电子商务综合辅导：SET与电子商务 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/260/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_260619.htm 一、SET概述 由于Internet爆炸式的迅速流行，电子商务引起了越来越多的人的注意，它被公认为是未来IT业最具潜力的新增长点。在开放的网络(如Internet)上处理交易，如何保证传输数据的安全成为电子商务能否普及最重要的因素之一。调查公司曾对电子商务的应用前景进行过在线调查，当问到为什么不愿在线购物时，绝大多数人的回答是担心遭到黑客的侵袭而导致信用卡信息丢失。SET(Secure Electronic Transaction安全电子交易)正是在这种背景下应运而生的。SET是由VISA和MASTCARD所开发，是为了在Internet上进行在线交易时保证用卡支付的安全而设立的一种开放的规范。由于得到了IBM、HP、Microsoft、NetScape、VeriFone、GTE、VeriSign等很多大公司的支持，它已成为了事实上的工业标准，目前它已获得IETF标准的认可。 SET要达到的最主要的目标是：●信息在Internet上的安全传输。保证网上传输的数据不被黑客窃听。 ●定单信息和个人帐号信息的隔离。在将包括持卡人帐号信息的定单送到商家时，商家只能看到定货信息，而看不到持卡人的帐户信息。 ●持卡人和商家相互认证，以确定通信双方的身份。一般由第三方机构负责为在线通信双提供信用担保。 ●要求软件遵循相同的协议和消息格式，使不同厂家开发的软件具有兼容和互操作功能，并且可以运行在不同的硬件和操作系统平台上。 SET规范涉及的范围： ●加密算法的应用(例如RSA和DES)。 ●证书信息和对象格式。

●购买信息和对象格式。 ●认可信息和对象格式。 ●划帐信息和对象格式。 ●对话实体之间消息的传输协议。 SET协议中的角色有： 持卡人：在电子商务环境中，消费者和团体购买者通过计算机与商家交流，持卡人通过由发卡机构颁发的付款卡(例如信用卡、借记卡)进行结算。在持卡人和商家的会话中，SET可以保证持卡人的个人帐号信息不被泄漏。 发卡机构：它是一个金融机构，为每一个建立了帐户的顾客颁发付款卡，发卡机构根据不同品牌卡的规定和政策，保证对每一笔认证交易的付款。 商家：提供商品或服务，使用SET，就可以保证持卡人个人信息的安全。接受卡支付的商家必须和银行有关系。 银行：在线交易的商家在银行开立帐号，并且处理支付卡的认证和支付。 支付网关：是由银行操作的，将Internet上的传输数据转换为金融机构内部数据的设备，或由指派的第三方处理商家支付信息和顾客的支付指令。 SET是针对用卡支付的网上交易而设计的支付规范，对不用卡支付的交易方式，像货到付款方式、邮局汇款方式则与SET无关。另外像网上商店的页面安排，保密数据在购买者计算机上如何保存等，也与SET无关。 二、SET的购物流程 电子商务的工作流程与实际的购物流程非常接近，它与现实购物的流程很相似，这使得电子商务与传统商务可以很容易融合，用户使用也没有什么障碍。从顾客通过浏览器进入在线商店开始，一直到所定货物送货上门或所定服务完成，然后帐户上的钱转移，所有这些都是通过公共网络(Internet)完成的。如何保证网上传输数据的安全和交易双方的身份确认是电子商务能否得到推广的关键。这也正是SET所要解决的最主要的问题。下面我们从一事实上完整的购物处理流程来看SET是如

