DIANZI SHANGWU ANQUAN XIEYI

电子商务安全协议

陈如刚 杨小虎 编著

浙江大學出版社

电子商务安全协议

陈如刚　杨小虎编著

浙江大學出版社

图书在版编目（CIP）数据

电子商务安全协议 / 陈如刚，杨小虎编著．—杭州：浙江大学出版社，2000.7
ISBN 7-308-02363-X

Ⅰ.电... Ⅱ.①陈... ②杨... Ⅲ.计算机网络-商业经营-支付方式-安全-协议 Ⅳ.F713.36

中国版本图书馆 CIP 数据核字(2000)第 35198 号

编　　著：陈如刚　杨小虎
责任编辑：樊晓燕
封面设计：刘依群

出版发行：浙江大学出版社
（杭州浙大路 38 号　邮政编码 310027）
（网址：http://www.zjupress.com）
（E-mail：zupress@mail.hz.zj.cn）
排　　版：浙江大学出版社电脑排版中心
印　　刷：浙江大学华家池印刷厂
经　　销：浙江省新华书店
开　　本：787mm×1092mm　16 开
印　　张：9.25
字　　数：237 千
版 印 次：2000 年 7 月第 1 版第 1 次印刷
印　　数：0001—3000
书　　号：ISBN 7-308-02363-X/F・309
定　　价：18.00 元

简　介

《电子商务安全协议》一书，针对电子商务的重要环节——网上支付，系统而全面地介绍了实现网上支付的主要安全协议：SET、SSL 和 S-HTTP 协议，并对电子商务系统建设中的一些安全问题作了深入分析。本书内容丰富、实用易懂，可作为大专院校电子商务等专业的教学用书，也可供从事计算机、电子商务等行业的专业人员参考使用。

前　言

随着因特网技术的飞速发展，电子商务已成了广受人们关注的热门话题。在电子商务的各个环节，特别是网上支付中，如何保证网上传输信息的安全性，是交易顺利完成的关键之一。网络安全一直是困扰电子商务发展的一个重要因素。

电子商务安全协议的提出为安全问题提供了解决方案。本书详细介绍了目前电子商务系统中应用较多的一些安全协议：安全电子交易协议 SET（Secure Electronic Transaction）、安全套接字层协议 SSL（Secure Socket Layer）和安全 HTTP 协议 S-HTTP 。SET 协议是由 VISA、MasterCard 等国际信用卡组织会同一些计算机供应商开发的，于 1997 年 5 月 31 日正式推出协议的 1.0 版。SET 协议为在因特网上安全地进行交易提出了一整套完整的方案，使参加交易的各方，包括持卡人、商户、银行等对在因特网上进行交易增加了安全感，将会大大推动电子商务的发展。SET 协议是本书内容的重点。

安全套接字层协议 SSL（Secure Socket Layer）是由 Netscape Communication 公司为 TCP/IP 套接字开发的一种加密方法，它能提供对多种基于套接字的 INTERNET 协议数据包加密的功能。HTTP 协议是 WEB 技术的基础。安全 HTTP 协议 S-HTTP 是为提高 WEB 数据传输的安全性而提出的，是对 HTTP 协议的扩展。S-HTTP 协议允许浏览器和服务器对 HTTP 数据包进行加密、签名和认证。本书详细介绍了这些协议的业务流程，对协议中的安全机制作了全面分析，还对安全系统建设中的一些问题进行了一些讨论。

本书的 1～10 章由陈如刚编著，11～12 章由杨小虎编著。

目　录

第 1 章　SET 简述

1.1　网上交易

随着因特网的迅速发展，电子商务也正以惊人的速度向前发展。这是人人皆知的事实。SET 协议是有关电子商务安全的协议，具体地说是有关网上交易安全的协议。为了更好地理解 SET 协议，有必要先了解一下网上交易的全过程。

为了实现网上交易，必须要有网上商店。也就是说，商户要在网上将商品销售出去，首先要建立自己的网上商店。网上商店的形式多种多样。商户为了吸引顾客到他的网上商店购物，想尽方法，动足脑筋。现在的网上商店越建越精彩，访问人数也越来越多。

