2006解析PKI体系在网络支付中的应用二 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_2006_E8_A7_A3_E6_9E_90_c40_62347.htm 模式3：网上证券 网上证券广义地讲是证券业的电子商务，它包括网上证券信息服务、网上股票交易和网上银证转账等。一般来说，在网上证券应用中，股民为客户端，装有个人证书；券商服务器端装有Web证书。在线交易时，券商服务器只需要认证股民证书，验证是否为合法股民，是单向认证过程，认证通过后，建立起安全通道。股民在网上的交易提交同样要进行数字签名，网上信息要加密传输；券商服务器收到交易请求并解密，进行资金划账并做数字签名，将结果返回给客户端。 三、PKI在企业网络安全中应用 近几年，我国在推动中国PKI技术发展与应用方面取得巨大的进展，在PKI自主技术开发方面也取得了一定的成绩。但是，PKI作为信息安全的核心技术，在我国网络信任体系建设、数字签名法、信息安全重点基础建设方面尚未得到广泛的推广应用。2005年亚洲PKI论坛第五届国际研讨会中，以电子政务与电子商务的应用为切入点，推动中国PKI技术的应用与发展。下面是我们经常遇到的几种常见应用。 ① 虚拟专用网络(VPN) 通常，企业在架构VPN时都会利用防火墙和访问控制技术来提高VPN的安全性，这只解决了很少一部分问题，而一个现代VPN所需要的安全保障，如认证、机密、完整、不可否认以及易用性等都需要采用更完善的安全技术。在实现上，VPN的基本思想是采用秘密通信通道，用加密的方法来实现。具体协议一般有三种：PPTP、L2TP和IPSec。 基于PKI技术的IPSec协议现在已经成为架构VPN的

基础，它可以为路由器之间、防火墙之间或者路由器和防火墙之间提供经过加密和认证的通信。虽然它的实现会复杂一些，但其安全性比其他协议都完善得多。由于IPSec是IP层上的协议，因此很容易在全世界范围内形成一种规范，具有非常好的通用性，而且IPSec本身就支持面向未来的IPv6协议。总之，IPSec还是一个发展中的协议，随着成熟的公钥密码技术越来越多地嵌入到IPSec中，相信在未来几年内，该协议会在VPN世界里扮演越来越重要的角色。 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