电子商务概论知识辅导：PKI基础 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/170/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_170720.htm 正如我们在前面所提到的，电子商务的基础设施之一是网络基础设施。借助于网络基础设施可使不同的网络节点之间互相交换数据，共享网络资源。建立网络基础设施的目的就是使不同的实体只要需要，就可以方便地使用基础设施提供的服务。安全基础设施与网络基础设施遵循同样的原则，安全基础设施为整体应用系统提供安全基本框架，它可以被应用系统中任何需要安全应用的对象使用。因此，其在设计上必须具有一般性和通用性。只有这样，那些需要使用这种基础设施的对象在使用安全服务时，才不会遇到困难。本章将介绍公钥基础设施（PKI）的有关基本内容。 PKI基础一、PKI的定义PKI（Public Key Infrastructure）是一个用非对称密码算法原理和技术来实现并提供安全服务的具有通用性的安全基础设施，是一种遵循标准的利用公钥加密技术为网上电子商务、电子政务的开展，提供一整套安全的基础平台。PKI管理平台能够为网络中所有需要采用加密和数字签名等密码服务的用户提供所需的密钥和证书管理，用户可以利用PKI平台提供的安全服务进行安全通信。二、公钥基础设施的内容构建实施一个PKI系统将包括认证机构CA、证书库、密钥备份及恢复系统、证书作废处理系统，PKI应用接口系统等主要组成部分。1、认证机构(Certificate Authority)认证机构简称CA，是PKI的核心组成部分，也称作认证中心。它是数字证书的签发机构。CA是PKI的核心，是PKI应用中权威的、可信任的、公正的第三

方机构。2、证书库在使用公钥体制的网络环境中，必须向公钥的使用者证明公钥的真实合法性。因此，在公钥体制环境中，必须有一个可信的机构来对任何一个主体的公钥进行公证，证明主体的身份以及它与公钥的匹配关系。目前较好的解决方案是引进证书(Certificate)机制。（1）证书ITU（International Telecommunications Union，国际电信同盟）在1988年制定的X.500系列标准中的X.509就是被广泛采用的标准。X.509标准与公钥基础设施密切相关，它定义了公开密钥与密钥主体的结合，由此实现通信实体鉴别机制，并规定了实体鉴别中所使用的方法和数据接口，即证书。证书是公开密钥体制的一种密钥管理媒介。它是一种权威性的电子文档，形同网络环境中的一种身份证，用于证明某一主体的身份以及其公开密钥的合法性。（2）证书库证书库是证书的集中存放地，是网上的一种公共信息库，供广大公众进行开放式查询。到证书库访问查询，可以得到想与之通信实体的公钥。证书库是扩展PKI系统的一个组成部分，CA的数字签名保证了证书的合法性和权威性。3、密钥备份及恢复系统密钥备份及恢复系统对用户的解密密钥进行备份，当丢失时进行恢复。但签名密钥不能备份和恢复。4、证书作废处理系统证书由于某种原因需要作废，终止使用，这将通过证书作废列表CRL来完成。5、PKI应用接口系统PKI应用接口系统是为各种各样的应用提供安全、一致、可信任的方式与PKI交互，确保所建立起来的网络环境安全可信，并降低管理成本。PKI应用接口系统是一个全功能、可操作PKI的必要组成部分。熟悉客户／服务器结构的人都知道，只有客户端提出请求服务，服务器端才会为此请求做响应处理。这个原理同样适用于PKI

。其软件功能有：n 询问证书和相关的撤消信息。n 在一定时刻为文档请求时间戳。n 作为安全通信的接收点。n 进行传输加密或数字签名操作。n 能理解策略，知道是何时和怎样去执行取消操作。 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