第五章
网上支付及结算方式

知识目标

» 了解网上支付的基本流程；
» 了解网上支付各实体之间的关系；
» 掌握银行卡类网上支付模式和虚拟货币网上支付模式；
» 了解第三方网上支付方式。

技能目标

» 能够应用银行卡进行网上支付；
» 能够应用第三方网上支付方式进行网上支付。

引例

六成网上购物者首选网上支付①

在2007年召开的第三届“中国电子支付高层论坛”上，中科院金融科技研究中心、《电子商务世界》杂志联合发布了《2007中国消费者网上支付应用调查报告》。报告显示，安全、便捷的支付成为当前网上支付市场主要需求点，银行具有网上支付服务安全措施升级的主导能力，六成网上购物者首选网上支付。

本次调查主要面向有网上购物行为的个人消费者，开展网上支付应用情况和需求调查，并通过电话、样本深度访谈、专家咨询等方法获得相关的资料和信息。网上购物年龄分布显示：18～26岁的人群占45.5%，27～35岁的人群占41.4%；职业分布显示：除了学生以外，大部分消费者来自工商、医疗、教育等领域，公司职员占到了35.5%；学历分布显示：基本为大专和本科以上学历。消费者方面，具有稳定收入和工作，受过高等教育的年轻人群更愿意选择网上购物，且他们选择网上购物的概率比选择大型商场和连锁超市的概率高出14%。性别方面，女性在网上购物当中占到了45%，超过了男性。消费金额方面，50～100元之间最高，占比为27.8%，100～200元之间占比26.8%，即200元以下是最受消费者认可的。消费者倾向的支付手段——网上支付，已经远远高出其他方式，成为网上购物的主要支付手段之一，占比为61.7%。消费者首选购物网站方面，淘宝占比为42.3%，这表明在购物网站当中C2C的网站仍然被消费者广泛关注。另外，商城的销售模式也会直接影响到网上支付。在影响网上支付使用的因素上，49.2%的人群认为安全是影响网上支付的重要因素，30.3%的人群认为便捷是影响网上支付的因素。另外，部分消费者认为安全并不仅仅是网上安全，还有信用安全。有第三方保障的平台，其网上支付的使用率达到了80%。

本次调研也针对银行进行了一些系统分析。调查中发现，目前有59.6%的被访者使用了数字证书，87.7%的被访者首选的网上银行为工商银行、建设银行和农业银行三家大型国有商业银行。绝大部分电子支付以网上银行为支撑和前提，银行在整个网上支付业务链上处于最关键的安全控制环节，并对整条支付服务产业链的安全措施升级具有主导作用。

鉴于以上调查结果，报告研究者对网上支付提出了相关建议。

首先，融合支付和交易，打消用户安全顾虑，重点关注小额交易。如果支付单纯是支付，市场空间极其有限。如今，被消费者广泛认同的网站是自己拥有支付平台的网站，因此，要考虑如何更好地与商城建立紧密的合作关系，包括第三方信用保证。调查表明，300元以下的金额对90%的消费者都可以接受，因此，小额支付应该是支付厂商关注的，在小额支付当中尤其是数字产品方面前途无量。

① 一泓.六成网上购物者首选网上支付[N].金融时报，2007-08-15(9).

其次，有关网上商城。支付厂商在选择支付平台时，不应只为了便宜，而是为了让消费者更好地在网络商城购物。另外，应加强25～35岁年龄之间市场的开发，年轻群体对网上购物的需求很旺盛，同时承担能力也很强。女性对网上支付产品的关注和需求日益加大，网上商城对此也要重点关注。

此外，有关政策。鼓励发展网上产业，规范虚拟货币，引导银行创新。建议政府部门重点调查现有虚拟货币的存在形式、发放主体，规范虚拟货币的流通，引导主流虚拟货币运营商逐步向规范的第三方支付平台过渡。并鼓励银行开展网上支付业务创新，在持续推动安全控制技术应用的基础上，逐步满足网络消费者对网上银行服务、便捷等方面的需求。

结合以上案例思考：大部分人选择网上支付，那么网上支付的具体流程是什么？

第一节　网上支付的流程

基于Internet平台的网上支付的基础其实就是传统的支付过程。用户通过Internet进行网上支付的过程与目前商场中的销售点系统（即POS信用卡支付结算系统）的处理过程非常相似。其主要不同在于：网上支付方式采用PC、Internet、Web服务器作为操作和通信工具，而POS信用卡支付结算方式则是使用专用刷卡机、专用终端和专用通信通道。

在处理网上支付时借鉴了很多传统支付方式的应用机制与过程，只不过流动的媒介不同：一个是传统纸质货币与票据，大多手工作业；而另一个是电子货币且网上作业。如果熟悉传统的支付结算方式，如纸质现金、支票、POS信用卡等方式的支付结算过程，将有助于对网上支付结算流程的理解。图5-1为基于Internet平台的网上支付流程图。

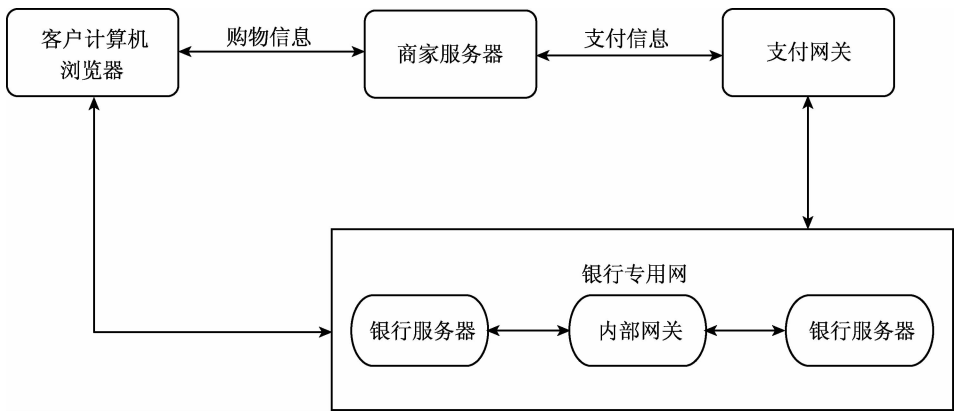


图5-1　基于Internet平台的网上支付流程

（1）客户建立与Internet的连接，通过浏览器进行商品的浏览、选择与订购，填写订单，

选择相应的网上支付工具(如信用卡、电子钱包、电子支票等),并且得到银行的授权使用。

(2) 客户核对相关订单信息并确定订单信息,也可选择对支付信息进行加密,然后在网上提交订单。

(3) 商家服务器对客户的订单信息进行检查、确认,并把相关的、经过加密的客户支付信息等转发给支付网关,直至银行专用网络的银行后台专业服务器确认,以期从银行等电子货币发行机构得到支付资金的授权。

(4) 银行对信息验证及确认后,通过建立起来的、经由支付网关的加密通信通道,给商家服务器回送确认及支付信息;同时,为进一步保证安全,可以选择性地给客户发送支付授权请求。

(5) 银行得到客户传来的进一步授权结算信息后,把资金从客户账号转拨至商家银行账号上,借助金融专用网进行结算,并分别给商家、客户发送支付结算成功信息。

(6) 商家服务器收到银行发来的结算成功信息后,给客户发送网络付款成功信息和发货通知。

至此,一次典型的网上支付结算流程结束。商家和客户可以分别借助网络查询自己的资金余额信息,以进一步核对。

图 5-1 所示的网上支付流程只是目前各种网上支付结算方式应用流程的普遍情况,并不是说所有网上支付方式的应用流程都和图 5-1 一模一样。在实际应用中,由于技术、资金数量、管理机制上的不同,网上支付方式的应用流程还是有所区别的,如信用卡、电子现金、网络银行账号的网上支付结算流程就有所差别,但大致都遵循图 5-1 的流程。

图 5-1 所示的网上支付流程有一个特点,即实现的资金是立即支付。它适用于数目众多的较小额度金额的电子商务业务,对客户与商家来讲都是方便的。但是,对较大金额的资金支付结算,如大企业与大企业间的电子商务业务,实现 Internet 上的立即支付并不现实。目前,传统上独立于商务交易环节的金融 EDI(电子数据交换)或银行专业 EFT(电子资金转账)系统是比较普遍的支付结算方式。随着网络银行业务的发展,特别是企业网络银行业务的成熟与发展,也可基于 Internet 平台在电子商务交易与支付环节分离时进行较大额度资金的网上支付结算。

第二节　网上支付的模式

使用不同网上支付工具进行网上支付的应用流程是有区别的。目前,主要的网上支付工具有信用卡、借记卡、电子现金、电子支票等。这些支付工具的支付、结算和运行各有特点,根据其支付流程的差别,可以把网上支付模式分为银行卡类网上支付模式、虚拟货币网上支付模式和其他网上支付模式。

一、银行卡类网上支付模式

最常见的用于支付的银行卡有信用卡、借记卡等,其中信用卡支付是网上支付中最常见的方式。通常,信用卡网上支付有以下四种类型:

1. 无安全措施的信用卡网上支付模式

无安全措施的信用卡支付方式指的是消费者没有经过任何安全措施防护，将信用卡信息（包括卡号和密码）直接传输给商家，然后通过商家和银行各自的授权来检查信用卡的合法性，其基本流程如图 5-2 所示。这种信用卡支付方式出现在网上支付的早期，由于当时电子商务各方面的发展，尤其是银行对电子商务的支持还非常不成熟，因此这种支付方式的安全性较差、风险较大。

图 5-2　无安全措施的信用卡网上支付流程示意图

在无安全措施的信用卡支付方式中，消费者通过网上订货，然后将信用卡信息在网上或网下（电话、传真等）传输，无安全措施。消费者（即持卡人）将承担信用卡信息在传输过程中被盗取或商家获取信用卡信息等风险；由于商家没有消费者的签字，如果消费者拒付或否认购买行为，商家将会承担一定的风险。

2. 通过第三方代理人的信用卡网上支付模式

在上述无安全措施的信用卡支付过程中，一个致命的问题就是商家完全掌握持卡人的信用卡信息，同时无安全措施的传输也可能产生持卡人的信用卡信息被第三方窃取的风险。

提高信用卡处理安全性的一个途径就是在买方和卖方之间启动第三方代理，目的是使商家看不到消费者的信用卡信息，避免信用卡信息在网上多次公开传输而导致信息泄露。

通过第三方代理人的信用卡支付方式的基本流程，如图 5-3 所示。

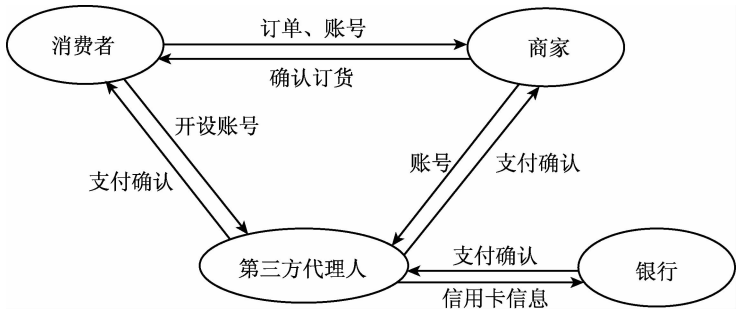


图 5-3　通过第三方代理人的信用卡网上支付流程示意图

（1）消费者在线或离线在第三方代理人处开设账号。

（2）消费者用该账号从商家处在线订货，即将订单和账号传送给商家。

（3）商家将买方账号提供给第三方代理人，由第三方代理人验证账号信息和商家身份。

（4）第三方代理人将商家信息传给消费者，由消费者确认购买和支付，然后将账号信息传给银行进行支付确认，再由商家确认订货，完成支付过程。

这种支付方式的特点：① 支付是在双方都信任的第三方参与下完成的；② 信用卡信息不会在开放的网络上多次传送，消费者可以离线在第三方开设账号，这样消费者就没有信用

卡信息被盗窃的风险；③ 由于第三方是买卖双方信任的，因此商家也没有风险；④ 买卖双方预先获得第三方的某种协议，即消费者在第三方处开设账号，商家成为第三方的特约商户。

资料链接 5-1

软件供应商的解决方案

目前，已经有人使用第三方代理人信用卡支付方式的应用软件，如 CyberCash 软件。该软件提供了第三方代理人的解决方案。买方必须首先下载 CyberCash 软件，即“钱夹”。该软件提供多种支付工具，其中包括信用卡、数字或电子现金、电子支票，打开“钱夹”可以选择其中的一种支付方式。该软件的特点是：开设账号时信用卡信息通过网络传输。CyberCash 软件信用卡服务不向买卖双方额外收费，所有 CyberCash 费用都通过信用卡处理系统支付。该软件的使用步骤如下：

（1）在建立“钱夹”的过程中，买方将信用卡信息提供给第三方——CyberCash。

（2）CyberCash 指定一个加密的代码代表信用卡号码，传送给买方。

（3）当买方向接收 CyberCash 的卖方购物时，只需简单地输入代码。

（4）卖方将代码及购买价格传送给 CyberCash。

（5）第三方证实这一事务处理并将资金及购买商品的授权传送给卖方。

另外，First Virtual 公司（2005 年被另一家公司收购）也提供第三方代理服务解决方案。FV 系统的交易流程如下：

（1）买方通过填写注册单，或通过语音电话向 First Virtual 公司提供他们的信用卡号码，申请 Virtual PIN，买方可以用它替代信用卡。

（2）为了购买产品，顾客通过他的 FV 账号向卖方选购，这种购买可能以如下两种形式中的一种发生：买方自动授权卖方通过浏览器获得其 FV 账号并向买方送账单；买方自己把账户信息传过去。

（3）卖方通过买方账号和 FV 支付系统服务器联系。

（4）FV 支付系统服务器确认买方账号，并清点出相应资金。

（5）FV 支付系统服务器向买方发送一个电子信息，这条信息是自动 WWW 格式，或者只是一个简单的 E-mail。买方可以有三种反应：是的，我同意支付；不，我拒绝支付；我从未发出过相关命令。

（6）如果 FV 支付系统服务器获得了一个“同意”的信息，就通知卖方，卖方准备发货。

（7）FV 在收到购买完成的信息后在买方账户上记借，买方在收到产品/信息后，如果拒绝付款，可以终止他们的账户。

FV 第三方代理软件的特点是：卖方在 FV 上注册，一次性付费 10 美元，一次交易 0.29 美元以及 2%的附加费，买方通过账户进行一次支付需要 1 美元的费用，每个买方的启动费用是 2 美元；整个系统建立在现存的机制上以方便买卖双方，买方只需要一个电子邮箱和 First Virtual 账户即可，卖方无须具有计算机技能或者 Internet 销售服务器，只需通过 FV 就可直接处理销售业务。

3. 基于 SSL 协议机制的信用卡网上支付模式

随着银行信息化水平的提高，更多先进和高效的信用卡支付方式被开发，信用卡简单加

密支付就是其中一种。使用简单加密信用卡模式付款时，买方信息经过加密后向卖方传输，采用的加密协议有 SHTTP、SSL 等。目前，消费者客户端上的网络浏览器软件、商家的电子服务器软件等大都支持 SSL 协议，银行以及第三方的支付平台也都研发了大量支持 SSL 协议的应用服务与产品。这些都为持卡客户借助 SSL 协议机制，利用信用卡进行网上支付提供了方便。使用基于 SSL 协议的信用卡网上支付模式进行网上支付前，消费者必须离线或在线到发卡银行进行信用卡注册，得到发卡银行网上支付授权。下面是具体的流程：

(1) 在第一次使用该支付方式时，消费者(持卡人)需到发卡银行申请，开通信用卡网上支付功能，此后，就可以方便地使用这种方式支付。

(2) 持卡人在电子商务网站选择商品或服务，填写订货信息，并提交选购的商品信息，选择信用卡支付及信用卡类别。提交所有信息后，系统会生成一个带有信用卡类别的订货单发往商家电子商务服务器。

(3) 商家电子商务服务器向持卡人回复已收到订货单查询 ID，但并不确认发货；商家电子商务服务器生成相应的订单号，同时，将信用卡类别信息通过第三方机构发往发卡银行。

(4) 在订货单提交后，持卡客户端浏览器弹出新窗口页面，提示即将建立与发卡银行端网络服务器的安全连接，SSL 协议机制开始介入。

(5) 持卡客户端自动验证发卡银行端网络服务器的数字证书。验证后，SSL 协议完成。这意味着，持卡客户端浏览器与发卡银行端网络服务器的安全连接通道已经建立，将进入正式加密通道。此时，在浏览器右下方的状态栏以及网址中的“http://”变成了“https://”，表明 SSL 协议在发挥作用。

(6) 在发卡银行的支付页面会出现商家发来的订单号及支付金额信息，持卡人填入自己的信用卡号以及支付密码，确认支付。这时持卡人也可以取消支付，此时之前发给商家的订货单作废。

(7) 支付成功后，屏幕提示将离开安全的 SSL 连接。持卡客户确认离开后，持卡客户端与银行服务器 SSL 连接结束，SSL 介入结束。

(8) 发卡银行通过后台系统将相应的资金转入商家的账户上，并向商家发送付款成功的信息。商家收到该信息后，将发送付款成功信息给持卡人，并在规定时间内将商品送到持卡人手上。持卡客户可根据订货单查询 ID，通过在线方式或者电话查询该订货单的执行情况。

至此，基于 SSL 协议的信用卡支付方式的网上支付过程就完成了。在上述支付过程中，有些银行还会专门采用网上支付卡的方式来保证持卡人的支付安全。具体做法是：为持卡人提供一个网上支付卡及密码，持卡人可根据需要利用自助系统将其信用卡上的资金随时转移到该网上支付卡；在支付过程中，持卡人只需在网上传输网上支付卡的信息，就可以达到支付的目的。

著名的 CyberCash 公司研发的安全 Internet 信用卡支付模式就是这种模式。IBM 等公司也提供这种 SSL 支付模式软件系统。

4. 基于 SET 协议机制的信用卡网上支付模式

基于 SET 协议机制的信用卡网上支付模式是在电子商务过程中利用信用卡进行网上支付时，遵守 SET 协议的安全通信与控制机制，实现信用卡的即时、安全、可靠的在线支付。

这种模式运用了一系列先进的安全技术与身份认证手段。可以看出，前面三种信用卡支付模式要么靠其他机构的诚信来解决持卡人的信用卡安全问题，要么单靠加密技术解决安全问题，但网上支付各方的真实身份问题及抵赖性问题等还有待更严密的逻辑与技术工具来解决。基于 SET 协议机制的信用卡支付模式可以解决这些问题。

SET 协议有以下参与人：

（1）持卡人。持卡人通过发卡机构颁发的支付卡进行结算，在持卡人和商家的会话中，SET 协议可以保证持卡人的个人账户信息不被泄露。

（2）发卡机构。发卡机构是一个金融机构，为每一个建立账户的顾客颁发支付卡。

（3）商家。商家负责提供商品和服务，商家使用 SET 协议可以保证持卡人个人信息的安全。接受用银行卡支付货款的商家必须与银行有合作协议。

（4）银行。此处的银行是指在线交易中商家开设账户的银行，负责处理支付卡的认证和支付。

（5）支付网关。支付网关是由银行操作的，将网上传输的数据转化为金融机构内部数据的设备，可以由指派的第三方处理卖方支付信息和顾客的支付指令。通常几个商家和银行共用一个支付网关。

基于 SET 协议机制的信用卡网上支付模式的具体流程如下：

（1）持卡人在消费前先确认商家的合法性，由商家出示其证书，消费者确认后即可下订单，其订单以数字签名方式确认。而持卡人所提供的信用卡资料另由收单银行以公钥加密。这里，商家会收到两个经过加密的资料：一个是订单资料；另一个是关于支付的资料。商家只可以解密前者。

（2）商家收到买方发来的信息后，将加密的客户支付资料发给支付网关。

（3）由支付网关将持卡人信用卡信息传送至卖方银行，并进一步通过金融内部网络数据传送至发卡行进行审核。

（4）经发卡行审核无误后，批准支付并确认，信息通过卖方银行传送至支付网关，并最终传送至商家。

持卡人的证书必须由发卡行颁发。在首次网上购物之前，持卡人必须先通过一个客户终端程序将包括自己的姓名、卡号等可以证明持卡人身份的基本资料发给发卡银行。这些资料使用银行的公钥加密，可安全地送至银行。发卡银行在确认此账号正确无误后，便发给持卡人一张具有电子安全数字签名的证书。持卡人只要将该证书存储即可进行电子购物。同时，商家也必须取得卖方银行的电子证书才可以接受 SET 方式的支付。

基于 SET 协议的信用卡网上支付模式的优点是充分发挥了认证中心的作用，确保各参与方身份及其所提供信息的真实性、保密性和完整性，缺点是机密、认证多，因而比 SSL 协议慢一些，参与各方的开销也较大。

借记卡与信用卡的最大区别，就是持卡人必须在发卡行本人的账户上保留足够的存款余额，一般不允许透支。也有少数借记卡允许短期透支，但必须在当月月底之前还清全部贷款金额。借记卡的支付过程与信用卡类似，在此不再赘述。

二、虚拟货币网上支付模式

虚拟货币支付系统虽已有三十多年的发展历史，但现金仍是目前主要的支付手段之一。

现金作为支付手段一直存在的原因在于：现金具有可转让性，是一种法定货币，可以为任何人持有或使用而不需要银行账户，同时，对接收方来说无风险。

虚拟货币具有货币现金的属性，因此成了网上支付的工具。

虚拟货币是一种表示现金的加密序列数，它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各种金额的市值。用户在开展虚拟货币业务的银行开设账户并在账户内存钱后，就可以在接受虚拟货币的商店购物了。虚拟货币内只能装电子货币，如电子零钱、安全零钱、电子信用卡、在线货币、数字货币等。这些电子支付工具都支持单击式支付方式。使用虚拟货币进行网上购物时，需要在虚拟货币服务系统中进行。电子商务活动中的虚拟货币软件通常都是免费提供的。用户可以直接使用与自己银行账号相连的电子商务系统服务器上的虚拟货币软件，也可以通过各种保密方式使用因特网上的虚拟货币软件。

虚拟货币的发行方式有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。在现实中，虚拟货币的传输过程经过了公钥或私钥加密系统加密，保证了只有真正的卖家才可以对其使用。

（一）虚拟货币的属性

虚拟货币有货币价值、可交换性、可存储性和不可重复性四个属性。

（1）货币价值：虚拟货币必须有一定的现金、银行授权的信用或银行证明的现金支票进行支持。当虚拟货币被一家银行产生并被另一家所接受时不能存在任何不兼容性问题。如果失去了银行的支持，虚拟货币会有一定风险，可能存在支持资金不足的问题。

（2）可交换性：虚拟货币可以与纸币、商品/服务、网上信用卡、银行账户存储金额、支票或负债等进行互换。一般倾向于虚拟货币在同一家银行使用。事实上，不是所有的买方会使用同一家银行的虚拟货币，他们甚至使用的不是同一个国家的银行的虚拟货币。因而，虚拟货币就面临多银行的广泛使用问题。

（3）可存储性：可存储性允许用户在家庭、办公室或旅途中将虚拟货币存储在一个计算机的外存、IC 卡，或者其他更易于传输的标准或特殊用途的设备中，即用户从银行账户中提取一定数量的虚拟货币，存入上述设备中。由于在计算机上产生或存储货币使伪造货币变得非常容易，因此最好将货币存入一个不可修改的专用设备中。这种设备应该有一个友好的用户界面，以助于通过口令或其他方式的身份验证，以及对于卡内信息的浏览显示。

（4）不可重复性：必须防止虚拟货币的复制和重复使用（double-spending）。因为买方可能用同一个虚拟货币在不同国家、地区的网上商店同时购物，这可能造成虚拟货币的重复使用。一般的虚拟货币系统会建立事后检测和惩罚机制。

（二）虚拟货币网上支付模式的流程

使用虚拟货币进行网上支付，需要在客户端安装专门的虚拟货币客户端软件，在商家服务器端安装虚拟货币服务器软件，在发行银行运行对应的虚拟货币管理软件等。为了保证虚拟货币的安全及可兑换性，发行银行还应该从第三方 CA 处申请数字证书以证实自己的身份，获取自己的公开密钥/私人密钥对，且把公开密钥公开出来，利用私人密钥对虚拟货币进行签名。

虚拟货币的网上支付业务流程涉及商家、客户和发行银行三个主体和初始化协议、提款协议、支付协议以及存款协议四个安全协议。其详细流程如下：

1. 买方购买虚拟货币

用户在虚拟货币发行银行开设虚拟货币账户并购买虚拟货币。用户要从网上的货币服务器(或银行)购买虚拟货币，首先要在该银行建立一个账户，将足够资金存入该账户以支持今后的支付。目前，多数虚拟货币系统要求买方在一家网上银行上拥有一个账户。这种要求对全球性交易和多种现金交易来说是非常必要的，买方应该能够在国内获得服务并进行国外支付，但需要建立网上银行组织作为虚拟货币的交换所。

2. 存储虚拟货币

用户可以使用 PC E-Cash 等终端软件从虚拟货币银行取出一定数量的虚拟货币存在硬盘上。一旦账户被建立起来，买方就可以使用虚拟货币软件产生一个随机数作为货币，它是银行使用私人密钥进行了数字签名的随机数(通常少于 100 美元)，再把货币发回给买方。这样虚拟货币就生效了。

