SET安全协议：SET安全协议的缺陷 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_62058.htm 从1996年4月SET安全协议1.0版面市以来，获得了业界的支持，促进了SET良好的发展趋势。但也发现了一些问题，主要包括以下几方面：(1)协议没有说明收单银行给在线商店付款前，是否必须收到消费者的货物接受证书。否则的话，在线商店提供的货物不符合质量标准，消费者提出疑义，责任由谁承担。(2)协议没有担保“非拒绝行为”，这意味着在线商店没有办法证明订购是不是由签署证书的消费者发出的。(3)SET技术规范没有提及在事务处理完成后，如何安全地保存或销毁此类数据，是否应当将数据保存在消费者、在线商店或收单银行的计算机里。这些漏洞可能使这些数据以后受到潜在的攻击。(4)在完成一个SET协议交易的过程中，需验证电子证书9次，验证数字签名6次，传递证书7次，进行5次签名、4次对称加密和4次非对称加密。所以，完成一个SET协议交易过程需花费1.5～2分钟，甚至更长的时间(新式小型电子钱包将多数信息放在服务器上，时间可缩短到10～20秒)。SET协议过于复杂，使用麻烦，成本高，且只适用于客户具有电子钱包的场合。(5)SET的证书格式比较特殊，虽然也遵循X.509的标准，但它主要是由Visa和Marster Card开发并按信用卡支付方式来定义的。银行的支付业务不光是卡支付业务，而SET支付方式和认证结构适应于卡支付，对其他支付方式是有所限制的。(6)一般认为，SET协议保密性好，具有不可否认性，SETCA是一套严密的认证体系，可保证B-C类型的电子商务安全顺利地进行。事实上，

安全是相对的，我们提出电子商务中信息的保密性问题，即要保证支付和定单信息的保密性，也就是要求商户只能看到定单信息(OI)，支付网关只能解读支付信息(PI)。但在SET协议中，虽然账号不会明文传递，它通常用1074位RSA不对称密钥加密，商户电子证书确实指明了是否允许商户从支付网关的响应消息中看到持卡人的账号，可是事实上大多数商户都收到了持卡人的账号。