# 第 7 章　支付协议与结算认证系统


通过对本章内容的学习，要了解电子商务存在哪些风险，SSL 协议的优点及应用，SET 协议的应用，SSL 和 SET 协议的比较，客户认证主要包括哪些方面，认证中心的功能，证书的发放。重点要掌握电子商务的安全要求，SSL 安全协议的基本概念和服务，SSL 安全协议的结构及运行步骤，SET 协议的目标、工作原理，SET 支付系统的组成，SET 安全协议涉及的范围以及各种安全认证技术，数字证书的分类，证书如何申请 CA：Certificate Authority，电子商务认证中心 CA：Client Authentication，客户认证个人证书：Personal Digitali，DRA：Registration Authority，注册审批机构等内容。

## 教学要求

| 知识要点 | 能力要求 | 相关知识 |
| --- | --- | --- |
| 网络支付协议其他协议 | (1) 熟悉 SSL 网络传输安全协议的内容<br>(2) 熟悉 SET 协议的内容和应用领域<br>(3) 了解 SSH、SOCKS、S-HTTP 等协议 | (1) SSL 整体结构和运行方式<br>(2) 各类支付协议及未来的发展趋势 |
| 结算认证系统 | (1) 掌握 CA 认证的基本体系与功能<br>(2) 熟悉各类数字证书的运用 | (1) 认证中心功能的实现<br>(2) 安全认证技术的内容 |
| 中国电信CA认证系统 | 中国电信 CA 认证系统的技术特点 | 学会使用中国电信 CA 认证 |

## 贝宝(Paypal)


Paypal 是最早从事第三方支付的企业之一，创办于 1998 年。Paypal 是第三方支付行业中，迄今全球最成功的案例。仅 2006 年三季度，Paypal 的交易量即高达 91 亿美元。消费者网上购物付款时，因为要向素未谋面的商家提供自己的银行账户信息，会感到担心。有了 Paypal，消费者只需放少量的钱，通过 Paypal 的账户付款即可。Paypal 所起的作用，便是在银行账户与商家之间搭起桥梁。

2005 年 7 月 11 日，贝宝中国(Paypal China)网站(www.paypal.com.cn)正式开通，标志着贝宝正式登录中国市场。与此同时，贝宝与银联电子支付服务有限公司(ChinaPay)建立战略伙伴关系，在支付渠道和商户共享方面开展全面的合作。贝宝与银联电子支付合作，将使中国用户能用 15 家银行的 20 多种银行卡，通过贝宝进行安全、快捷、便利的网上支付。

1. 贝宝为买家和卖家提供的服务

贝宝是一种在线付款与收款的方式。

对于买家而言，用贝宝付款和收款是完全免费的，买家可以使用网上银行账户付款，买家的账户信息会被安全保存，绝对不会透露给任何其他人。

对于卖家而言，接受大多数主要的银行卡和其他付款类型。贝宝对卖家是完全免费的。操作很容易，立即注册，开始快速接受付款。

2. 贝宝账户注册方便

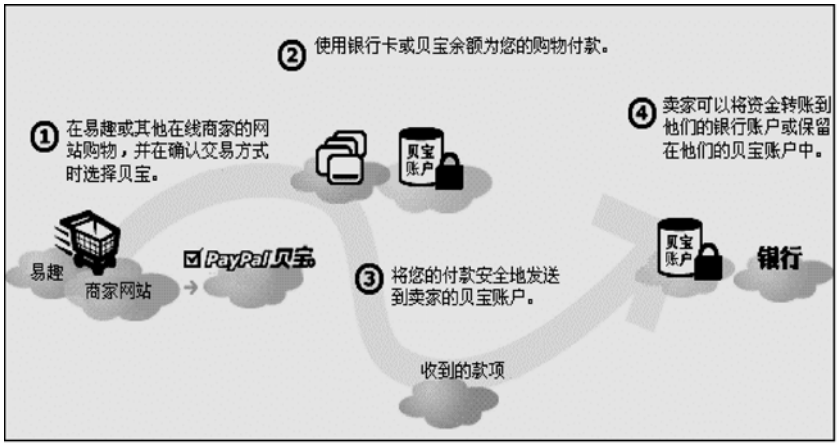
(1) 任何人只要有一个电子邮件地址，就可以使用贝宝在线发送和接收款项。

(2) 企业账户，以公司、单位名称或个体工商户字号开设的贝宝账户。企业账户可以设立不同级别的多用户访问权限。

注册一个贝宝账号后，该地址将是用户的用户名，可以通过它进行转账、支付和收款。Paypal 海外在线支付目前已经与中国 14 家银行进行了整合，可以支持 24 种中国银行卡，因此可以通过银行卡方便地往贝宝账户上充值，也可以把贝宝账户里的钱转到任意一张银行卡上，在此过程中，不需要向贝宝提供用户的银行账户信息。有了贝宝，付款和收款都是即时的，无疑提高了买卖双方的交易效率。

3. 贝宝使得付款变得轻松容易

贝宝支付流程，如下图所示。




贝宝除了给网上的买家、卖家带来了安全、方便、快捷的支付体验外，一些时尚的年轻人甚至在网上交易之余，把“贝宝”当作了自己网络生存的“理财工具”。

与以前常用的几种支付方式相比，贝宝给网络交易带来方便。以前经常使用传统的邮局汇款、银行汇款、网上银行等，为了付款和收款，依然需要到邮局、银行排队等候，还不得不在网上透露自己的银行账(卡)号，事实上并没有做到真正的“足不出户”。同时，安全上也存在着隐患。贝宝给网络交易带来安全、方便、快捷的支付。

## 章前导读

基于互联网的电子商务已经成为研究和应用的热点，而支付处理作为电子商务的一个重要组成部分，涉及 Internet 上消费者与商家之间的交易安全。为保证支付软件的可靠实现，本

章将形式化方法应用于支付协议实现模型的分析，如简单网络支付协议和普遍流行的加密技术加以实现 CA 认证系统。

## 7.1 电子支付安全技术概述

网上支付专用网络的软件系统是特殊设计的，其应用单位是银行与银行(或非银行金融机构)、银行与商家之间。它具有专用系统和软件的高度安全性。使用专用网络系统进行电子货币支付在安全上有严格要求，其发送资金信息的报文是专门设计的，还必须在用户认证、安全传输、数据验证等方面进行控制。

### 7.1.1 电子支付网络与密码系统

随着经济的发展，支付已经成为日常商业活动中使用最为普遍和最为常用的一种支付手段和结算工具。但是，随着电子支付使用的日益广泛和普及，银行的手工处理支付的工作已被电子支付所替代，量越来越大，提高了工作效率和结算速度，还有利于通存通兑，提高防伪功能。

1. 电子支付密码原理及业务流程

电子支付密码又称电子印鉴，是一种先进的防伪及身份识别技术，目前已被广泛应用于银行支票防伪、同城实时清算等系统中。

电子支付密码器外形如电子计算器，是一种小巧、便于携带的小型设备。当用户要开具票据时，只要在电子支付密码器上输入票据的号码、日期、金额等要素，电子支付密码器就会计算出一串数字并且显示出来，用户将这串数字抄写在票据上交给银行，银行将票据上的同样的要素输入计算机，并且根据用户账号找到相对应的用户预留密钥，然后执行与电子支付密码器相同的加密计算，将计算出的结果与票据上的数字串进行比较就可知票据的真伪。

1) 支付密码系统实现的基本原理

电子支付是一种通信频次大、数据量小、实时性要求高、分布面很广的通信行为，因此电子支付的网络平台应是交互型的、安全保密的、可靠的通信平台，必须面向全社会，对所有公众开放。电子支付的网络平台有 PSTN、公用/专用数据网、Internet、EDI 等。最早的网络平台是 PSTN(公共交换电话网，Public Switched Telephone Network)、X.25 和 X.400 网络，后来是 X.435、X.500 等，这些网络的普及面明显跟不上业务发展的需要。当前电子支付的网络平台主要是 Internet，现代化大容量的电子支付需要数字化、安全、可靠、快捷的网络平台来支撑。

支付密码系统实现的基本原理是用户在银行开设账户的同时，配备一个支付密码器，银行在支付密码器中设置了与银行校验机数据库中一致的加密算法和密钥。用户在日常开具兑付票据时，将票据上的票据种类、票据号码、账号、签发日期、金额诸要素输入到支付密码器中计算出一组数字密码即支付密码，并抄录或打印在票据上表明签发人的身份。

2) 支付密码系统的业务流程

收款行在收到一张客户签发的结算票据时，不管该票据的付款行是否与收款行在同一系

统、同一行处、系统都能通过计算机网络系统使该票据的合法性和真伪得到付款行认证，使得票据实现实时抵用。显然，为实现上述目标，建立一个可靠的计算机网络系统是必不可少的；另一个重要问题是解决当付款行在没有票据实物的情况下如何验证其真伪。

(1) 客户签发结算票据的支付系统原理框图，如图 7.1 所示。

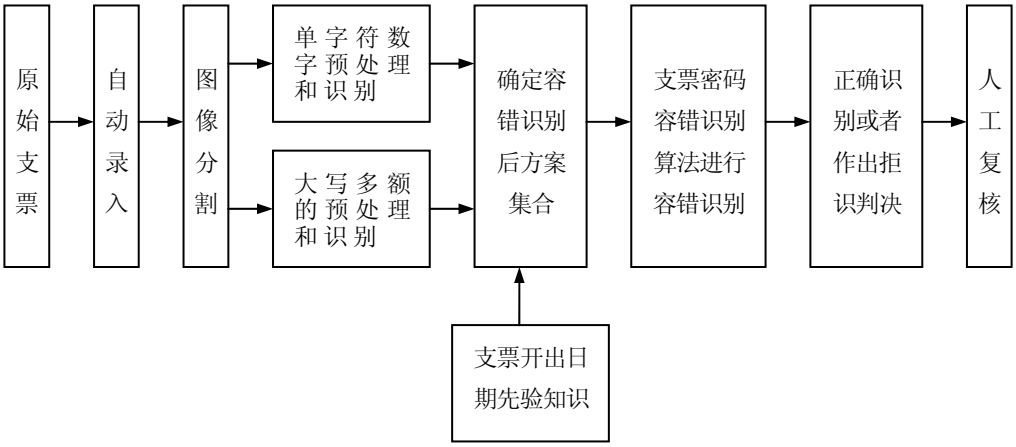



图 7.1　包含汉字和大写数字的系统原理框图

(2) 客户申请使用支付密码器。将票据的诸要素输入支付密码器，由支付密码器计算出该票据的支付密码，将支付密码填写在结算票据的特定位置。某一银行向用户提供电子支付密码器的流程如图 7.2 所示。

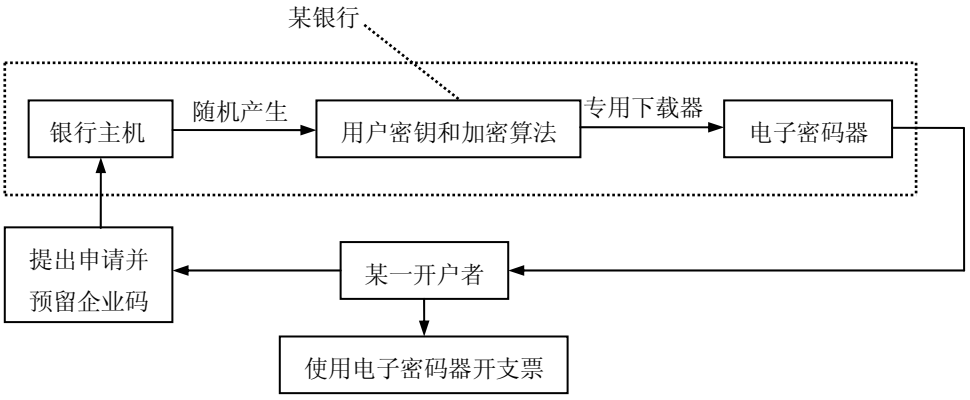



图 7.2　银行向客户提供电子支付密码器的流程

(3) 支付密码的认证和自动容错流程。银行受理该结算票据后，将票据的诸要素及支付密码输入计算机，通过自动容错处理后，计算机将所有输入要素送交该结算票据的开户行票据校验机，进行票据的真伪核验，并返回票据的核验结果，如图 7.3 所示。

