

电子商务概论知识辅导：CA系统构造 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_170715.htm

在第一节中，我们简单介绍了PKI non-SET CA和PKI SET CA的总体结构，尽管这两大类系统在结构和功能方面存在差异，但他们的基本构造和功能还是十分相近的。

一、第一层CA CA系统的第一层为的根CA，其作用等同于PKI中定义的PAA，是政策审批授权者，它的职责是制定CA的政策和规范；审核二级CA(PCA或BCA)的具体政策和操作管理规范；审批PCA(BCA)的建设，为其发放证书；RCA还负责与其他CA系统的交叉认证。

1、制定CA总政策根CA是政策审批授权者，负责制定金融CA系统的总体政策，以及为具体政策制定提供统一的依据。

2、管理二级CA（PCA或BCA）对二级CA的管理包括：（1）审批二级CA的建设申请和审批二级CA制定的运营政策。（2）

对二级CA申请者进行资信审查，为其发放二级证书。（3）

对已批准的二级CA，根据总政策进行复查，以决定最后是否继续允许该二级CA的运行。

3、证书的管理（1）管理证书和证书废止列表根CA必须管理其所签发的所有证书，包括根证书、二级CA的证书和为其他CA系统发放的交叉认证证书。

一级CA必须对外发布其签发的所有证书，以使用户查询。同时，还要根据运行政策，定期发布证书废止列表。（2）

管理密钥的备份CA系统必须能够保证用户密钥的安全备份，以便为客户提供密钥的恢复服务。如果有关方面制定了密钥托管政策，CA系统还必须能够按相关政策法规，安全保存用户的

密钥，以便必要时为客户恢复密钥。（3）证书归档根CA系

统对所签发过的所有证书进行归档，包括证书本身及证书废止列表归档。归档的目的是保存历史数据，以备事后发生纠纷时能够对用户签名进行追溯验证。（4）操作方式鉴于根CA发证量小，为了安全起见，根CA以离线方式操作。证书申请、签发和CRL等均以软盘 / 光盘为传递介质，并对上传和下载进行加密和保护。

4、与其他CA系统的交叉认证

根据电子商务的发展，一个CA系统有可能与其他CA系统互通。如有互通的需求，则由一级CA决定采取何种技术手段和管理手段进行互通。如果对方CA申请得到本CA系统的承认，则一级CA负责审核对方CA系统的政策，操作管理规范以及系统的安全措施，评估将会带来的风险和效益，从而决定是否承认另一个CA系统。如果承认，则为对方签发交叉认证证书，并提供交叉认证证书的查询手段。如果CA系统需要得到另一个CA系统的承认时，则应向该CA系统提供有关政策、操作管理规范和安全措施的文档，并申请对方签发交叉认证证书。

二、第二层CA

第二层CA在non-SET CA中称为政策CA（PCA），在SET CA中称品牌CA（BCA），它们的原理及功能作用与PKI中的PCA相同。

1、制定具体运营政策和操作规范

PCA(BCA)根据RCA的总政策和自身业务需求及实际情况，制定二级CA运营所需要的具体执行政策。例如我国金融CA的第二级PCA中，根据我国金融界电子商务市场的实际需要，在第二级制定三个PCA，即银行BPCA（Bank Policy CA）、证券SPCA(Securites Policy CA)及保险IPCA(Insurance Policy CA)。如图9.3所示。RCABPCASPCAIPCA

银行运营CA 证券运营CA 保险运营CA

图9.3 政策CA的策略

第二级政策CA，可设置包括银行、证券及保险在内的全部政策性CA。在此之下，

可设置银行运营CA、证券运营CA以及保险运营CA。这就是第二层政策CA的作用。2、管理三级CA（1）PCA根据业务需求决定如何设置第三级CA，并对第三级CA的申请进行审核和签发证书。（2）要对第三级CA的运行情况进行定期复核。（3）并对第三级运营CA所颁发的证书进行策略的制定。

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