3. 用虚拟货币购买商品或服务

买方向同意接收虚拟货币的卖方订货，用卖方的公开密钥加密后，将购买信息传送给卖方。

4. 资金清算

接收虚拟货币的卖方与虚拟货币发行银行之间进行清算，虚拟货币银行将买方购买商品的货币支付给卖方。这时可能有两种支付方式：双方的和三方的。双方支付方式涉及两方，即买卖双方。在交易中卖方用银行的公开密钥检验虚拟货币的数字签名，如果对于支付满意，卖方就把数字货币存入他的机器，随后再通过虚拟货币银行将相应面值的金额转入账户。所谓三方支付方式，是指在交易中，虚拟货币被发给卖方，卖方迅速把它转发给发行虚拟货币的银行，银行检验货币的有效性，并确认它没有被重复使用，然后再将它转入卖方账户。在许多情况下，双方交易是不可行的，因为可能存在重复使用的问题。为了检验是否重复使用，银行将从卖方获得的虚拟货币与已经使用虚拟货币数据库进行比较。(出于对重复使用的考虑，虚拟货币以某种全球统一标识的形式注册)但是，这种检验方式十分费时费力，尤其是对于小额支付来说。

5. 确认订单

卖方获得付款后，向买方发送订单确认信息，并发货。

(三) 虚拟货币网上支付模式的优势和劣势

虚拟货币是以数字形式存在的现金货币。它比现有的实际现金(纸币和硬币)有更明显的优点，如实际现金要承担较大的存储风险、高昂的传输费用、较大的安全保卫和防伪的投资，而它完全脱离实物载体，使用户的支付变得更加方便。

虚拟货币在给人们带来好处的同时也会带来问题。虚拟货币可以提高效率，方便用户使用，但同时虚拟货币具有灵活性和不可跟踪性，它会带来发行、管理和安全验证等方面的问题。技术上各个商家都可以发行虚拟货币，如果不加以控制，电子商务将不可能正常发

展，甚至由此带来相当严重的金融问题。虚拟货币的安全使用也是一个重要的问题，包括限于合法人使用、避免重复使用等。对于无国家界限的电子商务来说，虚拟货币还存在税收和法律、外汇汇率的不稳定性、货币供应的干扰和金融危机可能性等潜在问题。因此，有必要制定严格的金融管理制度，保证虚拟货币的正常运作。

资料链接 5-2

中银电子钱包

电子钱包最早于 1997 年由英国国民西敏寺银行开发成功，现今，电子钱包已经在世界各国得到广泛使用，特别是预付式电子钱包的应用更为普及。在我国最早的应用是中国银行把长城借记卡和电子钱包结合起来，提供“中银电子钱包”的网上支付。

中银电子钱包的特点是：确保信息的保密性。SET 协议通过多种先进的信息加密技术，确保数据信息在网络传输中的安全性；确保支付信息的完整性。SET 协议利用散列方法确保数字签名、认证等技术手段对交易双方进行全面的认证。中银电子钱包对持卡人和商户双方的认证是通过电子证书来实现的。该电子证书是由权威性的认证机构即认证中心来管理并颁发的，交易时，一定会通过此电子证书对各方的身份进行验证。

中银电子钱包的功能有：管理账户信息、管理电子证书、处理交易记录、导入导出信息、设置相关选项和更改口令等。

使用中银电子钱包进行网上支付的基本流程是：

（1）消费者在自己的计算机上安装中国银行电子钱包软件。

（2）登录中国银行官网，在线申请获得持卡人电子安全证书。

（3）登录中国银行网上特约商户购物网站选购商品、填写送货地址并最后确认订单。

（4）选择采用长城电子借记卡支付，将自动启动电子钱包软件，按提示依次输入卡号、密码等信息，即可完成在线支付。

（5）消费者等待商家送货。

三、其他网上支付模式

（一）智能卡支付模式

智能卡是在法国问世的。20 世纪 70 年代中期，法国 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，率先成功开发 IC 存储卡。经过二十多年的发展，真正意义上的智能卡，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 年共同研制成功。

智能卡系统的工作过程是：首先，在适当的机器上启动用户的因特网浏览器，这里所说的机器可以是 PC，也可以是一部终端电话，甚至是付费电话；然后，通过安装在 PC 上的读卡机，将用户的智能卡登录到为用户服务的银行 Web 站点上，智能卡会自动告知银行该用户

的账号、密码和其他一切加密信息；最后，用户就能够从智能卡中下载现金到厂商的账户上，或从银行账号下载现金存入智能卡。例如，用户想购买一束 50 元的鲜花，当用户在花店选中了满意的花束后，将用户智能卡插入花店的计算机中，登录用户的发卡银行，输入密码和花店的账号，片刻之后，花店的银行账户上增加了 50 元，而用户的现金账户上减少 50 元，这样就完成了鲜花的购买。

1. 智能卡的在线支付模式

智能卡的在线支付模式根据获取智能卡信息手段的差异而不同，可以分为带读卡器的智能卡网上支付模式和不带读卡器的网上支付模式。由于智能卡的在线支付模式和电子钱包及信用卡的 SET 协议支付模式基本相同，因此，在此只对智能卡在线支付模式的处理流程进行简单介绍，其支付过程中相关安全认证技术的运用，可以参考前面所述的信用卡 SET 协议网上支付模式或者电子钱包的支付模式。

(1) 带读卡器的智能卡网上支付模式。使用这种模式进行网上支付时，客户需要购买一个专用的智能卡读卡器，安装在连接互联网的客户计算机上，这需要增加一定成本。在操作方面，由于是智能卡硬件的自动化操作，所以不但更加安全保密，而且减少了客户的一些重复劳动。

(2) 不带读卡器的智能卡网上支付模式。有的银行发行的智能卡有一个智能卡卡号，即拥有智能卡的顾客在发卡行同时拥有一个与这个智能卡对应的资金账户。这种智能卡的网上支付模式类似于信用卡的网上支付模式。在这种方式下，客户不用购买一个专用的智能卡读卡器，而是通过直接在网页上填写智能卡号与应用密码来支付。这种做法势必牺牲一些智能卡本身的安全保密度，因此目前智能卡很少采用这种网上支付方法。

不带读卡器的智能卡网上支付模式的基本流程与信用卡的网上支付模式一样，可以采用 SSL 协议机制支付方式，也可以采用 SET 协议机制支付方式。

随着技术的进步，非接触式智能卡正逐渐投入应用。这种非接触式智能卡用于网上支付，并不一定属于不带读卡器的智能卡网上支付模式，因为其智能卡信号是无线传播的。

2. 智能卡的离线支付模式

由于智能卡的存储能力强，可以存入电子现金等虚拟货币，因而持卡人可使用智能卡进行离线支付。

所谓离线支付，不是指智能卡与持卡客户或商家的计算机离线，而是指使用智能卡进行网上支付时，智能卡的读卡器不需要和发卡银行的网络实时连接，直接通过读卡器的读/写功能完成支付结算。

智能卡的离线支付使得持卡人的网上支付行为不受网络好坏与银行处理效率的影响，使支付更加方便快捷，扩大了智能卡的使用范围。不过，离线支付必须使用读/写卡设备，且只适用于在卡内存放电子现金、电子零钱等虚拟货币的智能卡，因为只有这些虚拟货币的转让不需要银行的实时中介。

利用电子现金的智能卡离线网上支付模式的流程如下：

(1) 智能卡客户到发行电子现金的银行申请电子现金，将电子现金下载存入智能卡。

(2) 持卡客户在网上商店选购商品，填写订单，选择智能卡支付。

(3) 支付时将智能卡插入智能卡读卡器中。

(4) 客户输入智能卡 PIN,确认支付金额。

(5) 读卡器对客户输入的 PIN 与卡中的 PIN 自动比较,如果一致,打开智能卡,受理支付请求。

(6) 读卡器将客户智能卡中的电子现金发送给商家(商家也可应用智能卡存放电子现金)。这个过程中,读卡器需要进行查对黑名单、核实资金是否能用、对支付后的余额进行更新等处理,且将交易记录写入自身的日志文件和客户的智能卡中。

(7) 商家收到电子现金后,确认客户的订单并且发货。商家可用收到的电子现金进行其他网上支付业务,也可以到发行电子现金的银行进行兑换。

(二) 手机银行支付模式

在我国,随着通信网络的迅速发展,为了拓展服务领域,各商业银行相继推出了一系列功能各异的电话银行系统。它们利用先进的交互式语音应答设备,使客户可以利用家中、办公室或外地的电话机直接连通银行计算机行业系统,随时随地处理与银行之间的账务往来,即通常所说的"电话理财"服务。手机银行是手机支付的方式之一,下面简要介绍其功能及基本使用流程:

1. 手机银行的功能

手机银行在各银行都限定以个人客户为对象,主要提供转账、余额查询和交易明细等服务内容。具体而言,它将银行业务与现代通信技术有机结合起来,可以获得如下服务:

(1) 金融理财查询功能。该功能主要对账户余额、最近账户明细账、证券保证金、外汇牌价、股票行情、黄金价格、国债行情、存款利率、银行最新金融产品等信息进行查询。

(2) 提醒功能。该功能主动通知定期存款到期、贷款到期、汇款到账、挂失到期、信用卡到期、信用卡透支、电费、电话费、手机缴费等内容。

(3) 外汇买卖功能。该功能将手机银行与个人外汇实盘买卖业务联系起来,使客户可以通过手机享受包括汇率查询、外汇买入、外汇卖出、撤单、成交查询等各种外汇业务服务。涉及币种有人民币、港元、美元、日元、英镑、瑞士法郎、欧元、澳大利亚元、加拿大元等。

(4) 黄金与国债买卖功能。

(5) 证券服务功能。对深、沪两地证券的行情查询、实时股票买入/卖出、撤单、成交查询、股票预定价格通知、股票预定价格买卖等。

2. 手机银行的实现流程

目前,实现手机银行功能的基本流程是:中国移动的全球通用户在网络覆盖范围内使用该公司推出的手机银行卡,由客户端主动发起,通过手机操作智能菜单,依托移动 GSM 无线网络,以短信息为传输手段,将客户要求办理的转账支付业务或金融信息查询业务等传递给银行,银行再将通过银行主机处理的客户的业务结果和金融信息查询结果实时传递给用户,达到客户随时随地享受银行服务的目的。手机银行要实现其业务功能,需要按以下步骤进行操作:

(1) 用户申请注册。

① 用户携带有效身份证件到移动通信公司指定的营业厅办理手机银行开户手续,同时将 SIM 卡更换成手机银行卡,即 STM 卡。

② 用户携带有效身份证件及复印件到商业银行指定网点办理手机银行开户手续,申请

时需填写手机银行注册申请表。

③ 银行经办人员从前台业务菜单上按注册申请表输入客户注册资料。

④ 前台终端资料录入完毕，提交信息，发送给数据中心后台服务器处理。

(2) 用户发送业务信息。

① 用户通过手机银行的界面提示，选择业务种类，并输入账号、金额等信息，然后向移动公司发送短信息。

② 用户手机短信息经移动公司业务短信息业务平台处理后，通过专线传送到银行数据中心。

③ 银行数据中心收到移动短信指令，实时进行处理。

④ 银行数据中心将处理成功或不成功的信息按 SMPP 协议，通过专线传输到移动短信息平台。

⑤ 最后通过移动短信息平台，将银行相关信息传送到用户手机。

(3) 银行向客户发送提醒信息。

如果进行网上支付，其基本流程和上述过程类似，不再赘述。

第三节　第三方网上支付方式

第三方平台结算支付模式是当前国内服务商数量最多的支付模式。在这种模式下，支付者必须在第三方支付中介开立账户，向第三方支付中介提供信用卡信息或账户信息，在账户中“充值”，通过支付平台将账户中的虚拟资金划转到收款人的账户，完成支付行为。收款人可以在需要时将账户中的资金兑换成实体的银行存款。

由于第三方支付平台结算支付模式架构在虚拟支付层，本身不涉及银行卡内资金的实际划拨，信息传递流程在自身的系统内运行，所以电子支付服务商有比较自由的系统研发空间。目前，国内很多第三方支付平台运用客户的 E-mail 作为账户，也即所谓的 E-mail 支付。

资料链接 5-3

第三方支付当“飞毛腿”——服务跑得欢

年近 50 岁的陈女士申请了浦发银行、建设银行和深圳平安银行 3 张信用卡，但只有浦发银行的信用卡与借记卡绑定可以自动还款，另外两张信用卡还款让陈女士一度觉得很烦，一个月要跑两家银行，两次排队还款，每次来回往返加排队，至少 1 小时。后来，她通过浦发网上银行划款到建设银行和深圳平安银行还信用卡透支款，结果每月要被浦发银行收取手续费。后来已上大学的女儿告诉陈女士，通过快钱网还款既不用到银行网点排队，也不用支付跨行还款手续费。陈女士试用后发现果然如此。

使用快钱网办理过业务的用户会发现，经过“快钱”这个无形“飞毛腿”的帮助，各种账单费用的缴纳便捷很多。

在快钱网开设的账单中心页面上，用户可以进行信用卡还款、缴纳水、电、煤气、通信等公共事业费、房租、房贷、保险账单等，甚至儿女孝顺父母的零用钱、父母给子女的生活费都可以通过快钱网支付。用户只要在“账单中心”填写要支付的金额和支付对

象，选择支付方式后即可进行支付。

以信用卡跨行还款为例。快钱网支持的信用卡还款银行最多，用户可以使用16家银行的借记卡，通过网上银行为13家银行的信用卡进行还款，其中包括了工商银行、农业银行、建设银行和交通银行等大银行，招商银行和平安等中小银行，以及东亚等外资银行。在到账时间上，工商银行、建设银行、农业银行、深圳发展银行和光大银行为“T＋3”工作日，其他银行为“T＋1”工作日。通过快钱平台的手机话费充值功能，用户还可以使用银行卡或快钱账户在线为自己的手机充值。

喜欢网上消费的人发现，有快钱这样的第三方支付平台，生活平添了许多乐趣。比如，喜爱网络游戏的玩家在闯关的关键时刻突然花完了点卡，需花10分钟外出购买。但现在，他只要在游戏网站上单击快钱的浮标，进入快钱的页面，就可以为账户充值了，在有些网站，甚至可以单击浮标直接实现从快钱账户扣款。一般的支付网站通常需要用户每次在线支付时输入银行卡号和密码，而快钱的用户用电子邮件地址或手机号码就可以完成付款了。使用快钱网平台，用户还能在消费中获得各种商户的优惠券，能在对应的商家网站消费时享受到相应的优惠。优惠券领域涉及数字娱乐、教育培训、时尚服饰、旅游机票等。

据上海快钱信息服务有限公司的CEO关国光介绍，“现在使用快钱支付还是年轻人的习惯”。据了解，目前快钱的主要用户年龄为18～35岁，购买的产品也主要集中于网络游戏、机票、金融产品等。关国光说，中国的GDP有2.5万亿元，现金流是其20倍，意味着一年内现金流量是50万亿元，个人消费占GDP的44%，然而其中只有5%的货币被电子化。这些数据显示，快钱未来的商机拓展空间巨大，无论是产品和服务内容的扩展，还是客户的扩容。

为了覆盖尽可能多的年龄层，而且尽量不改变用户原来的支付习惯，快钱正不断提供更多的支付方式和渠道。比如，快钱的用户可以通过互联网、手机等线上支付，也可以通过电话、POS等终端进行线下支付；支付的产品不仅有人民币支付，还有外卡支付、神州行卡支付、联通充值卡支付、VPOS支付等，目的是为用户做到“总有一款适合你”。

一、第三方网上支付的流程

第三方平台结算支付是典型的应用支付层架构。提供第三方结算电子支付服务的商家往往都会在自己的产品中加入一些具有自身特色的内容。但是总体来看，其支付流程都是付款人提出付款授权后，平台将付款人账户中的相应金额转移到收款人账户中，并要求其发货。有的支付平台会有“担保”业务，如支付宝。担保业务是将付款人将要支付金额暂时存放在支付平台的账户中，等到付款人确认已经收到货物（或是服务）或在某段时间内没有提出拒绝付款的要求，支付平台才将款项转到收款人账户中。

1. 第三方平台结算支付的流程

第三方平台结算支付模式的资金划拨是在平台内部进行，此时划拨的是虚拟的资金，真正的实体资金还需要通过实际支付层来完成。有担保功能的第三方平台结算支付的流程为：

（1）付款人将实体资金转移到支付平台的支付账户中。

（2）付款人购买商品（服务）。

（3）付款人发出支付授权，第三方平台将付款人账户中相应的资金转移到自己的账户中保管。

（4）第三方平台告诉收款人已经收到货款，可以发货。

（5）收款人完成发货许诺（或完成服务）。

（6）付款人确认可以付款。

（7）第三方平台将临时保管中的资金划拨到收款人账户中。

（8）收款人可以将账户中的款项通过第三方平台和实际支付层的支付平台兑换成实体货币，也可以用于购买商品。

2. 第三方平台支付模式的优势与劣势

第三方平台支付模式的优势表现在以下几个方面：

（1）比较安全。信用卡信息或账户信息仅需要告知支付中介，而无须告诉每一个收款人，大大减少了信用卡信息和账户信息失密的风险。

（2）支付成本较低。支付中介集中了大量的电子小额交易，形成规模效应，因而支付成本较低。

（3）使用方便。对支付者而言，他所面对的是友好的界面，不必考虑背后复杂的技术操作过程。

（4）支付担保业务可以在很大程度上保障付款人的利益。

第三方平台支付模式的劣势反映在以下几个方面：

（1）这是一种虚拟支付层的支付模式，需要其他的“实际支付方式”完成实际支付层的操作。

（2）付款人的银行卡信息将暴露给第三方支付平台，如果这个第三方的信用度或者保密手段欠佳，将带给付款人相关风险。

（3）第三方结算支付中介的法律地位缺乏规定，一旦其破产，消费者所购买的电子货币就可能成了破产债权，无法得到保障。

（4）由于有大量资金寄存在第三方支付平台账户内，而第三方平台是非金融机构，所以有资金寄存的风险。

二、几种典型的第三方网上支付方式

（一）网上支付系统支付方式

网上支付系统（network payment system，NPS）是由深圳全动科技公司开发的，目前被腾讯网站采用作为网上支付系统。

NPS为消费者网上购物提供了安全、便利的支付平台，还为商家开展B2B、B2C、C2C交易等电子商务服务和其他增值服务提供支持，使从购买到完成付费的过程变得完整，通过提供完善的支付功能，提高了互联网电子商务的经济效益。

利用NPS进行支付的具体操作步骤如下：

（1）消费者到网上商城浏览商品。

（2）输入购物订单等信息。通常，在购物网站选择物品后，都会生成订单号等识别信息。在系统页面上选择购物订单，并输入商家号、订单号、金额、用户等相关信息，然后就进入支付环节。

（3）选择使用支付卡的银行。在 NPS 在线支付平台上，客户可以方便地选择各协议银行的银行卡用于支付。

（4）出现有关提示。在选择相应的银行后，出现“正在连接银行网关”的提示，这表明系统正在尝试连接到银行网关。

（5）转到相应银行的支付平台。经过支付系统跳转，会转到相应银行的支付平台。这时，用户所填的信息都只有银行能获得，所以不用担心密码、账户被截取。当然，用户必须注意地址栏中确实是银行的官方地址，曾经有不法分子做出和商业银行相似的页面来蒙蔽用户，以骗取其账户密码，但一般只要看清域名地址就可以很容易辨别出是不是伪造的网站了。

（6）进入银行支付页面。在该页面中输入账号、支付密码和验证码，就可以提交了。

（7）支付成功。提交并确认后，钱就从客户的账户转到商家账户，支付成功。

这时，客户就可以等待收货了。

（二）支付宝

支付宝是支付宝网络技术有限公司针对网上交易而特别推出的安全付款服务。其运作的实质是以支付宝为信用中介，在买家确认收到商品前，由支付宝替买卖双方暂时保管货款的一种增值服务。用户进行交易时，首先要将银行账户和支付宝账户挂钩，并将资金从银行账户转入支付宝账户，支付时用支付宝账户中的资金进行支付。

1. 支付宝的交易流程

在使用支付宝进行网上支付前，首先必须为支付宝账户充值，这样才能通过支付宝向他人的账户转账。

（1）选择充值银行，为支付宝账户充值。选择充值的银行后，就会跳转到相应银行的网上支付系统，用户可以在网上方便地将其银行账户上的资金转移到支付宝账户，进行充值。

（2）付款。支付宝有两种付款方式：一种是直接付款，原理和过程跟一般的支付网关类似，付款后，货款立即转入卖家的账户，但为了安全起见，每天的交易限额为 500 元；另一种是支付宝交易，付款后钱不是马上转入卖家账户，而是转存到支付宝中介账户中，等买家确认收到卖家商品并且满意后，货款才从支付宝中介账户转到卖家账户。后一种方式较好地维护了买家的利益，保证了网上购物的安全性。

2. 支付宝的特点

（1）安全。支付宝在技术层面和非技术层面上都实现了安全性。在技术层面上，浏览器与支付宝网站之间的通信采用 SSL 加密技术，从而实现了通信过程的安全。每个用户都将拥有一个数字证书，密码被盗后如果没有数字证书就只能进行查询操作，不能进行支付或者提现，这进一步提高了安全性。另外，支付宝还提供了用户绑定手机的功能。开通了手机绑定功能后，可以使用手机短信来及时关闭或开启余额支付功能，当账户余额变动时，系统还会发短信提醒。在非技术层面上，支付宝本质上是一个中介服务，实现了实名认证，能有效地防范交易中的风险。

（2）快捷。支付宝内部的转账全部实时到账，提现或者充值只需 1～2 天即可到账。

（3）方便。商家可以在支付宝内生成支付按钮，放入任何网站即可使用支付宝收款，而且账户信息变动时，可以实现短信实时通知。

（4）免费。支付宝是免费的。

（5）物流便利。与物流系统对接，卖家和买家都能对货物的运送状况进行查询，并且在买家收到货物并确认无误后，3 天内支付宝自动将货款转入卖家账户。

资料链接 5-4

2010 年第三季度的第三方网上支付交易规模达 2 484 亿元　支付宝份额过半①

艾瑞咨询发布的 2010 年第三季度中国第三方网上支付市场监测数据显示，2010 年第三季度行业的交易规模达到 2 482 亿元，环比上涨 18.3%，同比上涨 80.5%。

2010 年第三季度第三方网上支付市场交易规模中，支付宝市场份额有所扩大，占比达到 50.03%，继续保持市场第一的位置；财付通、快钱分别以 20.27%及 6.13%的市场份额位居第二位、第三位，具体如图 5-4 所示。

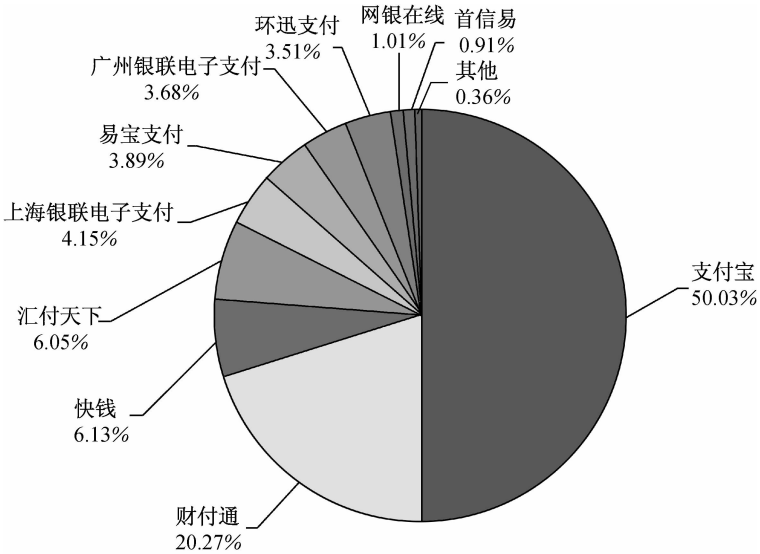


图 5-4　2010 年第三季度第三方网上支付核心企业交易规模市场份额示意图

注：2010Q3 中国第三方网上支付交易额规模为 2 482 亿元。

来源：综合企业及行业专家访谈，根据艾瑞统计模型核算得出。

艾瑞咨询分析认为，支付行业企业的运营逐渐呈现出两个主要趋势：一种是以拓展应用服务领域，通过用户规模的扩张不断获取用户增值的运营方式；另一种是以深耕某一支付应用服务领域，通过不断为企业提供支付解决方案为主的增值服务方式。未来，这两种运营方式将促使第三方支付企业在更多的应用服务领域实现纵深化发展。

（三）贝宝

贝宝是由上海网付易信息技术有限公司与世界领先的网络支付公司——PayPal 公司通力合作，为中国市场量身定做的网络支付服务，可以让用户在互联网上即时支付和收取交易

① Q3 第三方支付交易规模达 2 482 亿元　支付宝份额过半[EB/OL]. 2010-10-28[2011-4-10]. http://it.sohu.com/20101028/n276693153.shtml.

