解析PKI体系在网络支付中的应用 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__E8_A7_A3_E6_9E_90PKI_E4_c40_62355.htm PKI（Public Key Infrastructure）含义为“ 公钥基础设施 ”，PKI技术是利用公钥理论和技术建立的提供信息安全服务的基础设施，PKI的基础技术包括加密、数字签名、数据完整性机制、数字信封、双重数字签名等。PKI基础设施采用证书管理公钥，通过第三方的可信任机构--认证中心，把用户的公钥和用户的其他标识信息捆绑在一起，在Internet网上验证用户的身份。PKI基础设施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，保证网上数据的安全传输。 从广义上讲，所有提供公钥加密和数字签名服务的系统，都可归结为PKI系统的一部分，PKI的主要目的是通过自动管理密钥和证书，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。 一、PKI原理 PKI公共密钥体系是利用公共密钥算法的特点，建立一套证书发放、管理和使用的体系，来支持和完成网络系统中的身份认证、信息加密、保证数据完整性和抗抵赖性。PKI 体系可以有多种不同的体系结构、实现方法和通信协议。 公共（非对称）密钥算法使用加密算法和一对密钥：一个公共密钥（公钥，public key）和一个私有密钥（私钥，private key）。其基本原理是：由一个密钥进行加密的信息内容，只能由与之配对的另一个密钥才能进行解密。公钥可以广泛地发给与自己有关的通信者，私钥则需要十分安全地存放起来。使用中，甲方可以用乙方的公钥

对数据进行加密并传送给乙方，乙方可以使用自己的私钥完成解密。公钥通过电子证书与其拥有者的姓名、工作单位、邮箱地址等捆绑在一起，由权威机构（CA, Certificate Authority）认证、发放和管理。把证书交给对方时就把自己的公钥传送给了对方。证书也可以存放在一个公开的地方，让别人能够方便地找到和下载。 公共密钥方法还提供了进行数字签名的办法：签字方对要发送的数据提取摘要并用自己的私钥对其进行加密；接收方验证签字方证书的有效性和身份，用签字方公钥进行解密和验证，确认被签字的信息的完整性和抗抵赖性。公共密钥方法通常结合使用对称密钥（单密钥）方法，由计算效率高的对称密钥方法对文件和数据进行加密。目前在 Internet 上主要使用 RSA 公共密钥方法，密钥长度 512 或 1024 位，是广泛使用的 SSL/TLS 和S/MIME 等安全通信协议的基础。 