尽管网上商店形式多样，但基本方法大致相同，都要建立一个商品目录的表单，将网上的可供商品情况告诉消费者，让消费者选购。为了方便消费者查询，许多网上商店采用数据库技术，为消费者提供多种检索查询手段，使消费者能在很短的时间内，找到自己想要的商品。

在因特网上先后出现了许多信息查询工具，如 Gopher、Archie、WAIS 等，但近年来使用最广泛、发展最迅速的当推全球网络信息查询系统(World Wide Web)，简称 WWW，我们一般称其为“环球网”或“万维网”。由于 WWW 能灵活地传送文本、图形、影像、声音等多种信息，已经成为因特网上主要的信息发布手段。可以说，因特网上的网上商店都是建立在 WWW 上的。

消费者要在网上购物，必须使用浏览器软件，浏览查询 WWW 上的信息，根据所要找的网上商店的域名，进入网上商店，浏览购物。目前最流行的浏览器是网景公司的 Netscape 和微软公司的 Internet Explorer，这些大家应该很熟悉了，这里就不再作进一步的介绍了。

消费者通过浏览器进入网上商店后，可以在网上商店浏览，查看网上商店陈列的商品。有些网上商店提供了查询功能，消费者可以根据自己的需要进行查询，以便较快找到自己所需的商品。许多商店都采用购物篮的方法，消费者在网上商店购物，就像在自选商场购物一样，看到合适的商品，就放入购物篮，然后继续浏览，直到不想再购物为止。商店会将消费者所选的所有商品列出给消费者查看，让消费者再一次确定是否购买。最后，商店将要求消费者填写订单，将消费者的一些必须告诉商店的信息，比如购物者的姓名、收货人的姓名地址、联系电话、E-mail 信箱、付款方式等填入表内，通过因特网传送给商店。在商店收到货款并将商品送到消费者手中后，网上购物过程就完成了。

网上交易中，交易双方最关心的是支付问题。商品售出后，如何收到钱款，这是网上商店建设中很重要的一个问题。我国大陆的许多网上商店，虽然实现了网上购物，但还没有实现网上支付，支付还是采用汇款或当面付现金的方法。消费者在网上选购好商品后，网上商店会采用邮寄或送货上门等方法将商品送到消费者手中。一些采用邮寄方法的商户，为了保证能收到消费者的购物款，要求消费者先将购物款汇给商店，商店在收到消费者的汇款后，才能将商品邮寄给消费者。采用送货上门的商店，一般都采用在将商品送到消费者手中时，向消费者收钱。这样有时就会碰到问题，一些消费者上网购物是为了送礼，希望商店将商品直接送给礼品的接受

者，付款的和收货的不是同一个人，送货上门时收钱就不行了。商户为了能将网上商店开下去，无法拒绝此类订单，只好跑两趟，先到付款者家里收取购物款，再将商品送到收货人手中。

为了在网上实现支付，人们首先想到的是信用卡。现在我们对信用卡已经非常熟悉了。在美国等一些西方国家，信用卡已发展得非常成熟，利用信用卡实现的电话购物、邮购等业务也相当普遍。我国大陆的信用卡业务起步较晚，但发展非常迅速，许多商店早就能接受信用卡消费，而且已经使用联网的读卡机，将信用卡信息直接传输到银行，对信用卡进行实时认证，实现支付。在因特网上同样也能利用信用卡来实现支付，但要采取一定的安全措施。消费者在网上购物后，只要将自己的信用卡信息传送给商店，再由商店传送给银行，由银行按照信用卡账号进行扣款，就能实现网上支付。西方发达国家的网上商店，基本上都实现了网上支付。但是由于网上支付的安全问题没有真正解决，所以许多消费者还不敢在网上进行支付。

众所周知，因特网上的信息是很多的，但因特网又是很不安全的。经常会听到诸如某网站被黑客攻破，资料被窃取之类的消息。人们对于因特网的安全总是抱有怀疑。商户建立了网上商店，并不害怕有人来窃取信息。消费者上网进入网上商店购物，也不担心安全问题。但一碰到支付，涉及到钱的问题，买卖双方都会担心。消费者担心碰到的是一家黑店，付了钱拿不到东西，或者信用卡资料在传输途中被别人窃取，结果信用卡被别人冒用，损失更大。商户则担心商品送出后收不到钱，银行则担心产生坏账。