款项。贝宝利用 PayPal 公司在电子商务支付领域先进的技术、风险管理和控制以及客户服务等方面的能力，通过开发适合中国电子商务市场与环境的产品，为电子商务的交易平台和交易者提供安全、便捷和快速的交易支付支持。

1. 贝宝的交易流程

(1) 选购商品。首先在购物网站上选择自己需要的产品，在支付方式中选择 PayPal 贝宝进行支付。

(2) 登录贝宝支付。进入贝宝支付页面，如果是贝宝用户就直接登录支付，如果不是贝宝用户需注册成为用户。

(3) 选择余额支付或银行支付。使用贝宝账户登录后，可以选择余额支付或者是银行支付。

(4) 支付成功。选择银行后进入银行支付，支付成功后显示“支付成功”的页面；同时，用户也可以查看“我的贝宝”页面显示的交易情况。

2. 贝宝的功能

贝宝作为一种网上支付工具，有着多种功能，包括收付款、充值、提现等。下面逐一讨论贝宝的这些功能。

(1) 添加银行客户。

① 使用贝宝不一定要添加银行账户信息，因为对用户而言，只拥有贝宝账户就可以收款；当要付款时，只要用户的贝宝账户内有余款，用户就可以进行支付。只有在提现时才需要用户向贝宝提供相关银行账户信息。

② 使用贝宝添加银行卡。首先，登录“我的贝宝”页面，输入电子邮件地址和密码。然后，在“我的贝宝”里单击“添加银行账户”按钮，在表格中填写相关信息，包括账户持有者姓名、银行账号、开户行等。用户的个人信息和银行信息将由贝宝严格保护，不会泄露给任何第三方。

(2) 充值。充值是将一定数额的款项从用户的银行账户转到贝宝账户。在充值过程中，用户不需要向贝宝提供银行账户信息。登录贝宝后选择“充值”选项，选择用户银行，即可进入银行网银或银联电子支付服务有限公司的用户界面，进行充值。贝宝可支持 15 家银行的网上支付功能。

(3) 提现。提现时，需要选择用户的提现银行并输入相关信息，如银行卡号、开户行等。如果用户事先已经添加银行账户，则系统默认此银行账户。根据开户银行的不同，提现金额需要 1～7 天到账，但是用户可以随时将“贝宝”账户中的余额提现。

(4) 付(收)款。用户进入贝宝主页单击“付款”按钮，在付款页面提供的简单表格中，填入如下相关信息：对方的电子邮件地址，所付(要求对方付)的金额、购物描述等。这样，所付金额将即时到达对方的贝宝账户。如果要求对方付款，一旦对方确认，所付金额也将即时到达用户的贝宝账户。此外，在付、收款过程中，贝宝会即时发出邮件，提醒收付的双方。

(5) 管理贝宝账户。用户可以进入“我的贝宝”页面来管理个人信息，查看并管理自己的账户信息，查询并下载交易记录，提交争议申请和补偿申请。

(四) 工商银行第三方支付平台

要使用工商银行的网上支付平台，首先要注册成为工商银行个人网上银行——金融@

家的用户。可通过登录工商银行中国网站或者直接到工商银行营业网点注册个人网上银行，还可以在工商银行营业网点申请个人客户证书（U盾），以保证更安全的网上交易。工商银行还推出了手机银行支付方式，全面支持移动、联通客户，注册后即可通过手机进行消费支付。

用户在注册个人网上银行后，即可在网上商场中购物并进行在线支付。支付时，先登录个人网上银行，然后在个人账户页面进行本地或异地、行内或跨行的转账。这种转账都是即时的，行内转账一般几秒内能在对方账户上显示，跨行交易一般在一天左右到账。

如果注册了手机银行，可在网上商场中购物并使用手机支付。

进行在线支付时，如果用户没有申请U盾，则网上支付金额会受到限制；如果用户申请了U盾，则网上支付无金额限制，但如果设置了不使用证书签名的“交易限额”，则网上交易金额在交易限额内可以不使用证书，超过了交易限额才需使用证书签名。当日支付密码累计输入错误次数超过限额后，就不能再进行B2C支付，次日自动恢复支付功能。如果网上支付成功，将显示订单号和交易流水号。若支付指令提交后遇到了问题，用户可以登录工商银行个人网上银行，选择“我的账户”→“账户查询”→“网上购物明细查询”，打开相应页面查询该笔交易的处理状态，然后联系商户。

（五）首信易支付

首信易支付是国内首家“中立的第三方网上支付平台”。该平台开创了“跨银行、跨地域、多种银行卡、实时”交易模式、“二次结算”模式以及“信任机制”，为支付网关的发展奠定了基础。

所谓二次结算，是相对于普通的支付服务而定义的，是首信易支付所独有的结算模式。在二次结算的服务过程中，首信易支付不是单纯地作为连接各银行支付网关的通道，而是作为中立的第三方机构，保留商户和消费者的有效交易信息，为维护双方的合法权益提供了有力的保障。

由于采用了在网站和银行之间的二次结算，使得首信易支付能够成为支付过程中的公正第三方。交易双方在交易过程中的信息传递都在支付平台留有存证，交易双方都可方便地查询订单及相关信息。特别是在出现交易纠纷时，有关信息可作为仲裁的有力证据。

首信易支付采用了多层次的安全措施。在网络层上，运用了强大的防火墙体系；在系统层上，采用了防黑客入侵、防病毒和漏洞扫描；在应用层上，采用了BJ-CA证书结合应用软件，由此构建了一个相对安全的支付中介。

1. 首信易的基本支付流程

使用首信易支付作为支付平台，其基本支付流程如下：

（1）消费者网上浏览、选购商品。

（2）消费者在商户网站下订单。

（3）消费者选择支付方式——“首信易支付”，直接链接到首信易支付的安全支付服务器上。在支付页面上选择自己适用的支付方式，单击后进入银联支付页面进行支付操作。

（4）首信易支付将网上消费者的支付信息，按照各银行支付网关的结束要求，传递到各相关银行。

(5) 由相关银行检查网上消费者的支付能力,实行冻结、扣账或划账,并将结果信息转至首信易支付和消费者本人。

(6) 首信易支付将支付结果通知商户。

(7) 支付成功的,由商户向消费者发货或提供服务,并通知商城。

(8) 各个银行通过首信易支付向不同的、交易成功的商户实施清算。

2. 首信易其他方式支付流程

(1) 首信易的会员账号支付流程为:购物浏览→下订单→进入支付平台→选择银行卡→去银行网站输入卡号、密码→支付成功。

(2) 首信易支付的电话银行账户支付流程为:购物浏览→下订单→选择电话支付→拨打银行服务电话→银行审核通过→支付成功。

首信U豹具有与首信易支付安全连接和普通U盘存储两大功能。在U豹使用中执行了特制的加密算法,以动态确认用户的身份,无形中增加了一道安全之门,使用户的网上交易变得更加安全,更加方便。用户使用U豹存储、携带私人文件,设置密码保护后会更加安全便捷。

初次使用时,用户要先单击U豹存储区的"登录首信易支付平台.exe",使系统为用户的浏览器安装插件,之后才能够用于购物支付。

使用U豹需先注册,将U豹插在计算机的USB接口上,进入U豹登录区,双击"登录首信易支付平台"可自动登录首信易支付平台。输入默认密码,按提示填写账户信息,修改密码后,注册成功。此后,用户可以向账户充值,开始网上交易。

引例解析

在介绍完本章知识后,可将网上支付的基本流程总结如下:

(1) 客户建立与Internet的连接,通过网上商城进行商品的浏览、选择与订购,填写订单,选择相应的网上支付工具,并且得到银行的授权使用,如信用卡、电子钱包、电子支票等。

(2) 客户核对相关订单信息,对支付信息进行加密,在网上提交订单。

(3) 商家服务器对客户的订购信息进行检查、确认,并把相关的、经过加密的客户支付信息等转发给支付网关,直至银行专用网络的银行后台专业服务器确认,以期从银行等电子货币发行机构得到支付资金的授权。

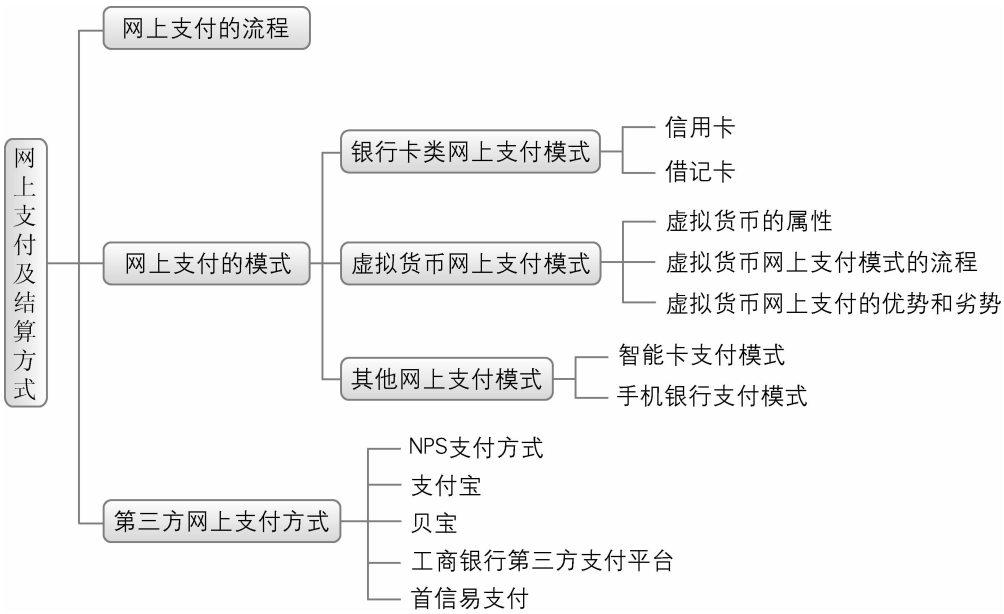
(4) 银行验证信息确认后,通过经由支付网关的加密通信通道,给商家服务器回送确认及支付信息,为进一步保证安全,给客户回送支付授权请求(也可以不回送授权请求)。

(5) 银行得到客户传来的进一步授权结算信息后，把资金从客户账号转拨至开展电子商务的商家银行账号上，借助金融专用网进行结算，并分别给商家、客户发送支付结算成功信息。

(6) 商家服务器收到银行发来的结算成功信息后，给客户发送网络付款成功信息和发货通知。

至此，一次典型的网上支付结算流程结束。商家和客户可以分别借助网络查询自己的资金余额信息，以进一步核对。

本章小结



综合训练

一、思考练习

1. 简述网上支付的基本流程。
2. 信用卡网上支付主要有哪几种模式？
3. 简述信用卡网上支付各种模式的基本流程。
4. 用支付宝进行网上支付的特点及基本流程是什么？
5. 第三方网上支付方式的优缺点分别是什么？

二、案例分析

联手支付宝　当当网搭建网上支付快车道①

2010年9月15日，当当网正式与支付宝达成战略合作协议，于同日起正式开通支付宝接口。至此，当当网的可选在线支付通道已经涵盖了财付通、快钱、易宝支付、首信易支付、银联支付以及支付宝等所有国内主要的支付平台。用户在当当网购物时可选择上述任意一种网关进行支付结算。

谈到此次与支付宝的合作，当当网市场负责人表示："当当网的宗旨是为用户提供便宜、方便、放心的网购服务，这一点上，以简单、安全、快速、信任为产品和服务核心的支付宝与我们有着共同的理念。通过引进支付宝这样先进、安全的第三方支付平台，当当网将给用户提供更方便和安全的支付手段。"

过去一年中，当当网在供应链优化、平台前端应用、个性化服务、价格和货品质量控制、物流配送速度、顾客关系管理等方面进行了大量改进，顾客服务得到大幅提升。就在不久前，当当网还对购物车进行了新一轮改版，易用性和用户体验相比旧版有很大提升。

有关方面从当当网方面了解到，为了庆祝本次签约并鼓励当当网用户尝试在购物时使用支付宝网关，从2010年10月11日至11月11日，当当网将与支付宝举办联合活动，凡是在当当网上购物满100元，并使用支付宝进行支付的用户，其支付宝账户就可获得10元返券。

问题

通过阅读上述材料，思考当当网选择支付宝的原因。

不同网上支付方式的应用及比较

【实训目的】

了解网上支付的基本流程，并熟悉几种主要的网上支付方式。

【实训内容与要求】

收集书中提到的网上支付方式的资料，并分组进行实际支付。通过操作与本章内容相结合，分析不同网上支付流程的异同以及各种流程的优点和局限性。

【成果与检验】

将尝试结果填入下表中，并在班级上交流经验。

支付方式	优　点	局限性

① 联手支付宝　当当网搭建网上支付快车道[N].新闻晚报，2010-09-22(11).

第六章
网上增值业务

知识目标

» 了解网上增值业务、网上信贷、网上保险、网上证券的概念；
» 了解网上保险的特点、种类；
» 了解网上证券的风险问题；
» 掌握网上信贷的种类和业务流程；
» 掌握网上保险的三种模式；
» 掌握网上证券的服务内容及对其的监管办法。

技能目标

» 掌握网上信贷业务的使用；
» 掌握网上保险的业务流程；
» 掌握网上证券的交易程序；
» 了解网上银行的其他增值服务。

引例

中国工商银行的电子化建设

一、中国工商银行简介

截至2008年年末，中国工商银行拥有385 609名员工、16 386家境内外机构，为1.9亿个个人客户与310万个公司客户提供广泛而优质的金融产品和服务。2008年《环球金融》、《银行家》、《亚洲银行家》、《财资》、香港上市公司商会等知名媒体及中介机构将“亚洲最佳银行”、“中国最佳银行”、“香港公司管治卓越奖”等131个奖项颁给了中国工商银行。

二、电子银行业务

中国工商银行的电子银行业务保持国内同行业领先地位。2008年电子银行交易额为145.29万亿元，比2007年增长41.2%。电子银行业务笔数占全行业务笔数的43.1%，提高5.9个百分点。推出第二代U盾、电话银行口令卡等产品，提高电子银行客户安全保障系数；推出手机银行(WAP)、贵宾版个人网上银行等新产品，优化多项原有产品功能，满足差异化、个性化服务需求。截至2008年年末拥有企业网上银行客户144万户、个人网上银行客户5 672万户；企业网上银行实现交易额110.50万亿元，增长28.9%；个人网上银行实现交易额9.77万亿元，增长135.4%。获《环球金融》杂志“亚洲最佳个人网上银行”、“中国最佳个人网上银行”、“中国最佳企业网上银行”等奖项；推出电话银行预约、电话银行个性化菜单定制等服务项目，开通电话银行贵宾服务专线；推出通过WAP方式接入手机银行业务，降低手机银行客户门槛，提高手机银行(WAP)安全性，手机银行的客户数量快速增加至55万户。

三、个人网上银行

拥有中国工商银行工银财富卡、理财金账户、牡丹灵通卡、牡丹灵通卡·e时代、牡丹信用卡或活期存折的客户，在中国工商银行营业网点注册网上银行或登录其网站自助注册网上银行后，就具备了网上交易资格。

目前个人网上银行能为客户提供的交易功能有账户查询、账户转账、个人汇款、在线缴费、代缴学费、委托代扣、个人理财、外汇买卖、银证转账、国债买卖、基金、网上保险、网上贷款、网上购物、工商银行信使服务、银行卡服务等。

个人网上银行为客户提供全天候24小时服务。

四、企业网上银行

企业网上银行是指通过互联网或专线网络，为企业客户提供账户查询、转账结算、在线支付等金融服务的渠道，根据功能、介质和服务对象的不同，可分为普及版、标准版和中小企业版。

企业网上银行业务功能分为基本功能和特定功能。基本功能包括账户管理、网上汇款、在线支付等功能；特定功能包括贵宾室、网上支付结算代理、网上收款、网上信用证、网上票据和账户高级管理等业务功能。

思考题：

什么是网上增值业务？目前网上银行主要提供哪些网上增值业务？

第一节　网上增值业务概述

伴随着银行电子化的进程，银行建立了一大批电子银行应用系统，实现了电子化和现代化。可以说电子银行系统提供的新的交易处理模式，使其成为银行赖以生存和发展的基础。随着20世纪90年代电子商务和互联网的发展，银行的支付服务和信息服务深入社会的各个领域。银行实现电子化后，银行同外部环境之间的关系，表现在金融交易和金融信息交换两个方面。前者是基础，后者是由前者派生出来的。

一、网上增值业务的概念

网上增值业务即电子银行的增值业务，是指电子银行为客户提供的超出常规服务范围的服务。也就是说，电子银行除为客户提供基础网上服务（网上支付与结算）外，还提供其他特殊的金融服务。

网上增值服务就是电子银行提供的第二项金融服务。网上增值服务主要体现在金融服务品种的在线多元化和品牌化两个方面。银行业务品种多元化，是电子银行金融服务的优势。一般来说，电子银行的网上增值服务主要有网上投资、个人理财助理、企业银行和其他金融服务。其中，具有代表性的网上增值服务是网上信贷、网上保险和网上证券。

二、网上增值业务的重要性

电子银行交易处理的最大特点就是电子化，在银行的数据库里存放了大量的交易数据，银行充分利用数据仓库技术和信息技术，对这些数据资源按一定的主题进行加工处理，从而能为企业客户提供除基础传统服务以外的信息增值服务。

传统的银行与外部环境之间的关系只是进行金融交易，因此，银行只起信用中介作用。而电子银行不同，银行的电子化，不仅大大增强了银行的信用中介作用，而且使银行能从大量的各种交易数据中提取有用的成分，产生具有高附加值的各种金融信息产品，为客户提供信息增值服务。

电子银行建立网上增值业务的重要性主要表现在以下几个方面：

（1）银行在实现电子化过程中，必然要改变业务流程，需要对组织机构进行重组，电子化将大大提高银行的业务处理效率，进而增强银行的信用中介作用。

（2）银行的作用从传统的单纯信用中介，发展到强化了的信用中介，并能提供信息增值服务，意味着银行发生了革命性的变化。

（3）银行的收入结构发生根本性的变化，即由原先以发放信贷盈利为主的收入结构，逐渐转变为以劳务服务和金融信息咨询服务获取非利息收入为主的收入结构。

（4）银行的电子化过程及网上增值业务的建立，使银行的职能、业务重点、收入结构、业务流程、业务模式和组织结构等发生了一系列根本性变化。

第二节　网上信贷

作为新兴的低成本零距离贷款方式，网上消费信贷的作用日益增强。全球第一家网上互助借贷平台“Zopa”于2005年3月在伦敦诞生，如今其业务已经扩展到意大利、美国和日本，平均每天线上的投资额达到200多万英镑。2006年2月，美国第一家网上借贷平台繁荣市场公司(Prosper Marketplace Inc)诞生，截至2008年年底其注册用户超过90万，累积交易量达1.8亿美元。2007年10月，建设银行浙江省分行与阿里巴巴合作推广“E贷通”系列产品，包括网络联贷联保、大买家供应商融资、网络速贷通等。其中，网络联贷联保只需要阿里巴巴诚信通客户组建联保体，联保体成员之间互相担保；大买家供应商融资则是供应商企业以网上大买家的订单为依据申请贷款，不需要提供抵(质)押或担保。

本节就以建设银行浙江省分行与阿里巴巴网站合作的网上信贷业务为例进行讲述。

一、网络联贷联保

1. 网络联贷联保的概念

网络联贷联保业务是一款不需要任何抵押的贷款产品，由三家或三家以上企业通过网络自愿共同组成一个联合体，联合体成员之间协商确定授信额度，共同向银行申请贷款，由银行确定联合体授信总额度及各成员额度；同时企业之间实现风险共担，当联合体中有任意一家企业无法归还贷款时，联合体其他企业需要共同替它偿还所有贷款本息。比如，联合体中A、B、C各获得贷款50万元，则每个企业承担的贷款责任都是150万元，如果A到期无法归还贷款50万元，则需要B、C企业共同替A归还其50万元贷款及利息。

据2007年的《中国中小企业信息化发展报告》显示，我国约有4 200万户中小企业，而阿里巴巴平台注册用户就有2 400万，约占全部中小企业的一半。调查表明，2 400万注册用户中90%有信贷需求，有需求用户中80%的贷款需求无法得到满足，最大的障碍就是担保问题。为了解决这些企业的贷款需求，2007年2月，建设银行与阿里巴巴在浙江省率先推出网络联贷联保业务。在挑选客户时，建设银行借助阿里巴巴原有的信用评级，挑选那些在阿里巴巴有4年以上诚信通历史的企业作为客户，同时还专门设计了网络银行客户的系列评级评价办法，首次将网络商业信用纳入信用评价指标体系。对那些违约、不诚信的借款人，阿里巴巴网站会对其进行网络曝光。为了强化风险控制，浙江省人民政府、杭州市人民政府分别和中国建设银行股份有限公司、阿里巴巴(中国)有限公司签署三方合作的《网络银行业务合作协议》，共同出资组建更大规模的网络银行风险池。截至2009年6月底，建设银行与阿里巴巴合作的贷款项目已经发放贷款26亿元，放贷客户数1 390家，不良贷款率仅为1.08%，低于之前银监会公布的1.77%的商业银行不良贷款率。这样就发挥了网络优势，创新了风险控制模式。

2. 网络联贷联保的优势

网络联贷联保具有六大优势：

(1) 低利息:利息远远低于民间无抵押借贷,参考年利率为 8%～12%。

(2) 无抵押:无须任何抵押物也有机会得到贷款。

(3) 高额度:可以按实际需求申请,每家企业最高可获得 200 万元的贷款。

(4) 按日计息:按照实际使用天数付息,不支用就不用支付利息。

(5) 专款专用:建设银行设立专门款项支持中小企业发展。

(6) 流程简单:网络报名后,通过银行初审、复审即可获得贷款。

3. 网络联贷联保的业务流程

网络联贷联保的具体业务流程如图 6-1 所示。

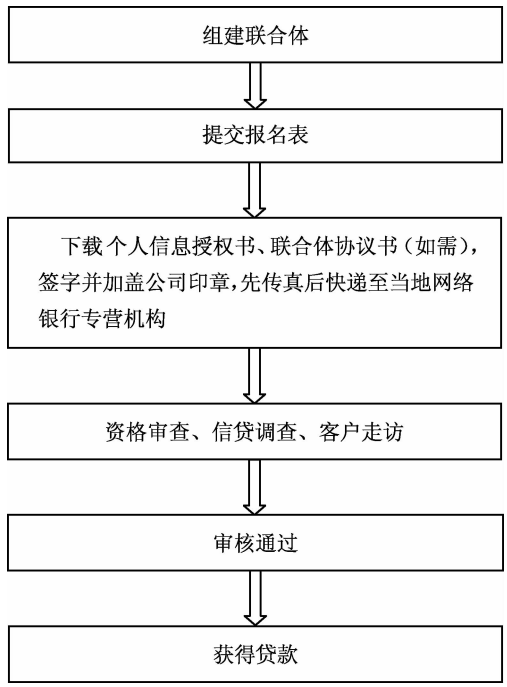


图 6-1　网络联贷联保的业务流程

4. 申请条件

申请网络联贷联保需要满足以下条件:

(1) 营业年限至少 18 个月。

(2) 网络信用记录良好,在金融机构无不良信用记录。

(3) 目前暂未在建设银行各分支机构有贷款余额。

(4) 法定代表人、实际控制人及主要股东个人愿意为贷款承担无限连带保证责任。

(5) 是阿里巴巴 B2B 平台会员。

(6) 联保体已组建成立。

二、网络供应商融资

1. 网络供应商融资的概念

网络供应商融资是供应商在正常经营过程中，以其持有的经商业银行和大买家确认的，尚未履行交货义务，相应款项尚未收付的购货订单为依据，向银行申请融资的信贷业务，主要解决供应商原材料备货等临时性资金周转，解决部分客户经营规模较小、无法提供抵(质)押物、银行融资难的问题。

2. 网络供应商融资的优势

(1) 无抵押：企业申请该贷款无须向银行提供任何抵押物或质押物，无须联保。

(2) 低利息：远低于民间贷款和融资公司贷款。

(3) 申请简单：是指定公司认可的供应商即可申请。

(4) 流程简单：填写并提交报名表，通过银行审核后即可获得贷款。

(5) 按日计息：按照实际使用天数付息，不支用就不用支付利息。

3. 网络供应商融资的业务流程

网络供应商融资的业务流程如图 6-2 所示。

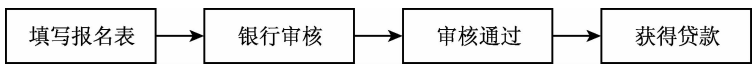


图 6-2　网络供应商融资的业务流程

4. 申请条件

网络供应商融资时需要满足以下条件：

(1) 企业的工商部门注册年限已满 18 个月或企业法定代表人(或实际管理人)从事当前行业 5 年(含 5 年)以上。

(2) 需为公司性质的企业或个体工商户。

(3) 属于本省 AA 级以上企业认可的供应商。

(4) 工商注册地在浙江省下辖的各县、市的所有企业。

(5) 上年经营非亏损企业。

(6) 目前在建设银行各分支机构没有未还清的贷得贷款。

三、网络速贷通

1. 网络速贷通的概念

网络速贷通是对借款人不进行信用评级和一般额度授信，依据客户提供的足额有效的抵(质)押担保，并结合客户第一还款来源及网络信用而办理的信贷业务，对网络信用好的电子商务客户给予一定比例的追加贷款额度。

网络速贷通也就是抵押贷款，企业需提供变现能力较强的抵(质)押物，凭抵(质)押担保获贷。抵押物包括个人住房、商铺、别墅、厂房、土地等有效资产；质押物包括存单、国债、保证金、银行承兑汇票等质押权利凭证。单笔贷款期限最长可达 3 年。目前，阿里巴巴与中国

