤和应用网关防火墙有个共同的特点，都是依靠特定的逻辑判断是否允许数据包通过。一旦满足逻辑，则防火墙内外的计算机系统建立直接联系，防火墙外部的用户便有可能直接了解防火墙内部的网络结构和运行状态，这不利于抗击非法访问和攻击。

(3) 代理服务型防火墙。代理服务(Proxy Service)也称链路级网关(Circuit Level Gateways)或 TCP 通道(TCP Tunnels)，也有人将它归于应用级网关一类。它是针对数据包过滤和应用网关技术存在的缺点而引入的防火墙技术，其特点是将所有跨越防火墙的网络通信链路分为两段。防火墙内外计算机系统间应用层的“链接”，由两个终止代理服务器上的“链接”来实现，外部计算机的网络链路只能到达代理服务器，从而起到了隔离防火墙内外计算机系统的作用。此外，代理服务也对过往的数据包进行分析、注册登记，形成报告，同时当发现被攻击迹象时会向网络管理员发出警报，并保留攻击痕迹。

应用代理型防火墙是内部网与外部网的隔离点，起着监视和隔绝应用层通信流的作用。同时也常结合过滤器的功能。它工作在 OSI 模型的最高层，掌握着应用系统中可用作安全决策的全部信息。

(4) 复合型防火墙。由于对更高安全性的要求，常把基于包过滤的方法与基于应用代理的方法结合起来，形成复合型防火墙产品。这种结合通常采用以下两种方案。

- 方案 1：屏蔽主机防火墙体系结构。在该结构中，分组过滤路由器或防火墙与 Internet 相连，同时一个堡垒机安装在内部网络，通过在分组过滤路由器或防火墙上过滤规则的设置，使堡垒机成为 Internet 上其他节点所能到达的唯一节点，这确保了内部网络不受未授权外部用户的攻击。
- 方案 2：屏蔽子网防火墙体系结构。堡垒机放在一个子网内，形成非军事化区，两个分组过滤路由器放在这一子网的两端，使这一子网与 Internet 及内部网络分离。在屏蔽子网防火墙体系结构中，堡垒主机和分组过滤路由器共同构成了整个防火墙的安全基础。

4. VPN 技术

VPN(Virtual Private Network)，即虚拟专用网。VPN 也是一项保证网络安全的技术之一，它是指在公共网络中建立一个专用网络，数据通过建立好的虚拟安全通道在公共网络中传播。VPN 解决了内部网的信息如何在 Internet 上安全传送的问题。虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商与公司的内部网建立可信的安全连接，并保证数据的安全传输。使用 VPN 有节省成本、提供远程访问、扩展性强、便于管理和实现全面控制等好处，是目前和今后企业网络发展的趋势。

1) VPN 的功能特征

VPN 的工作原理是：信息的发送进程通过可信任的内部网发送明文到 VPN 服务器，由 VPN 根据安全策略对数据包(包括源 IP 地址和目的 IP 地址等)进行加密，并附上数字签名；然后 VPN 服务器对数据包加上新的数据报头，其中包括一些安全信息和参数，对加密后的数据包重新进行封装。此数据包通过 Internet 上的“隧道”传输，到达目的方的 VPN 服务器，由该服务器解包，核对数字签名，并且解密。最后，明文信息通过内部网传输到目的地。

VPN 具有虚拟的特点，VPN 并不是某个公司专有的封闭线路或者是租用某个网络服务商提供的封闭线路，但同时 VPN 又具有专线的数据传输功能，因为 VPN 能够像专线一样在公共网络上处理自己公司的信息。VPN 可以说是一种网络外包，企业不再追求拥有自己的专有网络，而是将对另外一个公司的访问任务部分或全部外包给一个专业公司去做，这类专业公司的典型代表是电信企业。

通过将数据流转移到低成本的 IP 网络上，一个企业的 VPN 解决方案将大幅度地减少用户花费在城域网和远程网络连接上的费用。同时，这将简化网络的设计和管理，加速连接新的用户和网站。另外，VPN 还可以保护现有的网络投资。随着用户的商业服务不断发展，企业的 VPN 解决方案可以使用户将精力集中到自己的生意上，而不是网络上。VPN 可用于不断增长的移动用户的全球 Internet 接入，以实现安全连接；可用于实现企业网站之间安全通信的虚拟专用线路，用于经济有效地连接到商业伙伴和用户的安全外联网虚拟专用网。

VPN 具有以下优点：

- 低成本。企业不必租用长途专线建设专网，不需大量网络维护人员和设备。
- 易扩展。网络路由设备配置简单，无须增加太多的设备，省时省钱。
- 完全控制主动权。VPN 上的设施和服务完全掌握在企业手中。比方说，企业可以把拨号访问交给网络服务商去做，由自己负责用户的查验、访问权、网络地址、安全性和网络变化管理等重要工作。