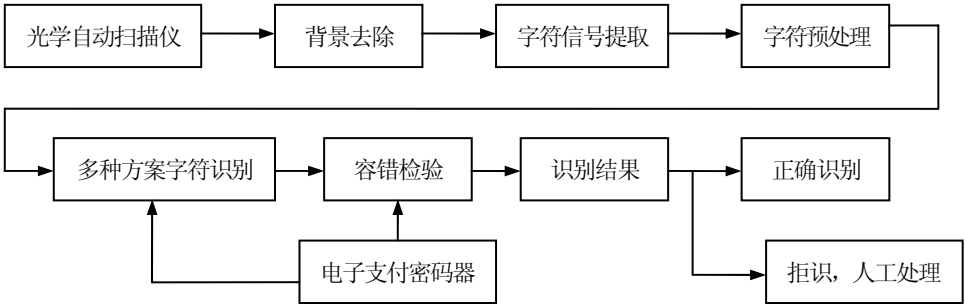



图 7.3　基于电子支付密码的自动容错识别系统处理流程

2. 电子支付密码系统的模式

在使用电子支付密码系统方面，各银行针对自身的实际情况，建立了不同的应用模式。主要有下列几种。

(1) 密码签模式。由银行按照支票号码、用户账号等参数进行一次加密计算得到一组支付密码，并将其打印出来交给用户。在使用时，用户将这些支付密码抄写到支票上即可。其优点是简单，成本低。缺点是防伪能力差。

(2) 单一的支付密码器。这种模式已经具备了典型的电子支付密码器应用的各种要素。用户使用电子支付密码器，输入支票号码、金额、日期等要素，将电子支付密码器计算出的结果抄写到支票上，然后由银行执行同样的运算以验证真伪。用户的预留密钥及加密算法均存放于电子支付密码器中。

(3) 使用 IC 卡的支付密码器。IC 卡也称智能卡，在一张名片大小的卡片内安装了一小片集成电路，这片电路能够存储数据，进行复杂的数学计算，其功能相当于一台超小型的计算机。具备运算能力的 IC 卡也称为 CPU 卡。

在使用 IC 卡的电子支付密码器模式中，采用了双重加密手段。由于 IC 卡具有强大的加密计算能力和堡垒式的防止非授权访问能力，人们使用 IC 卡的加密运算功能对由支付密码器计算出的结果进行第二次加密计算。即使支付密码器的用户密钥及银行加密算法被攻破，犯罪分子仍然无法获得所有的核心机密数据，也无法达到伪造支票数据的目的。

3. 数据加密技术

在计算机网络用户之间进行通信时，为了保护信息不被第三方窃取，必须采用各种方法对数据进行加密。最常用的方法就是私有密钥加密方法和公开密钥加密方法。

1) 私有密钥加密技术

私有密钥加密技术的原理是信息发送方用一个密钥对要发送的数据进行加密，信息的接收方能用同样的密钥解密，而且只能用这一密钥解密。由于这对密钥不能被第三方知道，所以叫做私有密钥加密方法。由于双方所用加密和解密的密钥相同，所以又叫做对称密钥加密法。最常用的对称密钥加密法叫做 DES(Data Encryption Standard)算法。

例如，甲乙两公司之间进行通信，每个公司都持有共同的密钥，甲公司要向乙公司订购钢材，用此共用的密钥加密，发给乙公司，乙公司收到后，同样用这一共用密钥解密，就可以得到这一份订购单，加密示意图如图 7.4 所示。

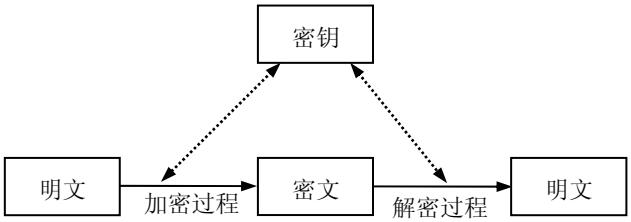



图 7.4　私有密钥加密示意图

由于对称密钥加密法需要在通信双方之间约定密钥，一方生成密钥后，要通过独立的安全的通道送给另一方，然后才能开始进行通信。这种加密方法在专用网络中使用效果较好，并且速度快。因为通信各方相对固定，可预先约定好密钥。

具体在电子商务网络支付应用时，作为银行内部专用网络传送数据一般都采用 DES 算法加密，比如传送某网络支付方式用的密码。军事指挥网络上一般也常用这种密钥加密法。

但是它也有缺点，与多人通信时，需要太多的密钥，有时不可能给每一对用户配置一把密钥，所以电子商务只靠这种加密方式是不行的，这就必须采用公开密钥加密法(Public Key Cryptography)。

2) 公开密钥加密技术

公开密钥加密法的加密和解密所用的密钥不同，所以叫非对称(Asymmetric Cryptography)密钥加密技术。其原理是共用两个密钥，在数学上相关，称作密钥对。用密钥对中任何一个密钥加密，可以用另一个密钥解密，而且只能用此密钥对中的另一个密钥解密。

商家采用某种算法(秘钥生成程序)生成了这两个密钥后，将其中一个保存好，叫做私人密钥(Private Key)，将另一个密钥公开散发出去，叫做公开密钥(Public Key)。任何一个收到公开密钥的客户，都可以用此公开密钥加密信息，发送给这个商家，这些信息只能被这个商家的私人密钥解密。只要商家没有将私人密钥泄漏给别人，就能保证发送的信息只能被这位商家收到。

公开密钥加密法的算法原理是完全公开的，加密的关键是密钥，用户只要保存好自己的私人密钥，就不怕泄密。著名的公开密钥加密法是 RSA 算法。RSA 是这个算法 3 个发明人(Rivest，Shamir 和 Adleman)姓名首字母。

非对称密钥加密法是后面要讲的数字签名手段的技术基础之一，可以用来解决在电子商务中如网络支付结算中“防抵赖”“认证支付行为”等作用。这可以从下面对公开密钥加密示意图看出来，如图 7.5 所示。

非对称密钥加密的作用是两位用户之间要互相交换信息，需要各自生成一对密钥，将其中的私人密钥保存好，将公开密钥发给对方。交换信息时，发送方用接收方的公开密钥对信息加密，只能用接收方的私人密钥解密。它们之间可以在无保障的公开网络中传送信息，而不用担心信息被别人窃取。

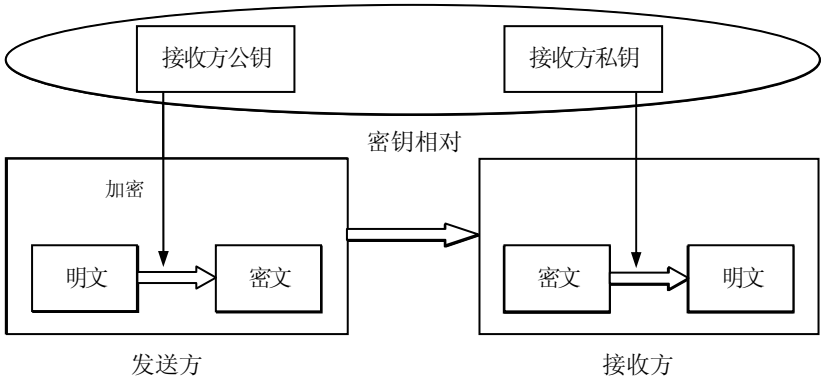



图 7.5　公开密钥加密技术示意图

3) 数字信封技术

对称密钥加密技术和非对称密钥加密技术各有优缺点，见表 7-1。

表 7-1　对称密钥和非对称密钥技术对比

| 特　性 | 对　称 | 非 对 称 |
|---|---|---|
| 密钥的数目 | 单一密钥 | 密钥是成对的 |
| 密钥种类 | 密钥是秘密的 | 一个私有、一个公开 |
| 密钥管理 | 简单、不好管理 | 需要数字证书及可靠第三者 |
| 相对速度 | 非常快 | 慢 |
| 用途 | 用来做大量资料的加密 | 用来做加密小文件或对信息签字等不太严格保密的应用 |

非对称(公开)密钥的强大的加密功能使它具有比对称密钥更大的优越性。但是，由于非对称密钥加密比对称密钥加密速度慢得多，在加密数据量大的信息时，要花费很长时间。而对称密钥在加密速度方面具有很大优势。所以，在网络交易中，对信息的加密往往同时采用两种加密方式，将两者结合起来使用，这就是数字信封技术。

数字信封(Digital Envelope)的原理是对需传送的信息(如电子合同、支付指令)的加密采用对称密钥加密法；但密钥不先由双方约定，而是在加密前由发送方随机产生；用此随机产生的对称密钥对信息进行加密，然后将此对称密钥用接收方的公开密钥加密，准备定点加密发送给接收方。这就好比用“信封”封装起来，所以称作数字信封(封装的是里面的对称密钥)，如图 7.6 所示。

接收方收到信息后，用自己的私人密钥解密，打开数字信封，取出随机产生的对称密钥，用此对称密钥再对所收到的密文解密，得到原来的信息。因为数字信封是用消息接收方的公开密钥加密的，只能用接收方的私人密钥解密打开，别人无法得到信封中的对称密钥。

在使用对称密钥加密时，密钥的传递及密钥的更换都是问题。采用数字信封的方式，对称密钥通过接收方的公开密钥加密后传给对方，可以保证密钥传递的安全。而且此对称密钥每次由发送方随机生成，每次都在更换，更增加了安全性。一些重要的短小信息，比如银行账号、密码等都可以采取数字信封传送。

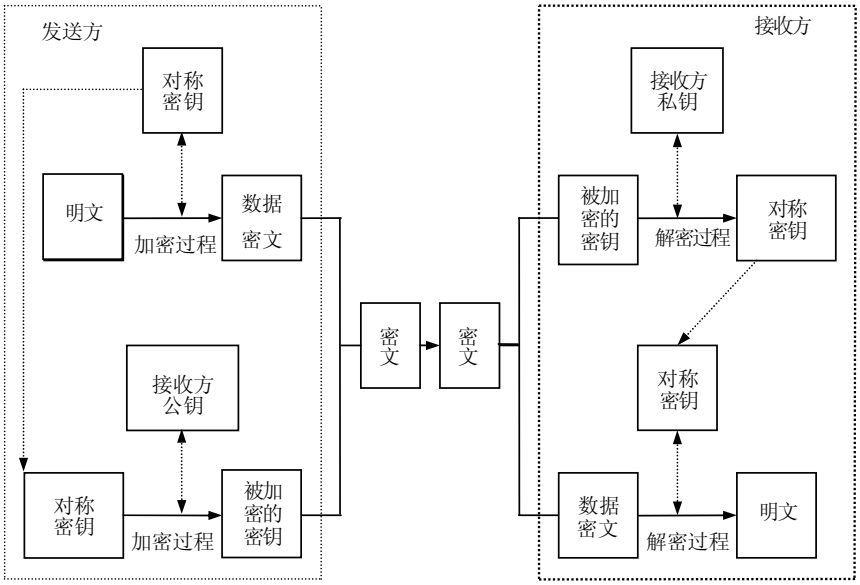



图 7.6　数字信封技术工作原理

4. 数字摘要与数字签名技术

1) 数字摘要技术

数字摘要主要采用的方法是用某种算法对被传送的数据生成一个完整性值，将此完整性值与原始数据一起传送给接收者，接收者用此完整性值来检验消息在传送过程中有没有发生改变。这个值由原始数据通过某一加密算法产生的一个特殊的数字信息串，比原始数据短小，能代表原始数据，所以称作数字摘要(Digital Digest)，如图 7.7 所示。

