# CA系统设计文档

1. 总体设计
   1. 系统主要分三个子系统
      1. KMS：密钥管理系统，主要负责用户密钥对的安全管理功能
      2. CA：证书认证系统，主要负责证书的管理，用户的管理
      3. RA：注册中心，主要负责用户的证书审核
   2. 子系统关系图



* 1. 系统技术架构图



* 1. 用户证书颁发流程



* 1. 用户证书有效性查询流程



1. KMS系统设计
   1. 设计图



* 1. 功能描述
     1. 系统初始化流程



* + 1. 密钥生成
       1. 根据用户选择生成用户需要类型的密钥对



1. CA系统设计
   1. 设计图



* 1. 系统初始化流程



* 1. 角色设计（角色划分）
     1. 超级管理员：1个，可以参与系统的各个操作
     2. CA管理员：多个，可以管理管理RA
     3. RA管理员：多个，可以管理用户的证书提交申请
     4. 用户：普通用户提供注册申请等功能
  2. 功能设计
     1. 用户接口
        1. 注册
        2. 登陆
        3. 查询
     2. 证书接口
        1. 制作证书
        2. 生成CSR
        3. 获取可用用户密钥
        4. 查询证书
        5. 吊销证书
        6. 生成CRL
        7. 下载CRL

1. RA系统设计
   1. 功能设计
      1. 用户接口
         1. 注册
         2. 查询
         3. 登陆
      2. 证书接口
         1. 申请证书
         2. 批准证书
         3. 提交CSR
         4. 证书查询