电子商务概论知识辅导：PKI_CA系统 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_170714.htm CA是PKI中的“ 认证机构 ”。它为电子商务环境中各个实体颁发电子证书，即对实体的身份信息和相应公钥数据进行数字签名，用以捆绑该实体的公钥和身份，以证明各实体在网上身份的真实性，并负责在交易中检验和管理证书。CA是电子商务交易中权威性、可信赖性及公正性的第三方机构，是电子商务的重要基础设施，是电子商务的安全保证。 PKI/CA系统作为PKI的CA系统分两大类总体结构：SET CA系统和non-SET CA系统。一、PKI non-SET CA系统1、总体结构Root CAPolicy CAOperation CA高级证书普通证书VPN, WAP,Web证书第一层根CA第二层根CA第三层运营CA图9.1 PKI non-SET CA总体结构PKI non-SET CA系统目前一般为层次结构，在此我们介绍的的参考模型为三层结构。如图9.1所示。（1）RCA系统结构的第一层为根CA，即Root CA(简称RCA)。RCA的职责是：n 负责制定和审批CA的总政策。n 为自己“ 自签 ”根证书，并以此为根据为二级CA签发并管理证书。n 与其他PKI域的CA进行交叉认证。（2）PCA系统结构的第二层CA为政策性CA，称Policy CA，简称PCA。PCA的职责是：n 根据根CA的各种规定和总政策，制定具体政策、管理制度和运行规范。n 安装根CA为其签发的证书。n 为第三级CA签发证书。n 管理证书及证书撤消列表(CRL)。（3）OCA系统结构的第三层为终端用户CA，也称运营CA（Operation CA），简称OCA。OCA的职责是：n 安装政策CA签发的证书。n 根据根证书

及二级CA证书，直接为最终用户颁发终端实体证书，即支持电子商务各种应用的数字证书。n 管理所发证书及证书撤消列表(CRL)。2、系统目标non-SET CA系统，由根CA(Root CA)、政策CA(Policy CA)及运营CA(Operation CA)组成，具有完善的证书管理功能。non-SET CA签发的各种证书，其主要目标是支持广泛的电子商务应用模式、网上安全银行应用模式、网上证券以及电子政务等广泛的应用。（1）non-SET CA系统所签发的证书n 高级企业证书、高级个人证书（具有加密和数字签名两种功能）n 普通企业书证、普通个人证书（即SSL证书，具有加密功能）n Web证书（Web Server证书）n VPN证书（虚拟专用网证书）n WAP证书（移动手机上网证书）n S／MIME证书（安全电子邮件证书） 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