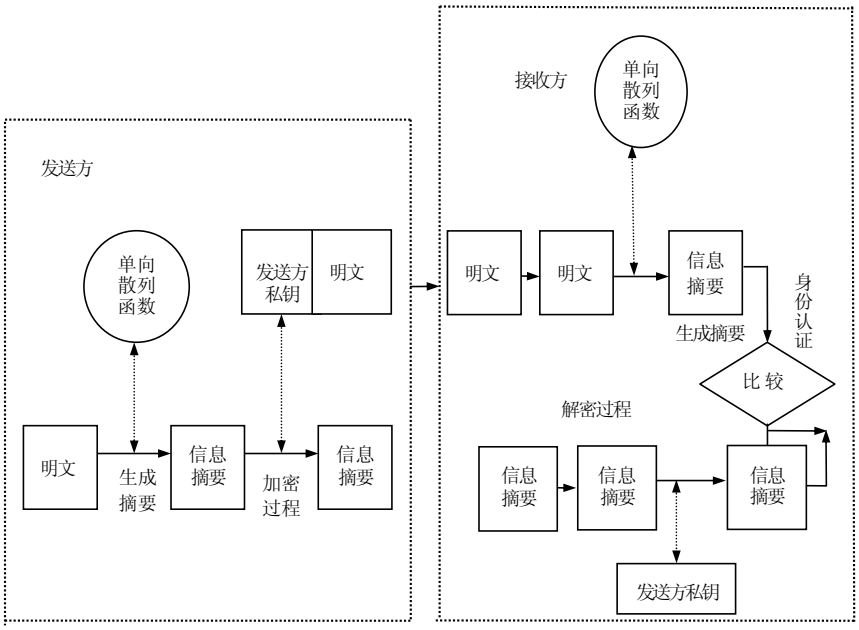



图 7.7　数字摘要技术工作原理

①生成数字摘要的算法必须是一个公开的算法，数据交换的双方可以用同一算法对原始数据经计算而生成的数字摘要进行验证。②算法必须是一个单向算法，就是只能通过此算法从原始数据计算出数字摘要，而不能通过数字摘要得到原始数据。③不同的两条消息不能得到相同的数字摘要。

由于每个信息数据都有自己特定的数字摘要，就像每个人的指纹一样，所以，数字摘要又称做数字指纹或数字手印(Thumbprint)。就像可以通过指纹来确定是某人一样，可以通过数字指纹来确定所代表的数据。

2) 数字签名技术

在电子商务中，为了保证电子商务安全网络支付中的不可否认性，必须具有数字签名技术，比如“电子支票上的签名认证”。

数字签名(Digital Signature)，就是指利用数字加密技术实现在网络传送信息文件时，附加个人标记，完成传统上手书签名或印章的作用，以表示确认、负责、经手、真实等；或数字签名就是在要发送的消息上附加一小段只有消息发送者才能产生而别人无法伪造的特殊数据(个人标记)，而且这段数据是原消息数据加密转换生成的，用来证明消息是由发送者发来的。在网络支付 SET 机制中是用发送方的私人密钥对用 HASH 算法处理原始消息后生成的数字摘要加密，附加在原始消息上，生成数字签名。数字签名=信件发送者私人秘钥加密 HASH(信件)。数字签名可以解决下述网络支付中的安全鉴别问题。

(1) 接收方伪造。接收方伪造一份文件，并声称这是发送方发送的付款单据等。

(2) 发送者或接收者否认。发送者或接收者事后不承认自己曾经发送或接收过支付单据。

(3) 第三方冒充。网上的第三方用户冒充发送或接收消息如信用卡密码。

(4) 接收方篡改。接收方对收到的文件如支付金额进行改动。

数字签名与手书签名的区别在于手写签名(包括盖章)是模拟的，因人而异，即使同一个人也有细微差别，比较容易伪造，要区别是否是伪造，往往需要特殊专家。而数字签名是 0 和 1 的数字串，极难伪造，要区别是否为伪造，不需专家。对不同的信息数字指纹，即使是同一人，其数字签名也是不同的。这样就实现了文件与签署的最紧密的“捆绑”。

3) 双重签名技术

在网络支付过程中，客户需要发送订购信息给商户，发送支付信息给银行。这两条信息是相互关联的，以保证该支付仅为该订单付款。为了保护客户的隐私，商家不需要知道客户的银行卡号码，银行也不需要知道客户的订单细节。这时，仅靠发送方对整个信息的一次数字签名显然是不够的，需要双重签名技术来实现。双重签名 DS(Dual Signature)是 SET 引入的重要创新。

### 7.1.2 网络支付安全交易

认证机构的功能是向各方发放证书。某些接收行也可能有自己的注册机构，由注册机构向商家发放证书，商家通过向客户出示证书向客户说明商家是合法的。认证机构和注册机构的工作应是协调的。

1. 电子支付安全交易控制

典型的专用金融服务系统是 SWIFT，处理电子票据(支票等)的安全传输。SWIFT 从 3 个

方面进行安全控制，由此可保证电子文档的可靠、完整和安全传输。一是用户身份与操作合法性验证，通过逻辑读写控制进行用户登录的用户、密码验证。二是数据完整性控制，对传输的数据进行验证。主要有对自然突发性错误进行验后反馈校验；对蓄意篡改性错误进行宏观检查校验。三是数据安全性控制，进行数据加密处理，防止网络传输中的“窃听”。主要应用于 SWIFT 网络中的传输过程控制，在一定条件下也应用于用户与 SWIFT 网络之间的传输控制。

2. 安全电子交易协议(SET)

SET 协议是 VISA 国际组织、MasterCard 国际组织创建安全电子交易的一个国际标准。其主要目的是解决信用卡电子付款的安全保障性问题，保证信息的机密性，保证信息安全传输，不能被窃听，只有收件人才能得到和解密信息；保证支付信息的完整性，保证传输数据完整地接收，在中途不被篡改；认证商家和客户，验证公共网络上进行交易活动的商家、持卡人及交易活动的合法性；广泛的互操作性，保证采用的通信协议、信息格式和标准具有公共适应性。从而可在公共互联网上集成不同厂商的产品。SET 安全交易系统的主要措施有加密技术、数字签名、电子认证、数字信封、数字现金的安全交易等几个方面。

## 7.2　网络支付协议

电子商务发展的核心问题是交易的安全性问题，电子商务的安全问题是一个系统性问题，它包括信息安全、身份认证和信用管理 3 个方面，需要从技术上、管理上和法律上来综合建设和完善安全保障体系。

### 7.2.1　网络支付的安全问题

在电子商务过程中，买卖双方是通过网络来联系的，而且彼此远隔千山万水。由于 Internet 既不安全，也不可信，因而建立交易双方的安全和信任关系相当困难。

1. 电子商务交易带来的安全威胁

1) 销售者面临威胁

对销售者而言，其面临的安全威胁主要有以下几个方面。

(1) 中央系统安全性被破坏。入侵者假冒成合法用户来改变用户数据(如商品送达地址)、解除用户订单或生成虚假订单。

(2) 竞争者检索商品递送状况。恶意竞争者以他人的名义来订购商品，从而了解有关商品的递送状况和货物的库存情况。

(3) 客户资料被竞争者获悉。

(4) 被他人假冒而损害公司的信誉。诈骗人建立与销售者服务器名字相同的另一个服务器来假冒销售者。

(5) 消费者提交订单后不付款。

(6) 虚假订单。

(7) 获取他人的机密数据。比如，某人想要了解另一人在销售商处的信誉时，他以另一人的名字向销售商订购昂贵的商品，然后观察销售商的行动。假如销售商认可该订单，则说明被观察者的信誉高；否则，则说明被观察者的信誉不高。

2) 购买者面临威胁

对购买者而言，其面临的安全威胁主要有下述 4 点。

(1) 虚假订单。一个假冒者可能会以客户的名义来订购商品，而且有可能收到商品，而此时客户却被要求付款或返还商品。

(2) 付款后不能收到商品。在要求客户付款后，销售商中的内部人员不将订单和钱款转发给执行部门，因而使客户不能收到商品。

(3) 机密性丧失。客户有可能将秘密的个人数据或自己的身份数据(如账号、口令等)发送给冒充销售商的机构，这些信息也可能会在传递过程中被窃取。

(4) 拒绝服务。攻击者可能向销售商的服务器发送大量的虚假定单来穷竭它的资源，从而使合法用户不能得到正常的服务。

2. 电子商务的安全风险来源

1) 信息传输风险

信息传输风险是指进行网上交易时，因传输的信息失真或者信息被非法窃取、篡改和丢失，而导致网上交易的不必要损失。

(1) 冒名偷窃。如“黑客”为了获取重要的商业秘密、资源和信息，常常采用源 IP 地址欺骗攻击。

(2) 篡改数据。攻击者未经授权进入网络交易系统，使用非法手段，删除、修改、重发某些重要信息，破坏数据的完整性，损害他人的经济利益或干扰对方的正确决策。

(3) 信息丢失。交易信息的丢失，可能有 3 种情况，一是因为线路问题造成信息丢失；二是因为安全措施不当而丢失信息；三是在不同的操作平台上转换操作不当而丢失信息。

(4) 信息传递过程中的破坏。信息在网络上传递时，要经过多个环节和渠道。由于计算机技术发展迅速，原有的病毒防范技术、加密技术、防火墙技术等始终存在着被新技术攻击的可能性。计算机病毒的侵袭、“黑客”非法侵入、线路窃听等很容易使重要数据在传递过程中泄露，威胁电子商务交易的安全。

(5) 虚假信息。用户以合法身份进入系统后，买卖双方都可能在网上发布虚假的供求信息，或以过期的信息冒充现在的信息，以骗取对方的钱款或货物。现在还没有很好的解决信息鉴别的办法。

2) 信用风险

信用风险主要来自 3 个方面。

(1) 来自买方的信用风险。对于个人消费者来说，可能有在网络上使用信用卡进行支付时恶意透支，或使用伪造的信用卡骗取卖方的货物行为；对于集团购买者来说，存在拖延货款的可能，卖方需要为此承担风险。

(2) 来自卖方的信用风险。卖方不能按质、按量、按时寄送消费者购买的货物，或者不能完全履行与集团购买者签订的合同，造成买方的风险。

(3) 买卖双方都存在抵赖的情况。网上交易时，物流与资金流在空间上和时间上是分离的，

因此如果没有信用保证网上交易是很难进行的。

3) 管理方面的风险

(1) 交易流程管理风险。客户进入交易中心，买卖双方签订合同，交易中心不仅要监督买方按时付款，还要监督卖方按时提供符合合同要求的货物。

(2) 人员管理风险。人员管理常常是网上交易安全管理上的最薄弱的环节，其原因主要是因工作人员职业道德修养不高，安全教育和管理松懈所致。一些竞争对手还利用企业招募新人的方式潜入该企业，或利用不正当的方式收买企业网络交易管理人员，窃取企业的用户识别码、密码、传递方式以及相关的机密文件资料。

(3) 网络交易技术管理的漏洞也带来较大的交易风险。有些操作系统中的某些用户是无口令的，如匿名 FTP，利用远程登录(Telnet)命令登录这些无口令用户，允许被信任用户不需要口令就可以进入系统，然后把自己升级为超级用户。

4) 法律方面的风险

在目前的法律上还是找不到现成的条文保护网络交易中的交易方式，因此还存在法律方面的风险。一方面，在网上交易可能会承担由于法律滞后而无法保证合法交易的权益所造成的风险，如通过网络达成交易合同，可能因为法律条文还没有承认数字化合同的法律效力而面临失去法律保护的危险。另一方面，在网上交易可能承担由于法律的滞后完善所带来的风险，即在原来法律条文没有明确规定下而进行的网上交易，在后来颁布新的法律条文下属于违法经营所造成的损失。如一些电子商务公司在开通网上证券交易服务一段时间后，国家颁布新的法律条文规定只有证券公司才可以从事证券交易服务，从而剥夺了电子商务服务公司提供网上证券交易服务的资格，给这些电子商务中间商经营造成巨大损失。

3. 电子商务的安全管理

网上交易安全管理，应当跳出单纯从技术角度寻求解决办法的圈子，采用综合防范的思路，从技术、管理、法律等方面去思考。建立一个完整的网络交易安全体系，至少从 3 个方面考虑，并且三者缺一不可。

