安全电子交易（SET）协议与CA认证（上） PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/63/2021_2022__E5_AE_89_E5_85_A8_E7_94_B5_E5_c40_63788.htm 安全电子交易（SET）协议与 CA认证 一、安全电子交易规范（SET） 1．SET的作用 SET（Secure Electronic Transaction）协议是维萨（VISA）国际组织、万事达（MasterCard）国际组织创建，结合IBM、Microsoft、Netscope、GTE等公司制定的电子商务中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，保证采用的通讯协议、信息格式和标准具有公共适应性。从而可在公共互连网络上集成不同厂商的产品。 2．SET的应用流程 电子商务的工作流程与实际的购物流程非常接近。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，然后帐户上的资金转移，所有这些都是通过Internet完成的。其具体流程为： 持卡人在商家的WEB主页上查看在线商品目录浏览商品。 持卡人选择要购买的商品。 持卡人填写定单，定单通过信息流从商家传过来。 持卡人选择付款方式，此时SET开始介入。 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。 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。 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。 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货款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。 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。 前三步与SET无关，从第四步开始SET起作用。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，以确认对方身份。 3．SET技术概要 （1）加密技术 SET采用两种加密算法进行加密、解密处理,其中密钥加密是基础、公钥加密是应用的核心：用同一个密钥来加密和解密数据。主要算法是DES，例如加密银行卡持卡人的个人识别代码（PIN）；公开密钥要求使用一对密钥，一个公开发布，另一个由收信人保存。发信人用公开密钥加密数据，收信人则用私用密钥去解密。主要算法是RSA，例如加密支付请求数据。加密过程可保证不可逆，必须使用私用密码才能解密。 （2）数字签名 金融交易要求发送报文数据的同时发送签名数据作为查证。这种电子数字签名是一组加密的数字。SET要求用户在进行交易前首先进行电子签名，然后进行数据发送。 （3）电子认证 电子交易过程中必须确认用户、商家及所进行的交易本身是否合法可靠。一般要求建立专门的电子认证中心（CA）以核实用户和商家的真实身份以及交易请求的合法性。认证中心将给用户、商家、银行等进行网络商务活动的个人或集

团发电子证书。（4）电子信封 金融交易所使用的密钥必须经常更换，SET使用电子信封来传递更换密钥。其方法是由发送数据者自动生成专用密钥，用它加密原文，将生成的密文连同密钥本身一起再用公开密钥手段传送出去。收信人再解密后同时得到专用密钥和用其加密后的密文。这样保证每次传送都可以由发送方选定不同的密钥进行交易。 根据SET标准设计的软件系统必须经过SET验证才能授权使用。首先进行登记，再进行SET标准的兼容性试验，目前已经有多家公司的产品通过了SET验证。 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