建设银行为中小企业提供网络速贷通，贷款最高额度可达 2 000 万元。

2. 网络速贷通的优势

(1) 高抵(质)押折扣率：最高可达 100%。

(2) 手续简单：免除评级和授信环节。

(3) 流程简单：填写报名表提交，通过银行审核后即可获得贷款。

(4) 期限长：最长可达 3 年。

3. 网络速贷通的业务流程

网络速贷通的业务流程与网络供应商融资类似，也需经过填写报名表、银行审核、审核通过、获得贷款四个步骤。

4. 申请条件

(1) 工商注册年限已满 18 个月的企业。

(2) 需为公司性质的企业，个体工商户暂不能申请。

(3) 需要提供建设银行认可的抵押物或质押物。

(4) 上年经营非亏损企业。

(5) 目前在建设银行各分支机构无贷款余额，若在建设银行还有贷款正在使用或未还清，则必须结清后才能申请网络速贷通。

(6) 公司注册地在贷款所开放城市以外的暂不能申请，属于分公司或子公司的暂不能申请。

第三节　网 上 保 险

网上保险是电子商务环境下保险业创新的产物。利用电子商务，保险公司不仅可以通过网络直接接触成千上万的新客户，而且随时可以为老客户提供详尽周到的服务，与各行各业开展广泛的交流与合作，精减业务环节、降低运营成本、提高企业的效益。对于客户来说，他们可以不受时间和空间的限制，无论身在何处都可以享受 7×24 小时的不间断服务。理智的客户还可以通过对各家保险公司的充分对比分析，最终决定购买哪家公司的保险产品。

一、网上保险概述

(一) 网上保险的概念

网上保险又称网络保险或者保险电子商务。广义的网上保险是指以信息技术为基础，建立网络化的经营管理体系，以网络为主要渠道来开展保险经营和管理活动的行为；狭义的网上保险是指保险人或保险中介人以互联网和电子商务技术为工具，向客户提供保险产品和服务信息，并通过在线订立契约，直接向客户销售保险产品或提供各种保险服务的经营行为。网上保险的最终目标是实现保险业务的电子化交易，即通过网络实现信息咨询、投保、核保、给付、理赔等业务。

保险作为一种特殊的商品，与一般意义上物化的商品有着显著的区别：

(1) 保险是一种承诺。保险合同属于诺成性合同，同时也是一种格式合同。

（2）保险是一种无形产品。保险商品的表现形式是契约。

（3）保险是一种服务商品。保险企业为客户提供的从承保到理赔的全过程服务，主要是咨询服务。

保险电子交易的实现，要求保险公司根据外部条件和自身的实际情况制定循序渐进的分阶段发展规划。分阶段实现保险电子商务的目标，不仅能够充分利用保险公司现有的各种技术资源，尽量减少保险公司部署电子商务的投入代价，更好地适应企业自身的技术应用水平，避免业务过程的一次性改造可能给企业经营带来的过度冲击和震荡，而且可以让企业在电子商务的每一个应用阶段充分获取应用效益，不断增强企业对电子商务的认识与信心，通过投入、应用获益、提升的良性循环最终实现网上保险电子交易。

（二）我国网上保险的现状

1997 年年底，中国保险学会和北京维信投资顾问有限公司共同发起成立了我国第一家保险信息网站——中国保险信息网（网址为 www.china-insurance.com），现已经更名为中国保险网，如图 6-3 所示。该网站在当年促成了我国网上投保第一单，拉开了我国网上保险的序幕。2000 年，太平洋保险、平安保险、泰康人寿等保险公司，相继在上海、深圳和北京宣布开通电子商务系统，开通了网上保险服务，所涉业务涵盖了人寿保险、财产保险、意外伤害保险、旅游交通保险等近百个保险险种。2002 年 11 月，中国人保的网上保险平台投入运营。我国保险公司力图通过网上保险，简化保险商品交易手续，扩大知名度，开展宣传、咨询、营销和客服等项目。保险业与电子商务的结合，为保险代理打开了方便之门，标志着中国的保险公司开始将目光投向了互联网技术。

图 6-3　中国保险网主页

由于高收入上网人群的大幅上升和第三方支付市场交易规模的迅速扩大，从 2008 年开始，保险电子商务取得了突飞猛进的发展。据资料显示，2008 年第一季度，工商银行网上保险业务交易笔数达到 3 万余笔，交易突破 44 亿元，交易额较 2007 年增长了 60 多倍。目前，工商银行网上保险频道险种包括万能险、投连险、意外险、交强险、车险、家财险、医疗险、续期缴费 8 类 40 余款产品，并实现了中国平安、太平洋、太平人寿、泰康、中德安联、都邦、光大永明、上海东大保险 8 家公司的网上保险销售。同时，工商银行网站保险频道还提供了在线

保险规划功能，系统可根据客户填写的基本信息帮助客户自动推荐保险产品，不仅增加了网上保险的互动性，而且也满足了客户个性化的服务需求。

2009 年 5 月，独立的第三方支付企业快钱公司正式宣布，与 9 家保险公司达成战略合作伙伴，为保险公司提供对网销、电销、理赔、续保、财务集中管理等不同业务领域的支付解决方案。2009 年，其交易额突破 1 000 亿元人民币。截至 2010 年 2 月 28 日，快钱公司已拥有 5 700 万注册用户和逾 41 万商业合作伙伴。

对于网上保险，当务之急是要制定相应的规范。只有人才、技术、管理、法律等诸方面的条件具备且成熟，网上保险才会真正健康、迅速地发展。

（三）我国网上保险存在的问题

虽然我国保险业内部网络化建设在近几年有一定的发展，但由于相关环境及网上保险技术还有所欠缺，使得网上保险仍然存在一些问题。

1. 客户消费习惯的改变尚需时日

我国保险业的成熟度低、国民的保险意识差，相关知识少，从保险需求上说自然也比较弱，保险市场的现状是有人卖却没人买。另外，中国互联网络发展状况统计报告显示，截至 2009 年年底，中国网民规模达到 3.84 亿人，其中 10～19 岁网民占 31.8%，20～29 岁网民占 28.6%，30～39 岁网民占 21.5%。从网民的个人月收入情况看，1 500 元以下的占到网民人数的一半以上，个人月收入 3 000 元以上的仅占网民人数的 12.9%。网上保险的客户是在线网民，而国内目前的互联网用户结构显然不利于发展保险电子商务。此外，人们通常认为保险产品是卖出去的而不是客户主动购买的，也就是说，保单的销售是出于保险营销人员的动机而不是客户的动机，而互联网通常是一种被动的销售媒介，保险公司主要依赖它开发潜在客户群。

2. 网上支付系统不完善，被视为保险电子商务发展的瓶颈

目前，在线保险交易中，客户必须在与所投保的保险公司签订支付合作协议的指定银行建立账户，以便进行在线交易实时扣款。如果客户不具备上述条件，由于目前银行间的资料交换不完善，尚不具备实时跨行转账交易能力，那么客户将不能进行在线实时交易结算。网上交易条件的局限无疑限制了客户源。

3. 业务风险不容忽视

一是虚假网络保险的风险。假保险公司及其网站的出现，严重损害消费者权益，阻碍了网络保险的发展。2005 年，广州出现全国首个利用假保险网站销售假保单的案件；2009 年，海南查获假保险公司恒亚迪保险股份有限公司网上销售假保单案件。此外，网络的普及促使保险业务人员自建网站或博客，开通网上门店，进行产品宣传和销售。而监管部门和保险公司对此类行为尚无明确规范，可能引发销售误导等风险。

二是信息不对称风险。一方面，保险公司并未给客户提供全方位的保单查询平台，客户难以甄别自己通过网络购买的保险是否属实；另一方面，通过保监局的网站和营销员系统可以查询到中介机构和营销员的资质情况，但由于对保险业的相关信息缺乏了解，客户往往不能有效地查询销售者资质状况。

三是道德风险。由于未履行如实告知义务引发的道德风险。首先，保险人在网络环境中核实投保人的告知内容较为困难，投保人有可能利用这一缺陷隐瞒与保险标的有关的重

要事实，进行保险欺诈。其次，保险利益认定难度的增加易引发道德风险。网络保险较难认定投保人是否对保险标的具有保险利益，易引发理赔纠纷，因为会出现难以认定而不认定的情况，也给保险欺诈提供机会。

4. 保险产品供给不足是网上保险的主要制约因素

目前，我国网络保险在产品结构、业务流程、服务功能等方面与发达国家相比，还存在较大差距，未能给客户带来较优的消费体验。一是产品种类单一，以我国开展网络保险业务较早的人保财险、太保集团、平安集团、泰康人寿、太平人寿五家保险公司为例，其意外伤害险产品最多，占产品总数的39%，而市场潜力同样较大的货运险产品仅占2%；二是网上交易仅限于投保流程，五家公司中仅两家能实现投保、批改（或保全）的网上操作，三家公司仅能进行网上投保，理赔等业务流程暂不能实现网上操作；三是服务功能不完善，以国外网络保险常见的在线试算保费、制定个性化保险方案两项服务为例，五家公司中仅三家能在线试算保费，仅一家能提供个性化的保险方案。

5. 外部环境有待改善

保险作为一种以合同形式存在的特殊商品，通过网络以电子形式销售后，面临法律效力和网络安全等问题。目前，制约我国网络保险发展的外部环境主要包括：一是网络保险相关法律法规不健全。我国电子商务立法较滞后，电子合同成立的时间和地点、要约的撤销和撤回、如何确定法律效力、消费者权利如何保证等问题都没有明确的司法解释。法律法规的缺失导致网站经营者无章可依，为销售方的违规操作提供了空间，使得监管部门难以对网络保险销售进行有效监督，难以事前控制风险。二是网络安全缺乏充分保障。投保过程中，客户需提供个人详细信息，尤其是人身保险，需描述个人健康状况等隐私信息，其安全性受到客户的密切关注。此外，网络保险面临交易资金安全的问题。目前，资金结算方式都是将资金交由第三方进行保管，在交易完成后再由第三方将资金划转给销售方，一旦发生意外，第三方无法拒绝将资金划转，导致客户既无法获得保险保障，又难以追回资金。一项调查显示，66%的被调查者最关心保费网上支付是否安全。

二、网上保险的特点

1. 方便性

用户无须走进人多嘈杂的保险公司排队等候，只需自行上网完成申报程序，因此无论用户在何时何地都可以方便而及时地办理及享受保险业务和服务。网上保险实现了全天24小时作业，缩短了保险公司与客户的距离。

2. 成本低

保险公司通过Internet可直接与投保人建立关系，并能简捷、方便地完成交易和传递信息；同时还可在保险活动“价值链”中超越一些不必要的中间环节，节省代理费或佣金，形成一种新型的低成本运作的供应链结构。这样一来，顾客可以以较低的价格获得保险产品和优质的保险服务。

3. 人性化

投保人在网上可以阅读和咨询自己需要的险种，实现保险产品的在线保费计算、对比、购买、支付与投保功能。这让投保人有了更多的选择空间，足不出户就可以做到保险产品货

比三家，网上投保。

4. 透明化

投保人可以直接在网上查询保险公司、经纪人、代理人，了解他们的情况，直接从网上购买保险。这样消除了用户对上门推销者的怀疑，让双方都能互相了解，有利于业务的进行和发展。

5. 风险低

投保人可以通过比较险种、自行计算保费，从而减少中介环节因利益驱动给投保人带来的风险。当然也应看到：由于目前网络本身安全性问题，也给网上保险带来一定的风险。但是随着网络技术的进步和措施的完善，这一风险会逐步降低。

6. 个性化

网上保险销售可凭借现代高科技的支撑，充分实现以客户为中心，最大限度地满足顾客个性化的服务需求，为客户提供更多的保单组合消费，使投保人的保险消费结构更加优化。对保险公司来说，通过网络可以加强对投保人潜在需求的深层把握，有利于险种创新、拓展业务。

7. 竞争有优势

因特网的主要特征是其信息传递和处理的快速性、共享性以及信息传播的广阔性。依托因特网技术，保险公司可利用网上销售平台，进行企业文化、保险产品和公司实力的宣传，主导客户的消费理念。在市场经济条件下，谁先开通网上保险业务谁就先取得这一竞争的主动权，这是各家保险公司必须关注的问题。

全球最大的保险及资产管理集团之一的法国安盛集团，早在 1996 年就实行网上直销。目前，该集团约 8%的新业务是通过互联网来完成的。1999 年，法国安盛集团在上海设立了一家合资企业——金盛人寿保险有限公司，成了保监会成立后批准的首家寿险公司，并于 2000 年启动了网上服务，内容包括公司介绍、产品介绍、代理人俱乐部、客户专门服务等。

三、网上保险的模式

网上开展保险业务的模式主要有以下三类：

1. 传统的保险公司提供网上保险服务

传统保险公司提供网上保险服务的模式是指一些传统的保险公司利用计算机网络技术对传统保险业的产业进行改造，全面提高企业整体素质，实现了保险行业传统服务模式的重大变革。其目的在于推广本公司的险种，侧重改进公司的服务内容和形式。该模式下用户在网上选择自己需要的险种，调用其相关资料进行阅读，如有特殊问题可在网上咨询解决。然后，用户在选定险种的电子意向书上填入保险金额、保费交付方式、被保险人、被保险人健康状况、受益人、联系地址等项目。如果符合条件，用户将在网上收到保险公司发来的已填好的保单。如果满意，用户只需通过网上银行将保费划拨到保险公司账户上，并输入密码，一份保险契约就完成了。当出险时，也可通过同样的方式在网上告知保险公司出险情况，保险公司派人进行勘查、理赔，赔付金额也可通过网上银行完成结算。使用这种模式的保险公司有中国平安保险公司、太平洋保险公司等。

资料链接 6-1

中国平安网上保险

中国平安保险(集团)股份有限公司(www.pingan.com,如图 6-4 所示)是中国第一家以保险为核心的,集证券、信托、银行、资产管理、企业年金等金融业务为一体的紧密、高效、多元的综合金融服务集团。该公司成立于 1988 年,总部位于深圳。2004 年6 月和 2007 年 3 月,该公司先后在香港联合交易所主板及上海证券交易所上市,股份名称"中国平安"。网站上的保险业务包括"个人客户"、"企业客户"、"网上商城"、"一账通"等。其中,"个人客户"和"企业客户"的业务主要包括保险、银行和投资三大类,为客户提供多种个人保险、企业保险、银行保险和投资保险服务。"网上商城"的主要产品有保险网上直销(汽车保险、意外保险、旅游保险、签证保险、家庭财产保险等)、贷款 & 储蓄、投资理财、信用卡商城和万里通积分。

图 6-4　中国平安首页

2. 专门财经网站或综合门户网站开辟的保险频道

随着保险领域竞争的不断加剧,保险公司数量增多,各公司提供的险种和服务、收取的保费等都不完全相同。这就使得消费者面临选择的困难。为了方便广大群众购买保险服务,查询有关保险的资料,一些专门财经网站或综合门户网站开辟了保险频道,满足消费者的保险需求。例如,和讯、上海热线和新浪等保险频道。

资料链接 6-2

新浪的保险超市

新浪推出的保险超市(http://money.finance.sina.com.cn/insurance/mall,如

图 6-5 所示)是国内门户网站推出的首家网上保险超市。根据丰富的资讯及对自身投资需求的准确判断,用户可用最少的时间成本和投资成本,通过新浪保险超市平台与保险公司进行网上买卖操作。该保险超市所提供的保险种类有意外保险、旅游保险、健康保险、养老保险、少儿保险、投资保险、家财保险、汽车保险和个性定制的保险 DIY 等。

图 6-5　新浪网的保险超市页面

3. 第三方保险商务平台

这种模式也称为独立的保险网,它们不属于任何保险公司或附属某大型网站,为保险公司、保险中介及相关机构或个人所公用,可容纳大多数保险企业开设门店及网上交易和清算。它们通过在互联网上建立交易平台、内容平台等,介绍行业内的信息和资讯,进行不同保险公司业务的比较,并给出建议和投资组合分析,让广大的投保人可以在保险公司中“货比三家”。这类平台有易保网、中国保险网等。

资料链接 6-3

易保网网上保险广场

易保网是中国保险监督管理委员会批准的、由金兰(北京)国际保险经纪有限公司设立的,集国内最专业的汽车保险报价、销售、理赔服务、品牌专修等于一身的电子商务服务平台。鉴于目前国内保险公司主体众多,各保险公司服务特色不同,价格参差不齐的现状,易保网颠覆传统车险销售模式,利用互联网为消费者提供了一个完善的、简便的、清晰的车险销售平台。易保网的业务主要有车险报价、理赔服务、4S 店专修等,主张消费者自己选择保险公司、自己选择险种、自己填写投保信息并完成支付,为保险公司、保险中介和被保险人建立沟通的渠道和平台。

四、网上保险的电子商务系统及业务流程

（一）网上保险电子商务系统

保险公司建立网上保险系统的主要目的有两个：一是更好地满足投保人的需求，吸引潜在客户，促进客户关系管理；二是提高业务流程的运行效率，强化内部管理，降低经营成本。一个完整的网上保险系统需要投保人、保险公司、认证中心、银行、医院等合作伙伴，以及工商税务部门、保险监管机构、Internet 服务提供商等的通力合作，才能有效地推进保险电子商务的发展。一个完整的网上保险电子商务系统如图 6-6 所示。图 6-6 中的 CA 为从事保险电子商务的投保人、合作伙伴提供数字证书和提供认证服务，银行为投保人提供网上保险的支付服务。

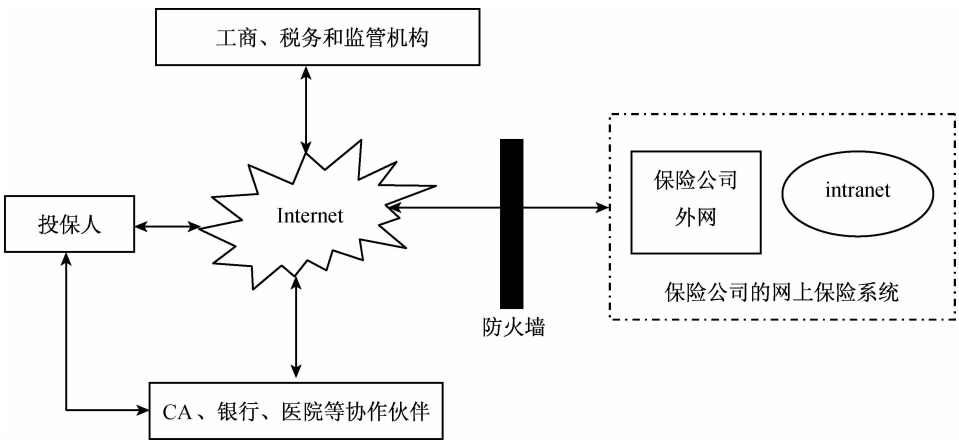


图 6-6　一个完整的网上保险电子商务系统

（二）网上保险的业务流程

网上保险的电子商务操作系统应与各家保险公司的实务操作规定相吻合，主要体现在展业、投保、核保、缴费、保全、理赔和查询七大流程中。保险企业电子商务化，绝不是对传统保险业务的简单电子化和网络化，而是依靠信息技术改变基本业务的处理方式。

1. 展业

展业的内容为宣传和推销，主要利用网站首页的广告和相关栏目对公司及产品进行宣传，使客户了解公司和产品后，产生购买欲望来完成公司展业过程。网站首页设计要将公司的基本情况和经营的特点及各产品的详细情况展现给广大客户。客户决定网上投保时，输入本人的基本情况后能生成“供客户选择的、多方案的客户保险建议书”。

2. 投保

网上在线投保就是客户以直接在网上填写并提交投保单的方式，递交投保信息。客户在线投保一般经历两个步骤：首先，登录相应的保险网站，进入产品页面查看具体的险种；然后，根据自己的需要选择险种并填写投保意向书。

3. 核保

目前，根据保险公司电子化的应用程度和各投保险种的繁简程度以及网上业务的具体情况，各险种可采取实时核保和延时核保两种方式。

（1）实时核保。对于某些比较简单并且符合网上业务初级核保原则的险种或者保险企业网络化程度比较高的情况，可以采用网上实时核保的方式。若保险公司实时接收了客户的投保申请，客户可选用相应的银行卡进行网上实时支付，也可采用单到付款或汇款付款。

（2）延时核保。它与实时核保的区别是：当客户递交保单后，离线等待，待保险公司履行核保程序后，再登录网站查询核保结果。在网上投保后，所有经保险公司签发的保单将由专人送达投保人。

4. 缴费

目前，电子支付还没有真正普及，在实际保费支付中根据客户的习惯和业务需求，保费的支付方式主要有三种形式：单到付款、网上支付和银行汇款。

（1）单到付款。当客户在网上填写并递交投保单后，经由保险公司核保确认并出具保单和保费收据，再由专人负责送交客户。当客户收到保单和保费收据后，根据保单上列出的保费金额，支付相应保费。

（2）网上支付。投保人收到核保确认信息后，可以选择网上直接支付保费。投保人通过电子商务支付网关登录相应银行卡支付结算平台，输入相应付费信息后，一次性扣款，由银行代理自动缴付保险费。保险公司收到保险费用后通过专人或邮递等方式，将保险单和保费收据送交投保人或者直接通过电子邮件传递电子保单和电子保费收据。

（3）银行汇款。投保人收到核保确认信息后，通过银行将保费汇入公司账号，保险公司收到投保人汇款后，通过专人或邮递等方式，将保单和保费收据送交客户或者直接通过电子邮件传递电子保单和电子保费收据。

5. 保全

投保人网上保全操作应与保险公司的保全实务操作相对应，主要内容为：保险合同内容变更、保险合同解除、保险合同复效、生存给付等。

6. 理赔

保险公司开展网上理赔业务，主要借助网络直接、快速的优势，提高自身的理赔服务质量。事实证明，快速优质的理赔服务、高效严格的理赔管理对保险业务的发展起着至关重要的作用。因此，在保险电子商务网站上，推出网上报案功能，使公司能准确、迅速地响应客户的报案，组织人员进行理赔。

理赔服务的流程大致为：投保人在保险事故发生之日内通过 CA 认证，进入网上报案中心进行报案，也可以由业务代表转达报案、电话报案、亲自到公司报案。客户报案后准备相关文件。保险公司核对后对符合要求的案件立案调查，并判定保险事故发生后被保人是否受损、保险损失是否在可赔付范围之内、核实其他事故、诊断证明，对保险赔付额进行计算，最后确定保险金给付对象。在这个过程中，客户可通过网络查询理赔的进度。

典型案例

“泰康在线”第一例网上保险理赔案

泰康在线推出了可以全程在网上投保的“旅游救援保障计划”后，其投保、核保、承保、支付以及出单，所有的环节均可通过网络自动完成，是国内首家实现全程在线服务的保险网站。在这家国内领先的网上保险企业，毫不意外地出现了我国第一例网上保险理赔案。

家住上海的客户凌先生在一次外出旅行时，无意中看到了有关“泰康在线”的新闻报道，得知通过泰康在线可以在网上投保旅游险。2001 年 8 月，凌先生一家五口打算去山东旅游，出游前，凌先生在网上为全家每个人购买了一份期限从 8 月 11 日至 8 月 20 日、总保额为 15 万元的“旅游救援保障计划”。凌先生在网上投保的两天后，收到了泰康在线通过电子邮件发给他的电子保单和电子签名。8 月 16 日，凌父在烟台旅游时突发急病，凌先生马上拨打了“旅游救援保障计划”上的救援电话。救援中心在接到报案后，马上为凌先生的父亲安排在当地医院进行治疗，使其转危为安。回到上海后，凌先生通过泰康上海分公司获得了医疗保险金理赔。凌先生表示，自己选择泰康的旅游保险最重要的原因是，这种保险可以进行网上投保和支付保费，非常方便。凌先生对泰康人寿的服务非常满意，认为泰康公司的理赔速度快，救援服务及时、周到，公司的服务非常专业、规范。网上投保不仅手续简便、快捷，符合现代人的工作及生活节奏，而且泰康在线提供的旅游保险保障范围广、价格低廉，是出行投保的第一选择。

这起我国首例网上保险的理赔案，其意义非常深远，它预示着保险业务的全面网络化的时代已经临近。

泰康在线利用最先进的网络技术，在国内首先实现了从保单设计、投保、缴费、出单到后续服务的全过程电子化，提供网上保险、保户服务、营销服务等多项网上保险服务，是真正意义上的在线保险。此外，用户还可获得便捷的保单查询、自动生成的提醒通知书、网上变更保单信息、网上续缴保费、网上理赔、网上投诉等完整的人性化服务。

7. 查询

客户网上查询既要使客户能查到与投保相关的各种信息资料，又要体现一定的保密性。查询内容主要为：公司的基本情况、公司产品情况、公司投保规则和个人投保的情况。特别是对客户投保情况查询的设计要尽量全面，应包括客户的承保情况、缴费情况、理赔情况和保单变更情况。

资料链接 6-4

泰康人寿网上保险

泰康人寿保险股份有限公司是 1996 年 8 月 22 日经中国人民银行总行批准成立的全国性、股份制人寿保险公司，公司总部设在北京。2000 年 11 月，泰康人寿全面完成经国务院同意、保监会批准的外资募股工作，建立了国际化的公司治理结构。

1. 主要业务

泰康人寿首页(网址为 www.taikang.com,如图 6-7 所示)的导航栏目包括关于泰康、新闻中心、产品博览、网上专卖店、客户服务、乐活泰康、公开信息披露等。