为了提高因特网的安全，特别是网上交易的安全，许多专家、学者提出了一个又一个的方案，所建系统的安全性越来越高。这里所要讨论的SET 协议，就是一个目前世界上最安全的网上交易的方案之一。

1.2 传统的信用卡交易流程简介

SET 交易是使用信用卡在因特网上进行的一种交易。为了能较清楚地了解 SET 交易的情况，应该先对传统的信用卡交易有一个大致的了解，下面就作一简单介绍。

长期以来，人们都习惯拿着现金去商店买东西，一手交钱一手交货。自从有了信用卡后，人们开始习惯使用信用卡进行消费。信用卡消费主要有压卡机压卡和使用读卡设备通过银行专用网络进行扣款等方式。

1.2.1 使用压卡机的信用卡交易

持卡人到商店购物，如果用信用卡付款，须将信用卡交给商店营业员，同时还须出示自己的身份证，证明信用卡是本人的，营业员按照信用卡号查询信用卡废除名单(黑名单)，然后用压卡机将卡上的卡号等压印到付款单据上，填写消费金额，交持卡人签名，最后还要核对签名是否与信用卡上持卡人的签名一致。然后，商户可以凭此单据从收单银行得到钱款，收单银行则从持卡人的发卡银行得到钱款，而发卡银行将按照压卡单据将钱款从持卡人的账户中扣除。一次完整的交易支付过程就完成了。

在支付过程中，持卡人的信用卡账户中并不一定有钱，往往是在支付过程完成以后，持卡人才将货款存入信用卡账户。银行对不同的信用卡给以不同的最大透支额，即在信用卡账户中没有资金时，允许持卡人进行消费的最大金额。这个允许透支额与持卡人的信用程度有关，银行将根据持卡人的信用程度及持卡人申领信用卡时的要求，发给透支额较低的普通卡或透支额较高的金卡。而商户则根据信用卡的透支额来决定消费的最大金额，如果消费金额超过了信用卡的最大透支额，则不能接受信用卡消费，或与银行通过电话进行授权，在得到银行的授权

后，即银行同意接受此次交易后，商户才能受理此笔信用卡交易。

商户在接受持卡人的信用卡时，并不关心卡里是否有钱，而是先要确认这张卡是不是黑卡，所以必须先要查黑名单，如果商户接受的是黑卡并且已经登记在黑名单里了而没有查出来，商户将无法从银行得到钱款，所以商户在接收信用卡时必须仔细地查黑名单。而由于黑名单的更新是有一定时间的，有时候信用卡持卡人已向银行挂失，但银行还来不及将其写入黑名单下发给商户，商户无法知道，使一些不法之徒有机可乘，这时，银行就要产生坏账。

1.2.2 使用专用网络的信用卡交易

通过网络实现信用卡交易，使信用卡交易变得十分方便和安全。此种方法的前提是商户必须与银行联网，商店里要安装一台专用的读卡机，也叫POS机，此POS机上连有电话线，能自动拨号与银行的计算机连接。持卡人购物后，将信用卡交给商店营业员，通过读卡机读卡，并通过电话线将信息传送到收单银行；收单银行再通过银行专用网络将信用卡号、扣款金额等数据传送给持卡人的发卡银行请求授权；发卡银行将检查该信用卡的有效性及信用额度，决定是否授权，并通知收单银行；收单银行将应答传送给商店，在读卡机的屏幕上显示出来；如果成功，联着读卡机的打印机将打印出签购单，持卡人要在签购单上签名，商店营业员要核对签购单上的签名与信用卡背面的签名是否一致，如果一致，持卡人可将货物取走，一次信用卡消费正式完成。这是国外信用卡的受理情况。而在国内，各银行的规定有所不同，有些银行规定在读卡时还须由持卡人输入自己的密码，此密码与其他数据一起传送给持卡人的发卡银行，由发卡银行来验证密码是否正确。有些银行则规定受理信用卡时要出示身份证，等等。