何工作的，如图1所示。 图1 1. 持卡人使用浏览器在商家的Web主页上查看在线商品目录浏览商品。 2. 持卡人选择要购买的商品。 3. 持卡人填写定单，包括：项目列表、价格、总价、运费、搬运费、税费。定单可通过电子化方式从商家传过来，或由持卡人的电子购物软件(wallet)建立。有的在线商场可以让持卡人与商家协商物品的价格(例如出示自己是老客户证明，或给出了竞争对手的价格信息)。 4. 持卡人选择付款方式。此时SET开始介入。 5. 持卡人发送给商家一个完整的定单及要求付款的指令。在SET中，定单和付款指令由持卡人进行数字签名。同时利用双重签名技术保证商家看不到持卡人的帐号信息。 6. 商家接受定单后，向持卡人的金融机构请求支付认可。通过Gateway到银行，再到发卡机构确认，批准交易。然后返回确认信息给商家。 7. 商家发送定单确认信息给顾客，顾客端软件可记录交易日志，以备将来查询。 8. 商家给顾客装运货物，或完成订购的服务。到此为止，一个购买过程已经结束。商家可以立即请求银行将钱从购物者的帐号转移到商家帐号，也可以等到某一时间，请求成批划帐处理。 9. 商家从持卡人的金融机构请求支付，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帐。 第三步与SET无关，从第四步开始SET起作用，一直到第九步，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，持卡人、商家、网关都通过CA来验证通信主体的身份，以确保通信的对方不是冒名顶替。 三、SET的加密技术 目前广为命名用的加密方法主要有两种：密钥加密系统和公钥加密系统，在SET的加密处理中，这两种方法都用到

了。SET将对称密钥的快速、低成本和非对称密钥的有效性完美地结合在一起。以下是SET命名用的加密技术。 密钥系统：又称对称密码系统，它使用相同的密钥进行加密和解密运算，发送者和接收者必须有相同的钥匙，最著名的密钥系统算法是数据加密标准(DES)。 公钥系统：又称非对称密码系统，它使用两个钥匙：一个用来加密，一个用来解密。每一个用户都有两个钥匙：一个公开密钥和一个私有密钥，用户可以散发他的公钥，由于两个钥匙之间存在的数学关系，任何人用公开密钥将数据加密，只有私有密钥的拥有者可将数据解密，为了保证私有密钥不被任何人知道，任何用户的密钥对应该由其自己生成。最有名的公共密钥算法是RSA(由Rivest、Shamir和Adleman三人发明)。 考虑网上商店的情况，对于成千上万消费者和商家在Internet上交换信息，要对每一个消费者通过某个渠道发放一个密钥，在现实中是不可取的。而用公开密钥，商家生成一个公共密钥对，任何一个消费者都可用商家公开发布的公钥与商家进行保密通信。 数字信封：SET依靠密码系统保证消息的可靠传输，在SET中，使用随机产生的对称密钥来加密数据，然后，将此对称密钥用接收者的公钥加密，称为消息的“ 数字信封 ”，将其和数据一起送给接收者，接收者先用他的私钥解密数字信封，得到对称密钥，然后使用对称密钥解开数据。 数字签名：由于公开密钥和私有密钥之间存在的数学关系，使用其中一个密钥加密的数据只能用另一个密钥解开。发送者用自己的私有密钥加密数据传给接收者，接收者用发送者的公钥解开数据后，就可确定消息来自于谁。这就保证了发送者对所发信息不能抵赖。 图2 消息摘要：消息摘要(message digest)是一个唯一

对应一个消息或文本的值，由一个单向Hash加密函数对消息作用而产生。用发送者的私有密钥加密摘要附在原文后面，一般称为消息的“ 数字签名 ”。数字签名的接收者可以确信消息确实来自谁，另外，如果消息在途中改变了，则接收者通过对收到消息的新产生的摘要与原摘要比较，就可知道消息是否被改变了。因此消息摘要保证了消息的完整性。 双重签名：它是数字签名的新应用。考虑下面的情况，王先生要买李小姐的一处房产，他发给李小姐一个购买报价单及他对银行的授权书的消息，要求银行如果李小姐同意按此价格出卖，则将钱划到李小姐的帐上。但是王先生不想让银行看到报价，也不想让李小姐看到他的银行帐号信息。此外，报价和付款是相连的、不可分割的，仅当李小姐同意他的报价，钱才会转移。要达到这个要求，采用双重签名即可实现。