图 6-7　泰康人寿首页

(1) 关于泰康:介绍公司简介、泰康大事记、组织结构、分支机构、企业文化。

(2) 新闻中心:主要有公司公告、媒体报道、业界新闻、精彩活动。

(3) 产品博览:划分为个人产品和团体产品。其中,个人产品包括网上直销、银行保险和电话直销,团体产品包括基础产品和员福套餐。

(4) 网上专卖店:可在线购买的业务有投资理财、少儿保险、组合保险、旅游签证保险、定期寿险、健康保险、养老保险和意外保险等。

(5) 客户服务:包括 e 站到家、友问友答、服务指南、查询服务、业务办理、理赔服务、法律服务、单证下载、卡单激活等。

(6) 乐活泰康:包括理财频道、少儿频道、健康频道、养老频道、旅游频道、官方博客、个人博客等。

2. 投保流程

泰康人寿的投保流程如图 6-8 所示。

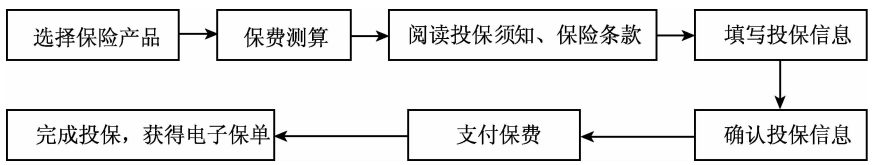


图 6-8　泰康人寿投保流程

3. 支付方式

(1) 银行卡支付:一是利用中国工商银行、招商银行、中国民生银行、中国建设银行的网银支付;二是可以通过快钱或支付宝来选择更多银行卡的网银支付。

(2) 信用卡支付:通过快钱可以选择10家银行的信用卡且无须开通网银功能实现支付。

(3) 授权银行转账支付:可以选择授权保险公司从银行账户中转账扣款支付保费。

4. 理赔流程

(1) 报案:发生保险事故后,可拨打电话、登录泰康人寿网站、委托业务员或直接前往公司营业厅等方式及时报案。

(2) 申请:查阅并准备相关资料,下载并填写理赔申请书,到公司申请。

(3) 审核:泰康公司受理理赔申请后,将进行必要的审核及调查,并作出理赔决定。

(4) 结案:泰康公司作出理赔决定后,将迅速通知申请人理赔结论,并通过银行转账方式及时支付保险金。

第四节 网上证券

随着全球电子商务的迅猛发展,其应用形式和应用领域日益广泛,投资者也开始利用互联网资源,获取证券的即时报价,分析市场行情,并通过互联网委托下单,实现实时交易。这样就产生了网上证券交易。

一、网上证券概述

1. 网上证券交易的概念

网上证券交易是指证券公司利用互联网等网络技术,为投资者提供证券交易所的即时报价、查找各类金融信息、分析市场行情等服务,并帮助投资者完成网上开户、委托、支付、交割和清算等证券交易的全过程,实现实时交易。投资者通过Internet证券交易商,可以在任何地方、任何时候兼顾自己的投资。Internet证券商通常在其Web网站上发布证券交易行情,同时为其客户提供网上填写证券买卖单证的服务,然后把这些买卖单证实时传递给证券交易所。

2. 国内外网上证券的发展状况

目前风靡世界的网上证券交易起源于美国。1995年,美国嘉信理财(Charles Schwab)公司推出世界上第一个互联网在线交易——网上证券平台,网上证券交易开始在美国获得了初步的发展。由于网上证券交易的交易速度快、成本低廉、不受时间和地域限制的优势,逐渐被人们认同,越来越多的投资者选择了网上证券交易。

在亚洲,网上证券交易的发展极为迅速,其中韩国最具有代表性。在韩国,网上证券交易的市场极为集中,在几十家从事网上证券交易的证券公司中,三星、大宇、LG、现代等前五

家最大的公司占了90%以上的市场份额。目前，韩国已经成为世界网上证券交易比例最高的国家之一。

我国网上证券交易的起步时间只比美国晚几年，但受客观因素的影响，开展的网上证券交易一直是小规模试点。我国率先开展网上证券交易的是中国华融信托投资公司湛江营业部，该营业部于1997年3月推出了视聆通多媒体公众信息网网上交易系统。至1998年年末，该营业部网上交易开户数已达7 000户，网上交易量已占该部总交易量的20%多。我国网上交易在开始阶段是由证券公司全权委托IT公司负责的，即IT公司负责开发网络站点，为客户提供投资资讯，而证券公司以营业部的身份在后台为客户提供网上交易的通道。2000年3月，中国证监会公布的《网上证券委托暂行管理办法》规定，只有获得中国证监会颁发的经营证券业务许可证的证券公司，在达到《证券经营机构营业部信息系统技术管理规范》的要求后，经向中国证监会申请并得到批准，才可开展网上委托业务；未经中国证监会批准，任何机构不得擅自开展网上委托业务。2001年2月5日，中国证监会根据《网上证券委托暂行管理办法》正式核准首批23家证券公司开展网上证券交易，如国信证券(www.guosen.com.cn)、西南证券(www.swsc.com.cn)等。中国证监会的统计数据显示，截至2007年年底，我国网上证券委托交易量占沪、深交易所的比例已上升到30%，网上开户数640万户，占证券市场总开户数的比例为23%。

二、网上证券信息服务

网上证券的信息服务主要包括查询上市公司历史资料、查询证券公司提供的咨询信息、查询证券交易所公告、股票网上发行、资金划转、网上实时委托下单、电子邮件委托下单、电子邮件对账单、公告板、电子讨论、双向交流等。目前，投资者可以使用计算机、手机、双向寻呼机、机顶盒、手提式电子设备等多种信息终端进行网上证券交易。证券投资者可随时随地查询证券实时行情和财经信息，接受投资指导，参与投资论坛，进行委托交易。同时，投资者可根据自己的风险收益偏好和投资需求，定制个性化的证券信息，享受专业化理财服务。与传统证券信息服务相比，网上证券信息服务不仅信息容量大，而且更新速度快，极大地改善了信息服务质量，提高了信息服务效率。网上证券信息服务划分为基础信息服务、市场行情服务和市场交易服务。

1. 基础信息服务

不同的网上证券服务平台提供的基础信息服务有所不同，但基本上包括以下内容：证券交易所公告与提示、财经要闻、证券市场、公司资料、研究与出版、市场指南、客户服务等。

2. 市场行情服务

市场行情服务包括行情显示和行情分析两种服务。

(1) 行情显示：具有证券类型、证券排序、行情预警、自设选项、图形分析、定时刷新等功能。

(2) 行情分析：具有实时走势图、实时分析手段、盘后分析、板块设定、证券切换、日期选择等功能。

3. 市场交易服务

市场交易服务包括网上委托买入、委托撤单、委托查询、成交查询等网上交易过程以及

资金明细查询、修改密码、网上交易对账等多项辅助服务。

三、网上证券的监管

为加强证券公司利用互联网络开展证券委托业务的管理，规范市场参与者的行为，防范和化解市场风险，切实保护投资者的利益，中国证监会制定了《网上证券委托暂行管理办法》（以下简称《办法》），主要采纳了以下措施：

（1）开户审查。《办法》对在线证券交易的委托手续做了明确规定，依据第六条的规定，只有在证券公司合法营业场所依法开户的投资者才有权申请进行网上委托，获批准者才能进行网上委托；必须由本人亲自申请，不得代理；投资者申请时应向证券公司提供身份证明原件，证券公司应向投资者提供证实证券公司身份、资格的证明材料。

（2）加密和身份认证。网络的开放性、信息的易获取性或篡改性，要求在线证券交易必须采取相应的技术安全措施，也就是通常采用的加密和身份认证机制。《办法》第十七条和第十八条分别规定了这两个安全措施，要求证券公司在通过互联网传输信息的过程中，必须对网上委托的客户信息、交易指令及其他敏感信息进行可靠的加密；采用可靠的技术或管理措施，正确识别网上投资者的身份，防止仿冒客户身份或证券公司身份；必须有防止事后否认的技术或措施。

（3）技术标准控制。技术系统必须达到一定的标准，《办法》第二十条要求，网上委托系统中有关数据安全、身份识别等关键技术产品，必须通过国家权威机构的安全性测评；网上委托系统及维护管理制度应通过国家权威机构的安全性认证；涉及系统安全及核心业务的软件应由第三方公证机构（或双方认可的机构）托管程序源代码及必要的编译环境。密码产品的主管机关是国家密码委员会；与互联网有关的安全产品、系统及管理体系的测评认证，由国家技术监督局所属的中国国家信息安全测评认证中心负责。

（4）风险揭示。《办法》第七条规定，证券公司应制定专门的业务工作程序，规范网上委托，并与客户本人签订专门的书面协议，协议应明确双方的法律责任，并以风险揭示书的形式，向投资者解释相关风险。第二十二条对揭示的方式和内容做了规范：证券公司应在入口网站和客户终端软件上进行风险揭示。揭示的风险至少应包括：因在互联网上传输的原因，交易指令可能会出现中断、停顿、延迟、数据错误等情况；机构或投资者的身份可能会被仿冒；行情信息及其他证券信息，有可能出现错误或误导；证券监管机关认为需要披露的其他风险。

（5）业务监督管理。《办法》对网上证券业务管理有严格的要求，如第十五条要求证券公司应安排本单位专业人员负责管理、监督网上委托系统的运行，并建立完善的技术管理制度和内部制约制度。第十六条规定，网上委托系统应包含实时监控和防范非法访问的功能或设施；应妥善存储网上委托系统的关键软件（如网络操作系统、数据库管理系统、网络监控系统）的日志文件、审计记录。另外，第十九条还要求证券公司根据本公司的具体情况采取技术和管理措施，限制每位投资者通过网上委托的单笔委托最大金额、单个交易日最大成交总金额。

（6）禁止托管。《办法》要求证券公司应提供一个固定的互联网站点，作为网上委托的入口网站（第二十一条），同时要求证券公司必须自主决策网上委托系统的建设、管理和维

护。有关投资者资金账户、股票账户、身份识别等数据的程序或系统不得托管在证券公司的合法营业场所之外(第十一条)。禁止开展网上证券转托管业务。

(7) 分业经营。《办法》第十条规定,开展网上委托业务的证券公司禁止直接向客户提供计算机网络及电话形式的资金转账服务。这里的转账是银证转账,是指投资者以电子方式,在其证券资金账户和其他账户之间直接划转资金的转账方式。目前,通过电话或网上银行手段,技术上可实现银证转账。例如,投资者持有某些种类的银行信用卡,通过拨打银行或证券公司提供的电话号码,按指令操作,有可能在证券账户与信用卡账户之间划转资金。根据分业经营的原则,需隔离证券交易和商业银行业务的风险,同时为了防止网上委托的数据受到非法窃取或改动,以致通过网络将非法收益转入银行账户,《办法》规定开展网上证券委托业务的证券公司不能直接向客户提供网络或电话形式的转账业务,采用网上委托方式的投资者,可以使用商业银行提供的银证转账业务。

(8) 信息保密。为防止投资者或第三人利用网络获取证券公司业务信息,《办法》第十二条规定网上委托系统和其他业务系统在技术上的隔离,即禁止通过网上委托系统直接访问任何证券公司的内部业务系统。为了保护客户资料不被盗用,《办法》第十三条要求未申请网上委托的投资者的所有资料与网上委托系统进行技术隔离。另外,第十四条规定网上证券公司具有对在线交易所有信息备份并安全存储的义务:网上委托系统应有完善的系统安全、数据备份和故障恢复手段。在技术和管理上要确保客户交易数据的安全、完整与准确。客户交易指令数据至少应保存 15 年(允许使用能长期保存的、一次性写入的电子介质)。

(9) 信息披露。《办法》除了要求证券公司向投资者事先揭示在线交易的风险外,还要求证券公司披露的各种信息要真实有效。第二十三条明确规定:证券公司开展网上委托业务的同时,如向客户提供证券交易的行情信息,应标识行情的发布时间或滞后时间;如向客户提供证券信息,应说明信息来源,并应提示投资者对行情信息及证券信息等进行核实。另外,第九条要求证券公司应定期向进行网上委托的投资者提供书面对账单。

(10) 预防措施。《办法》第八条要求开展网上委托的证券公司,必须为网上委托客户提供必要的替代交易方式,以防止在网络发生事故后,不能正常进行交易。

上述是《办法》规定的一些证券公司的义务,目的是通过制度措施来保障交易安全。但是,网络作为一种新型的技术手段,还需要投资者具有自我保护的知识和意识。第一,应从安全性、稳定性、信息质量、传输速度、技术服务等方面,综合比较,选择进行网上委托的网站及其相应的证券公司。第二,要及时检查委托成交情况以及清算结果,检查证券公司提交的书面对账单,发现问题要及时通知证券公司,积极协助处理。第三,要通过学习或咨询,选择并使用适当的安全防范技术,如密码设备、数据备份等,不能为了方便而省去必要的安全操作,各类数据和资料要安全存放。第四,要注意核实证券公司开展网上委托业务的资格,认真阅读与证券公司签订的有关协议文本,明确双方的法律责任。第五,要注意分析、核实从网上获取的各类信息,做一个成熟的投资者。

虽然中国证监会制定了《网上证券委托暂行管理办法》,但是我国网上证券交易的规范和监管还是存在着以下问题:第一,监管依据尚不足,还没有出台与《办法》相配套的法律法规;第二,还没有建立起一个适应网上证券交易特点的监管体系;第三,对网上交易的开放性

认识不足，尚没有形成全球化的协调监管机制。

四、网上证券交易的风险问题

如果要用一句话来概括网上证券交易的风险，就是未来的不确定性。这种不确定性的程度决定了风险的大小。经验告诉人们，一件事物越复杂，人们对其了解得越少，要对其准确预测的难度也就越大，因此风险也越高。证券市场就是这种高度复杂的事物之一，其表现形式多种多样。例如，上市公司的经营亏损和证券收益率的不确定性，以及证券市场的变化与股价的波动等。这种不确定性主要是由市场上各参与者之间市场信息不完全和不对称引起的。认识证券市场的复杂性，了解其运作的内在规律和风险，可以提高投资者的风险意识，增强防范风险和承受风险的能力。证券投资既有其高收益的一面，也有其高风险的一面，“收益自得、风险自担”，这是每个投资者入市前应有的清醒认识。

网上证券交易系统是整个证券市场的一个子系统，证券市场上客观存在的政策风险、投资风险、开户风险、业务风险、设备系统故障风险及各种不可抗力风险等，同样存在于网上证券交易过程中，而且由于其采用的技术手段有别于其他交易方法，使其具有因网络技术等因素带来的独特风险。在网上证券交易过程中可能有以下情况出现：

1. 技术风险

（1）由于线路繁忙，投资者存在遇到行情不能及时进入网上证券交易系统，使投资人不能及时增大收益或阻止损失的风险。

（2）由于网络故障，投资人通过网上证券交易系统进行证券交易时，投资人计算机界面已显示委托成功，而券商服务器未接到其委托指令，从而存在投资人的利益不能增大或损失不能停止的风险；或投资人计算机界面对其委托未显示成功，于是投资人再次发出委托指令，而券商服务器已收到投资人两次委托指令，并按其指令进行了交易，使投资人由此而产生重复买卖的风险。

（3）由于黑客的侵入，网络发生故障，投资人存在不能及时进入网上证券交易系统，无法进行正常交易的风险。

（4）由于投资人不慎将资金账号、证券账号及交易密码遗失，使其持有的证券被他人盗卖的风险。

（5）由于证券交易可以委托他人代理，从而存在未按投资者本人意图买卖证券和提取资金的风险。

（6）由于投资人自身操作失误，出现证券种类、买卖方向、价格、数量输入错误而产生的风险。

（7）由于不可抗力因素，使投资人不能及时进行交易的风险。

2. 网络欺骗

网络欺骗是网上证券委托纠纷发生率最高的形式之一，其主要表现形式是虚假信息的发布。证券市场本身是一个真假信息并存的场所，而且其信息的时效性要求非常高。在网上证券交易条件下，一方面，网络作为证券市场的信息载体，传播速度极快，覆盖范围极广，使得虚假信息更加严重；另一方面，证券公司的网站均为投资者提供了电子布告栏系统服

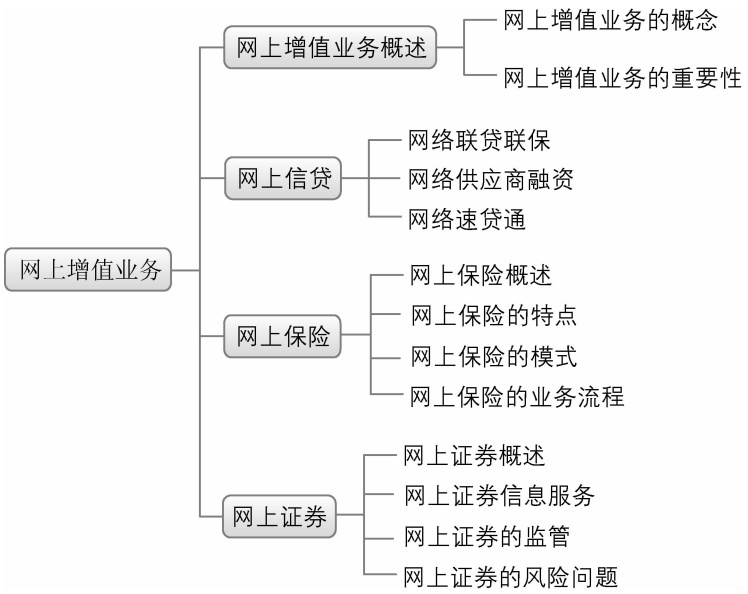
务，由于网络的交互性、匿名性特点，投资者可以在网站上匿名地自由发言，而且对这些所谓消息的追索难度非常大，从而使得网络成为某些不怀好意者制造虚假消息进行网上欺诈的场所，如发布假行情、假公告等虚假信息，误导投资者，甚至操纵市场。

引例解析

网上增值业务，暂时没有统一的定义，本书是指电子银行的增值业务，即电子银行为客户提供的超出常规服务范围的服务。也就是说，电子银行除为客户提供基础网上服务（网上支付与结算）外，还提供其他特殊的金融服务。

现在各大银行都提供了网上增值服务，所提供的服务却又有不同。一般来说，电子银行的网上增值服务主要有网上投资、个人理财助理、企业银行和其他金融服务。其中，具有代表性的是网上信贷、网上保险和网上证券。

本章小结



综合训练

一、思考练习

1. 试比较网络联贷联保、网络供应商融资、网络速贷通的异同。
2. 网上保险的特点是什么？

3. 简述网上保险的业务流程。

4. 网上证券能提供哪些信息服务?

5. 试分析网上证券存在的问题,并思考如何有效监管网上证券交易。

6. 我国的网上证券存在哪些风险问题?

二、案例分析

网络民间借贷“初绽放”

在网上,没有担保,没有抵押,就能向陌生人借到钱,你相信吗?近两年,民间借贷网站风生水起:宜信、拍拍贷、搜好贷、天天贷、e借通、ezmoney。在那里,聚集了一批想借钱和有钱借的人,而网站只是一个中介,不吸储也不放贷,仅收取2%~4%的服务费。

宜信、拍拍贷、搜好贷、天天贷、e借通、ezmoney等网站与“淘宝网”类似,不同的是,后者交易商品,而前者交易借贷。借款方可以自由发布自己的借款金额、用途、还款期和回报率等信息,之后,若干愿意投资的人开始竞拍。有意思的是,出借方往往不止一人——假设借入1 000元,可能是10个人各出100元凑够借款额。

这种“草根金融”网站在鲜花与争议中存活了3年多。有人认为,这是一种全新的金融模式,甚至被誉为“网络版孟加拉乡村银行”;也有人认为,处在监管空白下的网上借贷,是金融诈骗的滋生地,是高利贷的温床。

为此,菠萝网的创始人、拍拍贷的CEO顾少丰对这种“草根金融”模式进行了解说。

国内首家网络借贷平台——拍拍贷于2007年8月在上海成立,是中国第一个P2P(个人对个人)信用网上借贷平台。罗艺是拍拍贷的用户之一。2009年,他开奶茶店的创业资金缺1.2万元,同学介绍他上“拍拍贷”网站借钱。他在网站上发布了借款需求,写明借款金额、用途、还款期、利率、还款能力,并向网站提供了身份证、毕业证等一系列个人信息。“起初,我并没有抱太大希望,原本还是打算向朋友借,但没想到十几天后,真的有20人借钱给我,其中还有一个就是介绍我上网借钱的那位同学。有的借500元,有的借1 000元,也有人借了50元。”罗艺介绍说,他们最后协商的利率是一年20%,之后的14个月里,他每月把1 000元打入网站的固定账户,偿还陌生网友。

这种“整借零投”的方式,无疑分散了风险。但并不是每个借款人都这么幸运,有的人甚至借3 000元都会因出借方不足而流标。“即便已经有2 900元竞标,只要剩下的100元没人愿意借,借款都将失败。”顾少丰介绍,早期网站的成功借款率不到20%,如今,这个概率已经接近50%。

在拍拍贷的平台上,借款的金额限定在3 000~100 000元。网站首页上显示了借款人的借款金额、借款人信用等级、借款进度、借款期限等信息,主要用于个人初期创业、短期信用卡资金周转或装修、购物等消费,也有一些是借钱给家人治病或者求学的。很多借款人的需求都在5万元以下,甚至是几百元,借款期限最短1个月,最长12个月,年利率最高为21%。在通常情况下,1万元以下的借款进度较快。“其实,这种模式源于对欧美P2P网上借贷的模仿。”顾少丰表示,有投资就有风险。国外一般都有完备而透明的个人信用认证体系,个人信用记录、社会保障号、个人税号、银行账号等材料可以得到充分验证。但是,国内信用体系还不是很完备,因此国内投资人必须谨慎行事,在放款前详细认证借贷方的资信状

况，另外选取比较成熟和规范的贷款网站也很重要。①

从现有金融政策法规角度来看，由于网站不属于金融机构，国家对于民间借贷中介还没有一个明确的界定，所以并没有将其纳入监管范围，存在一定的监管空白。不少金融专家也表示，金融领域的每一次创新，总会伴随着产生各种新的问题，而监管和法律的完善必然会慢上半拍，P2P 网上借贷亦是如此。或许，我们在期望政府升级配套制度的同时，更应该提升自身的认识，毕竟这是风险完全集中于放贷者个人的新模式。②

问题

根据所提的 P2P 网上借贷模式的发展，分析这种模式的优势和不足。

网上增值业务

【实训目的】

网上增值业务是各银行电子化建设所提供的服务，通过此次实训，了解并比较各商业银行提供的网上增值业务，熟悉具有代表性的网上信贷、网上保险和网上证券的相关操作或流程。

【实训内容与要求】

1. 通过互联网访问各商业银行，了解并比较各商业银行提供的网上增值服务。

2. 登录网站 http://www.china-insurance.com，了解并熟悉有关网上保险的发展信息，掌握网上保险的操作流程。

3. 登录一家网上证券电子商务网站，了解并熟悉有关“网上证券交易程序”，试着根据其操作步骤完成网上证券交易的程序。

【成果与检验】

通过实际操作，检验自己是否掌握了网上增值业务的类型以及网上信贷、网上保险、网上证券的操作流程，并在课堂上交流经验。

---

① 网络民间借贷“初绽放”[EB/OL]. 2010-08-24[2011-5-5]. http://www.cnhubei.com/news/ctjb/ctjbsgk/ctjb33/201008/t1383630.shtml.

② 让大家贷款给大家 P2P 网络信贷正流行[EB/OL]. 2010-05-23[2011-5-5]. http://blog.sina.com.cn/s/blog_4ccc95790100jfpq.html.

