- 假设存在一个可信的CA机构,我们操作系统和浏览器已经存储了这个CA的根证书

类CSR文件
通用名(common_name)
机构名(organization_name)
公钥(public key)
指纹SHA-256

数字证书
通用名(common_name)
机构名(organization_name)
公钥(public key)
颁发日期(Validity Start Date)
截止日期(Validity End Date)
指纹SHA-256
RSA摘要签名(Sign)