(1) 技术方面的考虑。如防火墙技术、网络防毒、信息加密存储通信、身份认证、授权等。但只有技术措施并不能完全保证网上交易的安全。

(2) 必须加强监管。建立各种有关的合理制度，并加强监督，如建立交易的安全制度，交易安全的实时监控、提供实时改变安全策略的能力，对现有的安全系统漏洞的检查及安全教育等。在这方面，主要充分发挥政府有关部门、企业的主要领导、信息服务商的作用。

(3) 社会的法律政策与法律保障。通过健全法律制度和完善法律体系，来保证合法网上交易者的权益，同时对破坏合法网上交易权益的行为进行立法严惩，如尽快出台电子证据法、电子商务法、网上消费者权益法等。这方面，主要发挥立法部门和执法部门的作用。

### 7.2.2　SSL 网络传输安全协议

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的探索，SSL 安全协议和 SET 安全协议就是这种探索的两项重要成果，它们已经广泛在国际间的电子支付中使用。

1. SSL 安全协议主要提供的服务

1) SSL 安全协议的基本概念

安全套接层 SSL 协议(Secure Socket Layer)是由美国网景(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 协议中，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和服务器间事务安全的协议，它涉及所有 TCP/IP 应用程序。

2) SSL 安全协议主要提供 3 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。

(2) 加密数据以隐藏被传送的数据。

(3) 维护数据的完整性，确保数据在传输过程中不被改变。

2. SSL 安全协议的运行

1) SSL 整体结构

SSL 是一个介于 HTTP 协议与 TCP 协议之间的一个可选层，其位置大致如下。

```
－－－－－－－－
    ｜HTTP｜
－－－－－－－－
    ｜SSL｜
－－－－－－－－
    ｜TCP｜
－－－－－－－－
    ｜IP｜
－－－－－－－－
```

如果利用 SSL 协议来访问网页，其步骤如下。

用户在浏览器的地址栏里输入 http://www.sslserver.com。

HTTP 层：将用户需求翻译成 HTTP 请求，如：GET/index.htmHTTP/1.1。

SSL 层：借助下层协议的信道安全协商出一份加密密钥，并用此密钥来加密 HTTP 请求。

TCP 层：与 Web Server 的 443 端口建立连接，传递 SSL 处理后的数据，接收端与此过程相反。

SSL 在 TCP 之上建立了一个加密通道，通过这一层的数据经过了加密，因此达到保密的效果；上述过程通过以下 3 个元素来完成。

(1) 握手协议(Handshake Protocol)。这个协议负责协商被用于客户机和服务器之间会话的加密参数。当一个 SSL 客户机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。也就是说，用来协商密钥，协议的大部分内容就是通信双方如何利用它来安全地协商出一份密钥。

(2) 记录协议(Record Protocol)。定义了传输的格式，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 MAC(消息认证代码)；然后

结果被加密并传输。接收方接收数据并对它解密，校验 MAC，解压缩并重新组合它，并把结果提交给应用程序协议。

(3) 警告协议。这个协议用于指示在什么时候发生了错误或两个主机之间的会话在什么时候终止。

2) SSL 安全协议的运行步骤

(1) 建立一个虚拟的通信信道。SSL 客户机连接到 SSL 服务器，并要求服务器验证它自身的身份。

(2) 密码交换阶段，服务器通过发送它的数字证书证明其身份。这个交换还可以包括整个证书链，直到某个根证书权威机构(CA)。通过检查有效日期并确认证书包含有可信任 CA 的数字签名，来验证证书。

(3) 身份验证。服务器发出一个请求，对客户端的证书进行验证。但是，因为缺乏公钥体系结构，当今的大多数服务器不进行客户端认证。

(4) 协商用于加密的消息。加密算法和用于完整性检查的哈希函数，通常由客户机提供它支持的所有算法列表，然后由服务器选择最强健的加密算法。

(5) 确定会话密钥。客户机和服务器通过下列步骤生成会话密钥。

① 客户机生成一个随机数，并使用服务器的公钥(从服务器的证书中获得)对它加密，发送到服务器上。

② 服务器用更为随机的数据(客户机的密钥可用时，则使用客户机密钥；否则以明文方式发送数据)响应。

③ 使用哈希函数，从随机数据生成密钥。

当上述步骤完成之后，两者间的资料传送就会加上密码，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，如果没有原来编制的密码算法，也不能获得可读的有用资料。

在电子商务交易过程中，由于有银行参与，按照 SSL 协议，客户购买的信息首先发往商家，商家再将信息转发到银行，银行验证客户信息的合法性后，通知商家付款成功，商家再通知客户购买成功，将商品寄送给客户。

3. SSL 安全协议的应用

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。

1) 银行卡非 SET 电子商务支付系统(SSL)

使用 SSL 协议、RSA 加密算法、数字签名和防火墙等保证交易的安全，支付时使用的是银行发行的储值卡(借记卡)、信用卡。该方式风险较高，只要银行肯参与，该系统就是可行的。该系统的主体有持卡人、商家、支付网关和发卡银行。其流程如下。

(1) 持卡人登录商品发布站点，验证商家身份。

(2) 持卡人决定购买，向商家发出购买请求。

(3) 商家返回同意支付等信息。

(4) 持卡人验证支付网关的身份。

(5) 商家用支付网关的公开密钥加密支付信息。

(6) 支付网关解密商家传来的信息。

(7) 支付网关用它的私有密钥加密结果，把结果返回给商家。

(8) 商家用支付网关的公开密钥解密后返回信息给持卡人，送货，交易结束。

2) 支付系统的特点

(1) 有银行的参与，支付网关必须得到银行的授权。

(2) 商家及支付网关使用证书，支付网关为自签名的 Root CA。

(3) 持卡者支付时使用的微型电子钱包是一个 APPLET 应用程序，放在支付网关的服务器上，并经过支付网关的签名认证。

(4) 商家与持卡者通信用 SSL 协议，商家与支付网关通信使用 RSA 算法加密。

(5) 持卡者必须与支付网关签约，成为其会员。

(6) 支付网关与发卡行的通信可通过 POS 机拨号上银行的前置机(业务量不大时用)，或走专线，用 ISO8583 等协议上银行的前置机。

3) 银行直接参与的非 SET 电子商务支付系统

该系统支付信息不经过商家，直接到银行站点支付，即银行直接接收处理用户的支付信息。该系统风险较小。该系统的主体有持卡者、商家和发卡银行，其支付流程如下。

(1) 持卡者登录商品发布站点。

(2) 持卡者决定购买，向商家发出购买请求，并跳转到发卡行支付站点。

(3) 持卡者验证发卡行支付站点身份，通过 SSL 向发卡行传送支付信息。

(4) 银行处理用户的支付信息，划账。

(5) 商家定期到发卡行站点查询成交商品，送货，交易完成。

4) SSL 协议的基本属性

SSL 协议的优点是它提供了连接安全，具有下述 3 个基本属性。

(1) 连接是私有的。在初始握手定义了一个密钥之后，将使用加密算法。

(2) 可以使用非对称加密或公钥加密(例如 RSA 和 DSS)来验证对等实体的身份。

(3) 连接是可靠的。消息传输使用一个密钥的 MAC，包括了消息完整性检查。其中使用了安全哈希函数(例如 SHA 和 MD5)来进行 MAC 计算。

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”。但是上述流程中也可以注意到，SSL 协议有利于商家而不利于客户。客户的信息首先传到商家，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都是一些大公司，信誉度较高，这个问题没有引起人们的重视。随着电子商务参与的厂商迅速增加，对厂商的认证问题越来越突出，SSL 协议的缺点完全暴露出来。SSL 协议逐渐被新的 SET 协议所取代。

### 7.2.3 SET 协议

安全电子交易协议 SET(Secure Electronic Transcation)是美国 VISA 和 Master Card 两大信用卡组织等联合推出的用于电子商务的行业规范，其实质是一种应用在 Internet 上、以信用卡

为基础的电子付款系统规范，目的是为了保证网络交易的安全。SET 已获得 IETF 标准的认可，是电子商务的发展方向。

1. SET 支付系统的组成

SET 支付系统主要由持卡人、商家、发卡行、收单行、支付网关、认证中心 6 个部分组成。对应地，基于 SET 协议的网上购物系统至少包括电子钱包软件、商家软件、支付网关软件和签发证书软件。

基于 SET 的电子商务支付系统由以下 6 部分组成。

(1) 持卡人(Card Holder)。指由发卡银行所发行的支付卡的授权持有者。

(2) 商家(Merchant)。指出售商品或服务的个人或机构。商家必须与收单银行建立业务联系，以接受支付卡这种付款方式。

(3) 发卡银行(Issuing Bank)。指向持卡人提供支付卡的金融机构。

(4) 收单银行(Acquiring Bank)。指与商家建立业务联系的金融机构。

(5) 支付网关(Payment Gateway)。实现对支付信息从 Internet 到银行内部网络的转换，并对商家和持卡人进行认证。

(6) 认证中心 CA(Certificate Authority)。在基于 SET 协议的电子商务体系中起着重要作用。可以为持卡人、商家和支付网关签发 X.509V3 数字证书，让持卡人、商家和支付网关通过数字证书进行认证。CA 同时要对证书进行管理。

2. SET 协议的工作流程

(1) 消费者利用自己的 PC 通过因特网选定所要购买的物品，并在计算机上输入订货单、订货单上需包括在线商店、购买物品名称及数量、交货时间及地点等相关信息。

(2) 通过电子商务服务器与有关在线商店联系，在线商店做出应答，告诉消费者所填订货单的货物单价、应付款数、交货方式等信息是否准确，是否有变化。

(3) 消费者选择付款方式，确认订单签发付款指令。此时 SET 开始介入。

(4) 在 SET 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消费者的账号信息。

(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，再到电子货币发行公司确认。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) 在线商店发送货物或提供服务并通知收单银行将钱从消费者的账号转移到商店账号，或通知发卡银行请求支付。在认证操作和支付操作中间一般会有一个时间间隔，例如，在每天的下班前请求银行结一天的账。

前两步与 SET 无关，从第三步开始 SET 起作用，一直到第六步，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 都有明确的规定。在操作的每一步，消费者、在线商店、支付网关都通过 CA(认证中心)来验证通信主体的身份，以确保通信的对方不是冒名顶替。所以，也可以简单地认为 SET 规格充分发挥了认证中心的作用，以维护在任何开放网络上的电子商务参与者所提供信息的真实性和保密性。

3. SET 安全协议运行的目标

安全电子交易 SET 协议是一个通过开放网络进行安全资金支付的技术标准，这对于需要支付货币的交易来讲是至关重要的。它采用公钥密码体制(PKI)和 X.509 电子证书标准，通过相应软件、电子证书、数字签名和加密技术能在电子交易环节上提供更大的信任度、更完整的交易信息、更高的安全性和更少受欺诈的可能性。SET 协议用以支持 B to C 这种类型的电子商务模式，即消费者持卡在网上购物与交易的模式。

SET 协议比 SSL 协议复杂，因为前者不仅加密两个端点间的单个会话，它还可以加密和认定三方间的多个信息。由于设计合理，SET 协议得到了 IBM、HP、Microsoft、Netscape、VeriFone、GCT、VeriSign 等许多大公司的支持，已成为事实上的工业标准。目前，它已获得 IEFT 标准的认可。

SET 安全协议要达到的目标主要有下述 5 点。

(1) 保证信息在因特网上安全传输，防止数据被黑客或被内部人员窃取。

(2) 保证电子商务参与者信息的相互隔离。客户的资料加密或打包后通过商家到达银行，但是商家不能看到客户的账户和密码信息。

(3) 解决网上认证问题。不仅要对消费者的信用卡认证，而且要对在线商店的信誉程度认证，同时还有消费者、在线商店与银行间的认证。

(4) 保证网上交易的实时性，使所有的支付过程都是在线的。

(5) 效仿 EDI 贸易的形式，规范协议和消息格式，促使不同厂家开发的软件具有兼容性和互操作功能，并且可以运行在不同的硬件和操作系统平台上。

4. SET 安全协议的工作原理

图 7.8 显示了 SET 的成分，以及 SET 中消费者、商家、收单银行和认证中根据 SET 协议的工作流程图，可将整个工作程序分为下面 6 个步骤。

(1) 接通阶段。客户通过网络向服务商打招呼，服务商回应。

(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，也有的选用 Diffie-Hellman 和 Fortezza-KEA 密码算法。