第七章
网上支付的安全技术

知识目标

- 了解电子商务网上支付面临的安全问题；
- 了解计算机病毒的特点和种类；
- 了解防火墙的类型；
- 掌握电子支付中的安全技术；
- 掌握电子商务安全认证技术；
- 掌握电子安全交易 SSL 协议和 SET 协议的基本概念和原理。

技能目标

- 掌握计算机病毒的防治方法；
- 掌握防火墙的设置方法；
- 掌握数字证书的申请和使用方法。

引例

招商银行的网上支付安全技术

随着互联网的不断发展，在世界范围内掀起了一股电子商务热潮，但在电子商务网上支付中最关心的问题就是其账号及密码等信息的安全性，因此网上支付与网络安全关系紧密，缺一不可。目前国际流行的网上支付安全协议有两种：SET 协议与 SSL 协议。但目前国际上对这两种网络安全协议到底哪种才是未来的发展方向，还没有完全达成共识，我国已开展的网上支付银行还没有一家专门采用某一种安全协议。

招商银行在开发“一网通”网上银行系统时参考了专用协议方式，综合采用了业务和技术双重安全机制，开创性地实现了安全的网上支付。下面列举其中的六个要点：

(1) 客户使用专用账户进行支付交易。网上支付专用账户是“一卡通”的一个子账户，有独立的支付账号和支付密码，上网消费时客户只需输入该账号和密码，就可以实现在线付款。客户可以在任何时刻通过互联网或电话把“一卡通”中的资金转入专用账户，而资金只有转入这个专用账户才能用于消费。这就保证了“一卡通”账户中的其他资金的安全。

(2) 设置网上消费金额限制。对不同类型的客户设定不同的每日累计交易最高限额，设定后还可根据客户的要求加以调整。如对一般客户设定的最高限额最初为 2 000 元人民币，后来调整为 5 000 元人民币，最后调整为现在的 1 万元人民币。

(3) 支付卡信息直接传送到银行。客户在招商银行网页中输入网上支付卡信息，加密后直接传送到银行，不经过商家转发，这样可以避免泄露支付信息。

(4) 商家无法得到客户的支付信息。商家只从银行接收客户的订货信息，避免客户篡改已被银行确认的订单信息。

(5) 错误登录次数限制。客户如果在一天内登录错误次数达到 5 次，银行当天则拒绝为其服务。

(6) 网上传输采用 SSL 协议加密。

由于采用业务和技术双重安全机制，招商银行“一网通”网上银行系统运行以来，企业银行交易超过 5 万笔，个人支付交易超过 1 万笔，没有出现过一例支付信息安全问题。

随着电子商务的不断发展，国内商业银行必将推出更多的网上支付方式。招商银行着重开发的无限额支付系统和 B2B 网上信用证支付系统，会为中国电子商务的发展提供更为有力的结算支持。

请分析案例，并思考下面的问题：

1. 网上支付存在哪些网络安全问题？

2. 如何解决网上支付的安全问题？

第一节　网上支付安全概述

一、网上支付的网络安全问题

网上支付给人们带来交易便利的同时，也存在许多安全方面的问题。根据 CNNIC（中国互联网络信息中心）的调查，2009 年 1 月—2009 年 7 月，半年内有 57.6％的网民在使用互联网过程中遇到过病毒或木马攻击，同时，有 1.1 亿网民在过去半年内遇到过账号或密码被盗的问题，占总体网民的 31.5％。网络安全问题不容小视，安全隐患有可能制约电子商务、网上支付等交易类应用的发展。

典型案例

谨防网络购物诈骗

银川市的韩先生在网上购物时，即时交流工具突然收到一信息，称某数码网站正在搞优惠活动，他看中的一款手机仅售 850 元。随后他查询了该网站，发现该网站不仅有备案，而且网民评价也不错。于是，他就按照该网页提示，通过所谓的“工商银行”网上银行支付货款，可是不知为什么，每次到输入口令卡坐标密码时就发生错误。无奈之下他便到银行询问，这才发现银行卡上的 1 000 多元被窃取了。

网络技术方面本身存在的漏洞和权限，为不法分子进行不法行为提供了契机。概括起来，网络支付的安全威胁主要有以下几个方面：

（1）窃取。支付账号和密码等隐私信息在网络传送过程中被窃取或盗用。当一个客户的信用卡号码和密码在网上被窃取后，盗用者就可以利用客户的信用卡信息伪造一张新的信用卡，然后就可以从任何一个 ATM 或 POS 中取出客户的资金。

（2）篡改。如果在利用网络支付系统进行支付时，信息被他人恶意截取，容易发生交易信息、支付金额被篡改的事件，由此而产生多支付或少支付的问题，给交易双方增添了不少麻烦。

（3）冒用身份。由于支付方不知道商家到底是谁，商家不能确定信用卡等网络支付工具是否真实，以及由谁来支付资金和资金如何入账等，一些不法商家或个人便会利用网络贸易的非面对面的特点进行欺诈活动。

（4）网络支付系统的不稳定性。网络支付系统会突然因为非人为性中断瘫痪或被攻击或使用网络技术被故意延迟。由于客户的电子货币信息存放在相应的银行后台服务器中，当银行后台服务器出现错误、运行中断或瘫痪时，客户将无法使用电子货币，导致正在进行的网上交易中断，影响客户的支付行为。

（5）不承认或抵赖已经做过的交易。例如，发信者事后否认曾经发送过某条消息或内容，收信者事后否认曾经收到过某条信息或内容，购买者不承认确认了订货单，商家卖出的商品因价格差而不承认原有的交易。这种缺失诚信的现象对于网络贸易的发展非常不利。

二、网上支付的安全需求

由于网上支付存在上述安全问题，为了保障交易各方的合法权益、保证能够在安全的前提下开展电子商务交易，必须满足以下基本需求：

（1）身份真实性。只有信息流、资金流、物流的有效转换，才能保证电子商务的顺利实现，而这一切是以信息的真实性为基础的。传统的商务交易因为双方可以见面而不用担心身份的真实性，但网上交易的双方相隔甚远，互不了解，这就为一些不法商家或个人利用网络贸易的非面对面的特点进行欺诈活动提供了条件。所以需要为参与交易的各方提供可靠标识，使他们能正确识别对方并能互相证明身份。

（2）信息的完整性。电子商务简化了贸易过程，减少了人为的干预，同时也带来维护贸易各方商业信息的完整、统一的问题。数据输入时的意外差错或欺诈行为，可能会导致交易各方信息的差异。另外，数据传输过程中信息丢失、信息重复或信息传送的次序差异也会导致交易各方信息的不同。假如有不法分子对支付的数据（如支付金额）进行修改而发生多支付或少支付的问题，那么势必给交易双方增添不少麻烦。

（3）不可否认性，也称不可抵赖性。不可否认性是指信息的发送方不能否认曾经发送的信息、不能否认自己的行为。在传统的商务交易中，双方可通过书面文件上的手写签名或印章来预防抵赖行为的发生，但这在网上交易时是不可能实现的。进行网上交易时可能出现这样的情况：当交易一方发现交易行为对自己不利时，就会否认电子交易行为，这必然会损害另一方的利益。

（4）数据保密性。有关交易的各种信息，如付款人和收款人的标识、交易的内容和数量等，这些信息只能让交易的参与者知道，有时甚至要求只让参与方的部分人知道。因此，网上支付就会涉及数据保密性的问题，信息的传播、存储和使用具有保密的要求，对敏感文件、信息要进行加密，即使这些信息被截获，也应使截获者无法了解信息内容。

三、网上支付的安全技术措施

基于用户对网上支付的安全性的需求，网上支付的安全问题应主要从技术、法制、道德规范和管理策略等多个方面来解决。其中网上支付的安全技术措施主要包括以下几种：

1. 安全的网络平台

常用的方法是在网络中采用防火墙技术、虚拟专用网（VPN）技术和防病毒保护等。

2. 数据加密

数据加密被认为是电子商务最基本的安全保障形式，可以从根本上满足信息完整性的要求。它是通过一定的加密算法，利用密钥（secret keys）来对敏感信息进行加密，然后把加密好的数据和密钥通过安全方式发送给接收者；接收者可利用同样的算法和传递过来的密钥对数据进行解密，从而获取敏感信息以保证网络数据的机密性。

3. 数字签名

数字签名是公开密钥加密技术的另一类应用。它的主要方式是：报文的发送方从报文文本中生成一个散列值（或报文摘要），发送方用自己的私钥对这个散列值进行加密来形成

发送方的数据签名。然后，这个数据签名将作为报文的附件和报文一起发送给报文的接收方。报文的接收方首先从接收到的原始报文中计算出散列值（或报文摘要），接着再用发送方的公钥来对报文附加的数字签名进行解密。如果两个散列值相同，那么接收方就能确认该数字签名是发送方的。通过数字签名能够鉴别原始报文的完整性，实现不可抵赖性。

4. 安全协议

在国际上，比较有代表性的电子支付安全协议有 SSL 协议和 SET 协议。

安全套接层（secure socket layer，SSL）协议是由网景（Netscape）公司研究制定的安全协议。通俗地说，SSL 就是客户和商家在通信之前，在 Internet 上建立一个“秘密传输信息的信道”来保障传输信息的机密性、完整性和认证性。该协议向基于 TCP/IP 的客户端/服务器应用程序提供了客户端和服务器的鉴别、数据完整性及信息机密性等安全措施。该协议在应用程序进行数据交换前通过交换 SSL 初始握手信息来实现有关安全特性的审查。SSL 协议运行的基点是商家对客户信息保密的承诺。客户的信息首先传到商家，商家阅读后再传到银行。这样，客户资料的安全性便受到威胁。另外，整个过程只有商家对客户的认证，缺少客户对商家的认证。在电子商务的初始阶段，由于参加电子商务的公司大都有较好的信誉，这个问题没有引起人们的足够重视。随着越来越多的公司参与电子商务，对商家的认证问题也就越来越突出，SSL 的缺点逐渐暴露出来，SSL 协议也将逐渐被新的 SET 协议所代替。

安全电子交易（secure electronic transaction，SET）协议向基于信用卡进行电子化交易的应用提供了实现安全措施的规则。它是由 VISA 国际组织和 MasterCard 组织共同制定的一个能保证通过开放网络（包括 Internet）进行安全资金支付的技术标准。SET 协议在保留对客户信用卡认证的前提下，又增加了对商家身份的认证。由于设计较为合理，得到了诸如微软公司、IBM 公司、Netscape 公司等大公司的支持，已成为实际上的工业技术标准。

第二节　计算机病毒及其防治

一、计算机病毒的定义

计算机病毒（computer virus）简称病毒，是在计算机系统资源中自我繁衍和传播，并对计算机资源造成破坏的一组计算机程序代码。《中华人民共和国计算机信息系统安全保护条例》明确定义，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毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码”。计算机病毒具有自我复制能力、很强的感染性、一定的潜伏性、特定的触发性和很大的破坏性，与生物医学上的“病毒”同样有传染和破坏特性，因此由生物医学上的“病毒”概念引申出“计算机病毒”这一名词。

二、计算机病毒的特点

计算机病毒有以下几个特点：

（1）寄生性。计算机病毒寄生在其他程序之中，当执行这个程序时，病毒就起破坏作用，而在未启动这个程序之前，它是不易被人发觉的。

（2）传染性。计算机病毒具有很强的传染性，它可以从一个程序传染到另一个程序，从一台计算机传染到另一台计算机，从一个计算机网络传染到另一个计算机网络，在各个计算机系统上蔓延，同时使被传染的计算机程序、计算机、计算机网络成为计算机病毒的生存环境及新的传染源。

（3）潜伏性。一个编制精巧的计算机病毒程序，进入系统之后一般不会马上发作，可以在几周或者几个月内甚至几年内隐藏在合法文件中，对其他系统进行传染，而不被人发现。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。有些病毒像定时炸弹一样，编程者会预先设计好其发作时间。比如，黑色星期五病毒，不到预定时间人们一点都觉察不出来，等到条件具备时就会爆发，对系统进行破坏。

（4）隐蔽性。计算机病毒具有很强的隐蔽性，可以隐藏在操作系统、可执行程序或数据文件中，不易被人察觉和发现。

（5）破坏性。计算机中毒后，可能会导致正常的程序无法运行，把计算机内的文件删除或受到不同程度的损坏，如屏幕变得异常、系统速度变慢等。

（6）可触发性。病毒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称为可触发性。为了隐蔽自己，病毒必须潜伏，少做动作。如果完全不动，一直潜伏，病毒既不能感染也不能进行破坏，便失去了杀伤力。病毒既要隐蔽又要维持杀伤力，就必须具有可触发性。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。病毒运行时，触发机制检查预定条件是否满足，如果满足，启动病毒感染或破坏动作，进行攻击；如果不满足，则继续潜伏。

（7）针对性。一种计算机病毒（版本）并不是能传染所有的计算机系统或计算机程序。有的病毒是传染 Apple 公司的 Macintosh 系统的，有的是传染 Microsoft 公司的 Windows 系统的，有的病毒传染磁盘引导区，有的病毒传染可执行文件。

（8）衍生性。通过分析计算机病毒的结构可知，传染的破坏部分反映了设计者的设计思想和设计目的。但是，这可以被其他掌握原理的人以某个人的企图进行任意改动，从而又衍生出一种不同于原版本的新的计算机病毒，也即病毒的变种。这就是计算机病毒的衍生性。

三、计算机病毒的分类

1988 年 11 月 2 日下午 5 时 1 分 59 秒，美国康奈尔大学的计算机科学系研究生，23 岁的莫里斯（Morris）将其编写的蠕虫程序输入计算机网络，这个网络连接着大学、研究机关的 155 000 台计算机，在几小时内导致网络堵塞，运行迟缓。这件事情就像是计算机界的一次大地震，引起了巨大反响，震惊全世界，引起了人们对计算机病毒的恐慌，也使更多的计算机专家重视和致力于计算机病毒的研究。

从第一个病毒出现以来，世界上究竟有多少种病毒，说法不一。但是无论有多少种，病毒的数量仍在不断增加。据国外统计，计算机病毒以 10 种/周的速度递增。另据我国公安部统计，国内以 4～6 种/月的速度递增。早期的计算机病毒主要通过软盘、光盘等存储介质

传播，病毒的类型主要是文件型、引导型病毒等。随着网络应用的普及和存储介质的改变，计算机病毒的类型和传播方式有了很大的变化。

1. 按病毒存在的载体分类

（1）引导区病毒。这类病毒隐藏在硬盘或软盘的引导区，当计算机从感染了引导区病毒的硬盘或软盘启动，或当计算机从受感染的软盘中读取数据时，引导区病毒就开始发作。一旦它们将自己复制到机器的内存中，马上就会感染其他磁盘的引导区，或通过网络传播到其他计算机上。

（2）文件型病毒。文件型病毒寄生在其他文件中，常常通过对它们的编码加密或使用其他技术来隐藏自己。文件型病毒劫夺用来启动主程序的可执行命令，用做它自身的运行命令，同时还经常将控制权还给主程序，伪装计算机系统正常运行。这类病毒有黑色星期五病毒、CIH 病毒等。

（3）混合型病毒。这种病毒兼有文件型病毒和引导型病毒的特点，感染引导区也感染可执行文件，因此具有更广泛的传播性和破坏性。

2. 按病毒传染的方法分类

按此分类方法病毒可分为四种类型：入侵型病毒、嵌入式病毒、外壳类病毒和病毒生产机。入侵型病毒顾名思义是通过外部媒介侵入宿主机器的；嵌入式病毒则是通过嵌入某一正常的程序中，然后通过某一触发机制发作；外壳型病毒使用特殊算法把自己压缩到正常文件上，当用户解压文件时即执行病毒程序；病毒生产机是可以“批量生产”出大量具有同一特征的“同族”病毒的特殊程序，这些病毒的代码长度各不相同，自我加密、解密的密钥也不同，发作条件和现象不同，但其主体构造和原理基本相同。

3. 按病毒自身特征分类

根据病毒自身存在的编码特征可以将计算机病毒分为：

（1）伴随型病毒：这一类病毒并不改变文件本身，它们根据算法产生 EXE 文件的伴随文件。

（2）变型病毒：这一类病毒使用一个复杂的算法，使自己每传播一次都具有不同的内容和长度。此类病毒通常由一段混有无关指令的解码算法和被变化过的病毒体组成。

四、计算机病毒的防治

（一）我国计算机病毒传播的主要途径

我国计算机病毒主要通过电子邮件、网页下载或浏览、局域网和移动存储介质等途径传播，如图 7-1 所示。通过调查发现，病毒通过移动存储介质传播的比例在 2007 年高达 41.34%，通过加强管理 2008 年为 21.9%，呈现大幅下降趋势，但是 2009 年又出现上升势头，达到 25.40%。由于 U 盘等各种类型的移动存储介质的广泛使用，越来越多的病毒、木马将移动存储介质作为传播途径。病毒木马利用移动存储介质在内外网之间、涉密与非涉密系统之间进行数据复制交换的时候，窃取敏感或者涉密信息。随着移动存储介质的普及，必须进一步加强对此类介质的管理，严防在不同安全级别的系统之间交叉使用，同时通过修改系统配置，关闭系统自动运行功能等方法，提高系统的安全级别，防止病毒木马通过移动

存储介质传播。

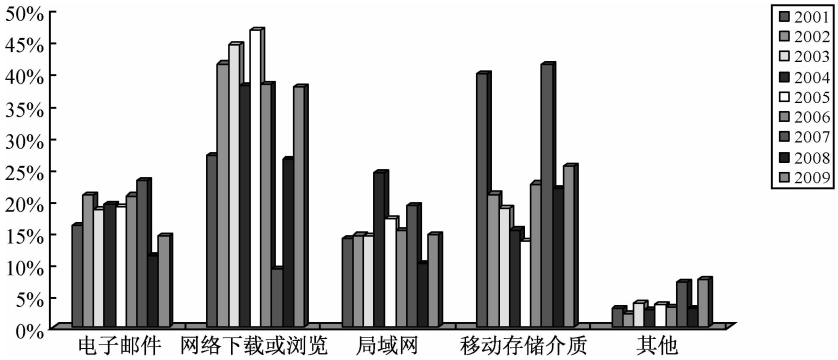


图 7-1　我国计算机病毒传播的主要途径

另外，2009 年的调查结果显示，病毒通过网页下载或浏览进行传播的比例以 37.89％位居首位，比 2008 年上升 11.48 个百分点，延续了从 2007 年以来的大幅度增长趋势，进一步说明了网页“挂马”仍然是最受恶意攻击者青睐的病毒散播方式。同时，通过网络监测和用户求救的情况也反映出，大量的网络犯罪就是通过“挂马”方式来实现的。挂马者主要利用微软以及其他应用普遍的第三方软件（如 Realplayer、Adobe Flash、暴风影音等）漏洞进行攻击。“挂马”是指在网页中嵌入恶意代码，当存在安全漏洞的用户访问这些网页时，木马会侵入用户系统，然后盗取用户敏感信息或者进行攻击、破坏。这种通过浏览页面方式进行攻击的方法具有较强的隐蔽性，用户难以发现，因此，潜在的危害性更大。用户必须持续重视浏览器和各种流行应用软件的安全性，提高对“挂马”攻击方式的防范能力。

（二）计算机病毒的预防

计算机病毒的预防是指通过建立合理的病毒预防体系和制度，及时发现入侵的病毒，并采取有效的手段阻止病毒的传播和破坏，主要从法律法规、安全管理和技术三个层面来实现。

1. 法律法规的措施

由于计算机病毒对计算机资源造成的破坏日益严重，如何严格地控制和清除计算机病毒的危害，已是一个严重的社会问题，应引起各方面的重视。从国家来说，制定出一定的法律法规，严惩病毒的制造者，可以减少病毒的产生。我国为预防计算机病毒颁布了以下法律法规：

（1）《中华人民共和国刑法》的第二百八十六条规定：违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

（2）《中华人民共和国计算机信息系统安全保护条例》的第二十三条规定：故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系

统安全专用产品的，由公安机关处以警告或者对个人处以 5 000 元以下的罚款、对单位处以 15 000 元以下的罚款；有违法所得的，除予以没收外，可以处以违法所得 1 至 3 倍的罚款。

（3）《计算机病毒防治管理办法》对计算机病毒的预防和治理，保护计算机信息系统安全，保障计算机的应用与发展制定了更全面的法律法规。

2. 安全管理措施

根据计算机病毒的特点，从根本上完全杜绝和预防计算机病毒的产生和发展是不可能的。目前出现的计算机病毒的攻击事件不但没有减少，而是日益增多，并且病毒的种类越来越多，破坏方式日趋多样化。因此，必须寻求一种解决方案，力争将计算机病毒的危害性降至最低。为此，公安部和国家计算机网络与安全管理中心 2003 年 8 月决定，在天津的计算机病毒防治产品检验中心的基础之上，建立国家计算机病毒应急处理中心（网址为 www.antivirus-china.org.cn，如图 7-2 所示）。该中心是我国计算机应急体系（CERT）中的一部分，国内从事病毒研究的机构和病毒防治产品的开发厂家以及各省市公共信息网络安全监察部门都是应急体系的成员。CERT 遵循的工作原则是“积极预防、及时发现、快速反应、确保恢复”。CERT 一旦发现计算机病毒，就及时向国家计算机病毒应急处理中心报告，对在我国发现的计算机病毒事件进行快速反应和处置，将出现的重大计算机病毒疫情报告公安部，向社会发布病毒疫情，减少计算机病毒对我国计算机信息系统和网络的破坏。

图 7-2　国家计算机病毒应急处理中心主页

3. 技术措施

通过采取管理上和技术上的措施，计算机病毒是可以防范的。虽然新出现的病毒可采用更隐蔽的手段，利用现有操作系统安全防护机制的漏洞，以及反病毒防御技术尚存在的缺陷，暂时在某一计算机上存活并进行某种破坏，但是只要在思想上有反病毒的警惕性，加强反病毒技术和管理措施，新病毒就无法逾越计算机安全保护屏障，不能广泛传播。预防病毒

的管理和技术措施如下：

（1）坚持以硬盘引导。

（2）用户应养成及时下载最新系统安全漏洞补丁的安全习惯，从根源上杜绝黑客利用系统漏洞攻击用户计算机的病毒。同时，安装和升级杀毒软件，开启病毒实时监控应成为每日防范病毒的必修课。

（3）定期做好重要资料的备份，以免造成重大损失。

（4）及时更新计算机的防病毒软件、安装防火墙。

（5）在使用即时通信工具时，不要随意接收好友发来的文件，避免病毒从即时聊天工具中传播过来。

（6）在打开通过局域网共享及共享软件下载的文件或软件程序之前，建议先进行病毒查杀，以免中毒。

（7）不要打开来源不明的电子邮件，在打开电子邮件时特别当心其中包含的附件，它们极有可能就是病毒或木马。

（8）将应用软件升级到最新版本，其中包括各种即时通信工具、下载工具、播放器软件、搜索工具条等；不要登录来历不明的网站，避免病毒利用其他应用软件漏洞进行木马病毒传播。

（9）在使用移动介质之前，先进行病毒查杀。

（10）在登录电子银行实施网上查询交易时，尽量选择安全性相对较高的USB证书认证方式。不要在公共场所，如网吧登录网上银行等一些金融机构的网站，防止重要信息被盗。

（11）在登录一些金融机构，如银行、证券类的网站时，应直接输入其域名，不要通过其他网站提供的链接进入，因为这些链接可能导入虚假的银行网站。

（三）计算机病毒的检测

计算机病毒感染系统后，必然会留下痕迹。病毒检测技术能够利用病毒留下的痕迹确认出病毒的存在，主要有病毒特征匹配法、完整性验证法、启发式行为监测法、软件模拟法和新一代病毒检测技术。在上述几种基本检测技术的基础上，随着病毒与反病毒斗争的不断升级，病毒检测技术也在不断地发展。新一代的病毒检测技术包括沙箱技术、启发式查毒技术、主动内核技术、智能引擎技术、嵌入式杀毒技术和压缩智能还原技术等。

通常判断计算机是否染上病毒有两种方法：一是人工检测；二是自动检测。人工检测要求检测人员有一定的业务素质，自动检测要有专门的检测软件。

1.人工检测

下列一些现象可以作为检测病毒的参考：

（1）引导时出现死机现象。

（2）程序装载、运行明显变慢。

（3）磁盘访问变慢。

（4）显示器屏幕出现异常显示。

（5）有规律地出现异常信息。

（6）磁盘空间突然变小或不识别磁盘设备。

（7）程序或数据无故丢失，文件名不能识别。

（8）无法启动系统。

（9）系统经常性死机。

（10）网络阻塞或瘫痪。

2. 自动检测

通常反病毒软件具有对特定种类的病毒检测的功能，有的软件可查出几十种甚至几百种的病毒，并且大部分反病毒软件可同时清除检测到的病毒，而不会破坏系统中的正常数据。目前，一些计算机使用者经常利用反病毒软件实时监控计算机系统的运行情况，当有病毒出现时，反病毒软件会给出提示或警告信息，便于发现和清除病毒。

（四）计算机病毒的清除

在正确检测出病毒的基础上，还需要将病毒从被感染文件中清除，同时尽量使被感染文件恢复到被感染前的状态。对文件病毒的清除过程实质上是病毒感染过程的逆过程。目前最简单、最常用和最有效的方法是使用查杀病毒软件来清除计算机病毒。现在流行的检查计算机病毒的软件较多，最常用的有金山毒霸、Kaspersky（卡巴斯基）、ESET NOD32、江民杀毒、瑞星杀毒。这些杀毒软件除了能查、除病毒外，也能清查 BO 等黑客程序。清除文件型病毒通常分析病毒和被感染文件之间的链接方式，确定病毒程序处于被感染文件中的位置，找到病毒程序开始和结束的位置，还原被感染文件夹的主要部分，恢复被感染文件的文件头部参数。对引导型病毒的清除，通常先寻找一台同类型、相同硬盘分区的无毒计算机，将其引导扇区中的引导记录写入引导磁盘，无毒引导磁盘启动系统，将此可引导磁盘插入染毒计算机，将引导记录写入被感染的引导扇区，覆盖病毒感染后的引导记录，即可恢复。对于宏病毒，可通过应用软件提供的删除宏功能清除数据文件中的宏病毒代码。

总而言之，在计算机病毒的防治中，除了通过预防措施、检测技术和清除技术为用户提供一个相对安全的网络环境外，更应以预防为主，提高用户的安全防范意识和病毒防治技术，从根本上防止计算机病毒的感染和传染。

第三节　防火墙及其设置

“防火墙”（firewall）一词来源于早期欧式建筑中为了防止火灾的蔓延而在建筑物之间修建的矮墙。计算机网络中的防火墙是指设置在本地网络与外界网络之间的一道防御系统，是这一类防范措施的总称。防火墙主要用于逻辑隔离外部网络与受保护的内部网络，其应用示意图如图 7-3 所示。