商店得到授权成功的应答，对持卡人来说已完成购物，但对商店来说还要进行扣款确认工作，将确认请求通过收单银行发给发卡银行，得到确认成功应答后，才能得到货款。这样做给交易带来极大的灵活性，比如，客人住进宾馆，宾馆可先让客人预付住宿费，通过信用卡先授权一笔预计的金额，在客人离店时，再按照实际费用进行确认；在商店购物时，可以先授权，等货物备齐，商店送货上门后，向银行发确认请求。不过国内银行联网交易目前还都统一采用实时扣款，即授权和确认同时进行的方法。

1.2.3 邮购与电话购物

邮购的方法如下所述。

商户将自己的可供商品制成目录，通过各种渠道发给顾客。顾客在家里查看商品目录，选择自己喜欢的商品。将选中的商品以及要购买的数量等数据填写在邮购单上，同时还要将自己的信用卡号等信息以及送货地址等也填在邮购单上，寄给商户。商户收到邮购单后，按照顾客的信用卡号、邮购商品总金额等信息向银行请求授权，得到银行授权后，商户就可以按顾客所填的送货地址送货上门。商户在货物送到时要求收货人在收货单上签字。银行会按照商户提供的持卡人的信用卡账号，将购物款从持卡人的账户扣除，划入商户的账户。

电话购物与邮购过程基本类似，只是顾客通过电话将要购买的商品告诉商户，而不是像邮购那样通过填写订单的方式。

1.2.4 借记卡

以上所述的是持卡人有一定信用度的信用卡，信用卡持卡人可以在一定金额范围内进行透支，即可以在信用卡账户内没有钱的情况下买东西。中国银行的长城卡、工商银行的牡丹卡

等都属于信用卡。另外还有一种银行卡，叫做借记卡，工商银行的浦江卡、灵通卡等都属于借记卡。这种卡不能透支，当借记卡账户里有钱时，可以在银行的自动取款机提取现金，也可以在商店里购物，但是不能通过压卡机压卡的方式进行交易，只能通过使用银行专用网络的方式进行交易。所用的方式与信用卡完全相同，但必须输入密码，当信息传送到发卡银行后，发卡银行将核对持卡人输入的密码是否正确，还要检查持卡人的账户余额是否大于交易金额，如果账户余额小于本次交易额，银行将拒绝此次交易。

1.3 SET 协议

1996 年 2 月 1 日，VISA、MasterCard 等国际信用卡组织会同一些计算机供应商，开发了安全电子交易(Secure Electronic Transaction)协议，简称 SET 协议，并于 1997 年 5 月 31 日正式推出协议的 1.0 版。

SET 协议为在因特网上安全地进行交易提出了一整套完整的方案，特别是采用数字证书的方法，用数字证书来证实在网上购物的确实是持卡人本人，以及向持卡人销售商品并收钱的商户确实是真实存在的商户。保护了在因特网上进行交易的各方，包括持卡人、商户、银行等的安全。

SET 协议发布以来，许多计算机软件开发商都纷纷按照 SET 协议进行电子商务软件的开发。到目前为止，已有 IBM、HP/VERIFONE、微软等近 20 家知名厂商开发出了符合 SET 协议标准的安全电子商务产品。国外许多网上支付系统都已采用 SET 协议标准。我国大陆也有好几家单位在建设遵循 SET 协议的网上安全交易系统，并且已经有系统正式开通。

SET 协议文本《SET Secure Electronic Transaction Specification》1.0 版共包括三本书：《Book 1: Business Description》，《Book 2: Programmer's Guide》，《Book 3: Formal Protocol Definition》。

这三本书可以从因特网上找到，并可从网上下载(网址：http://www.setco.org)。

SETCo 是 VISA 与 MasterCard 两大国际信用卡组织发起组建的安全电子交易管理机构，成立于 1997 年 12 月 19 日。SETCo 的主要职能是对 SET 协议进行维护与管理，并进行 SET 协议新版本的开发工作，同时，还对各软件开发商开发的 SET 软件进行标准一致性测试(Compliance Testing)。在 SETCo 网站上可以查看到已经通过测试以及正在测试的各开发商所开发的软件的名单。通过测试的软件必定符合 SET 标准，并将获得 SET 商标。图 1.1 显示的是 IBM 公司开发的为中国工商银行上海市分行制作的电子钱包软件的登录窗口，其中就有 SET 商标。