(3) 会谈密码阶段。客户与服务商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。客户与服务商之间的相互交换结束的信息。

当上述动作完成之后，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用资料。

在电子商务交易过程中，由于有银行参与，按照 SSL 协议，客户购买的信息首先发往商家，商家再将信息转发银行，银行验证客户信息的合法性后，通知商家付款成功，商家再通知客户购买成功，将商品寄送客户。

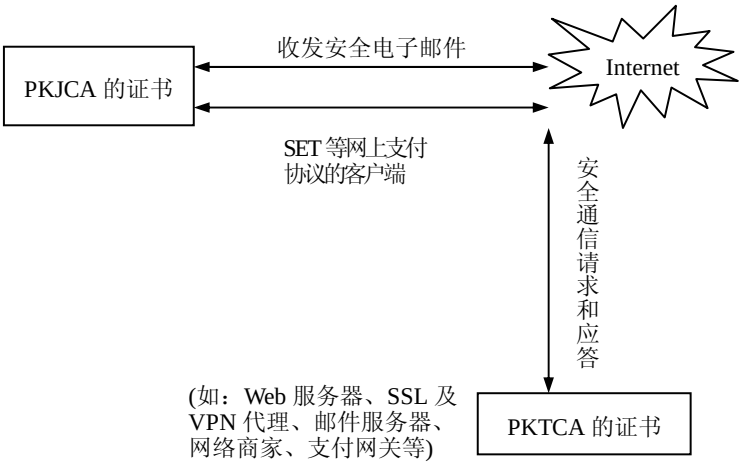



图 7.8　SET 协议的工作原理图

5. SET 安全协议涉及的范围

SET 协议规范所涉及的对象有如下几类。

(1) 消费者。包括个人消费者和团体消费者，按照在线商店的要求填写订货单，通过发卡银行选择信用卡进行付款。

(2) 在线商店。提供商品或服务，具备相应电子货币使用的条件。

(3) 收单银行。通过支付网关处理消费者和在线商店之间的交易付款问题。

(4) 电子货币。如智能卡、电子现金、电子钱包的发行公司，以及某些兼有电子货币发行的银行。负责处理智能卡的审核和支付工作。

(5) 认证中心(CA)。负责对交易双方的身份确认，对厂商信誉度和消费者的支付手段进行认证；CA 的作用如图 7.9 所示。

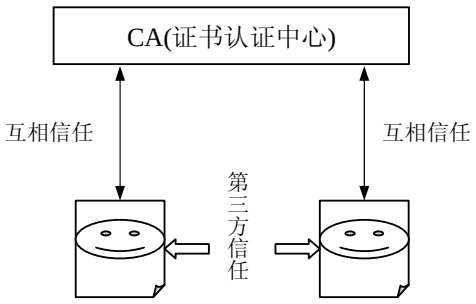



图 7.9　CA 的作用

### 7.2.4　其他协议

近年来，IT 业界与金融行业一起，推出不少更有效的安全交易标准。主要有以下几种。

1. 安全外壳协议 SSH

SSH(Secure Shell)是一种在不安全网络上用于安全远程登录和其他安全网络服务的协议。它提供了对安全远程登录、安全文件传输和安全 TCP/IP 和 X-Windows 系统通信量进行转发

的支持。它可以自动加密、认证并压缩所传输的数据。正在进行的定义 SSH 协议的工作确保 SSH 协议可以提供强健的安全性，防止密码分析和协议攻击，可以在没有全球密钥管理或证书基础设施的情况下，把工作得非常好，并且在可用时可以使用自己已有的证书基础设施(例如 DNS-SEC 和 X.509)。SSH 协议由下面 3 个主要组件组成。

(1) 传输层协议。它提供服务器认证、保密性和完整性功能，并具有完美的转发保密性功能。有时，它还能提供压缩功能。

(2) 用户认证协议。它负责从服务器对客户机的身份认证。

(3) 连接协议。它把加密通道多路复用组成几个逻辑通道。

SSH 传输层是一种安全的低层传输协议。它提供了强健的加密、加密主机认证和完整性保护功能。SSH 中的认证是基于主机的，这种协议不执行用户认证。可以在 SSH 的上层为用户认证设计一种高级协议。

这种协议被设计得相当简单而灵活，以允许参数协商并最小化来回传输的次数。密钥交互方法、公钥算法、对称加密算法、消息认证算法及哈希算法等都需要协商。

数据完整性是通过在每个数据包中包含一个消息认证代码(MAC)来保护的，这个 MAC 是根据一个共享密钥、数据包序列号和数据包的内容计算得到的。

在 UNIX、Windows 和 Macintosh 系统上都可以找到 SSH 实现。它是一种广为接受的协议，使用众所周知的建立良好的加密、完整性和公钥算法。

2. 套接字安全协议 SOCKS

套接字安全协议 SOCKS(Socket Security)是一种基于传输层的网络代理协议，它是一个应用层的用于穿越 IP 网络防火墙的协议。它的安全性是高度依赖于正规的认证和正规执行方法提供的有效封装，以及在 SOCKS 客户端和 SOCKS 服务端所选择的安全性，还有管理员对认证方法选项所作的小心周密的考虑。它设计用于在 TCP 和 UDP 领域为客户机/服务器应用程序提供一个框架，以方便并且安全地使用网络防火墙的服务。

SOCKS 最初是由 David 和 Michelle Koblas 开发的，其代码在 Internet 上可以免费得到。此后经历了几次主要的修改，但该软件仍然可以免费得到。

SOCKS 版本 4 为基于 TCP 的客户机/服务器应用程序(包括 Telnet、FTP 以及流行的信息发现协议，如 HTTP、WAIS 和 Gopher)提供了不安全的防火墙传输。

3. 安全超文本传输协议(S-HTTP)

安全超文本传输协议 S-HTTP(Secure Hypertext Transfer Protocol)是一种面向安全信息通信的协议，它可以和 HTTP 结合起来使用。S-HTTP 协议为 HTTP 客户机和服务器提供了多种安全机制，这些安全服务选项是适用于万维网上各类用户的。S-HTTP 还为客户机和服务器提供了对称能力(及时处理请求和恢复，及两者的参数选择)，同时维持 HTTP 的通信模型和实施特征。

S-HTTP 客户机和服务器是与某些加密消息格式标准相结合的。S-HTTP 支持多种兼容方案并且与 HTTP 相兼容。有 S-HTTP 性能的客户机能够与没有 S-HTTP 的服务器连接，但是这样的通信明显地不会利用 S-HTTP 安全特征。

S-HTTP 能与 HTTP 信息模型共存并易于与 HTTP 应用程序相整合。S-HTTP 依靠密钥对

的加密，保障 Web 站点间的交易信息传输的安全性。但作为金融业界的支付系统，一般都不采用这种协议模式。

## 7.3　结算认证系统

结算认证系统作为现代支付体系的核心，在银行业具有十分重要的地位。计算机技术、网络技术和通信技术在支付体系中的广泛应用，便出现了各种各样的电子支付结算系统。

### 7.3.1　证书简介

证书认证中心 CA 是负责发放和管理数字证书的权威机构。CA 系统遵循 PKI 安全体系，能够创建、签发、查询、吊销数字证书，为企业级的证书应用提供完整、灵活的解决方案。

1. 客户认证

客户认证 CA(Client Authentication)是基于用户的客户端主机 IP 地址的一种认证机制，它允许系统管理员为具有某一特定 IP 地址的授权用户定制访问权限。CA 与 IP 地址相关，对访问的协议不做直接的限制。服务器和客户端无需增加、修改任何软件。系统管理员可以决定对每个用户的授权、允许访问的服务器资源、应用程序、访问时间及允许建立的会话次数等。因此，在这些情况下，信息认证将处于首要的地位。

客户认证技术是保证网上交易安全的一项重要技术。客户认证主要包括身份认证和信息认证。

1) 身份认证

身份认证就是在交易过程中判明和确认贸易双方的真实身份，这是目前网上交易过程中最薄弱的环节。某些非法用户常采用窃取口令、修改或伪造、阻断服务等方式对网上交易系统进行攻击，阻止系统资源的合法管理和使用。因此，要求认证机构或信息服务商应当提供如下认证的功能。

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

(2) 完整性。要求信息在传输过程中保证其完整性，即信息接收者能够确认所获得的信息在传输过程中没有被修改、延迟和替换。

(3) 不可抵赖性。要求信息的发送方不能否认自己发出的信息。同样，信息的接收方不能否认已收到了信息。

(4) 访问控制。拒绝非法用户访问系统资源，合法用户只能访问系统授权和指定的资源。

一般来说，用户身份认证可通过下面 3 种基本方式或其组合方式来实现。

(1) 用户所知道的某个秘密信息，例如用户知道自己的口令。

(2) 用户所持有的某个秘密信息(硬件)，即用户必须持有合法的随身携带的物理介质，例如智能卡中存储用户的个人化参数，以及访问系统资源时必须要有的智能卡。

(3) 用户所具有的某些生物学特征，如指纹、声音、DNA 图案、视网膜扫描等，这些认证方法一般造价较高，多半适用于保密程度很高的场合。

2) 信息认证

随着网络技术的发展，通过网络进行购物交易等商业活动日益增多。这些商业活动往往通过公开网络进行数据传输，这对网络传输过程中信息的保密性提出了更高的要求。因此，认证机构或信息服务商应提供以下几方面的认证功能。

(1) 对敏感的文件进行加密，这样即使别人截获文件也无法得到其内容。

(2) 保证数据的完整性，防止截获人在文件中加入其他信息。

(3) 对数据和信息的来源进行验证，以确保发信人的身份。

通常采用秘密密钥加密系统(Secret Key Encryption)、公开密钥加密系统(Public Key Encryption)或者两者相结合的方式，以保证信息的安全认证。对于加密后的文件，即使他人截取信息，由于得到的是加密后的信息，因此无法知道信息原始含义；同时加密后，他人也无法加入或删除信息，因为加密后信息被改变后就无法得到原始信息。为保证信息来源的确定性，可以采用加密的数字签名方式来实现，因为数字签名是唯一的而且是安全的。

2. 安全认证技术

安全认证技术主要有数字摘要、数字信封、数字签名、数字时间戳、数字证书等。在前面的章节中对主要的安全认证技术已经作了介绍，这里不再赘述。

3. 数字证书的分类

数字证书通常分为 3 种类型，即个人证书、企业证书、软件证书。

1) 个人证书(Personal Digital ID)

个人证书是为某一个用户提供证书，以帮助个人在网上进行安全的电子交易操作。个人身份的数字证书通常是安装在客户端的浏览器内，并通过安全的电子邮件进行交易操作。

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，就开始发放个人数字证书，并将数字证书安置在用户所用的浏览器或电子邮件的应用系统中，同时也给申请者发一个通知。个人数字证书的使用方法是集成在用户的浏览器的相关功能中，用户其实只要作出相应的选择就行了。

个人数字证书有 4 个级别：第一级别是最简单的，只提供个人电子邮件地址的认证，它仅与电子邮件地址有关，并不对个人信息进行认证，是最初级的认证；第二级别提供个人姓名、个人身份(驾照、社会保险号、出生年月等)等信息的认证；第三级别是在第二级别之上加上了充当信用支票的功能；第四级别包括证书所有人的职位、所属组织等，但这一级别还没有最后定型。

2) 企业证书(Server ID)

企业证书，也就是服务器证书，它是对网上的服务器提供一个证书，拥有 Web 服务器的企业就可以用具有证书的 Internet 网站(Web site)来进行安全电子交易。

拥有数字证书的服务器可以自动与客户进行加密通信，有证书的 Web 服务器会自动地将其与客户端 Web 浏览器通信的信息加密。服务器的拥有者(相关的企业或组织)，有了证书，就可以进行安全电子交易。服务器证书的发放较为复杂。因为服务器证书是一个企业在网络上的形象，是企业在网络空间信任度的体现。