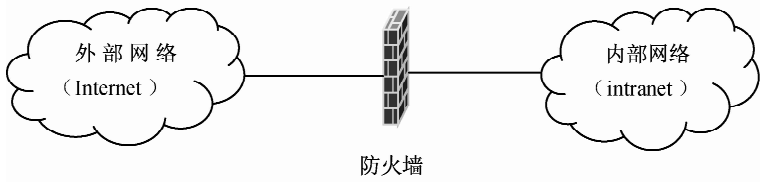


图 7-3　防火墙应用示意图

一、防火墙的概念

防火墙就是内部网络和外部网络之间的一个屏障，它主要可以防止外部网络（Internet）对内部网络（intranet）的未授权访问。防火墙由软件和硬件组成。准确地讲，它位于企业或网络计算机与外界之间，其作用是限制外界用户对内部网络的访问并管理内部用户访问外界网络的权限，在外部网络与内部网络之间建立起一个安全网关，从而保护内部网络免受非法用户的侵入。使用防火墙，可以提高系统的安全性。

一般的防火墙都可以达到以下目的：一是可以限制他人进入内部网络，过滤掉不安全服务和非法用户；二是防止入侵者接近防御设施；三是限定用户访问特殊站点；四是为监视 Internet 安全提供方便。由于防火墙假设了网络边界和服务，所以更适合用于相对独立的网络，如 intranet 等种类相对集中的网络中。部署防火墙是控制对网络系统访问的非常流行的方法。事实上，在 Internet 的 Web 网站中，超过 1/3 的 Web 网站都是由某种形式的防火墙加以保护的，这是对黑客防范最严、安全性较强的一种方式。任何关键性的服务器，都建议放在防火墙之后。

防火墙位于单位的专有网络（内部网络）和 Internet 之间。从一个网络流向另一个网络的全部信息都流经防火墙，不允许任何信息绕开防火墙。防火墙能直接监视并阻断两个网络之间的信息流，还能完成其他一些重要的任务，如用户的认证、记录通信信息以及产生报表等。

二、防火墙的基本类型

防火墙技术可根据防范方式和侧重点的不同而分为三大类：包过滤型（packet filter）、应用代理型（proxy service）和复合型（hybrid）。

1. 包过滤型

包过滤技术是防火墙最常用的技术，是一种通用、价廉、有效的安全手段。包过滤防火墙安装在路由器上，作用在网络层和传输层，它根据分组包头源地址、目的地址和端口号、协议类型等标志，确定是否允许数据包通过。只有满足过滤逻辑的数据包才被转发到相应的目的地出口端，其余数据包则被从数据流中丢弃。包过滤路由器的逻辑位置如图 7-4 所示。

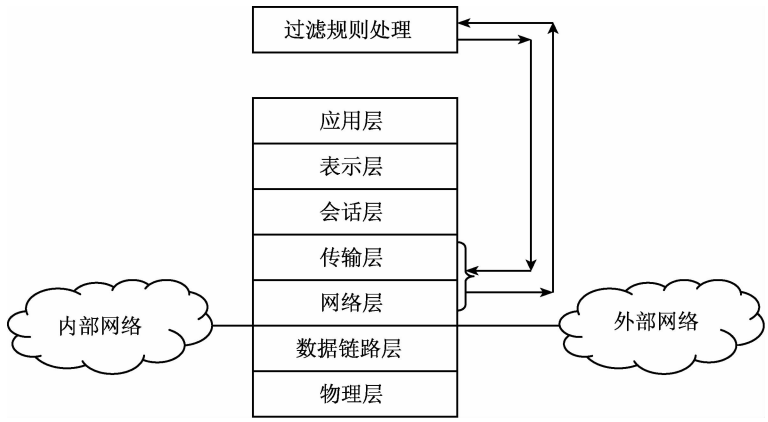


图 7-4　包过滤路由器的逻辑位置

2. 应用代理型

应用代理又称应用网关(application gateway)。代理技术与包过滤技术完全不同,包过滤技术是在网络层拦截所有的信息流,而代理技术作用在应用层,其特点是完全"阻隔"了网络通信流,通过对每种应用服务编制专门的代理程序,实现监视和控制应用层通信流的目的。应用网关对某些易于登录和所有输入/输出的通信环境给予严格的控制,以防有价值的程序和数据被窃取。实际中的应用网关通常由专用工作站实现。应用层网关的结构示意图如图 7-5 所示。

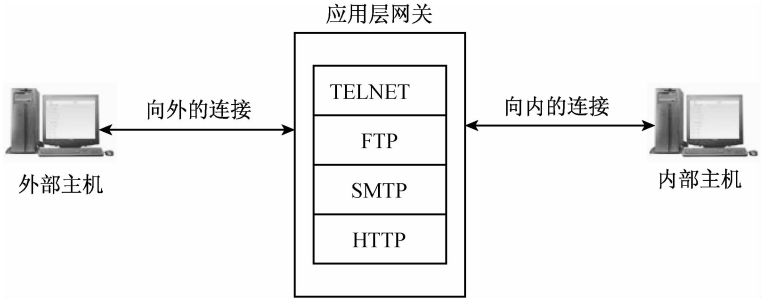


图 7-5　应用层网关的结构示意图

3. 复合型

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。这种结合通常有以下两种方案:

(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,同时一个堡垒主机安装在内部网络,通过在分组过滤路由器或防火墙上对过滤规则的设置,使堡垒主机成为 Internet 上其他结点所能到达的唯一结点。这确保了内部网络不受未授权外部用户的攻击。

(2) 屏蔽子网防火墙体系结构:堡垒主机放在一个子网内,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。在该结构中,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。

三、防火墙的设置

为更好地掌握防火墙的设置,下面以瑞星个人防火墙为例逐步介绍。

(一) 瑞星个人防火墙 2011 简介

瑞星个人防火墙 2011(界面如图 7-6 所示)为计算机提供全面的保护,能有效地监控任何网络的连接。通过过滤不安全的服务,可以极大地提高网络安全,同时减小主机被攻击的风险,使系统具有抵抗外来非法入侵的能力,防止计算机系统和数据遭到破坏。

图 7-6　瑞星个人防火墙 2011 界面

（二）瑞星个人防火墙的功能

瑞星个人防火墙具有以下几大功能：

1. 程序联网控制

程序联网控制的功能可以对应用程序的网络行为进行监控，默认的规则已经非常完善，高级用户可以根据自己的需要设定任意程序规则，对任意模块规则进行精确控制，真正做到“我的计算机我做主”。

2. 网络攻击拦截

通过总结和分析网络攻击的各种方式和行为，形成入侵检测规则库，每日随时更新，拦截来自互联网的黑客、病毒攻击，包括木马攻击、后门攻击、远程溢出攻击、浏览器攻击和僵尸网络攻击等。

3. 恶意网址拦截

瑞星个人防火墙对“恶意网址拦截”功能进行了整合与调整，将网站黑白名单整合于一项设置之中，更方便用户进行设置。

4. ARP 欺骗防御

越来越多的 ARP 欺骗攻击在局域网上泛滥，网络中出现大量 ARP 欺骗请求包，导致大量计算机无法上网或影响网络的稳定，带宽被严重浪费。开启瑞星个人防火墙 2011 的 ARP 欺骗防御功能，可以防止受到 ARP 欺骗攻击，能够捍卫用户上网的权利。

5. 对外攻击拦截

对外攻击拦截功能可以阻止计算机被黑客操纵，避免变为攻击互联网的“肉鸡”，保护带宽和系统资源不被恶意占用，避免成为“僵尸网络”成员。

6. 网络数据保护

网络数据保护可以实现用户的端口隐身和 MSN 聊天加密，避免黑客利用端口进行攻击。

7. IP 规则设置

根据用户定义的规则来过滤 IP 包。

8. 软件安全

用户可以通过瑞星密码来设置软件的密码保护，同时可以设置启动时的账户模式。

9. “云安全”计划

“云安全”计划可将用户和瑞星技术平台通过互联网紧密相连，组成一个庞大的木马/恶意软件监测、查杀网络。

（三）瑞星个人防火墙 2011 的安装

最新版本的瑞星个人防火墙可在瑞星网站（http://pc.rising.com.cn/rfw.html）下载，在其他专业下载网站也可以找到瑞星个人防火墙的安装文件。以下具体讲述安装步骤：

第 1 步：启动计算机并进入 Windows 系列操作系统，关闭其他应用程序。

第 2 步：双击运行瑞星个人防火墙的安装程序，根据安装向导进行操作。

第 3 步：在显示的语言下拉列表框中，用户可以选择“中文简体”、“中文繁体”和“English”中的一种，单击“确定”按钮开始安装。（以下内容以选择“中文简体”安装为例）

第 4 步：进入安装欢迎界面，单击“下一步”按钮继续。

第 5 步：阅读“最终用户许可协议”，选择“我接受”单选按钮，单击“下一步”按钮继续；如果用户选择“我不接受”选项，则退出安装程序。

第 6 步：在“验证产品序列号和用户 ID”窗口中正确输入产品序列号和用户 ID，单击“下一步”按钮继续。此时，如果用户输入错误，将不能继续安装，直至填写正确，才能进行下一步操作。

第 7 步：在“定制安装”窗口中选择需要安装的组件。用户可以在下拉列表框中选择全部安装或最小安装（全部安装表示将安装瑞星个人防火墙的全部组件和工具程序；最小安装表示仅选择安装瑞星个人防火墙必需的组件，不包括更多工具程序），也可以勾选需要安装的组件，如图 7-7 所示。单击“下一步”按钮继续安装，也可以直接单击“完成”按钮，按照默认方式进行安装。

第 8 步：在“选择目标文件夹”窗口中用户可以指定瑞星个人防火墙的安装目录，单击“下一步”按钮继续安装。

第 9 步：在“选择开始菜单文件夹”窗口中用户可以修改软件启动菜单名称，单击“下一步”按钮继续安装。

第 10 步：在“安装信息”窗口中显示了安装路径和组件列表，确认后单击“下一步”按钮开始安装瑞星个人防火墙。

第 11 步：在“结束”窗口中用户可以选择“运行注册向导”、“运行设置向导”和“运行瑞星个人防火墙主程序”来启动相应程序，最后单击“完成”按钮结束安装。

图 7-7　选择安装组件界面

（四）瑞星个人防火墙的设置

1. 网络防护

在“瑞星个人防火墙”主界面中单击“设置”超链接，打开“瑞星个人防火墙设置”窗口，在“网络防护”选项中可以对计算机的网络安全进行设置。下面主要介绍常用的几项功能：

（1）网络攻击拦截。网络攻击拦截作为一种积极主动的安全防护技术，在系统受到危害之前拦截入侵，在不影响网络性能的情况下能对网络进行监测。它能够防止黑客/病毒利用本地系统或程序的漏洞，对本地系统进行控制。通过使用此功能，可以最大限度地避免因为系统漏洞等问题而遭受黑客/病毒的入侵攻击。

网络攻击拦截设置的操作如下：在图 7-8 所示的窗口中勾选需要进行拦截的项目，然后单击“确定”按钮保存即可。

（2）恶意网址拦截。瑞星“云安全”计划每日随时更新恶意网址库，阻断网页木马、钓鱼网站等对计算机的侵害。恶意网址拦截设置界面如图 7-9 所示，其中包含“网站黑白名单”设置，用户可以根据自己的要求添加网址到网站黑白名单当中。具体操作如下：单击“网站黑白名单”后面的“设置”超链接，打开“网站黑白名单设置”对话框，在其中单击“增加”或“删除”按钮，即可添加或删除网址到网站黑白名单当中。

用户可以勾选“启用钓鱼网页扫描保护”复选框，以启用恶意网址拦截，防止受到钓鱼和病毒等恶意网站的侵害。在设置网站黑白名单后，也同样需要勾选“启用钓鱼网页扫描保护”复选框才能生效。

启用恶意网址拦截后，可以单击“添加”或“删除”超链接，选择增加或删除代理服务器的 IP 地址与端口号。

用户还可以对程序进行设置，防止程序访问网络时受到恶意网站的攻击。具体做法是：单击“排除程序”后面的“设置”链接，在打开的对话框中设置相应的参数。该操作用于添加不进行监控的程序。

图 7-8　网络攻击拦截设置界面

图 7-9　恶意网址拦截设置界面

（3）ARP 欺骗防御。ARP 欺骗是通过发送虚假的 ARP 数据包给局域网内的其他计算机或网关，冒充别人的身份来欺骗局域网中的其他的计算机，使得其他的计算机无法正常通信，或者监听被欺骗者的通信内容。用户可通过设置 ARP 欺骗防御，保护计算机的正常通信。

具体操作如下：选择“网络防护”→“ARP 欺骗防御”选项，打开如图 7-10 所示的设置界面。

“防御方式”选项组：用户可以选择定时检查本机 ARP 缓存、拒绝 IP 地址冲突攻击、禁

止本机对外发送虚假的 ARP 数据包。

“发现可疑或欺骗 ARP 数据包时如何提示我”选项组：这里有三种方式，分别是气泡通知、托盘动画和声音报警。

“防御范围”选项组：包括“防御局域网中的所有电脑”和“防御指定的电脑地址和静态地址”两个选项。

图 7-10　ARP 欺骗防御设置界面

（4）对外攻击拦截。通过使用“对外攻击拦截”功能，可以对本地与外部连接所收发的 SYN、ICMP、UDP 报文进行检测。在对外攻击拦截设置界面可对上述参数进行设置，然后单击“确定”按钮保存即可，如图 7-11 所示。

图 7-11　对外攻击拦截设置界面

(5) IP 规则设置。选择“网络防护”→“IP 规则设置”选项,打开相应的界面设置 IP 包过滤规则,如图 7-12 所示。

图 7-12　IP 规则设置界面

注意:规则设置越多性能越低;不需要增加与应用相关的规则,系统在需要时打开端口;不需要增加防范性规则,系统已经内置并且自动升级。

列表中显示当前使用的 IP 包过滤规则,具体列举项目为规则名称、状态、范围、协议、远程端口、本地端口、报警方式。

① 增加规则:单击“增加”超链接或通过右键快捷菜单选择“增加”命令,打开“IP 规则设置”对话框,输入规则名称、规则应用类型和如何处理触发本规则的 IP 包;单击“下一步”按钮,输入通信的本地计算机地址和远程计算机地址;单击“下一步”按钮继续,选择协议和端口号,并指定内容特征或 TCP 标志,设置是否指定内容特征等;单击“下一步”按钮继续,选择规则匹配成功后的报警方式,最后单击“完成”按钮。

注意:指定协议号范围是 0～255;匹配成功后的报警方式有托盘动画、气泡通知、弹出窗口、声音报警和记录日志 5 种。

② 编辑规则:选中待修改的规则,规则加亮显示,单击“编辑”超链接,打开“IP 规则设置”对话框,修改对应项目即可,修改方法与“增加规则”相同。

③ 删除规则:选中待删除的规则,规则加亮显示,单击“删除”超链接,确认删除后即可删除选中的规则。

注意:选中规则时可配合 Ctrl 或 Shift 键进行多选。

④ 导入规则:单击“导入”超链接,在弹出的文件选择对话框中选中已有的规则文件(*.fwr),再单击“打开”按钮,如果列表中已有规则,导入时会询问是否删除现有规则。选择“是”会删除现有规则后导入规则文件中的规则;选择“否”,会保留现有规则,导入规则文件中的规则。

⑤ 导出规则:单击“导出”超链接,在弹出的导出对话框中填写文件名,再单击“保存”按

钮即可。

⑥ 可信区设置：单击“可信区”后面的“设置”超链接，打开“可信区”对话框，单击“增加”按钮，在弹出的对话框为新规则命名，并指定本地及远程的 IP 地址或 IP 范围，单击“确定”按钮完成添加。在“可信区”对话框中选中某规则，单击“删除”按钮，即可删除该规则。

⑦ 黑白名单设置：单击“黑白名单”后面的“设置”超链接，打开“IP 包黑白名单设置”对话框，单击“增加”按钮，在弹出的对话框中为新规则命名，并指定 IP 地址或 IP 范围，单击“确定”按钮完成添加。同样，可以在图 7-12 所示窗口中单击“导入”按钮，导入已保存过的黑白名单规则文件。

2. 高级设置

（1）软件安全：包括瑞星密码和系统启动时账户模式两个功能。选择“高级设置”→“软件安全”命令进入设置页面，用户可以设置瑞星密码及其应用范围，还可以设置系统启动时的账户模式，如图 7-13 所示。

其中，瑞星密码功能可防止他人修改瑞星个人防火墙当前配置或工作状态，同时可防止病毒的恶意行为对计算机构成威胁。

图 7-13　软件安全设置界面

（2）“云安全”计划：“云安全”计划通过互联网，将全球瑞星用户的计算机和瑞星“云安全”平台实时联系，组成覆盖互联网的木马、恶意网址监测网络，能够在最短时间内发现、截获、处理海量的最新木马病毒和恶意网址，并将解决方案瞬时送达所有用户，提前防范各种新生网络威胁。每一位“瑞星全功能安全软件”的用户，都可以共享上亿瑞星用户的“云安全”成果。

设置方法：选择“高级设置”→“‘云安全’计划”命令进入设置页面，通过勾选“加入瑞星‘云安全’(Cloud Security)计划”复选框即可加入瑞星的“云安全”计划，如图 7-14 所示。

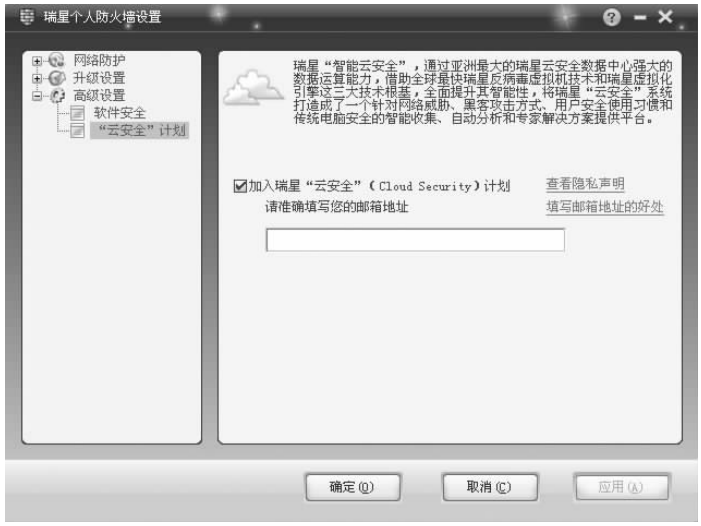


图 7-14 “云安全”计划设置界面

第四节 安全认证

在网上，双方要想谈一笔生意，任何一方都要鉴别对方是不是可信的，也就是要确定交易双方的身份。但是，如何才能保证所得到的公开密钥的正确性，即如何鉴别交易对方的真伪。为了解决这个问题，就引出了认证机制，其中涉及认证机构 CA 和数字证书。

一、认证中心

（一）认证中心概述

CA 认证系统的主要核心为认证中心(CA)。认证中心是一家能向用户签发数字证书以确认用户身份的管理机构。它负责审核、签发、管理、查询、吊销、备份、恢复所有实体所需的身份认证数字证书，是一种具有权威性、可信任性和公正性的第三方机构。在网络中，认证中心作为基础的安全设施向所有需要安全服务的对象(业务应用系统、硬件设备、企业用户、个人用户、执法机构等)提供安全服务，为用户制定完善的安全策略，确保用户数据的机密性、真实性、完整性、不可抵赖性及安全可靠的密钥管理。它所能提供的安全服务包括身份认证、数据完整性、机密性和抗抵赖性等基本服务，同时还包括电子签名、安全登录、时间戳安全通信、特权管理、制定并维护安全策略等广泛的 CA 数字证书应用服务。CA 的组成主要有：证书签发服务器，负责证书的签发和管理，包括证书归档、撤销和更新等；密钥管理中心，用硬件加密机产生公/私密钥对，提供 CA 证书的签发；目录服务器，负责证书和证书撤销列表的发布和查询。

CA 认证机构根据国家市场准入政策建设，由国家主管部门批准，具有权威性。CA 认证机构采用的密码算法及技术保障是高度安全的，具有可信任性。为了防止数字凭证的伪

造，认证中心必须公布其公共密钥或由更高级别的认证中心提供一个电子凭证来证明其公共密钥的有效性，后一种方法导致了多级别认证中心的出现。此外，CA 认证机构是不参与交易双方利益的第三方机构，具有公正性。CA 认证机构在《电子签名法》中被称做电子认证服务提供者。

（二）认证中心的分级结构

认证中心是分层分级负责发放和管理证书的权威机构。认证中心在大型网络环境下，采用树形分级结构，分层分级进行认证服务和认证证书的管理工作。上级认证中心负责签发和管理下级认证中心的证书，最下一级的认证中心直接面向最终用户。

1. 根认证中心

在各级认证机构组织中，将没有父认证中心的证书管理机构与认证机构称为根认证机构（root CA，RCA），也称为根认证中心。

2. 品牌认证中心

将品牌及品牌以下证书管理与认证机构称为品牌认证机构（brand CA，BCA），也称为品牌认证中心。品牌认证中心是根认证中心的下一级认证中心。

3. 区域认证中心

将各个地方的证书管理与认证机构称为区域认证机构（get-political CA，GPCA 或者 GCA，通常简称为 GCA），也称为区域认证中心。区域认证中心是品牌认证中心的下一级认证中心。

4. 持卡人认证中心

将管理与认证持卡人的认证机构称为持卡人认证机构（cardholder CA，CHCA 或者 CCA，通常简称为 CCA），也称为持卡人认证中心。持卡人认证中心是区域认证中心的下一级认证中心。

5. 商户认证中心

将管理与认证商户的认证机构称为商户认证机构（merchant CA，MCA），也称为商户认证中心。商户认证中心是区域认证中心的下一级认证中心。

6. 收单行支付网关认证中心

将管理与认证收单行支付网关的认证机构称为收单行支付网关认证机构（payment gateway CA，PGCA 或者 PCA，通常简称为 PCA），也称为收单行支付网关认证中心。收单行支付网关认证中心是区域认证中心的下一级认证中心。

这些认证中心是由上而下按层次（按级别）结构建立的。各级认证中心与认证证书的层级结构如图 7-15 所示。

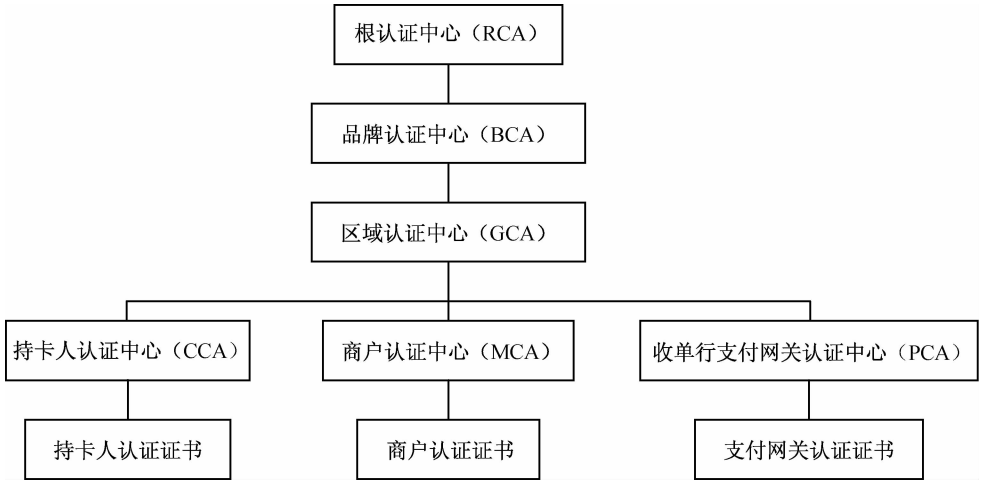


图 7-15　认证中心的层次结构

（三）认证中心的主要功能

1. 证书的颁发

认证中心的主要任务是受理认证证书的申请、颁发（签发）数字证书以及对数字证书进行管理。认证中心接收认证用户（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，并确定是否受理该数字证书申请。如果认证中心接收该数字证书申请，则进一步确定给用户颁发哪一种类型的证书。将新证书用认证中心的私人密钥签名以后，发送到目录服务器供用户下载和查询。为了保证信息的完整性，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

认证中心可以定期更新所有用户（包括下级认证中心和最终用户）的证书，或者根据用户的请求和需要进行更新。

3. 证书的查询

证书的查询可以分为两类：一类是证书申请的查询，是指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；另一类是用户证书的查询，该功能由目录服务器完成，目录服务器根据用户的请求返回相应的证书。

4. 证书的作废

一种情况是证书出了问题，需要申请作废。当由于用户的私钥泄密等原因造成用户需要申请证书作废时，认证中心根据用户的请求确定是否将该证书作废。另一种情况是证书已经过了有效期。这也是一种常见的证书作废的情况。认证中心将自动通过维护证书作废列表（certificate revocation list，CRL）来完成各种情况下的证书作废的管理。

5. 证书的归档

所有证书必须全部归档。证书具有一定的有效期，证书过了有效期之后就作废了，但是

不能将作废的证书简单地丢弃，因为有时可能需要认证以前在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。基于这些重要的需求，认证中心还具备管理作废证书和作废私人密钥的功能，将所有证书归档。

二、数字证书

由于在电子商务交易中，买卖双方在交易过程中是互不照面的，因此就需要用一种事物来表明自己的身份，以示自己是一个合法的用户或合法的商家。电子商务中的数字证书就是这样一种由权威机构发放的、用来证明身份的事物。