1.3.1 SET 交易参与方

持卡人(Cardholder)

同商店购物一样，SET 交易必须要有购物者。但与商店购物不同的是，SET 交易是在开放的网络中进行的，交易双方互不见面，而且无法使用现金。大家都知道，在商店里购物，对个人用户来说，如果不用现金，可以使用信用卡或其他各种银行卡，通过专用网络将信用卡上的信息传到银行进行扣款。在开放的网络——因特网上进行交易，也可以使用信用卡，SET 交易就是采用信用卡扣款的方式进行支付的。你要参加电子商务，就必须持有信用卡，所以在 SET 协议中将购物者称为持卡人。

持卡人要参加 SET 交易，必须要拥有一台电脑并且能够上网。还必须到发卡银行去申请

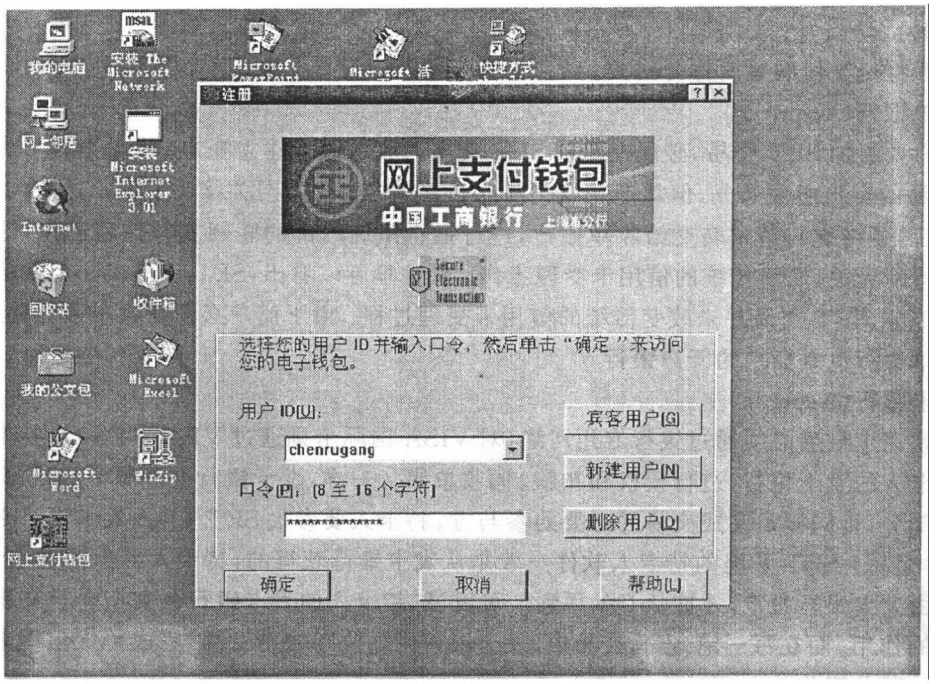

图 1.1　IBM 电子钱包登录窗口

并取得一套 SET 交易专用的持卡人软件，这套软件一般都称为电子钱包软件。软件安装好后的第一件事，就是上网去向数字证书认证中心（简称 CA）申请一张数字证书。有了数字证书，持卡人就可以开始安全地进行网上交易了。

商户（Merchant）

参加 SET 交易的另一方就是商户。商户要参与 SET 交易，首先必须开设网上商店，在网上提供商品或服务，让顾客来购买或得到服务。商户的网上商店必须集成 SET 交易商户软件，顾客在网上购物时，由网上商店提供服务，购物结束进行支付时，由 SET 交易商户软件进行服务。与持卡人一样，商户也必须先到银行进行申请，但不是到发卡银行，而是到接收网上支付业务的收单银行申请，而且必须在该银行设立账户。在开始交易之前，也必须先上网申请一张数字证书。