权威的认证中心对每一个申请者都要进行信用调查，包括企业基本情况、营业执照、纳税证明等；要对该企业对服务器的管理情况进行考核，一般是通过事先准备好的详细验证步

骤逐步进行，主要考虑是否有一套完善的管理规范；要对该企业的技术条件进行考核，是否有完善的加密技术和保密措施；也要对其设备的安全可靠性进行检查，包括是否有多层逻辑访问控制、生物统计扫描仪、红外线监视器等，认证中心经过考察后决定是否发放或撤销服务器数字证书。一旦决定发放后，该服务器就可以安装认证中心提供的服务器证书，安装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，它与服务器是密不可分的，数字证书与这对密钥一起表示该服务器的身份，是整个认证的核心。

3) 软件证书

通常是为网上下载的软件提供证书，应用并不广泛。软件(开发者)证书 Deve(ID)通常为 Internet 中被下载的软件提供证书，该证书用于和微软公司 Authenticode 技术(合法化软化)结合的软件，以使用户在下载软件时能获得所需的信息。

上述 3 类证书中前两类是常用的证书，第三类则用于较特殊的场合，大部分认证中心提供前两类证书，能完全提供各类证书的认证中心并不普遍。

数字证书的管理非常重要。它包括两方面的内容：一是颁发数字证书，二是撤销数字证书。在一些情况下，如密钥丢失或被窃，或者某个服务器变更了，就需要一种方法来验证数字证书的有效性，要建立一份证书取消清单并公之于众，这份清单是可伸缩的。由于数字证书也要有相应的有效期，为此，认证中心一般都制定相应的管理措施和政策，来管理其属下的数字证书。目前，数字证书可用于电子邮件、电子贸易、电子基金转移等各种用途。数字证书的应用范围和效果目前还是有限的。现在的网络认证体系很不健全，在 Internet 上的信任度还很低。

一些国家的银行和信用卡公司也在建立自己的认证体系，以保障它们自身的利益。

### 7.3.2　证书的发放

对于 SET 的用户，有多种方法向申请者发放证书，可以发放给最终用户签名或加密的证书，向持卡人只能发放签名的证书，向商户和支付网关可以发放签名并加密的证书。

1. 注册机构

电子商务授权机构(CA)也称为电子商务认证中心(Certificate Authority)，在电子交易过程中，无论是数字时间戳服务还是数字证书的发放，都不是靠交易双方自己完成的，而需要有一个具有权威性和公正性的第三方来完成，如图 7.10 所示。

认证是采用层级式的架构，而无论是付款人，收款人或收单银行都需要经过认证才能参与交易。如果甲想和乙通信，他首先必须从数据库中取得乙的证书，然后对它进行验证。如果他们使用相同的 CA，事情就很简单。甲只需验证乙证书上 CA 的签名；如果他们使用不同的 CA，问题就复杂了。甲必须从 CA 的树形结构底部开始，从底层 CA 往上层 CA 查询，一直追踪到同一个 CA 为止，找出共同的信任 CA。

图中的地区政策认证中心并不一定存在，品牌认证中心可能直接认证付款人，收款人及金融机构。

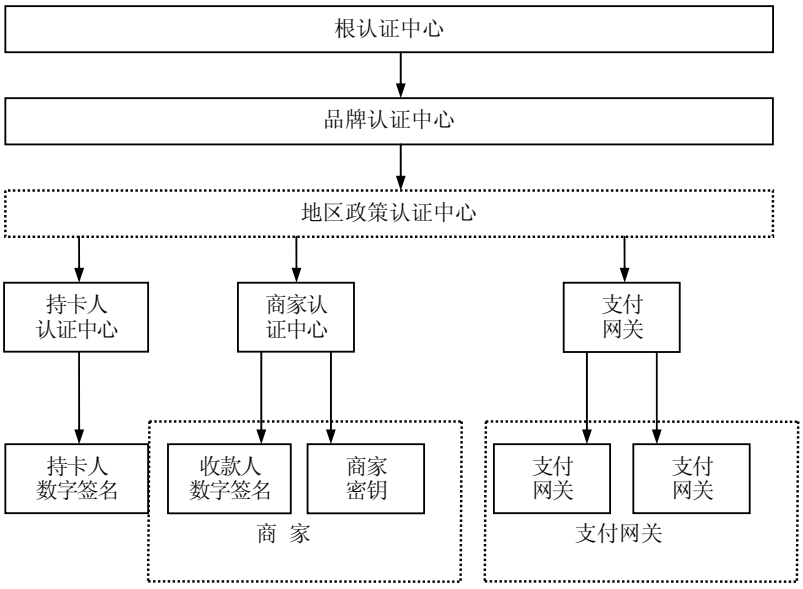



图 7.10　认证中心的结构示意图

1) 认证中心功能的实现

(1) 证书发放。通过注册中心的初始身份认证后，注册中心将用户申请提交给认证中心，认证中心根据证书操作管理规范定义的颁发规则在证书中插入附加信息并设置字段，并采取不同的方法将证书返回给用户(如用电子邮件形式)。

(2) 证书更新。证书更新包含两个方面内容：一是用户证书已经过期或者与证书相关的密钥到了它有效生命终点，或者证书中一些属性已经改变，这都需要更新用户的证。二是 CA 本身的证书也存在以上的问题，所以 CA 根证书也是需要更新的。

(3) 证书注销。在某种情况下，证书的有效性要求在证书结束日期之前终止或者要求用户与私钥分离时，证书要被撤销。例如签署者状态发生改变，证书中信息可能已经修改，与用户相关的私钥可能以某种方式泄露。大多数情况下，CA 用来公布已更改的证书状态机制是一个证书撤销列表(CRL)。CRL 包括已被撤销证书的序列号和撤销日期，还有标志撤销原因的状态。

(4) 证书验证。它包括五方面内容：一是证书是否包含一个有效的数字签名，以此证明证书内容没被修改；二是颁发者的公开密钥是否可以验证证书上的数字签名，以确认数据是否来源于真正的数据发送方；三是当前使用的证书是否在证书的有效期内；四是证书是否用于最初分发给它的目的；五是检查证书撤销列表 CRL，验证证书是否被撤销。

2) 选择认证中心时应考虑的问题

(1) 在提供证书对受托申请进行管理方面的运营服务经验。

(2) 灵活性。系统能够适应于支持多种选择或性能，如多种证书类型或算法。

(3) 选择性。能为用户提供引进的认证中心服务或认证中心产品许可证，并在今后由服务转向产品。

(4) 实用性。根据用户需求进行设计，使产品能够满足用户的特殊需求。

(5) 可靠性。认证中心的提供商和用户能够产生一种将会被大范围用户社区所接受的系

统，同时无需过分考虑依赖证书可靠性的问题。

(6) 认证中心提供商的财务稳定性。认证中心能够产生并维持业务，对各种各样的用户做出承诺。

(7) 可调节性。在不做大的修改和重新设计的情况下，确保认证中心能够满足迅速增长的需求。

(8) 认证中心提供的保证程度。由认证中心提供的保护措施，用于降低在系统运行中的损害和风险。

(9) 咨询范围。技术人员和商业人员可以随时为用户使用证书提供帮助，以便实现其商业目标。

(10) 认证中心还应能够为由一个认证中心解决方案支持的不同社区提供多种服务。最典型的例子应该是银行。在银行里，雇员在一个区域里进行操作，而账单持有人在一个完全不同的区域里操作。

2. 申请

认证中心的功能实际上是由两部分完成的，认证中心和注册机构 RA(Registration Authority，注册审批机构)。这两个功能可以都分配给认证中心，也可以由不同机构提供。将这两个功能分开使其中一个机构做出重要管理决定，另一个机构提供证书有效期限及系统安全的管理技术。注册机构负责作出诸如谁有权获得证书、何时吊销证书等决定，而另一机构，即认证中心，可以负责管理证书的有效期限。注册机构可以是一家使用雇员访问证书的公司，也可以是使用证书为其账单持有人从事电子银行业务的银行。

1) RA 的功能

(1) 主体注册证书的个人认证。

(2) 确认主体所提供的信息的有效性。

(3) 对被请求证书属性确定主体的权利。

(4) 确认主体确实拥有注册的私钥。

(5) 在需要撤销时报告密钥泄露或终止事件。

(6) 为识别身份的目的分配名字。

(7) 在注册初始化和证书获得阶段产生共享秘密。

(8) 产生公/私密钥对。

(9) 认证机构代表最终实施开始注册过程。

(10) 私钥的归档。

(11) 开始密钥恢复处理。

(12) 包含私钥的物理环网(例如智能卡)的分发。

2) 证书的申请操作流程

证书的申请操作流程如下。

(1) 用户带相关证明到证书业务受理中心申请证书。

(2) 用户填写证书申请表格和证书申请协议书。

(3) 证书业务受理中心录入人员将数据录入并提交给 RA 中心。

(4) 业务受理点的审核员通过离线方式审核申请者的身份、能力和信誉等。

(5) 审核通过后，RA 中心向 CA 中心转发证书的申请请求。

(6) CA 中心响应 RA 中心的证书请求，为该用户签发证书并返回给 RA 中心。

(7) RA 中心将签发的证书返回到地、市级业务受理中心。

(8) 如果证书介质是 IC 卡方式，则由印卡操作员对相应的 IC 卡进行印刷操作。

(9) 证书业务受理中心的制作操作员打印相应证书的密码信封，并将该用户的证书灌制到证书介质中后通知用户领取。

(10) 用户根据用户应用指南使用相关的证书业务。

3. 证书发放

1) 持卡人证书

它是支付卡的电子化表示，是金融机构以数字化形式签发的，不能被第三方改变。持卡人证书并不包括账号和终止日期，而是用单向哈希算法，根据账号、截止日期和密码值即可导出这个码值，反之则不行。在 SET 协议中，持卡人需向支付网关提供他的账户信息和密码值。持卡人向发卡行申请证书时，用自己的软件生成一对公用密钥和私有密钥，将账户信息和公用密钥交给发卡行保存，私有密钥自己保存。当持卡人的发卡行批准后，他就能获得持卡人证书，持卡人还需保存认证授权的公用密钥，用于验证商户证书和支付网关证书。当持卡人想通过电子方式购物时，该证书将与购买要求和加密的支付指令一起发往商户，当商户收到持卡人证书时，它至少能确认该账户信息曾被发卡行证实过。

2) 商户证书

商户证书就像是贴在收款台小窗上的付款卡贴面，以表示可以用什么卡来支付，它是由金融机构签发的，不能被第三方改变。在 SET 环境中，一个商户至少应有一对证书，与一个收单银行打交道。一个商户可以有多对证书，表示它能接受多种付款卡。

3) 支付网关证书

它可以被收单行获取，用于处理授权和购买信息，持卡人从该证书获得网关的加密密钥，授权该密钥用户保护持卡人的账户信息。支付网关证书由付款卡机构发给收单行。

4) 收单行证书

收单行必须拥有证书以便作为认证来接收和处理来自商户的证书申请，收单行证书由付款卡机构颁发。

5) 发卡行证书

发卡行必须拥有证书以便作为认证授权来接收和处理来自持卡人的证书申请，发卡行证书由付款卡机构颁发。

如果收单行和发卡行选择付款卡机构来处理证书申请，就不需要收单行证书和发卡行证书，因为这样它们就不需要处理 SET 信息了。

4. 证书的更新

数字证书网上更新流程如图 7.11 所示。具体步骤如下。

第一步，插入需要更新的电子令牌，并打开证书管理工具。单击“开始提交更新申请”按钮。第二步，申请提交成功后出现页面，按照提示，单击“下一步”按钮，继续进行更新。(**注意**：一旦申请提交成功，不得返回再次提交申请，以免造成证书更新失败而无法使用证书。

