

电子商务技术指导之鉴别PKI、SET、SSL-三 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/64/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_64653.htm 三 . SSL协

议SSL(SecuresocketLayer)安全套接层协议主要是使用公开密钥体制和X.509数字证书技术保护信息传输的机密性和完整性，它不能保证信息的不可抵赖性，主要适用于点对点之间的信息传输，常用WebServer方式。安全套接层协议（SSL

，SecuritySocketLayer）是网景（Netscape）公司提出的基于WEB应用的安全协议，它包括：服务器认证、客户认证（可选）、SSL链路上的数据完整性和SSL链路上的数据保密性。对于电子商务应用来说，使用SSL可保证信息的真实性、完整性和保密性。但由于SSL不对应用层的消息进行数字签名，因此不能提供交易的不可否认性，这是SSL在电子商务中使用的最大不足。有鉴于此，网景公司在从Communicator4.04版开始的所有浏览器中引入了一种被称作"表单签名

（FormSigning）"的功能，在电子商务中，可利用这一功能来对包含购买者的订购信息和付款指令的表单进行数字签名，从而保证交易信息的不可否认性。综上所述，在电子商务中采用单一的SSL协议来保证交易的安全是不够的，但采用"SSL表单签名"模式能够为电子商务提供较好的安全性保证。

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