支付网关（Payment Gateway）

买卖双方进行交易，最后必须通过银行进行支付。但由于 SET 交易是在公开的网络——因特网上进行的，而银行的计算机主机及银行专用网络是不能与各种公开网络直接相联的，为了能接收从因特网上传来的支付信息，在银行与因特网之间必须有一个专用系统，接收处理从商户传来的扣款信息，并通过专线传送给银行；银行对支付信息的处理结果再通过这个专用系统反馈回商户。这个专用系统就称之为支付网关。

由于商户收到持卡人的购物请求后，要将持卡人账号和扣款金额等信息传给收单银行，所以支付网关一般由收单银行来担任。但由于支付网关是一个相对独立的系统，只要保证支付网关到银行之间通讯的安全，银行可以委托第三方担任网上交易的支付网关。

支付网关一头必须联在因特网上，且每天 24 小时开放，接收商户传来的扣款信息，另一头则与收单银行相联，及时将信息转送给收单银行。

与持卡人和商户一样，支付网关也必须去指定的 CA 机构申请一张数字证书，才能参与

SET 交易活动。

以下将把支付网关简称为网关。

收单银行(Acquirer)

商户要参加 SET 交易,必须在参加 SET 交易的收单银行建立账户。收单银行虽然不属于 SET 交易的直接组成部分,但却是完成交易的必要的参与方。网关接收了商户送来的 SET 支付请求后,要将支付请求转交给收单银行,进行银行系统内部的联网支付处理工作,这部分工作与因特网无关,属于传统的信用卡受理工作。从这里可以看出,SET 交易实际上是信用卡受理的一部分,SET 交易并未改变传统的信用卡受理过程。由于商户必须在收单银行建立账户,所以收单银行也是商户的开户银行。

发卡银行(Issuer)

扣款请求最后必须通过银行专用网络(对 VISA 国际卡则通过 VISA NET)经收单银行传送到持卡人的发卡银行,进行授权和扣款。同收单银行一样,发卡银行也不属于 SET 交易的直接组成部分,且同样是完成交易的必要的参与方。持卡人要参加 SET 交易,发卡银行必须要参加 SET 交易。SET 系统的持卡人软件一般是从发卡银行获得的,持卡人要申请数字证书,也必须先由发卡银行批准,才能从 CA 得到。可以说,持卡人的发卡银行在安全电子交易中起着很重要的作用。而在每一笔 SET 交易中,发卡银行则同收单银行一样,完成传统信用卡联网受理的那一部分工作。

数字证书认证中心(Certificate Authority,简称 CA)

CA 虽然不直接参加 SET 交易,但在 SET 交易中起着非常重要的作用。为了保证 SET 交易的安全,SET 协议规定参加交易的各方都必须持有数字证书,在交易过程中,每次交换信息都必须向对方出示自己的数字证书,而且都必须验证对方的数字证书。而 CA 的工作就是 SET 交易数字证书的发放、更新、废除,建立证书黑名单等各种证书管理。参与 SET 交易的各方,包括网关、商户、持卡人,在参加交易前必须到 CA 申请数字证书,在证书到期时,还必须去 CA 进行证书更新,重新领一张新的证书。同时,CA 还要随时掌握哪些证书已经被废除,要将这些证书写入证书黑名单,作为交易时验证对方证书的依据。作为各级 CA,不仅要为网关、商户、持卡人颁发证书,还要为下一级 CA 颁发证书,同时自己也要向上一级 CA 申请证书。一个 CA,只有自己有了证书,才能为下级颁发证书,并在证书上进行数字签名。因为只有 CA 签名的数字证书才是有效的。

图 1.2 为简单的 SET 系统示意图。持卡人、商户、网关通过因特网进行交易,网关通过专线与收单银行之间传递交易信息,收单银行与发卡银行通过银行专用网络传递交易信息,CA 通过因特网向持卡人、商户、网关发放证书,并通过专用网络与收单银行、发卡银行建立联系,进行证书发放的身份认定工作。

1.3.2 SET 交易的准备及数字证书申请流程简介

SET 交易各方,持卡人、商户和网关为了参与交易,必须先要安装有关软件并申请得到一张数字证书。

持卡人必须要有一台能上因特网的 PC 机,然后到发卡银行申请参加网上交易。银行会要求持卡人填写一些必要的表格,持卡人将会得到一套 SET 交易持卡人软件。为了能运行此套软件,持卡人的计算机里应安装能运行此软件的操作系统,这些软件一般都能运行于 Windows 95 或 Windows NT 操作系统下。持卡人将此软件安装在自己的计算机里,按照银行

