电子商务技术指导之鉴别PKI、SET、SSL介绍 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_64667.htm 一．PKI技术为解决Internet的安全问题，世界各国对其进行了多年的研究，初步形成了一套完整的Internet安全解决方案，即目前被广泛采用的PKI体系结构，PKI体系结构采用证书管理公钥，通过第三方的可信机构CA，把用户的公钥和用户的其他标识信息（如名称、e-mail、身份证号等）捆绑在一起，在Internet网上验证用户的身份，PKI体系结构把公钥密码和对称密码结合起来，在Internet网上实现密钥的自动管理，保证网上数据的机密性、完整性。从广义上讲，所有提供公钥加密和数字签名服务的系统，都可叫做PKI系统，PKI的主要目的是通过自动管理密钥和证书，可以为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便的使用加密和数字签名技术，从而保证网上数据的机密性、完整性、有效性，数据的机密性是指数据在传输过程中，不能被非授权者偷看，数据的完整性是指数据在传输过程中不能被非法篡改，数据的有效性是指数据不能被否认。一个有效的PKI系统必须是安全的和透明的，用户在获得加密和数字签名服务时，不需要详细地了解PKI是怎样管理证书和密钥的，一个典型、完整、有效的PKI应用系统至少应具有以下部分：公钥密码证书管理。黑名单的发布和管理。密钥的备份和恢复。自动更新密钥。自动管理历史密钥。支持交叉认证。由于PKI体系结构是目前比较成熟、完善的Internet网络安全解决方案，国外的一些大的网络安全公司纷纷推出一系列的基于PKI的网络安全产品，

如美国的Verisign,IBM,Entrust等安全产品供应商为用户提供了一系列的客户端和服务器端的安全产品，为电子商务的发展提供了安全保证。为电子商务、政府办公网、EDI等提供了完整的网络安全解决方案。PKI是一种新的安全技术，它由公开密钥密码技术、数字证书、证书发放机构（CA）和关于公开密钥的安全策略等基本成分共同组成的。PKI是利用公钥技术实现电子商务安全的一种体系，是一种基础设施，网络通讯、网上交易是利用它来保证安全的。从某种意义上讲，PKI包含了安全认证系统，即安全认证系统-CA/RA系统是PKI不可缺的组成部分。PKI（PublicKeyInfrastructure）公钥基础设施是提供公钥加密和数字签名服务的系统或平台，目的是为了管理密钥和证书。一个机构通过采用PKI框架管理密钥和证书可以建立一个安全的网络环境。X.509格式的证书和证书废除列表(CRL)；CA/RA操作协议；CA管理协议；CA政策制定。