VPN 通过采用“隧道”技术，并在 Internet 工程工作组（IETF）制定的 IPSec 标准统一下，在公众网中形成企业的安全、机密、顺畅的专用链路。

目前的 VPN 还存在不足，总结起来主要有下面几个方面：

- 尽管 VPN 的设备供应商们可以为远程办公室或 Extranet 服务的专线或帧中继提供有效方式，可是 VPN 的服务提供商们只保证数据在共管辖范围内的性能，一旦出了其“辖区”则安全性则会没有保证。
- 作为一种典型技术，VPN 的应用时间还不长，VPN 的管理流程和平台相对于其他远程接入服务器或其他网络结构的设备来说，有时并不太好用。
- 不同厂商的 IPSec VPN 的管理和配置掌握起来是最难的，这需要同时熟悉 IPSec 和不同厂商的执行方式，包括不同的术语。

2）VPN 的基本类型

基于不同的角度或出发点，对 VPN 的分类方法是多种多样的，就目前而言，还没有一种公认的、最为合理的划分方式。下面是几种常用的划分方法。

（1）按接入方式划分：

- 专线 VPN。专线 VPN 是为已经通过专线接入 ISP（Internet 服务提供商）边缘路由器的用户提供的 VPN 实现方案。
- 拨号 VPN。拨号 VPN 又称 VPDN，指的是为利用拨号方式通过 PSTN（公用电活交换网）或 ISDN（综合业务数字网）接入 ISP 的用户提供的 VPN 业务。

（2）按隧道协议所属的层次划分：

- 工作在链路层的第二层隧道协议。如点到点隧道协议（PPTP）、第二层转发协议（L2F）、第二层隧道协议（LSTP）。

- 工作在网络层的第三层隧道协议。如通用路由封装协议(GRE)、IP 安全协议(IPSec)。
- 介于第二层和第三层之间的隧道协议。如 MPLS 隧道协议。

(3) 按 VPN 发起主体不同划分：

- 基于客户的 VPN。由客户发起的 VPN。
- 基于网络的 VPN。也称客户透明方式，是由服务器发起的 VPN。

(4) 按 VPN 业务类型划分：

- Intranet VPN。企业的总部与分支机构之间通过公网构筑的虚拟网。
- Access VPN。企业员工或企业的小分支机构通过公网远程拨号方式构筑的虚拟网。
- Extranet VPN。企业间发生收购、兼并或企业间建立战略联盟后，使不同企业间通过公网来构筑的虚拟网。

(5) 按 VPN 应用平台划分：

- 软件 VPN。利用软件公司提供的完全基于软件的 VPN 产品来实现的 VPN。
- 专用硬件 VPN。利用硬件厂商提供的专用硬件平台来实现的 VPN。
- 辅助硬件 VPN。辅助硬件平台的 VPN 主要是指以现有网络设备为基础、再增添适当的 VPN 软件实现的 VPN。

(6) 按运营商所开展的业务类型划分：

- 拨号 VPN 业务。它是第一种划分方式中的 VPDN。
- 虚拟租用线(VLL)。它是对传统租用线业务的仿真，用 IP 网络对租用线进行模拟，而这样一条虚拟租用线在两端的用户看来，等价于过去的租用线。
- 虚拟专用路由网(VPRN)业务。VPRN 是对多点专用广域路由网络的模拟，利用公共 IP 网络，在多个 VPN 成员之间建立起一个虚拟的隧道网络。
- 虚拟专用局域网段(VPLS)。VPLS 利用互联网络设施仿真局域网段，转发表中包含介质访问控制层的可达信息。

5. 网络入侵检测

随着网络技术的发展，网络环境变得越来越复杂，对于网络安全来说，单纯的防火墙技术暴露出明显的不足，如无法解决安全后门问题，不能阻止网络内部攻击，不能提供实时入侵检测能力，对于病毒束手无策等。因此，很多组织致力于提出更多更强大的主动策略和方案来增强网络的安全性，其中一个有效的解决途径就是入侵检测。入侵检测系统(Intrusion Detection System，IDS)可以弥补防火墙的不足，为网络安全提供实时的入侵检测及采取相应的防护手段，如记录证据、跟踪入侵、恢复或断开网络连接等。这引发了人们对入侵检测技术研究和开发的热情。

1) 入侵检测系统的概念

入侵检测通过对计算机网络或计算机系统中的若干关键点收集信息并进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。进行入侵检测的软件与硬件的组合就是入侵检测系统。

入侵检测系统执行的主要任务和功能包括监视、分析用户及系统活动；审计系统构造和弱点；识别、反映已知进攻的活动模式，向相关人士报警；统计分析异常行为模式；评估重要系统和数据文件的完整性；审计、跟踪管理操作系统，识别用户违反安全策略的行为。

入侵检测是对防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。其最重要的价值之一是能提供事后统计分析，所有安全事件或审计事件的信息都将被记录在数据库中，可以从各个角度来对这些事件进行分析归类，以总结出被保护网络的安全状态的现状和趋势，及时发现网络或主机中存在的问题或漏洞，并可归纳出相应的解决方案。