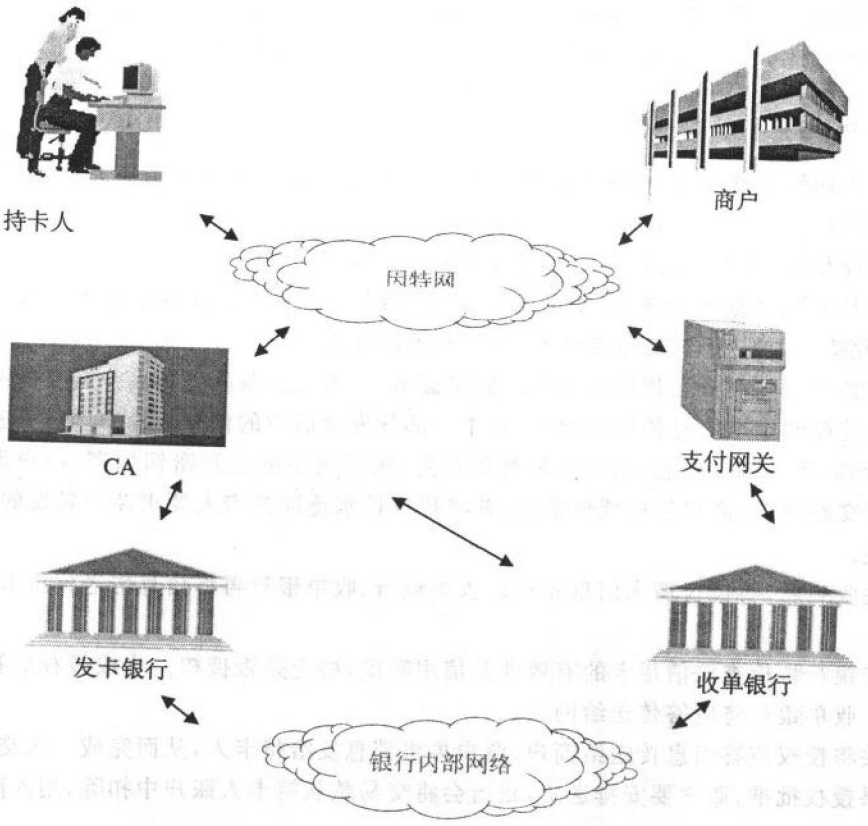

图 1.2　SET 系统示意图

所给的 CA 的网址上网，申请数字证书。

持卡人向 CA 发申请证书的初始请求，得到 CA 的应答，应答中包括 CA 的数字证书。

持卡人用 CA 证书中的 CA 公开密钥加密自己的信用卡账号等信息，发给 CA。

CA 会发一张登记表格要求持卡人填写，填写完登记表，持卡人软件将生成一对非对称密钥对，将其中的私人密钥保存好，用于以后的数字签名，将公开密钥连同填写好的表格及其他一些必要的数据用持卡人私人密钥进行数字签名，再用 CA 的公开密钥加密装入数字信封，发送给 CA。

CA 收到后将与持卡人的发卡银行联系，核对持卡人的各项信息，决定是否批准，如果批准，CA 将为持卡人生成一张数字证书，并用 CA 的私人密钥进行数字签名，然后传送给持卡人。

持卡人保存好数字证书，用于以后的 SET 交易。

商户要参加 SET 交易必须有一套 SET 交易商户系统软件。一般说来，商户在因特网上都已建立了网上商店，商户要将此商户软件与网上商店系统集成在一起，持卡人在网上商店购物后，如果要求网上支付，可马上从网上商店系统转到 SET 交易商户系统。

商户还要向收单银行申请加入 SET 交易，并在收单银行建立账户，SET 交易每一笔交易的钱款将从持卡人账户划到商户建立在收单银行的账户中。商户使用商户系统软件上网申请数字证书，申请过程与持卡人基本相同。但商户要生成 2 对非对称密钥对，1 对用于加密，称作