中途若有对话框弹出，请全部选择“是”选项。)第三步，选择证书类型，单击“下一步”按钮，在弹出的对话框中输入用户的电子令牌的密码。

5. 证书撤销

证书的撤销可以有许多理由，如私有密钥被泄密，身份信息的更新或终止使用等。对持卡人而言，他需要确认他的账户信息不会发往一个未被授权的支付网关，因此被撤销的支付网关证书需包含在撤销清单中并散发给持卡人。由于持卡人不会将任何敏感的支付信息发给商户，所以，持卡人只需验证商户证书的有效性即可。对商户而言，被撤销的支付网关证书需散发给商户。对支付网关而言，需检查持卡人不在撤销清单中，并需与发卡行验证信息的合法性；同样支付网关需检查商户证书不在撤销清单中，并需与收单行验证信息的合法性。

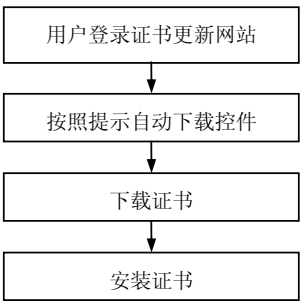



图 7.11　证书的更新流程图

### 7.3.3　应用案例——中国电信 CA 认证系统(CTCA)

目前，中国已有近 40 家 CA 认证中心，既有行业性认证中心，如中国人民银行认证中心(CFCA)、中国邮政认证中心、外经贸部认证中心等；也有地域性 CA 认证中心，如上海 CA 认证中心、广东 CA 认证中心等。

1. 中国电信 CA 认证系统的定位

中国电信 CA 认证系统目的是在 163/169 网上建立安全保障体系，为中国电信 2000 万网络用户提供端到端的安全服务。如果将 163/169 比喻成中国电信修的马路，中国电信 CA 认证系统就是马路上的安全警察。中国电信 CA 认证系统如图 7.12 所示。

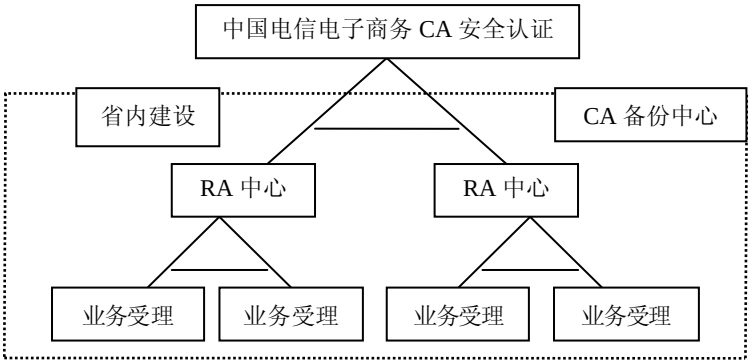



图 7.12　中国电信 CA 认证系统

2. 中国电信 CA 认证系统的发展历程

1998 年上半年进行 CA 认证系统的研究和开发，1998 年 8 月在湖南进行试点，建立了中国电信 CA 认证中心。

1999 年 8 月 3 日，通过国家密码办和信息产业部联合鉴定，并通过国家软件产品安全测评中心的测试，成为首家允许在公网上运营的 CA 认证系统。

1999 年底，按全国 CA 认证中心、省 RA 审核中心、业务受理点三级结构在全国范围内进行大规模推广。到 2000 年 8 月，31 个省建立了 RA 审核中心，也建立了上百个业务受理点。

目前，中国电信 CA 认证系统已经为各类用户发放 10 多万张数字证书(2006 年统计数)，基于 CTCA 系统开发的电子商务应用项目有 15 类。中国电信 CA 认证系统是目前国内覆盖最广、用户最多的、应用项目最多的 CA 认证系统。

3. 中国电信 CA 认证系统的技术特点

遵循国际 PKCS、PKIX 系列标准，签发证书符合 ITU-T、X.509、V3 标准。全部采用通过国家密码办规定的加密设备和加密算法。根据不同应用，系统可签发通用数字证书、SSL 证书、S/MIME 证书，可与标准浏览器、Web 服务器实现互通。

根据安全强度不同，系统支持 512 位和 1024 位公钥证书的签发。根据业务系统实时性的不同要求，系统具备两种黑名单查询方式，即实时证书状态查询(OCSP)和定期证书黑名单列表(CRL)。

4. 加快建立完善的电子商务 CA 认证系统

建立完善的运行维护体系，提供 7(天)×24(小时)不间断服务。建立全国 CA 技术支持中心、区域 CA 技术支持中心两级技术支撑体系。建立完善的数字证书业务营销体系，鼓励与社会合作，建立证书代理机制。

5. 中国电信 CA 认证系统与其他 CA 相比的优势

中国电信拥有丰富的运行维护经验。

中国电信拥有资金、极大的无形资产优势。

中国电信拥有 IT 人才优势，具有极强的技术支持力量。

中国电信是很适合于充当第三方公正的角色。

## 本章实训内容

### 一、申领个人安全证书实训

1. 实验目的

电子商务的安全的重要性已是不言而喻，安全问题是电子商务推进中的最大障碍。营造信誉良好、安全可靠的交易环境才能让众多的企业和消费者支持电子商务，因此网络安全成为电子商务尤为关注的重要环节。

2. 实验要求

掌握个人安全证书的申领和领取过程，了解如何申领和领取个人安全证书；理解数字证书的含义和中国金融认证中心的工作流程。

3. 实验内容

(1) 证书申领。

(2) 证书审批查询。

(3) 证书下载。

(4) 登录中国金融认证中心的网站，浏览相关内容。

1) 证书的定义

证书是一个经证书认证机构(CA)数字签名的包含用户身份信息以及公开密钥信息的电子文件，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。证书可用于安全电子邮件、网上缴费、网上炒股、网上招标、网上购物、网上企业购销、网上办公等安全电子商务活动。

2) 证书的种类及用途

除了根 CA、政策 CA、运营 CA 等各级 CA 的证书外，对于最终用户，按照证书的功能不同，证书有不同的分类。

企业高级证书——适用于企业做金额较大时的 B to B 网上交易，安全级别较高，可用于数字签名和信息加密。

企业普通证书——适用于企业用户用于 SSL、S/MIME 以及建立在 SSL 之上的应用，它的安全级别较低，建议用于金额较小的网上交易。

个人高级证书——适用于个人做金额较大的网上交易，安全级别较高，可用于数字签名和信息加密。

个人普通证书——适用于个人用户用于 SSL、S/MIME 以及建立在 SSL 之上的应用，它的安全级别较低，建议用于小额的网上银行和网上购物。

Web Server 证书——适用于站点服务器提供金额较小的 B to C 网上交易，若一个网站要提供 B to B 交易时，应申请 Direct Server 证书，并配合 Direct Server 软件来保证它的安全性。

Direct Server 证书——用于数字签名和信息加密。Direct Server 证书主要用于企业从事 B to B 交易时对 Web Server 的保护。

3) CFZA 证书的功能及特点

(1) 实体的鉴别。通过 CFCA 签发的数字证书，使电子交易的各方都拥有合法的身份，在交易的各个环节，交易的各方都可验证对方数字证书的有效性，从而解决相互信任问题。

(2) 保证电子交易中信息的保密性。信息泄漏主要指交易双方进行交易的内容被第三方窃取或交易一方提供给另一方使用的文件被第三方非法使用，通过对信息进行加密，从而解决了这方面的问题。

(3) 保证电子交易中数据的真实性和完整性。电子交易信息在网络上传输的过程中，可能被他人非法地修改、删除或重放(指只能使用一次的信息被多次使用)，这方面的安全性是由身份认证和信息的加密来保证的。

(4) 支持不可否认性。CFCA 的高级证书中使用了一套专门用来进行签名/验证的密钥对，以保证签名密钥与加密密钥的分隔使用。对签名/验证密钥对中用来签名的私有密钥而言，其产生、存储和使用过程必须安全，且只能由用户独自控制。

(5) 密钥历史记录。CFCA 能无缝地管理密钥历史记录，并在检索以前加密的数据时，能透明地使用其相应的密钥进行解密。因此，企业和用户就再也不用担心无法访问其历史数据了。

(6) 密钥备份与恢复。CFCA 的高级证书系统提供了备份与恢复解密密钥的机制。需注意的是，密钥备份与恢复只能针对解密密钥，签名私钥不能够做备份。

(7) 密钥自动更新。CFCA 的高级证书系统能实现完全透明的、自动(无需用户干预)的密

钥更换以及新证书的分发工作。

(8) CRL 查询。证书目录服务器中，提供客户端-服务器端自动在线证书撤销列表(CRL)的实时查询和自动检索。

(9) 时间戳。支持时间戳功能，确保所有用户的时间一致。

(10) 交叉认证。CFCA 的系统中所采用的网络信任域模型，使得单位除了可完全控制自己的信任域外，也可通过接纳其他单位而扩展自己的信任域。

4) 证书申请审批下载流程

(1) 证书申请审批下载。

① 证书申请。CFCA 授权的证书的注册审核机构(Registration Authority，RA)(各商业银行、证券公司等机构)，面向最终用户，负责接受各自的持卡人和商户的证书申请并进行资格审核，具体的证书审批方式和流程由各授权审核机构规定。

② 证书申请表直接到 RA 处领取。

③ 证书审批。经审批后，RA 将审核通过的证书申请信息发送给 CFCA，由 CFCA 签发证书。

系统——CFCA 将同时产生的两个码(参考号、授权码)发送到 RA 系统。为安全起见，RA 采用两种途径将以上两个码交到证书申请者手中： RA 管理员将其中的授权码打印在密码信封里当面交给证书申请者；将参考号发送到证书申请者的电子邮箱里。

SET 系统——持卡人/商户到 RA 各网点直接领取专用密码信封。

④ 证书发放/下载。CA 签发的证书格式符合 X.509 V3 标准。具体的证书发放方式各个 RA 的规定有所不同。可以登录 CFCF 网站 http://www.cfca.com.cn 联机下载证书或者到银行领取。