（一）数字证书概述

数字证书也称数字凭证、数字标识，是一个经证书认证机构数字签名的、包含用户身份信息及公开密钥信息的电子文件，它用电子手段来证实一个用户的身份和对网络资源访问的权限，是各实体（消费者、商户/企业、银行等）在网上进行信息交流及商务活动的电子身份证。在进行电子交易时，若双方出示了各自的数字证书，并用它来进行交易操作，则双方都不必担心对方身份的真实性。数字证书用于安全电子邮件、网上缴费、网上炒股、网上招标、网上购物、网上办公、电子资金移动等电子商务活动。

数字证书系统通过认证机构为公/私密钥对的持有者发放和管理数字证书。每一个数字证书包含了数字证书主体的一个公钥值和对其所做的无二义性的身份确认信息。其中，数字证书主体是指持有相应私钥的个人、设备或其他实体，且认证机构用自己的私钥给数字证书进行数字签名。数字证书的结构如图 7-16 所示。

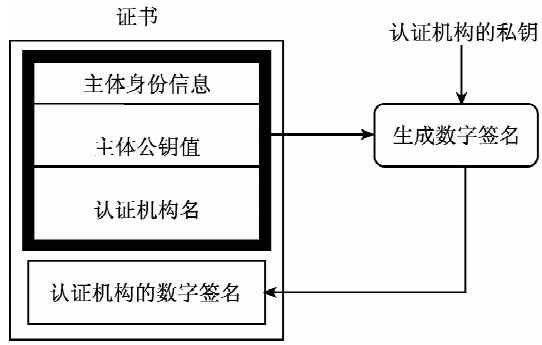


图 7-16　数字证书的结构

（二）数字证书的格式

数字证书中一般包含证书持有者的名称、公开密钥、认证机构的数字签名，此外还包括密钥的有效时间、认证机构的名称以及该证书的序列号等信息，如图 7-17 所示。交易伙伴可以利用数字证书来交换彼此的公开密钥。

国际电信联盟（ITU）在制定的 X.509 标准中对数字证书进行了详细的定义。一个标准的 X.509 数字证书包含以下主要内容：

（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序列号）。

（3）证书所使用的签名算法，如 RSA、DES 算法等。

（4）证书的发行机构名称。

（5）证书的有效期（通用的证书一般采用 UTC 时间格式）。

（6）证书所有人的名称。

（7）证书所有人的公开密钥。

（8）证书发行者的签名。

图 7-17　数字证书的格式

（三）数字证书的类型

1. 个人证书

个人数字证书是通过浏览器来申请获得的，认证中心对申请者的电子邮件地址、个人身份及信用卡号等进行核实后，发放个人数字证书，并将数字证书安置在用户所用的浏览器中或电子邮件的应用系统中，同时通知申请者。个人数字证书的使用方法集成在用户浏览器的相关功能中，只要在浏览器中进行相应的选择就可以了。

个人数字证书用于电子邮件时可起到类似密封和手写签名的作用，让接收方确定信件确实由用户发出，并为邮件的内容和附件加密，只有用户指定的接收方才能解密，从而防止了他人截获阅读的可能。

2. 服务器证书

服务器证书主要为网上的某个 Web 服务器提供凭证，拥有 Web 服务器的企业可以用具有凭证的互联网站点进行安全的电子交易。具有数字证书的 Web 服务器会自动地将其与客户端的 Web 浏览器的通信加密。服务器拥有者有了证书，就可以进行安全的电子交易了。

服务器证书的发放比较复杂。因为服务器证书是一个企业在网上的形象，是企业在网络空间信任度的体现，所以一个权威的认证中心对每一个申请者都要进行信用调查，包括企业的基本情况、营业执照、纳税证明等。

认证中心通过考查来决定是否发放或撤销服务器数字证书。一旦认证中心发放了数字证书，该服务器就可以安装认证中心提供的服务器证书，成功后即可投入服务。服务器得到数字证书后，就会有一对密钥（公开密钥和私有密钥），它与服务器之间是密不可分的。数字证书与这对密钥一起代表了该服务器的身份，是整个认证的核心。

3. 开发者证书

开发者证书通常为互联网中被下载的软件提供凭证。开发者证书又称代码签名数字证书。借助这种数字证书，软件开发者可以为软件做数字标识，在互联网上进行安全地传送。当用户从互联网上下载软件时，开发者证书与微软的 Authenticode（认证码）技术共同提供他们所需的软件信息和对该软件的信任。

上述三种证书中前两类是常用的凭证，第三类则用于较特殊的场合。大部分认证中心提供前两类凭证，能同时提供各类凭证的认证中心并不多。

三、数字签名

1. 数字签名的概念

为了鉴别文件或书信的真伪，传统的做法是相关人员在文件或书信上手写签名或印章，签名可以起到认证、核准、生效的作用。随着信息时代的来临，人们希望通过通信网络进行远距离贸易合同的传递，这就出现了文件真实性的认证问题，数字签名就应运而生了。如今，数字签名已经在电子邮件、电子转账、办公室自动化等系统中大量应用了。

所谓数字签名，就是通过某种密码运算生成一系列符号及代码组成电子密码进行签名，从而代替书写签名或印章。这种电子式的签名可进行技术验证，其验证的准确度是一般手工签名和图章的验证无法比拟的。数字签名是目前电子商务、电子政务中应用最普遍、技术最成熟、可操作性最强的一种电子签名方法。它采用规范化的程序和科学化的方法，用于鉴定签名人的身份以及对一项电子数据内容的认可。它还能验证文件的原文在传输过程中有无变动，确保传输电子文件的完整性、真实性和不可抵赖性。

2. 数字签名的原理

签名是针对某一文件的，数字签名也必须针对某一电子文件，加上签名者个人的数字标记形式，形成“数字签名”电子文件，而并非是“手工签名”类型的图形标志。这个电子文件从网上发送出去，接收方能识别签名，具有认证性。

数字签名采用双重加密的方法来实现，其工作原理如图 7-18 所示。

假如发送方想在通过互联网传递的信息中加上签名，可利用公开密钥系统来制作一个数字签名。其制作过程如下：

（1）发送方先利用自己的私人密钥产生一个数字签名，加密后的信息便成了一个已署名的信息。

（2）发送方将该署名的信息通过互联网传送给接收方。

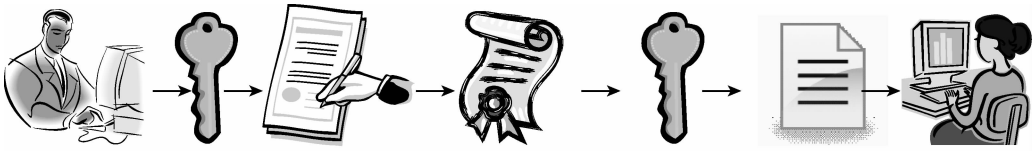


图 7-18　数字签名的工作原理

数字签名的核对过程如下：

(1) 接收方从互联网上收到发送方的信息及数字签名。

(2) 接收方向密钥管理员索取发送方的公开密钥。

(3) 接收方利用该公开密钥来核对数字签名，方法是利用该公开密钥将信息解密。如果解密后的信息等于原来的信息，则证明该信息是由发送方传送来的，因为只有发送方拥有可以制造该数字签名的私人密钥。因此，发送方不能否认曾传送该信息给接收方，这就是不可抵赖性。假如信息或数字签名在传送过程中被修改，接收方便会发觉解密后的数字签名跟原来的信息不符。

四、数字水印

1. 数字水印的概念

随着高质量图像输入/输出设备的发展，特别是精度超过 1 200 dpi 的彩色喷墨、激光打印机和高精度彩色复印机的出现，使伪造货币、支票以及其他票据变得更加容易。据统计，每年伪造的美元有 20 亿，假信用卡使美国银行损失达 20 亿美元，全世界的假护照有 300 万份。

在从传统商务向电子商务转化的过程中，会出现大量过渡性的电子文件，如各种纸质票据的扫描图像等。即使在网络安全技术成熟以后，各种电子票据也还需要一些非密码的认证方式。数字水印技术可以为各种票据提供不可见的认证标志，从而大大增加了伪造的难度。

数字水印(digital watermark)技术是指用信号处理的方法在合法文本中嵌入隐蔽的标记，这种标记通常是不可见或不可听的，只有通过专用的检测器或阅读器才能提取，从而使用户只能在屏幕上阅读合法文本。一旦该文本被复制，则该水印会在文本中央明显地显示版权信息，要想正常地阅读复制的文本，只有向有关权利人申请合法授权。采用数字水印技术，既不损害原作品，又达到了版权保护的目的。目前，用于版权保护的数字水印技术已经进入了初步实用化阶段。

据中国防伪技术协会预测，未来几年，防伪产品的市场总价值每年会超过 300 亿元。除去传统的防伪油墨，以及基于互联网技术的电话防伪和网上电子认证等防伪领域，用于标签和材料的防伪支出每年将在 75 亿元左右。数字水印技术开辟了一条崭新的信息安全途径，它的不可感知的隐蔽性和抵抗各种攻击的能力，可以实现数字产品的完整性保护和篡改鉴定，还可用于数字防伪。

2. 数字水印的特点

(1) 隐蔽性:在数字作品中嵌入数字水印不会引起明显的降质,并且不易被察觉。

(2) 隐蔽位置的安全性:水印信息隐蔽于数据而不是文件头中,文件格式的变换不会导致水印数据的丢失。

(3) 稳健性:数字水印在经历多种无意或有意的信号处理后,如信道噪声、滤波、数模与模数转换、重采样、剪切、位移、尺度变化以及有损压缩编码等,仍能保持完整性或仍能被准确鉴别。

第五节　SSL 协议

一、SSL 协议简介

SSL 协议是由网景公司在推出 Web 浏览器首版的同时提出的安全通信协议,目前已有 SSL 2.0 和 SSL 3.0 两个版本。SSL 协议采用公开密钥技术,目标是保证两个应用程序间通信的保密性和可靠性,可在服务器和客户机两端同时实现。现在 SSL 协议已经成为 Internet 上保密通信的工业标准。SSL 协议制定了一种能在应用程序协议(如 HTTP、TELNET、NNTP、FTP)和 TCP/IP 之间提供安全性分层的机制,能为 TCP/IP 连接提供数据加密、服务器认证、消息完整性以及可选的客户机认证。SSL 协议与相关网络层的关系如图 7-19 所示。

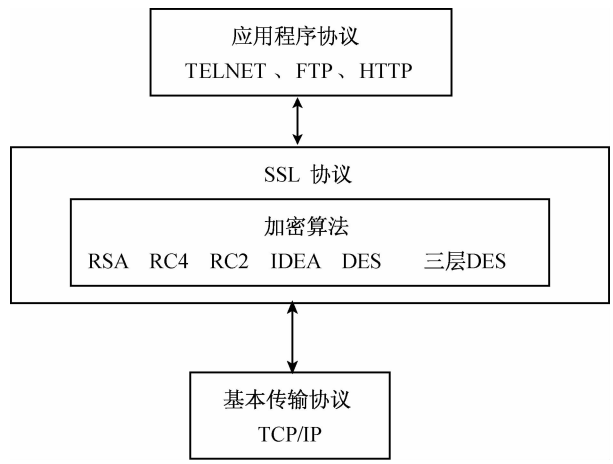


图 7-19　SSL 协议与相关网络层的关系

SSL 协议作用在应用层和传输层。它不是单个协议,而是两层协议,包括套接层 SSL 记录协议和应用层 SSL 握手协议、SSL 更改密文规范协议和 SSL 告警协议。

(1) 记录协议。这个协议用于交换应用层数据。应用程序消息被分割成可管理的数据块,还可以压缩,并应用一个消息认证代码(MAC),然后把结果加密传输。接收方接收到数据后对它解密,校验 MAC,解压缩并重新组合它,把结果提交给应用程序协议。

(2) 握手协议。这个协议负责协商用于客户机和服务器之间会话的加密参数。当一个SSL 协议客户端和服务器第一次开始通信时,它们在一个协议版本上达成一致,选择加密算法,选择相互认证,并使用公钥技术来生成共享密钥。

(3) 更改密文规范协议。它是使用 SSL 记录协议的、最简单的 SSL 相关协议之一。这个协议由单个报文组成,该报文由值为 1 的单个字节组成。这个报文的唯一目的就是使挂起状态被复制到当前状态,改变这个连接将要使用的密文簇。

(4) 告警协议。这个协议用于指示在何时发生了错误或两个主机之间的会话在何时终止。

HTTPS 是以安全为目标的 HTTP 通道,简单地讲是 HTTP 的安全版,即 HTTP 下加入 SSL 层。HTTPS 的安全基础是 SSL 协议。在 URL 前用 HTTPS 协议,就意味着要和服务器建立一个安全的连接,这时浏览器状态栏会显示一个锁,表示已建立安全连接。

二、SSL 协议的工作过程

SSL 协议的工作过程可分为六个步骤:

(1) 连接阶段:客户通过网络向服务商打招呼,服务商回应,建立安全会话。

(2) 交换密码阶段:客户与服务商之间交换双方认可的密码。

(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:客户与服务商之间交换结束信息。

SSL 协议在信息传递上的安全性,刚好适应了电子支付的需要,又由于构架简单、处理步骤少、速度快,所以虽然存在较大的安全性漏洞,但依然被广泛地应用在信用卡在线支付模式中。

第六节 SET 协议

一、SET 协议概述

1995 年 10 月,包括万事达公司、网景公司和 IBM 公司在内的联盟开始着手进行安全电子支付协议(SEPP)的开发。此前不久,VISA 和微软组成的联盟已经开始开发另外一种不同的网络支付规范,称为安全交易技术(STT)。这样便出现了一种混乱的局面,即两大信用卡组织万事达和 VISA 分别支持独立的网络支付解决方案。这种局面持续了数月,直到 1996 年 1 月,这些公司才宣布它们将联合开发一种统一的系统,称为安全电子交易(SET)。

SET 是一个通过开放网络进行安全资金支付的技术标准,由 VISA 和万事达联合 IBM、RSA、微软等信息产业公司在 1996 年共同制定,于 1997 年联合推出。由于它得到了 IBM、HP、微软等很多大公司的支持,已成为事实上的工业标准,目前已获得 IETF 标准的认可。

SET 协议主要用于信用卡网上支付的安全。它采用 RSA 双钥体系对通信双方进行认

证，选用 DES 等标准对称密钥加密算法进行信息的加密传输，利用双重签名机制确保三方通信，使用 Hash 算法来鉴别消息的真伪及有无篡改。SET 支付系统主要由持卡人、商户、发卡行、收单行、支付网关及 CA 六部分组成。其中，CA 是 SET 体系中的关键，支付网关是传递信息支付的枢纽。

二、SET 协议的运行原理

对持卡人来说，SET 协议是透明的，他们只需确认订单已发送给商户就行了，其他功能由软件自动执行。持卡人选择商品并下了订单后，商户会用一份自己证书的副本作为给持卡人的答复。持卡人证实卖主身份，然后用对称密钥加密订单，并用商户的公钥加密对称密钥。这样就只有商户可以解密这个对称密钥。订单中涉及财务数据的部分（结算卡号码）也可用同样的方式加密，但这次使用的是银行的公钥（商户不会见到结算卡的号码）。订单的第三部分是一个消息摘要，它能向商户证明订单没有被篡改，和持卡人发送时的订单完全一样。商户使用自己的私钥解密对称密钥，然后解密订单。它将结算信息连同订单副本一起转发给银行，因为它要依赖银行对交易进行认可。银行证实持卡人的身份和消息的完整性，并打开结算信息，证实结算的金额是该笔交易的金额，且是付给该商户的。银行还要检查商户的信用额度，保证交易可以进行，并准许商户将交易进行下去。最后商户将订购的商品发给持卡人。SET 协议的运行原理如图 7-20 所示。

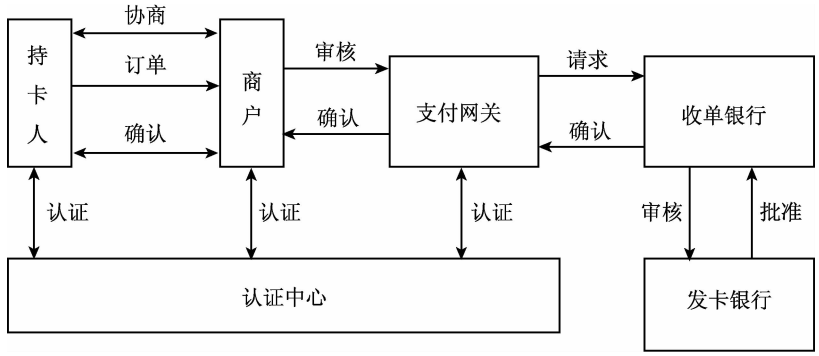


图 7-20　SET 协议的运行原理

SET 协议的工作流程主要包括以下几个步骤：

（1）消费者在网上商城选定商品并下电子订单。

（2）通过电子商务服务器与网上商户联系，网上商户作出应答，告诉消费者订单的相关情况（是否改动以及关于购买属性的关键字段）。

（3）消费者选择付款方式，确认订单，签发付款指令（此时 SET 协议介入）。

（4）在 SET 协议中，消费者必须对订单和付款指令进行数字签名，同时利用双重签名技术保证商家看不到其账号信息。

（5）在线商店接受订单后，向消费者所在银行请求支付认可，信息通过支付网关到收单银行，再到电子货币发行银行确认，批准交易后，返回确认信息给在线商店。

（6）在线商店发送订单确认信息给消费者，消费者端软件可记录交易日志，以备将来查询。

（7）在线商店发送货物。

三、SET 协议与 SSL 协议的比较

支付系统是电子商务的关键，SSL 协议和 SET 协议是两种重要的通信协议，每一种都提供了通过 Internet 进行支付的手段。SET 协议与 SSL 协议主要从以下几个方面进行比较：

1. 认证要求方面

SET 协议认证的安全需求较高，因此所有参与 SET 协议交易的成员都必须先申请数字证书来识别身份，并且 SET 协议解决了客户与银行、客户与商家、商家与银行之间的多方认证问题，而在 SSL 协议中只有商家服务器需要认证，客户端认证是有选择性的。

2. 对消费者而言

SET 协议保证了商家的合法性，并且保证用户的信用卡信息不会被窃取。SET 协议替消费者保守了更多的秘密使其在线购物更加轻松，而 SSL 协议则缺少对持卡人的认证。

3. 安全性

安全性是网上交易最关键的问题。一般公认 SET 协议的安全性较 SSL 协议高，主要原因是：在整个交易过程中，包括持卡人到商店、商店到付款转接站再到银行网络，都受到严密的保护；而 SSL 协议的安全范围只限于持卡人到商家的信息交流。

采用 SSL 协议，购买者将冒以下风险：购买者无法保证商家能够对他们的信用卡信息保密，无法保证商家是该支付卡的特约商户；商家在一个在线交易中同样要冒风险，如同进行邮件和电话订购交易一样，商家无法保证购买者就是该信用卡的合法拥有者。

4. 用户接口

SET 协议中客户端需安装专门的电子钱包软件，在商家服务器和银行网络上也需安装相应的软件，而 SSL 协议中浏览器和 Web 服务器已内置所需组件，无须安装专门软件。

5. 采用比率

由于 SET 协议的设置成本较 SSL 协议高许多，且进入国内市场的时间尚短，因此目前是 SSL 协议的普及率高，约占 80%。但是，由于网上交易的安全性需求不断增强，SET 协议的市场占有率将会有较大幅度的提高。

6. 处理速度

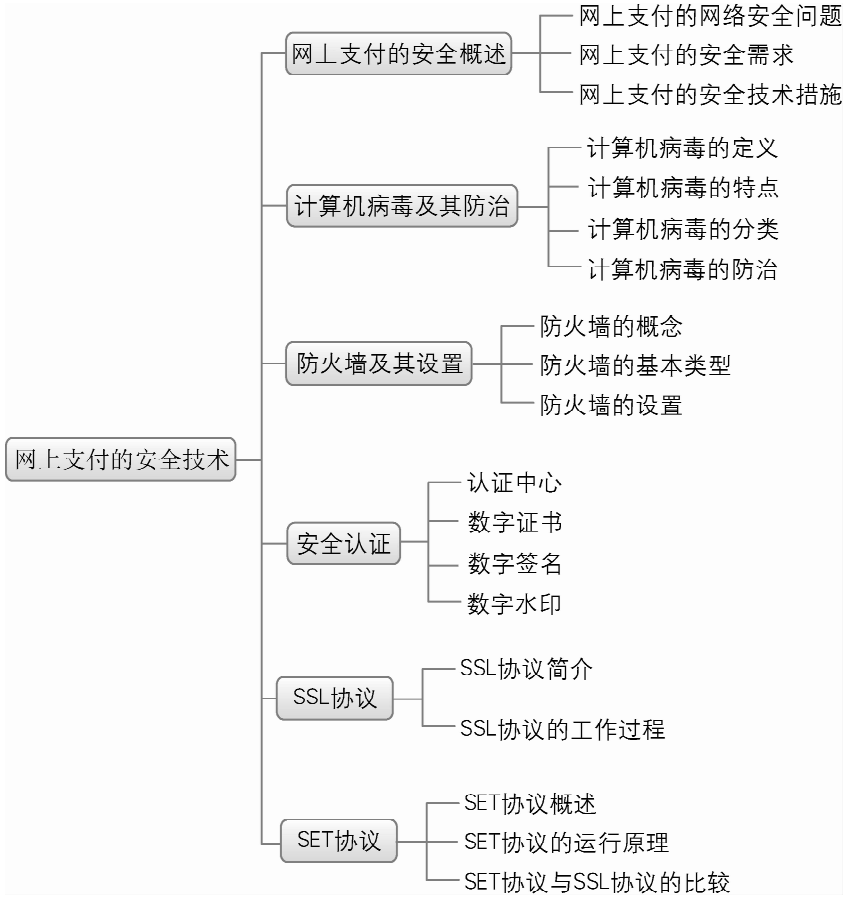
SET 协议非常复杂、庞大，处理速度慢，而 SSL 协议则简单得多，处理速度比 SET 协议快。

引例解析

网络支付的安全威胁主要有以下几个方面：窃取、篡改、冒用身份、网络支付系统的不稳定性、不承认或抵赖已经做过的交易。

基于用户对网上支付的安全性的需求，网上支付的安全问题主要从技术、法制、道德规范和管理策略等多个方面来解决。其中，网上支付的安全技术措施主要包括如下几个方面：安全的网络平台、数据加密、数字签名、安全协议。

本章小结



综合训练

一、思考练习

1. 简述网上支付的安全风险和安全要求。
2. 什么是计算机病毒？计算机病毒有哪些特点？
3. 如何防治计算机病毒？
4. 什么是防火墙？防火墙有哪些类型？
5. 简述认证中心的功能。
6. 什么是数字证书？数字证书有哪些类型？

7. 简述 SSL 协议的工作过程。

8. 简述 SET 协议的工作原理。

二、案例分析

阿里巴巴与网上支付安全

阿里巴巴电子商务平台的迅速崛起，引发了电子商务界的剧烈变化。阿里巴巴的出现，改变了大部分生意人的经商习惯，上网的人相继经历了“网民”—“网友”—“网商”等一系列转变。这也标志着经商模式的转变，传统经商模式正在被电子商务所替代。足不出户做生意，也就成为了可能。可以毫不避讳地说：未来的世界是网络的世界，未来的商界也一定是网络营销的世界。

但是，网络上信息瞬息万变，风险与商机并存，在线支付的使用及安全问题成了每个商人考虑的首要问题。怎么样才能让自己的资产在网海中安全地运用，从而达到资产增值的目的？这是一个一直困惑电子商务界的大问题。然而，阿里巴巴从大局出发，以创新为前提，首创在线安全支付工具——支付宝。这就意味着，在线支付的资金安全问题得到了彻底的解决。

支付宝公司从 2004 年建立开始，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，为构建健康的互联网环境迈出了非常有意义的一步。

支付宝提出的建立信任、化繁为简、以技术的创新带动信用体系完善的理念，深得人心。短短 3 年时间，用户覆盖了整个 C2C、B2C 及 B2B 领域。目前，除淘宝和阿里巴巴外，支持使用支付宝交易服务的商家已经涵盖了虚拟游戏、数码通信、商业服务、机票等行业。这些商家在享受支付宝服务的同时，更是拥有了一个极具潜力的消费市场。

支付宝在电子支付领域稳健的作风、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银行等合作伙伴的认同。目前，支付宝和工商银行、农业银行、建设银行、招商银行、上海浦发银行等国内各大商业银行，以及中国邮政、VISA 国际组织等各大机构，均建立了良好的战略合作关系。支付宝不断根据客户需求推出创新产品，成为了金融机构在电子支付领域最为信任的合作伙伴。

问题

为什么支付宝能使阿里巴巴实现网上支付的安全？

网上支付的安全技术

【实训目的】

网上支付的安全技术是电子商务安全的技术保障。通过此次实训，了解网上支付的安全技术措施，熟悉防病毒技术和个人防火墙的设置以及安全认证和安全协议技术。

【实训内容与要求】

(1) 下载并安装瑞星杀毒软件，查杀系统所有资源。

(2) 下载并安装江民防火墙，参照帮助文档设置防火墙。

(3) 浏览上海市数字证书认证中心网站(http://www.sheca.com)，了解数字证书的类型及每一种证书申请的流程。

(4) 访问中国金融认证中心网站(http://www.cfca.com.cn)，了解该认证中心发放哪些数字证书，试从该网站下载一份数字证书。

【成果与检验】

为自己的计算机设置防火墙，访问相关的认证中心，并下载一份数字证书。