 SET协议与SSL协议的比较 SET协议和SSL协议对于研究电子商务的人员来说并不陌生，当今电子商务发展的核心问题是交易的安全性问题，这也是企业应用电子商务最担心的问题，因此如何在开放的公用网上构筑安全的交易模式，一直是人们研究的热点和大家关注的话题，要构筑一个安全的电子交易模式，应满足以下五个方面，这也是OSI规定的五种标准的安全服务：（1）数据保密：防止信息被截获或非法存取而泄密。（2）对象认证：通信双方对各自通信对象的合法性、真实性进行确认，以防第三者假冒。（3）数据完整性：阻止非法实体对交换数据的修改、插入、删除及防止数据丢失。（4）防抗抵赖：用于证实已发生过的操作，防止交易双方对发生的行为抵赖。（5）访问控制：防止非授权用户非法使用系统资源。 迄今为止，国内外已经出现了多种电子支付协议，目前有两种安全在线支付协议被广泛采用，即安全套接层SSL协议和安全电子交易SET协议，二者均是成熟和实用的安全协议。 一、SSL协议 SSL（Secure Socket Layer即安全套接层）协议是Netscape Communication公司推出在网络传输层之上提供的一种基于RSA和保密密钥的用于浏览器和Web服务器之间的安全连接技术。它是国际上最早应用于电子商务的一种由消费者和商家双方参加的信用卡/借记卡支付协议。 1、SSL协议提供的服务主要有： 1）认证用户和服务器，确保数据发送到正确的客户机和服务器； 2）加密数据以防止数据中途被窃取； 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协议的工作流程： 服务器认证阶段：1）客户端向服务器发送一个开始信息“ Hello ”以便开始一个新的会话连接；2）服务器根据客户的信息确定是否需要生成新的主密钥，如需要则服务器在响应客户的“ Hello ”信息时将包含生成主密钥所需的信息；3）客户根据收到的服务器响应信息，产生一个主密钥，并用服务器的公开密钥加密后传给服务器；4）服务器恢复该主密钥，并返回给客户一个用主密钥认证的信息，以此让客户认证服务器。 用户认证阶段：在此之前，服务器已经通过了客户认证，这一阶段主要完成对客户的认证。经认证的服务器发送一个提问给客户，客户则返回（数字）签名后的提问和其公开密钥，从而向服务器提供认证。 从SSL协议所提供的服务及其工作流程可以看出，SSL协议运行的基础是商家对消费者信息保密的承诺，这就有利于商家而不利于消费者。在电子商务初级阶段，由于运作电子商务的企业大多是信誉较高的大公司，因此这问题还没有充分暴露出来。但随着电子商务的发展，各中小型公司也参与进来，这样在电子支付过程中的单一认证问题就越来越突出。虽然在SSL3.0中通过数字签名和数字证书可实现浏览器和Web服务器双方的身份验证，但是SSL协议仍存在一些问题，比如，只能提供交易中客户与服务器间的双方认证，在涉及多方的电子交易中，SSL协议并不能协调各方间的安全传输和信任关系。在这种情况下，Visa和MasterCard两大信用卡公组织制定了SET协议，为网上信用卡支付提供了全球性的标准。 二、SET协议 SET（Secure Electonic Transcation 即安全电子交易协议）是美国Visa和MasterCard两大信用卡组织等联合于1997

年5月31日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妥善地解决了信用卡在电子商务交易中的交易协议、信息保密、资料完整以及身份认证等问题。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（CardHolder）、商家（Merchant）、发卡行（Issuing Bank）、收单行（Acquiring Bank）、支付网关（Payment Gateway）、认证中心（Certificate Authority）等六个部分组成。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。 2、SET协议的工作流程 1）消费者利用自己的PC机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，在线商店作出应答，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，消费看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帐号信息。 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帐号转移到商店帐号，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帐。 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。 三、SET与SSL协议的比较 1、在认证要求方面，早期的SSL并没有提供商家身份认证机制，虽然在SSL3.0中可以通过数字签名和数字证书可实现浏览器和Web服务器双方的身份验证，但仍不能实现多方认证；相比之下，SET的安全要求较高，所有参与SET交易的成员（持卡人、商家、发卡行、收单行和支付网关）都必须申请数字证书进行身份识别。 2、在安全性方面，SET协议规范了整个商务活动的流程，从持卡人到商家，到支付网关，到认证中心以及信用卡结算中心之间的信息流走向和必须采用的加密、认证都制定了严密的标准，从而最大限度地保证了商务性、服务性、协调性和集成性。而SSL只对持卡人与商店端的信息交换进行加密保护，可以看作是用于传输的那部分的技术规范。从电子商务特性来看，它并不具备商务性、服务性、协调性和集成性。因此SET的安全性比SSL高。 3、在网络层协议位置方面，SSL是基于传输层的通用安全协议，而SET位于应用层，对网络上其他各层也有涉及。 4、在应用领域方面，SSL主要是和Web应用一起工作，而SET是为信用卡交易提供安全，因此如果电子商务应用只是通过Web或是

电子邮件，则可以不要SET。但如果电子商务应用是一个涉及多方交易的过程，则使用SET更安全、更通用些。 四、总结 SSL协议实现简单，独立于应用层协议，大部分内置于浏览器和Web服务器中，在电子交易中应用便利。但它是一个面向连接的协议，只能提供交易中客户与服务器间的双方认证，不能实现多方的电子交易中。SET在保留对客户信用卡认证的前提下增加了对商家身份的认证，安全性进一步提高。由于两协议所处的网络层次不同，为电子商务提供的服务也不相同，因此在实践中应根据具体情况来选择独立使用或两者混合使用。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com