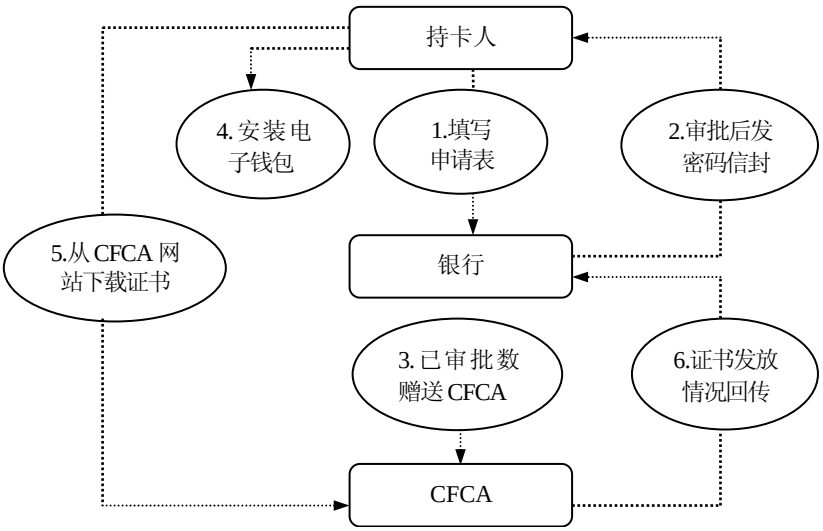
⑤ 证书生成。证书在本地生成，证书由 CFCA 颁发，用户私钥由客户自己保管。

⑥ 证书存放介质。硬盘、U 盘、IC 卡、CPU 卡、SIM 卡等。

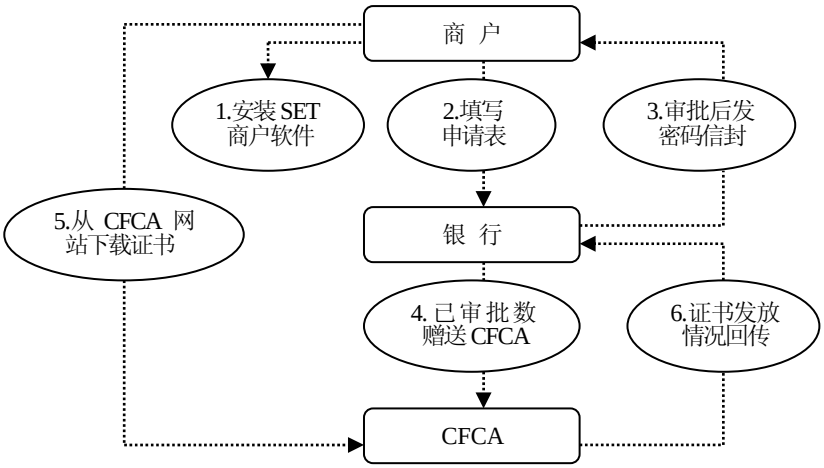
(2) 证书申请下载流程。

① SET 持卡人证书申请、审批流程。

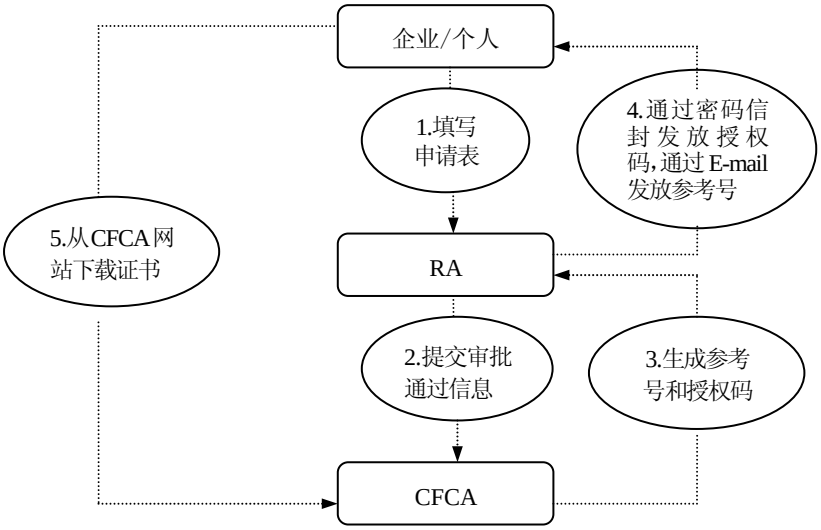
② SET 商户证书申请、审批流程。



4. 企业普通/个人普通/Web Server 证书申请、审批流程




5. 企业高级/个人高级/Direct Server 证书申请、审批流程




二、登录 www.sheca.com 掌握数字证书的具体操作

步骤按照网页上的提示进行操作。

三、中国银行网上支付——安全电子交易(SET)

按照如下流程所述，完成一次交易。

为了给中国银行广大的持卡人提供一个快捷、方便、安全的网上购物环境，中国银行按照 SET 标准建立了一整套购物及支付系统，使得中国银行的持卡人可以毫无后顾之忧地享受网上购物的乐趣。

安全电子交易主要参与对象有持卡人、商户、支付网关和电子证书认证中心。

一个基本的电子交易流程如下。

(1) 用户在自己的计算机内安装中银电子钱包软件。

(2) 登录中国银行网站(http://www.bank-of-china.com)，在线申请并获得持卡人电子安全证书。

(3) 登录到中国银行网上特约商户的站点，选购商品、填写送货地址并最后确认订单。

(4) 单击“长城电子借记卡支付”按钮，浏览器会自动启动电子钱包软件，用户只要按照画面提示输入借记卡卡号、密码等信息即可实时完成在线支付。

(5) 用户在家里坐等网上商户将选购的商品邮寄过来或送货上门。

**注意**：以上(1)、(2)步骤仅在初次使用中国银行长城电子借记卡进行网上购物时才进行，在第二次乃至以后进行网上购物时，不必重复上面(1)、(2)步骤。

在上述整个电子交易过程中，SET 协议利用各种加密方法、数字签名、证书认证等技术手段为网上交易的各方提供了最全面的保护，确保了电子交易安全、有序的进行。

## 四、构建一个基于 SSL 的网站

首先需要安装 Web 服务器程序，可以选择微软的 IIS 或者 Tomcat。接着，需要下载 Open SSL 应用程序，并且在 VC 环境下编译通过。

Open SSL 是开放源代码的应用程序，它不仅实现了 SSL 协议，而且实现了各种加密算法、证书的生成等功能。人们可以在 DOS 窗口下，使用命令行的方式利用其提供的功能来实现一个 CA，这样就可以用来生成客户证书。

网站建立成功后，用户访问网站的方式将发生改变，不是通过 HTTP，而是通过 HTTOS，S 表示安全的意思。

1) 建立 CA 中心

使用 Open SSL，人们可以自己承担其 CA 中心的职责：生成数字证书。

首先，在 C 盘建立一个新的目录 CARoot。其目录结构如下。

Certs：用来存放经过 CA 签发的数字证书。

Crl：用来存放证书撤销列表。

Private：用来存放数字证书对应的私钥。

Newcerts：用来存放新生成的数字证书。

(1) 编辑用于生成 RSA 密钥对的随机数文件。

C:\CARoot>editprivate.Rnd

(2) 生成 CA 根证书的 RSA 密钥文件。

C:\CARoot>genrsa-outprivate\ca.key-randprivate.Rns2048

如果想为生成的私钥文件加上密码保护，可以使用下面的命令。

C:\CARoot>genrsa-outprivate\ca.key-randprivate.Rnd-des32048

(3) 生成 CA 的根证书。

C:\CARoot>req-new-X509-days3650-keyprivate\ca.key-outprivata\ca.crt-configopenss

这样，CA 的根证书就生成了，以后所有的证书都要经过根证书的签名才有效。接下来，要为网站申请一个服务器证书，为用户申请客户证书。

2) 生成服务器证书

(1) 用 IISWEBSERNER 产生一个证书申请 certreq.txt。

打开 IISWEBSERNER→站点属性→目录安全性→服务器证书→创建一个新证书→现在准备请求，但稍候发送。

将生成的证书申请文件存放到 CARoot 目录中。

(2) 生成经过 CA 根证书签名的服务器证书。

C:\CARoot>ca-incertreq.Txt-keyprivate\.Key-outnewcerts\SernerCert.Cer-policy Policy-anything-onfigopenssl.cnf

3) 生成客户证书

(1) 生成一个新的 RSA 密钥对。

C:\ CARoot>genrsa-out Clien Certoo1.Ket-randprivate.Rnd2048

(2) 生成客户证书。

C:\ CARoot>req-new-X509-days3650-keyClient Cert001.Key？-out Client Cert001.Crt-configo penssl.cnf

(3) 使用 CA 根证书来签名客户证书

Ｃ:\ CARoot>ca-ss-cert Client Cert001.Crt-keyprivate\ca.key-configopenssl.Cnf-policyPolicy-anything-outsigned Cient Client Cert001.cer

生成的客户证书为 Client001.crt，通过这种方式，可以给多个用户颁发个人证书。

4) 导入证书

(1) 安装信任的根证书。根证书为 ca.cer，在客户端的 IE 中使用“工具”→“Internet 选项”→“内容”→“证书”→“导入”，把生成的 CA 根证书导入，使其成为用户信任的 CA。

(2) 导入服务器证书。打开 IISWEBSERVER→站点属性→目录安全性→服务器证书→处理挂起并安装证书→选择生成的服务器证书 Server Cert.cer。

(3) 安装客户证书。将客户的证书转变为 pkcs12 格式的证书，以便导入到 IE 中。

C:\CARoot>pkcs12－export－clcerts－in Client Cert001.crt－inkey Client Cert001.Key-out client001.P12

把 client001.P12 导入到客户端的 IE 中作为个人证书。

**【关键术语和概念】**

SSL　SET　握手协议　记录协议　警告协议　网上支付协议会议(NIST)　公钥加密算法　私钥加密算法　安全外壳协议　SOCKS 协议　安全超文本传输协议　客户认证 CA　身份认证　信息认证　数字摘要　数字信封　数字签名　数字时间戳　数字证书　个议

## 本 章 小 结

本章简要介绍了电子商务对安全性的要求，重点阐述了安全通信协议 SSL 和 SET，分析了其优缺点，分析了其他的安全协议的内容和应用规则。同时也详细介绍了客户认证中的身份认证、信息认证以及相关认证技术。重点总结了数字证书的分类，认证机构，证书的申请、发放、撤销等内容。

# 习　题

一、单项选择题

1. (　　)是由 VISACard 和 MasterCard 合作开发完成的，在互联网上实现安全电子交易的协议标准。

A. SSL　　B. SET　　C. DES　　D. RSA

2. EDI 软件具有将用户数据库系统中的信息译成(　　)的标准格式以供传输交换的能力。

A. EDI　　B. 文本文件　　C. 图形　　D. 脉冲电流

3. 1996 年 2 月 VISA 与 MasterSard 两大信用卡国际组织发起制定保障在因特网上进行安全电子交易的(　　)协议。

A. SSL　　B. IPSEC　　C. SET　　D. 数字签名

4. SET 采用优良的密钥体制，把(　　)与非对称密钥体制的有效性结合在一起。

A. 不对称密钥的有效性　　B. 对称密钥的低成本而快速

C. 非对称密钥的低成本而快速　　D. 对称密钥的有效性

5. SET 协议工作在 TCP/IP 的哪个层次？(　　)

A. 网络层　　B. 数据层　　C. 应用层　　D. 会话层

6. SET 协议涉及的对象不包括(　　)。

A. 消费者　　B. 离线商店　　C. 收单银行　　D. 认证中心(CA)

7. SET 协议通过(　　)技术保证数据的一致性和完整性。

A. 公共密钥　　B. 数字信封　　C. 数字签名　　D. 对称密钥

8. SET 协议主要保障(　　)的安全。

A. 网站数据　　B. 网站之间通信信道

C. 客户、商家和银行之间通过信用卡支付

D. 电子邮件

9. SSL 安全协议的主要功能不包括(　　)。

A. 维护数据的完整行，确保数据在传输过程中不被更改

B. 能绝对安全地传递数据

C. 加密数据以隐藏被传递的数据

D. 认证用户和服务器

10. SSL 协议层包括两个协议子层：记录协议和(　　)。

A. 握手协议　　B. 牵手协议　　C. 拍手协议　　D. 拉手协议

11. SSL 协议是由(　　)公司推出的一种安全通协议。

A. NETSCAPE　　B. IBM　　C. MasterCard　　D. Visa

12. SSL 协议是属于网络(　　)的标准协议。

A. 对话层　　B. 网络层　　C. 应用层　　D. 传输层

13. 采用数字签名进行远程授权的支付方式是(　　)。

A. 银行卡在线刷卡记账　　B. 银行卡从 ATM 机提款再支付

C. 银行卡 POS 结账　　D. 银行卡网上支付

## 二、多项选择题

1. 关于数字证书的原理说法错误的是(　　)。

A. 数字证书采用公钥体制，即利用一对互相匹配的密钥进行加密、解密

B. 每个用户自己设定一把公有密钥，用它进行解密和签名

C. 当发送一份保密文件时，发送方使用接收方的私钥对数据加密，而接收方则使用自己的私钥解密

D. 设定一把公共密钥为一组用户所共享，用于加密和验证签名

2. 互联网电子商务交易中网络安全要素应包括(　　)等方面。

A. 信息传输的保密性　　B. 数据交换的完整性

C. 交易场所的安全性　　D. 交易者身份的确定性

3. 顾客不能进行网上支付，往往因为(　　)。

A. 网上商店的硬件系统有故障

B. 银行的支付系统有故障

C. 银行的通信网络有故障

D. 顾客自己不熟悉支付流程

4. SSL 协议可用来对以下哪些协议进行加密？(　　)

A. FTP 协议　　B. Telnet 协议　　C. HTTP 协议　　D. IP 协议

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

A. SSL 协议属于网络应用层的标准协议

B. SSL 记录协议基本特点：连接是专用的、连接是可靠的

C. SSL 握手协议基本特点：连接是专用的、连接是可靠的

D. SSL 可用于加密任何基于 IPX/SPX 的应用

## 三、简述题

1. 简述电子支付协议的种类。
2. 简述与电子支付相关的协议。
3. 简述电子支付系统的要求。
4. 简述电子支付的标准。
5. 简述电子支付系统的特点。

## 四、分析题

1. 分析电子支付系统的功能。
2. 分析中国电子商务支付体系的结构及实现原则。