2）入侵检测系统的原理

目前大多数的 IDS 系统主要采用基于包特征的检测技术来组建，它们的基本原理是对网络上的所有数据包进行复制并检测，然后与内部的攻击特征数据库（规则库）进行匹配比较，如果相符即产生报警或响应。这种检测方式虽然比异常统计检测技术要更加精确，但会给 IDS 带来较大的负载，所以需要对检测策略做进一步调整和优化。具体做法是：根据企业自身网络的业务应用情况选择最适合的检测策略，并对所选的策略进行修改，选择具有参考价值的检测规则，而去除一些无关紧要的选项，如对于全部是 Windows 的应用环境，则完全可以把 UNIX 的规则去掉。有些 IDS 除了提供攻击特征检测规则的定制功能外，还提供了对端口扫描检测规则的自定义，如在 KIDS 中就可定义端口扫描的监控范围、信任主机地址排除和扫描模式等参数，这些参数的合理配置都能将 IDS 的检测能力优化到最理想的状态。

IDS 的主要设计思想是安全风险的“可视”和“可控”，它可以提供丰富全面的实时状态信息，使用好 IDS 的关键是要从这些信息中提取最具有价值的内容并加以利用，以便为企业网络安全管理的决策提供依据。

IDS 可以采用概率统计、专家系统、神经网络、模式匹配、行为分析方法等来实现其检测机制，以分析事件的审计记录、识别特定的模式、生成检测报告和最终的分析结果。

3）入侵检测系统的分类

通常，入侵检测系统按其输入数据的来源分为三种：

- 基于主机的入侵检测系统。其输入数据来源于系统的审计日志，一般只能检测该主机上发生的入侵。
- 基于网络的入侵检测系统。其输入数据来源于网络的信息流，能够检测该网段上发生的网络入侵。
- 分布式入侵检测系统，能够同时分析来自主机系统审计日志和网络数据流的入侵检测系统，系统由多个部件组成，采用分布式结构。

入侵检测系统还有其他一些分类方法，如根据布控物理位置可分为基于网络边界（防火墙或路由器）的监控系统、基于网络的流量监控系统以及基于主机的审计追踪监控系统；根据建模方法可分为基于异常检测的系统、基于行为检测的系统、基于分布式免疫的系统；根据时间分析可分为实时入侵检测系统、离线入侵检测系统。

网上银行的先驱

1995 年 10 月 18 日，美国的三家银行联合成立了世界上第一家虚拟网上银行——安全第一网络银行（Security First Network Bank，SFNB），通过 Internet 提供全球范围的金融服

务。1996 年 5 月,SFNB 在华尔街上市后,立即受到热捧,股价在收市时翻了一番,达到每股 41 美元。到 1998 年,在 SFNB 开立的客户户头已达一万多个,存款余额超过四亿美元,而其员工总数不过十人。1998 年,安全第一网络银行被加拿大皇家银行以两千万美元收购了除技术部门之外的所有部门。安全第一网络银行在网上银行发展历史上无疑具有里程碑的意义。

中国招商银行成立于 1987 年 4 月 8 日,是我国第一家完全由企业法人持股的股份制商业银行,总部设在深圳。1996 年,中国招商银行率先在国内推出了网上银行“一网通”的概念。1997 年 4 月,建立网上银行“一网通”并推出网上个人银行。1998 年 4 月,率先在国内推出网上企业银行,开通网上支付功能,成为国内首家提供网上支付服务的银行。网上企业银行是中国招商银行网上银行“一网通”的重要组成部分。招商银行已形成了以“一网通”为品牌的国内著名金融证券网站,功能包括“企业银行”、“个人银行”、“网上证券”、“网上商城”和“网上支付”5 个系统。目前,全国十三家分行开通了网上银行服务,在全国已有约四百八十家企业和七十万人次经由招商银行的网上银行进行交易活动或接受服务。招商银行的网上用户已超过三千万,网上交易额达一百五十亿元。

(注:以上资料源于樊世清.电子商务.北京:清华大学出版社,2012,有删改.)

1. 请结合案例试述目前有哪两种形式的网上银行?各自特点分别是什么?
2. 试述网上银行自产生以来所具备的独特优势。
3. 简述为什么说网上银行能够拓宽金融服务区域。

习题

1. 简述网上商务采购的含义。
2. 电子商务采购从商务模式上来讲,以什么采购为主?
3. 试述网上商务采购的流程。
4. 目前广泛使用的电子支付方式分为哪几类?
5. 简述电子货币的概念。
6. 简述网上银行的概念。
7. 从网络方面考虑电子商务面临的威胁主要有几个方面?
8. 简述 SSL 协议的概念。
9. 简述 SET 协议的目标。
10. 目前有哪些网络安全技术?