SET安全协议：SET安全协议的概念 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/62/2021_2022_SET_E5_AE_89_E5_85_A8_E5_c40_62066.htm SET协议(Secure Electronic Transaction，安全电子交易)是由VISA和Master Card两大信用卡公司联合推出的规范。SET主要是为了解决用户、商家和银行之间通过信用卡支付的交易而设计的，以保证支付信息的机密、支付过程的完整、商户及持卡人的合法身份，以及可操作性。SET中的核心技术主要有公开密匙加密、电子数字签名、电子信封、电子安全证书等。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。在开放的互联网上处理电子商务，如何保证买卖双方传输数据的安全成为电子商务能否普及的最重要的问题。为了克服SSL安全协议的缺点，两大信用卡组织，ViSa和Marter Card，联合开发了SET电子商务交易安全协议。这是一个为了在互联网上进行在线交易而设立的一个开放的以电子货币为基础的电子付款系统规范。SET在保留对客户信用卡认证的前提下，又增加了对商家身份的认证，这对于需要支付货币的交易来讲是至关重要的。由于设计合理，SET协议得到了IBM、HP、Microsoft、VeriFone、GTE、Verisign等许多大公司的支持，已成为事实上的工业标准。目前，它已获得了IETF标准的认可。1996年2月，Marster Card和Visa国际信用卡组织与技术合作伙伴GTE、Netcape、IBM、Terisa Systems、Verisign、Microsoft、SAIC等一批跨国公司共同开发了安全电子交易规范(SET)。SET是在开放网络环境中的卡支付安全协议，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-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。1997年2月，由Master Card和Visa发起成立SETCO公司(也获得了American Express和JBC Credit Card Compamy的赞同)。SETCO成立后，立即着手建设认证体系(CA)。即为了推动电子商务的发展，首先要验证或识别参与网上交易活动的各个主体(如持卡消费者、商户、收单银行的支付网关)的身份，并用相应的电子证书代表他们的身份。电子证书是由权威性的公正认证机构管理的，在每次交易活动时还需逐级往上验证各认证机构电子证书的真伪。各级认证机构是按根认证机构(Root CA)、品牌认证机构(Brand CA)，以及持卡人、商户或收单行支付网关认证机构(Holder Card CA or Merchant CA or Payment Gateway CA)由上而下按层次结构建立的。在认证机构的最高层(顶层)，即根认证机构(Root CA)，由SETCO负责管理，其功能为：(1)生成和安全保存符合SET协议要求的属于根认证机构的公、私密钥。(2)生成和自行签署符合SET协议要求的根证书及其数字签名。(3)处理品牌认证机构的申请，生成、验证品牌证书并在品牌证书上进行数字签名。(4)生成品牌证书撤销清单。(5)支持跨域交叉认证。(6)制定安全认证政策。安全电子交易是基于互联网的卡基支付，是授权业务信息传输的安全标准，它采取RSA公开密钥体系对通信双方进行认证，利用DES、RC4或任何标准对称加密方法进行信息的加密传输，并用HASH算法来鉴别消息真伪或有无篡改。在SET体系中有一个关键的认证机

构(CA)，CA根据X.509标准发布和管理证书。 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